netwrix

2024

Netwrix Auditor v10.7

6160 Warren Parkway, Suite 100, Frisco, TX 75034 | (949) 407-5125

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.

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

Netwrix Auditor v10.7 Documentation

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
- Active Directory Federation Services
- Microsoft Entra ID
- Exchange
- Office 365
- Windows file servers
- Dell Data Storage devices
- NetApp filer appliances
- Nutanix Files
- Network Devices
- SharePoint
- Oracle Database
- SQL Server
- VMware
- Windows Server
- 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 you achieve your specific business objectives, refer to the Netwrix Auditor Best Practices Guide.

CAUTION: To keep your systems safe, AUDITOR should not be exposed to inbound access from the internet.

Getting Started

In this section, we will cover:

- Pre-installation procedures
- Installation
- IT infrastructure and accounts configuration
- Product configuration
- Data collection
- AuditIntelligence: search, reports, alerts, risk assessment dashboards, and user behavior anomalies detection
- Operation and health

Pre-installation procedures	
Review recommendations and considerations for Netwrix Auditor deployment planning.	• Requirements
Make sure the data source you are going to audit is supported.	• Supported Data Sources
Open the required ports for connections.	• Protocols and Ports Required

Review system requirements.	• Requirements
Installation	
If you are using previous version of the product, upgrade to the latest version then.	• Upgrade to the Latest Version
Install the product and review additional installation scenarios.	• Installation
IT infrastructure configuration	
Configure target IT infrastructure depending on your data source.	• Supported Data Sources
Configure Auditor service accounts.	• Software Requirements
If you are going to use Group Managed Service Account (gMSA) for data collection and storage, refer to the following article for more information.	• Use Group Managed Service Account (gMSA)
Product configuration	
Configure role-based access and delegation.	• Role-Based Access and Delegation
Configure general product settings.	• Netwrix Auditor Settings
Create monitoring plans to start collecting data from your IT infrastructure.	• Monitoring Plans
Start data collection	

Understand how the product collects data.	• Data Collecting Account
Start data collection.	• Configure Data Collection Settings
Make collected data actionable	
View data and perform search.	• View and Search Collected Data
Review reports.	• View Reports
Create alerts to be notified about suspicious activity.	• Create Alerts
Identify configuration gaps in your environment and understand their impact on overall security with Netwrix Risk Assessment dashboard.	• IT Risk Assessment Overview
Detect behavior anomalies in your IT environment with NetwrixBehavior Anomalies dashboard.	• Behavior Anomalies
Schedule email delivery of a variety of reports or set of specific search criteria with subscriptions/	• Create Subscriptions
Operations and health	
Track changes to the product configuration with Netwrix self-audit.	• Self-Audit
Review Netwrix Auditor System Health event log.	• Netwrix Auditor Health Log

Review Health status dashboard.	• Health Status Dashboard
Schedule Health Summary email delivery.	• Health Summary Email
If some issues encountered while using the product, review the troubleshooting instructions.	• Troubleshooting

Product Editions

Netwrix Auditor is available in two editions:

- Full-featured Enterprise Advanced
- Free Community Edition that is distributed free of charge and is more limited

Netwrix Auditor Enterprise Advanced can be evaluated for 20 days. During this period you have free, unlimited access to all features and functions. After the evaluation license expires, the product will prompt you to supply a commercial license where you can choose if you want to stay on Enterprise Advanced version. Alternatively, you can switch to Free Community Edition.

Free Community Edition helps you maintain visibility into your environment by delivering daily reports that summarize changes that took place in the last 24 hours. However, you will no longer be able to use interactive search, predefined reports, alerts and dashboards, or store your security intelligence. After switching to free mode, you may need to re-arrange your audit configuration due to the limitations.

When running Free Community Edition, at any time you can upgrade to Enterprise Advanced version, simply by supplying a commercial license in Settings > Licenses.

Refer to a table below to compare product editions.

Feature	Free Community Edition	Enterprise Advanced
Deployment options	One Netwrix Auditor client instance per one Netwrix Auditor Server	Multiple Netwrix Auditor clients for Netwrix Auditor Server

Feature	Free Community Edition	Enterprise Advanced
Role–based access and delegation	–	+
Support plan	–	Full
Automatic audit configuration	+	+
Data sources		
Active Directory (including Group Policy and Logon Activity)	One domain	Unlimited
Microsoft Entra ID	One Office 365 tenant	Unlimited
Exchange	One domain	Unlimited
EMC	One server or one file share, or one IP range, or one OU	Unlimited
NetApp	One server or one file share, or one IP range, or one OU	Unlimited
Windows File Servers	One server or one file share, or one IP range, or one OU	Unlimited
Office 365 (including Exchange Online, SharePoint Online, and OneDrive for Business)	One Office 365 tenant	Unlimited

Feature	Free Community Edition	Enterprise Advanced
Network Devices	One network device or one IP range	Unlimited
Oracle Database	One Oracle Database instance	Unlimited
SharePoint	One SharePoint farm	Unlimited
SQL Server	One SQL Server instance	Unlimited
VMware	One VMware Virtual Center	Unlimited
Windows Server	One server or IP range or one Active Directory container	Unlimited
Netwrix Auditor tools		
Netwrix Auditor Object Restore for Active Directory	–	+
Netwrix Auditor Event Log Manager	–	+
Netwrix Auditor Inactive User Tracker	–	+
Netwrix Auditor Password Expiration Notifier	–	+
Data collection details		

Feature	Free Community Edition	Enterprise Advanced
Who	–	+
What	+	+
When	+	+
Where	+	+
Workstation	+	+
User Activity video recording	–	+
Intelligence		
Activity Summary	1 recipient	Multiple recipients
AuditArchive	–	Both Long-Term Archive and Audit Database
Search	–	+
Reports (including organization–level reports, overview diagrams, change and activity reports,	–	+

Feature	Free Community Edition	Enterprise Advanced
reports with video and review status) and special report packs		
State–in–time reports	–	+
Ability to save search as a custom report	–	+
Subscriptions	–	+
Alerts	–	+
Behavior Anomaly Discovery dashboard	–	+
IT Risk Assessment dashboard	–	+
Netwrix Auditor Integration API		
Data in	–	+
Data out	–	+

What's New

The following information highlights the new and enhanced features introduced in this Netwrix Auditor 10.7 version.

New Features

Integration with Netwrix Privilege Secure

Netwrix Auditor is able to store its collection credentials in Netwrix Privilege Secure, making the usage of Auditor more secure.

Data sensitivity tags in searches and alerts for NetApp, Qumulo, and Synology

Data sensitivity tags in searches and alerts enable customers using NetApp, Qumulo, and Synology systems to reduce the time to detect incidents involving sensitive data and accelerate the response to these kinds of threats. They can set up alerts that will be triggered whenever sensitive documents are accessed, modified or deleted, or filter out all activity that isn't related to sensitive data.

New sensitive data-related risks for SharePoint Online

Three new risks help users secure their overexposed sensitive data in SharePoint Online (NDC is required). The new risks include:

• Sensitive files shared with anonymous users

• Sensitive files shared with external users

• Sensitive documents accessible by everyone

New Exchange Online report to ensure the confidentiality of sensitive email communications

This new state-in-time report shows all Exchange Online mailboxes with forwarding enabled, including details on whether the recipient is an internal or external user. Customers can use

this report to review forwarding rules, detect Business Email Compromise (BEC) attacks, and mitigate the risk of ongoing data leakages.

More informative subject lines in email notifications

The subject line of email alerts may include the who, what, or where details of an alerted activity. For example, the subject line of an email alert will be "*J.Doe has added M.Smith to Domain Admins*" instead of "*User has been added to a privileged group*".

Major Enhancements

- Download and read actions in SharePoint Online reports can be easily differentiated.
- Configuration of government Microsoft 365 tenants became easier. In the UI you can choose the national cloud environment you want to use.
- Modern authentication options for email notifications are supported.
- Option to save and send a report at the same time.
- Support for various new network devices, NAS, and database versions.

Numerous additional enhancements have been made to improve administration, performance, and security.

Bug Fix List

See the Netwrix Auditor v10.7 Bug Fix List PDF for a list of bugs fixed in this version.

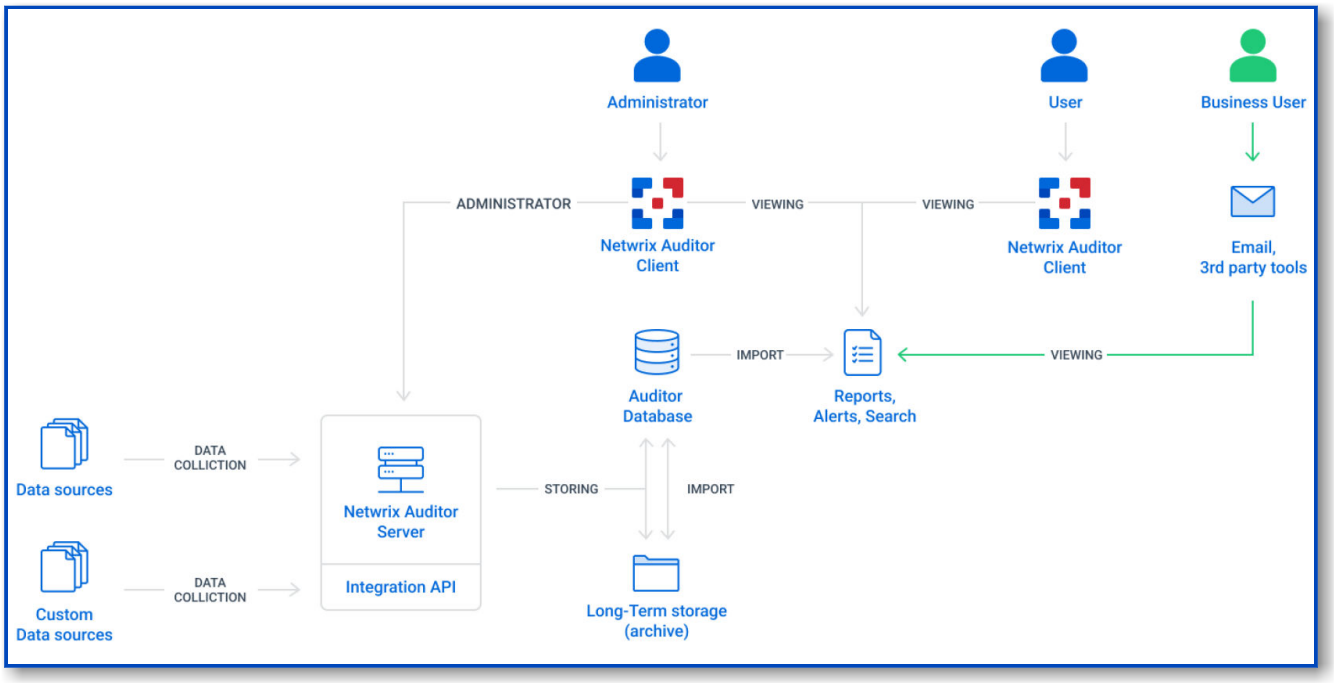
Requirements

This topic provides the requirements for the server where Netwrix Auditor will be installed. See the following topics for additional information:

- Supported Data Sources
- Hardware Requirements
- Software Requirements
- Requirements for SQL Server to Store Audit Data

Architecture Overview

Netwrix Auditor provides comprehensive auditing of applications, platforms and storage systems. The product 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 the product 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

NOTE: When auditing Active Directory domains, Exchange servers, expired passwords, and inactive users, the data sent by the product can be encrypted using Signing and Sealing. See the following Netwrix knowledge base article for additional information on how to secure Netwrix Auditor: Best Practices for Securing Netwrix Auditor.

Workflow Stages

The general workflow stages are as follows:

- 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.

- 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, the product 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.

    - See the Integration API topic for additional information on custom data source processing workflow.

- Audit data is stored to the Audit databases and the repository (Long-Term Archive) and preserved there according to the corresponding retention settings.

- 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.
- 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.

Supported Data Sources

This section lists platforms and systems that can be monitored with Netwrix Auditor.

Active Directory

Auditor supports monitoring the following domain controller operating system versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

See the Active Directory topic for additional information.

Active Directory Federation Services (AD FS)

Auditor supports monitoring the following AD FS operating system versions:

- AD FS 5.0 – Windows Server 2019
- AD FS 4.0 – Windows Server 2016
- AD FS 3.0 – Windows Server 2012 R2

See the AD FS topic for additional information.

Exchange

Auditor supports monitoring the following Exchange Server versions:

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013

See the Exchange topic for additional information.

File Servers

Dell Data Storage

Auditor supports monitoring the following device versions:

- Dell Data Storage (Unity XT, UnityVSA) running any of the following operating environment versions:
  - 5.2.x
  - 5.0.x
  - 4.5.x
  - 4.4.x
- Dell VNX/VNXe/Celerra families

NOTE: Only CIFS configuration is supported.

See the Dell Data Storage topic for additional information.

Dell Ilison/PowerScale

Auditor supports monitoring the following device versions:

- Dell Isilon/PowerScale versions 7.2 – 9.8

NOTE: Only CIFS configuration is supported.

Auditing of *System* zone is not supported. As stated by Dell, this zone should be reserved for configuration access only. Current data should be stored in other access zones. See the Isilon OneFS 8.2.1 CLI Administration Guide for additional information.

See the Dell Isilon/PowerScale topic for additional information.

NetApp Data ONTAP

Auditor supports monitoring the following device versions:

- Clustered-Mode
  - 9.0 – 9.14
  - 8.3

NOTE: Only CIFS configuration is supported.

See the NetApp Data ONTAP topic for additional information.

Nutanix

Auditor supports monitoring the following device versions:

- Files 3.6 - 4.3.0

See the Nutanix topic for additional information.

Qumulo

Auditor supports monitoring the following device versions:

- Core 3.3.5 - 6.x.x

See the Qumulo topic for additional information.

Synology

Auditor supports monitoring the following device versions:

- DSM 7.2
- DSM 7.1
- DSM 7.0
- DSM 6.2.3

See the Synology topic for additional information.

Windows File Servers

Auditor supports monitoring the following operating system versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 11
- Windows 10 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 7 (32 and 64-bit)

See the Windows File Servers topic for additional information.

Group Policy

Auditor supports monitoring the following domain controller operating system versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

See the Group Policy topic for additional information.

Logon Activity

Auditor supports monitoring the following domain controller operating system versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

See the Logon Activity topic for additional information.

Microsoft 365

Exchange Online

Auditor supports monitoring the following versions:

- Exchange Online version provided within Microsoft Office 365
- Microsoft GCC (government community cloud) and GCC High

  NOTE: DoD tenant types are not supported.

See the Exchange Online topic for additional information.

Microsoft Entra ID (formerly Azure AD)

Auditor supports monitoring the following versions:

- Microsoft Entra ID version provided within Microsoft Office 365
- Microsoft GCC (government community cloud) and GCC High

  NOTE: DoD tenant types are not supported.

See the Microsoft Entra ID (formerly Azure AD) topic for additional information.

Microsoft Teams (MS Teams)

Auditor supports monitoring the following versions:

- Microsoft Entra ID version provided within Microsoft Office 365
- Microsoft GCC (government community cloud) and GCC High

NOTE: DoD tenant types are not supported.

See the MS Teams topic for additional information.

SharePoint Online

Auditor supports monitoring the following versions:

- SharePoint Online version provided within Microsoft Office 365
- Microsoft GCC (government community cloud) and GCC High

NOTE: DoD tenant types are not supported.

See the SharePoint Online topic for additional information.

Network Devices

Cisco ASA Devices

Auditor supports monitoring the following device versions:

- ASA (Adaptive Security Appliance) 8 and above

See the Configure Cisco ASA Devices topic for additional information.

Cisco IOS Devices

Auditor supports monitoring the following device versions:

- IOS (Internetwork Operating System) 12, 15, 16, and 17

See the Configure Cisco IOS Devices topic for additional information.

Cisco Meraki Dashboard

Auditor supports monitoring the following device versions:

- Netwrix recommends the latest version of the Meraki Dashboard

See the Cisco Meraki Dashboard topic for additional information.

Cisco FTD

Auditor supports monitoring the following device versions:

- FTD (Firepower Threat Defense) 6.5

Fortinet FortiGate Devices

Auditor supports monitoring the following device versions:

- FortiOS 5.6 and above

See the Configure Fortinet FortiGate Devices topic for additional information.

HPE Aruba Devices

Auditor supports monitoring the following device versions:

- Aruba OS 6.46.4.x – 8.6.0.x (Mobility Master, Mobility Controller)

See the Configure Pulse Secure Devices topic for additional information.

Juniper Devices

Auditor supports monitoring the following device versions:

- vSRX with Junos OS 12.1, Junos OS 18.1, Junos OS 20.4R2
- vMX with Junos OS 17.1

See the Configure Juniper Devices topic for additional information.

PaloAlto Devices

Auditor supports monitoring the following device versions:

- PAN-OS 7.0, 8.0, 9.0, 10.0

See the Configure PaloAlto Devices topic for additional information.

Pulse Secure Devices

Auditor supports monitoring the following device versions:

- 9.1R3 and above

See the Configure Pulse Secure Devices topic for additional information.

SonicWall Devices

Auditor supports monitoring the following device versions:

- WAF 2.0.0.x / SMA v9.x & v10.x
- NS 6.5.x.x with SonicOS 6.5.x and 7.0.x
- SMA 12.2

See the Configure SonicWall Devices topic for additional information.

Oracle

Auditor supports monitoring the following versions:

- Database 23c On-Premise
- Database 21c On-Premise
- Database 19c On-Premise
- Database 18c On-Premise
- Database 12c On-Premise (12.1, 12.2)
- Database 11g, limited support

  NOTE: See the Considerations for Oracle Database 11g topic for additional information.
- Oracle Database Cloud Service (Enterprise Edition)

See the Oracle Database topic for additional information.

SharePoint

Auditor supports monitoring the following versions:

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2016

- Microsoft SharePoint Foundation 2013 and SharePoint Server 2013
- Microsoft SharePoint Foundation 2010 and SharePoint Server 2010

See the SharePoint topic for additional information.

SQL Server

Auditor supports monitoring the following versions:

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

NOTE: Linux-based versions are not supported.

See the SQL Server topic for additional information.

User Activity

Auditor supports monitoring the following versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 11
- Windows 10 (32 and 64-bit)

- Windows 8.1 (32 and 64-bit)
- Windows 7 (32 and 64-bit)

User Activity data source can support around 300 targets with one user session per target without scalability issues:

- Depending on how dense is the actual user activity, the number can be more for servers but less for workstations.
- 50-100 concurrent sessions per terminal server.

Netwrix recommends using the User Activity auditing only for those infrastructure areas that require more attention due to their sensitivity or criticality. Applicable usage scenarios include, for example:

- Terminal servers where users can log in from external locations
- Areas accessible by contractor personnel
- Servers with sensitive information
- Sessions with elevated privileges

See the User Activity topic for additional information.

VMware Servers

Auditor supports monitoring the following versions:

- VMware ESX/ESXi: 6.0 – 6.7, 7.0, 8.0
- VMware vCenter Server: 6.0 – 6.7, 7.0, 8.0

See the VMware topic for additional information.

Windows Servers

Windows Servers & Desktops

Auditor supports monitoring the following operating system versions:

- Windows Server 2022

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 11
- Windows 10 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 7 (32 and 64-bit)

DNS & DHCP

Auditor supports monitoring the following operating system versions:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

NOTE: DNS support is limited on Windows Server 2008 to Windows Server 2008 SP2 (32 and 64-bit). DHCP is not supported on Windows Server 2008.

Internet Information Services (IIS)

Auditor supports monitoring the following operating system versions:

- IIS 7.0 and above.

See the Windows Server topic for additional information.

Netwrix Integration API

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

Also, there are even add-ons that can export data collected by Auditor to other systems (e.g., ArcSight and ServiceNow).

See the Integration API topic for additional information.

Monitored Object Types, Actions, and Attributes

Netwrix Auditor monitored object types, actions, attributes and components for each data source are located in the following topics:

- Active Directory
- AD FS
- Exchange
- File Servers
    - Dell Data Storage
    - Dell Isilon/PowerScale
    - NetApp Data ONTAP
    - Nutanix
    - Qumulo
    - Synology
    - Windows File Servers
- Group Policy
- Logon Activity
- Microsoft 365
    - Exchange Online
    - Microsoft Entra ID
    - SharePoint Online
    - MS Teams

- Network Devices
- Oracle Database
- SharePoint
- SQL Server
- User Activity
- VMware
- Windows Server

Review the list of actions audited and reported by Netwrix Auditor. Actions vary depending on the data source and the object type.

Action	Active Directory	Active Directory Federation Services	Exchange Exchange Online	File Servers	Group Policy	Logon Activity	Microsoft Entra ID (formerly Azure AD)	Oracle database	SharePoint SharePoint Online	SQL Server	User Activity	VMware Servers	Windows Server	
Added	+	-	+*	+	+	–	+	+	+	+	–	+	+	
Removed	+	-	+*	+	+	–	+	+	+	+	–	+	+	
Modified	+	–	+*	+	+	–	+	+	+	+	–	+	+	

Action	Active Directory	Active Directory Federation Services	Exchange Exchange Online	File Servers	Group Policy	Logon Activity	Microsoft Entra ID (formerly Azure AD)	Oracle database	SharePoint SharePoint Online	SQL Server	User Activity	VMware Servers	Windows Server	
Add (failed attempt)	–	–	–	+	–	–	–	+	–	–	–	–	–	
Remove (failed attempt)	–	–	–	+	–	–	–	+	–	–	–	–	–	
Modify (failed attempt)	–	–	–	+	–	–	–	+	–	–	–	–	+	
Read	–	–	+*	+	–	–	–	+	+	–	–	–	–	

Action	Active Directory	Active Directory Federation Services	Exchange Exchange Online	File Servers	Group Policy	Logon Activity	Microsoft Entra ID (formerly Azure AD)	Oracle database	SharePoint SharePoint Online	SQL Server	User Activity	VMware Servers	Windows Server	
Read (failed attempt)	–	–	–	+	–	–	–	+	–	–	–	–	–	
Renamed	–	–	–	+	–	–	–	+	+**	–	–	–	–	
Moved	–	–	+*	+	–	–	–	–	+	–	–	–	–	
Rename (failed attempt)	–	–	–	+	–	–	–	+	–	–	–	–	–	
Move (failed	–	–	–	+	–	–	–	–	–	–	–	–	–	

Action	Active Directory	Active Directory Federation Services	Exchange Exchange Online	File Servers	Group Policy	Logon Activity	Microsoft Entra ID (formerly Azure AD)	Oracle database	SharePoint SharePoint Online	SQL Server	User Activity	VMware Servers	Windows Server	
attempt)														
Checked in	–	–	–	–	–	–	–	–	+	–	–	–	–	
Checked out	–	–	–	–	–	–	–	–	+	–	–	–	–	
Discard checkout	–	–	–	–	–	–	–	–	+	–	–	–	–	
Successful logon	–	+	–	–	–	+	+	+	–	+	–	+	–	
Failed logon	–	+	–	–	–	+	+	+	–	+	–	+***	–	

Action	Active Directory	Active Directory Federation Services	Exchange Exchange Online	File Servers	Group Policy	Logon Activity	Microsoft Entra ID (formerly Azure AD)	Oracle database	SharePoint SharePoint Online	SQL Server	User Activity	VMware Servers	Windows Server	
Logoff	–	–	–	–	–	–	–	+	–	–	–	–	–	
Copied	–	–	+*	+	–	–	–	–	+**	–	–	–	–	
Sent	–	–	+*	–	–	–	–	–	–	–	–	–	–	
Activated	–	–	–	–	–	–	–	–	–	–	+	–	–	
Support for state-in-time data collection	+	–	+	+	+	-	+	-	+	-	-	+	+	

* —these actions are reported when auditing non-owner mailbox access for Exchange or Exchange Online.

** — these actions are reported for SharePoint Online only.

*** — Auditor will not collect data on *Failed Logon* event for VMware in case of incorrect logon attempt through VMware vCenter Single Sign-On; also, it will not collect logons using SSH.

Hardware Requirements

This topic covers hardware requirements for Netwrix Auditor installation and provides estimations of the resources required for Netwrix Auditor deployment.

The actual hardware requirements will depend on the number of activities collected per day in addition to the number of files and folders monitored.

CAUTION: To keep your systems safe, AUDITOR should not be exposed to inbound access from the internet.

Full Installation

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

Requirements provided in this section apply to a clean installation on a server without any additional roles or third-party applications installed.

Use these requirements only for initial estimations and be sure to correct them based on your data collection and monitoring workflow.

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

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV

Auditor supports only Windows OS versions listed in the Software Requirements topic.

Netwrix Auditor and SQL Server instance will be deployed on different servers.

Requirements below apply to Netwrix Auditor server.

Hardware component	Evaluation, PoC or starter environment	Regular environment (up to 1m ARs*/day)	Large environment (1-10m ARs*/day)	XLarge environment (10m ARs*/day or more)
CPUs	2 cores	4 CPUs	8 CPUs	16 CPUs
RAM	8 GB	min 8 GB	min 16 GB	64 GB
Disk space	100 GB—System drive 100 GB—Data drive	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
Others	—	—	Network capacity 1 Gbit	Network capacity 1 Gbit

* — ARs stands for Activity Records, that is, Netwrix-compatible format for the audit data. See Activity RecordsActivity Records for more details.

** — By default, the Long-Term Archive and working folder are stored on a system drive. To reduce the impact on the system drive in large and xlarge environments, Netwrix recommends storing your Long-Term Archive and working folder on a data drive and plan for their capacity accordingly. For details, see:

- File-Based Repository for Long-Term Archive
- Working Folder

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 related 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.

For detailed information about hardware requirements for a standalone SQL Server, refer to the following Microsoft article: SQL Server: Hardware and software requirements

NOTE: In larger environments, SQL Server may become underprovisioned on resources. For troubleshooting such cases, refer to the Sample Deployment Scenarios topic.

Additional Sizing Information for File Data Source

Use this table to determine the requirements for file servers monitoring based on the number of files in the system. These requirements will add up to the requirements for other monitoring plans.

Netwrix Auditor	Per 1 Million Files	Per 5 Million Files
CPUs	0.2 CPUs	1.0 CPUs
RAM (Activity Records only)	0.125 GB RAM	0.625 GB RAM
RAM (Activity Records and State-in-Time)	0.5 GB RAM	2.5 GB RAM

If you are monitoring both Active Directory and Windows File Servers data sources, you calculate using the requirements for AD, and then add the requirements for your File Servers.

For example, you have a large Active Directory environment which requires 8 cores and 16 GB RAM. Add the requirements for 5 million files which are 1 CPU and 2.5 GB RAM. Therefore, you will need 9 CPUs and 18.5 GB RAM.

If you need assistance calculating the number of files you have and already using Netwrix Auditor, this information is displayed in the Environment Stats located on the Home Screen.

If you have not already started using Netwrix Auditor, you can download this file scanning tool by clicking the link.

Client Installation

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

Virtual deployment is recommended.

Hardware component	Minimum required	Recommended
CPUs	Any modern CPU (e.g. Intel or AMD 32 bit, 2 GHz)	Any modern 2 CPUs (e.g. Intel Core 2 Duo 2x or 4x 64 bit, 3 GHz)

Hardware component	Minimum required	Recommended
RAM	2 GB	8 GB
Disk space	200 MB	

Software Requirements

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

Component	Full installation (both Auditor Server and Client)	Client installation (client only)
Operating system (English-only)	Windows Server OS: • Windows Server 2022 • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 Windows Desktop OS (64-bit): • Windows 11 • Windows 10	• Windows Desktop OS (32 and 64-bit): Windows 10, Windows 11 • Windows Server OS: Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019
.NET Framework	• .NET Framework 4.8 and above. See the following Microsoft article for additional information about .Net Framework installer redistributable: Microsoft .NET Framework 4.8 offline installer for Windows.	—

Component	Full installation (both Auditor Server and Client)	Client installation (client only)
Installer	• Windows Installer 3.1 and above See the following Microsoft article for additional information about Windows Installer redistributable: Windows Installer 3.1 v2 (3.1.4000.2435) is available	• Windows Installer 3.1 and above See the following Microsoft article for additional information about Windows Installer redistributable: Windows Installer 3.1 v2 (3.1.4000.2435) is available

Other Components

To monitor your data sources, you will need to install additional software components on Auditor Server, in the monitored environment, or in both locations.

Data source	Components
• **Active Directory** • **Exchange Server** • **Exchange Online**	*On the computer where* Auditor *Server is installed:* • Windows PowerShell 3.0 and above
• **AD FS**	*On the computer where* Auditor *Server is installed:* • Windows Remote Management must be configured to allow remote PowerShell usage. For that, set up the **TrustedHosts** list: ◦ to include all AD FS servers, use the following cmdlet: `Set-Item wsman:\localhost\Client\TrustedHosts -value '*' -Force;` ◦ to include specific AD FS servers (monitored items), do the following:

Data source	Components
	◦ Use Get cmdlet to obtain the existing **TrustedHosts** list. ◦ If necessary, add the IP addresses of required AD FS servers to existing list (use comma as a separator). ◦ Provide the updated list to the cmdlet as a parameter. For example: `Set-Item wsman:\localhost\Client\TrustedHosts -value '172.28.57.240,172.28.57.127' -Force;` See the following Microsoft article Installation and configuration for Windows Remote Management for additional information about TrustedHosts.
• **Windows Server (with enabled network traffic compression)** • **User Activity**	*In the monitored environment:* • .NET Framework 4.8 and above. See the following Microsoft article for additional information about .Net Framework installer redistributable: Microsoft .NET Framework 4.8 offline installer for Windows.
• **Microsoft Entra ID Ports** • **SharePoint Online**	Usually, there is no need in any additional components for data collection.
• **Oracle Database**	Oracle Database 12c and above: *On the computer where* Auditor *Server is installed:* • Oracle Instant Client.

Data source	Components
	◦ Download the appropriate package from Oracle website: Instant Client Packages. Netwrix recommends installing the latest available version (Netwrix Auditor is compatible with version 12 and above). ◦ Install, following the instructions, for example, Instant Client Installation for Microsoft Windows 64-bit. Check your Visual Studio Redistributable version. Applicable packages for each Oracle Database version with downloading links are listed in the installation instructions: Instant Client Installation for Microsoft Windows 64-bit. Oracle Database 11g: Auditor provides limited support of Oracle Database 11g. See the Considerations for Oracle Database 11g topic for additional information. *On the computer where* 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 the following setup steps: • Download the 64-bit Oracle Data Access Components 12c Release 4 (12.1.0.2.4) for Windows x64 (ODAC121024_x64.zip) package. • Run the setup and select the Data Provider for .NET checkbox. Oracle Instant Client will be installed, too. • On the ODP.NET (Oracle Data Provider) step make sure the Configure ODP.NET

Data source	Components
	and/or Oracle Providers for ASP.Net at machine-wide level checkbox is selected .
• **Group Policy**	*On the computer where* Auditor *Server is installed:* • Group Policy Management Console. Download Remote Server Administration Tools that include GPMC for: ◦ Windows 8.1 ◦ Windows 10 • For Windows Server 2012 R2/2016, Group Policy Management is turned on as a Windows feature.

Using SSRS-based Reports

SQL Server Reporting Services are needed for this kind of reports. See the Requirements for SQL Server to Store Audit Data topic for additional information. If you plan to export or print such reports, check the requirements below.

NOTE: Please note that if you are going to use SQL Express plan, do not install SSRS and Auditor on the domain controller.

Export SSRS-based reports

To export SSRS-based reports, Internet Explorer recommended to be installed on the machine where Auditor client runs. If IE is not available, you can use the **Print** function or click the button **Open in browser** and export the report directly from Netwrix Auditor.

See the following Microsoft article for the full list of the supported browsers: Browser Support for Reporting Services and Power View.

Follow the steps to configure Internet Options to allow file downloads for the Local intranet zone.

Step 1 – Select **Internet Options** and click **Security**.

Step 2 – Select **Local intranet** zone and click **Custom level**.

Step 3 – In the Settings list, locate **Downloads** > **File download** and make sure the **Enabled** option is selected.

Printing

To print SSRS-based reports, SSRS Report Viewer and Auditor Client require ActiveX Control to be installed and enabled on the local machine. See the Impossible to Export a Report Netwrix knowledge base article for additional information.

You can, for example, open any SSRS-based report using your default web browser and click **Print**. The browser will prompt for installation of the additional components it needs for printing. Having them installed, you will be able to print the reports from Auditor UI as well.

Server and Client

It is recommended to deploy Auditor server on the virtualized server – to simplify backup, provide scalability for future growth, and facilitate hardware configuration updates. Auditor clent 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)
    - You can deploy Netwrix Auditor to VMware cloud. You can install the product to a virtual machine or deploy as virtual appliance.
- Microsoft Hyper-V
- Nutanix AHV (Acropolis Hypervisor Virtualization) 20180425.199

See the Virtual Deployment Overview topic for additional information.

Domains and Trusts

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

Installation on the domain controller is not supported.

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

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

If 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 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 Auditor Server host by its DNS or NetBIOS name.
In workgroups	• The computer where 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.

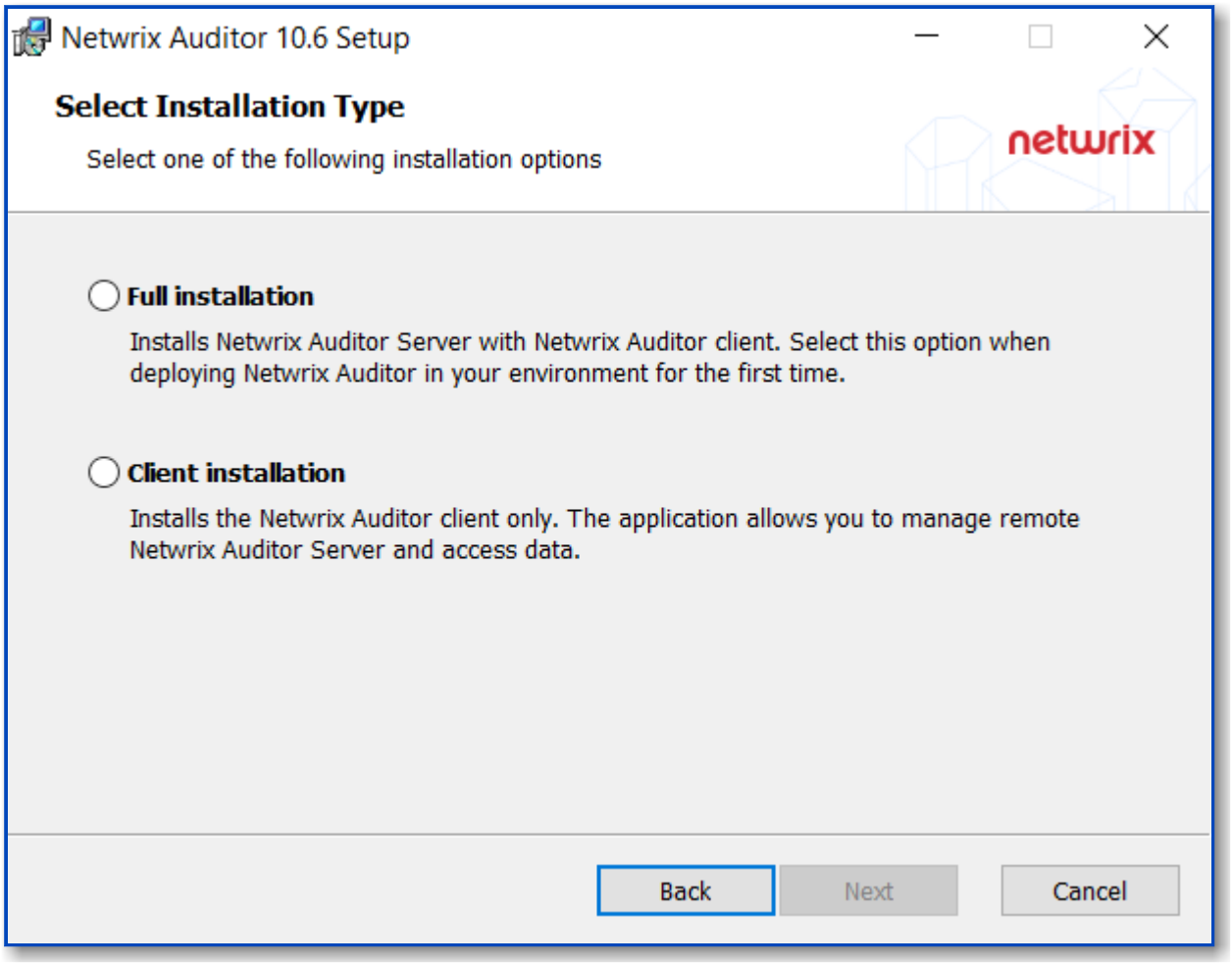
If Auditor Server and the audit system reside...	Mind the following restrictions...
	• For monitoring Windows Server and User Activity, each monitored computer (the computer where Netwrix Auditor User Activity Core Service resides) must be able to access the Auditor Server host by its DNS or NetBIOS 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.

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

Simple Deployment

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



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

Distributed Deployment (Client-Server)

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

Follow the steps to perform distributed deployment.

Step 1 – Install Auditor server and default client, selecting Full installation during the product setup.

Step 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 Auditor client using Group Policy. See the Install Client via Group Policy topic for additional information.

Default local client will be always installed together with the Auditor in all scenarios.

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.

Supported SQL Server versions and editions are listed below.

Due to limited database size, Express Edition (with Reporting Services) is recommended only for evaluation, PoC or small environments. For production environment, consider using Standard or Enterprise Edition.

Version	Edition
SQl Server 2022	• Standard or Enterprise Edition • Express Edition with Reporting Services (for evaluation, PoC and small environments)
SQL Server 2019 (on-premises Windows version) cumulative update 10 and above	• Standard or Enterprise Edition • Express Edition with Reporting Services (for evaluation, PoC and small environments)
SQL Server 2017	• Standard or Enterprise Edition • Express Edition with Reporting Services (for evaluation, PoC and small environments)
SQL Server 2016	• Standard or Enterprise Edition • Express Edition with Advanced Services (SP2) (for evaluation, PoC and small environments)
SQL Server 2014	• Standard or Enterprise Edition

Version	Edition
	• Express Edition with Advanced Services (for evaluation, PoC and small environments)
SQL Server 2012	• Standard or Enterprise Edition • Express Edition with Advanced Services (for evaluation, PoC and small environments)

NOTE: SQL express is only supported for small environments. It might cause performance issues on the medium and large environments.

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 the Add a database to an Always On availability group with the 'Availability Group Wizard' 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.

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 2016 SP2 Express with Advanced Services using the Audit Database Settings wizard or by manually downloading it from Microsoft web site. See the Install Microsoft SQL Server and Reporting Services section for additional information.

SQL Server and Databases

Netwrix Auditor uses SQL Server databases as operational storages that keep audit data for analysis, search and reporting purposes. Supported versions are SQL Server 2012 and later (Reporting Services versions should be 2012 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 Create a New Monitoring Plan topic.

For evaluation and PoC projects you can deploy Microsoft SQL Server 2016 SP2 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 of the Health Status dashboard. This feature, however, is supported only for SQL Server 2012 SP3 and later.

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>*.

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.

Database name	Description
Netwrix_CategoriesDB	Intended for integration with Netwrix Data Classification. This database is always created but is involved in the workflow only if the DDC Provider is enabled. See for more information.
Netwrix_CommonDB	Stores views to provide cross-database reporting.
Netwrix_ImportDB	Stores data imported from Long-Term Archive.
Netwrix_OverviewReportsDB	Stores data required for overview reports.
Netwrix_Self_Audit	Stores data collected by Netwrix Auditor self-audit (optional, created if the corresponding feature is enabled).

These databases usually do not appear in the UI; they are only listed in the **Database statistics** widget of the **Health Status** dashboard. 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).

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:

- Supported versions are 2012 and later.
- **NOTE:** Please, note that for the Reporting Services, only English operating systems are supported.
- Supported editions are Enterprise, Standard and Express with Advanced Services (it includes Reporting Services).
- 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:

- SQL Server Reporting Services

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

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.

SQL Server

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

- 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.
- In large and extra-large infrastructures 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.
- If you plan to have Netwrix Auditor and SQL Server running on different machines, establish fast and reliable connection between them (100 Mbps or higher).
- Both standalone servers and SQL Server clusters are supported, as well as AlwaysOn Availability Groups.
- You can configure Netwrix Auditor to use an existing SQL Server instance, or create a new one. As an option, you can install SQL Server 2016 Express Edition, using the Audit Database Settings wizard or manually downloading it from Microsoft web site (see Install Microsoft SQL Server and Reporting Services).

CAUTION: It is not recommended to install NETWRIX AUDITOR databases to a production SQL Server instance. Such instances may have a lot of maintenance plans or scripts running that may affect data uploaded by the product. The product databases are designed for reporting and searching and do not require maintenance or backup. For the long-term data storage, NETWRIX AUDITOR uses Long-Term Archive. See File-Based Repository for Long-Term Archive for additional information.

If you select to set up a new SQL Server instance, the current user account (this should be a member of local Administrators group) will be assigned the *sysadmin* server role for it.

You will also need to provide a path for storing the SQL Server databases - it is recommended to specify the data drive for that purpose (by default, system drive is used).

- 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.
- Consider that sufficient access rights will be required for the account that will write data to the audit databases hosted on the default SQL Server. This account should be assigned the following roles:
  - **Database owner (db_owner)** database-level role
  - dbcreator server-level role

  This account can be specified when you configure the Audit Database settings.

Database Sizing

For database sizing, it is recommended to estimate:

- Size of the environment you are going to monitor
- Amount of activity records produced by the audited system
- Retention policy for the audit databases
- 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 Auditor during the week, you can use the Activity records by date widget of the Health Status dashboard. See the Activity Records Statistics topic for additional information.

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 the Database Statistics topic for additional information.

This feature is supported only for SQL Server 2012 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

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. Consider the following:

- 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.
- 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*.

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 Auditor databases cannot be modified.

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:

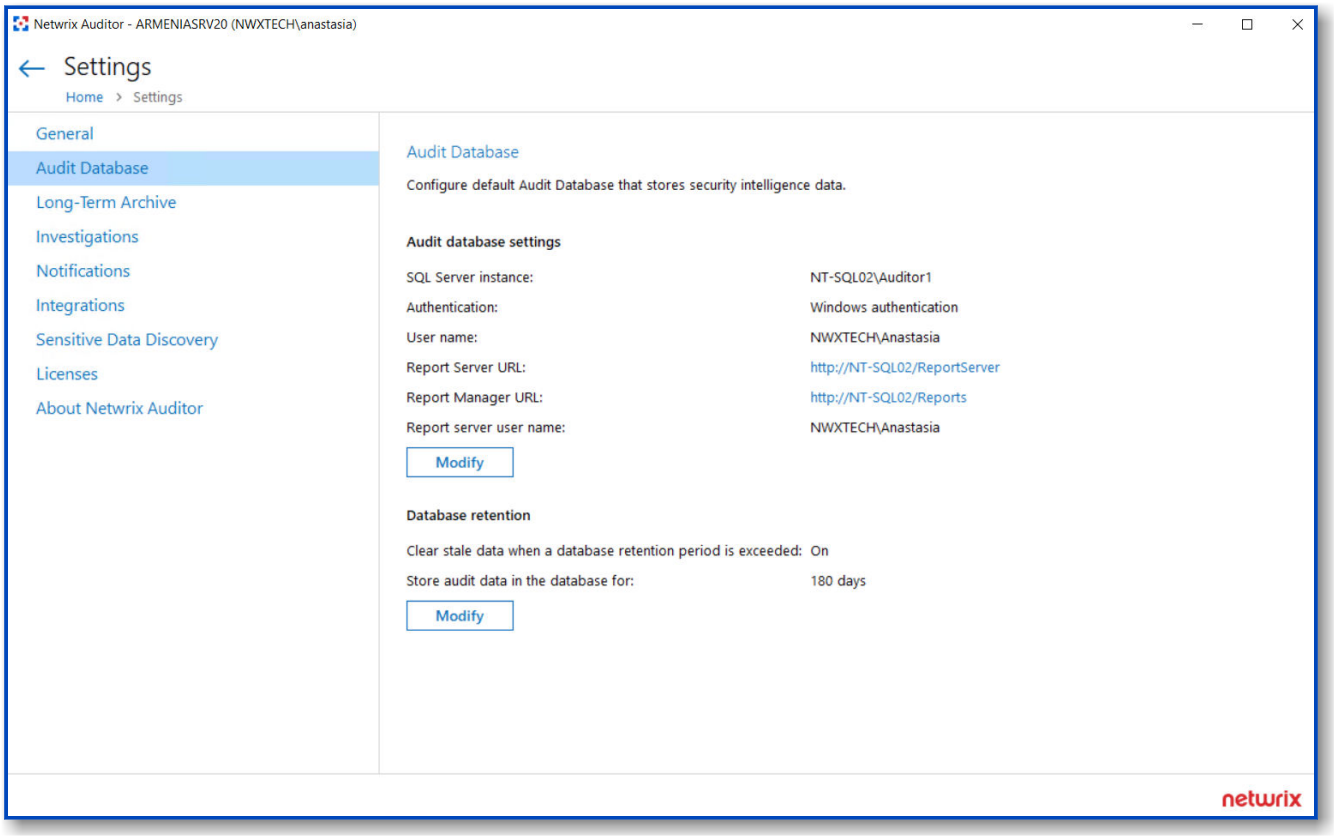
1. First monitoring plan for collecting data from SQL Servers, targeted at *Netwrix_Auditor_SQL_Monitoring* database.
2. Second monitoring plan for collecting data from Oracle servers, targeted at *Netwrix_Auditor_Oracle_Monitoring* database.

Database Retention

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

Follow the steps to change database retention after the product deployment.

Step 1 – In the Auditor main screen, select Settings > Audit Database.



Step 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).

This setting also applies to the *Netwrix_Auditor_API* database.

Configure Audit Database Account

This is the account that Auditor uses to write the collected audit data to the audit databases. Starting with version 9.96, you can use Group Managed Service Account (gMSA) for that purpose.

Remember, gMSA cannot be used to access SSRS. Use a standard account for that. See the SQL Server Reporting Services topic for additional information.

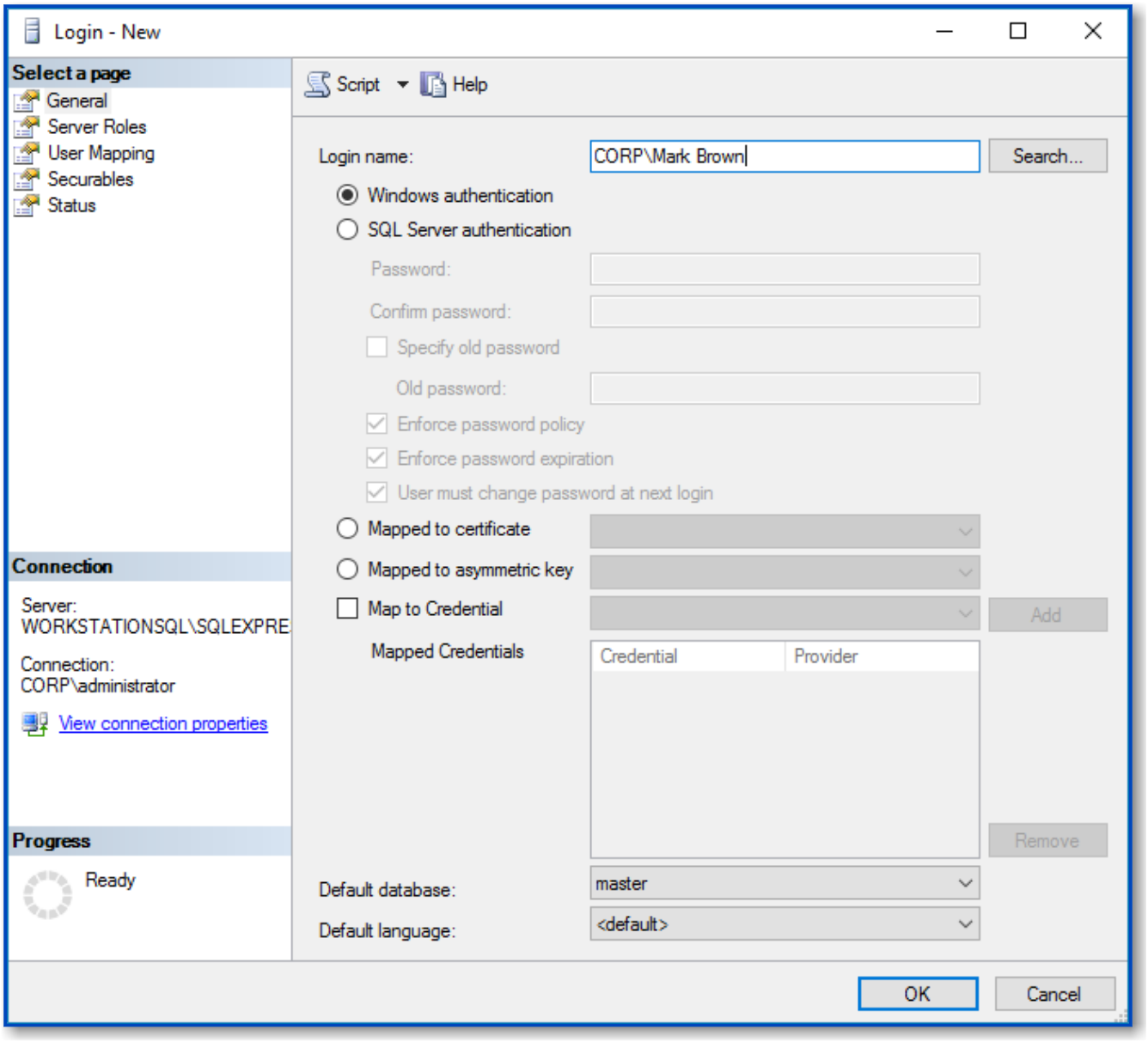
This account must be granted the **Database owner (db_owner)** role and the **dbcreator** server role on the SQL Server instance hosting your audit databases.

Follow the steps to assign the **dbcreator** and **db_owner** roles.

Step 3 – On the computer where SQL Server instance with the Audit Database resides, navigate to **Start** > **All Programs** > **Microsoft SQL Server** > **SQL Server Management Studio**.

Step 4 – Connect to the server.

Step 5 – In the left pane, expand the **Security** node. Right-click the **Logins** node and select **New Login** from the pop-up menu.



Step 6 – Click **Search** next to **Login Name** and specify the user that you want to assign the **db_owner** role to.

Step 7 – Select **Server roles** on the left and assign the **dbcreator** role to the new login.

Step 8 – Select the **User Mapping** tab. Select all databases used by Auditor to store audit data in the upper pane and check **db_owner** in the lower pane.

NOTE: This step is only required when changing the existing Audit Database Account to a new one.

Step 9 – 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.

If you need to migrate the Audit Database, see the How to Migrate Netwrix Auditor Databases to Another SQL Server Instance knowledge base article.

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 (2012 R2 and above required).

Consider the following:

- 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.

Configure SSRS Account

An account used to upload data to the SQL Server Reporting Services (SSRS) Server must be granted the Content Manager role on the SSRS **Home** folder.

NOTE: gMSA cannot be used to access SSRS. Use a standard account for that purpose.

Follow the steps to assign the Content Manager role.

Step 1 – Navigate to your **Report Manager** URL.

Step 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).

Step 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.

Step 4 – Select **Content Manager**.

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.

Follow the steps to assign the Browser role to a user.

Step 1 – Open the **Report Manager** URL in your web browser.

Step 2 – Depending on the user's delegated scope, select the entire Home folder or drill-down to specific data sources or event reports.

Step 3 – Navigate to **Manage Folder** (the path can slightly vary depending on your SQL Server version) and select Add group or user.

Step 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.

Step 5 – Select **Browser**.

As a rule, Auditor can use Reporting Services with the default settings. However, to ensure that Reporting Services is properly configured, perform the following procedure:

You must be logged in as a member of the local Administrators group on the computer where SQL Server 2016 Express is installed.

Follow the steps to verify Reporting Services installation.

Step 6 – Navigate to **Start >All Apps > SQL ServerReporting Services Configuration Manager**.

Step 7 – In the Reporting Services Configuration Connection dialog, make sure that your local report server instance (for example, *SQLExpress*) is selected, and click **Connect**.

Step 8 – 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*

Step 9 – 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.

Step 10 – 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.

File-Based Repository for Long-Term Archive

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

Location

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

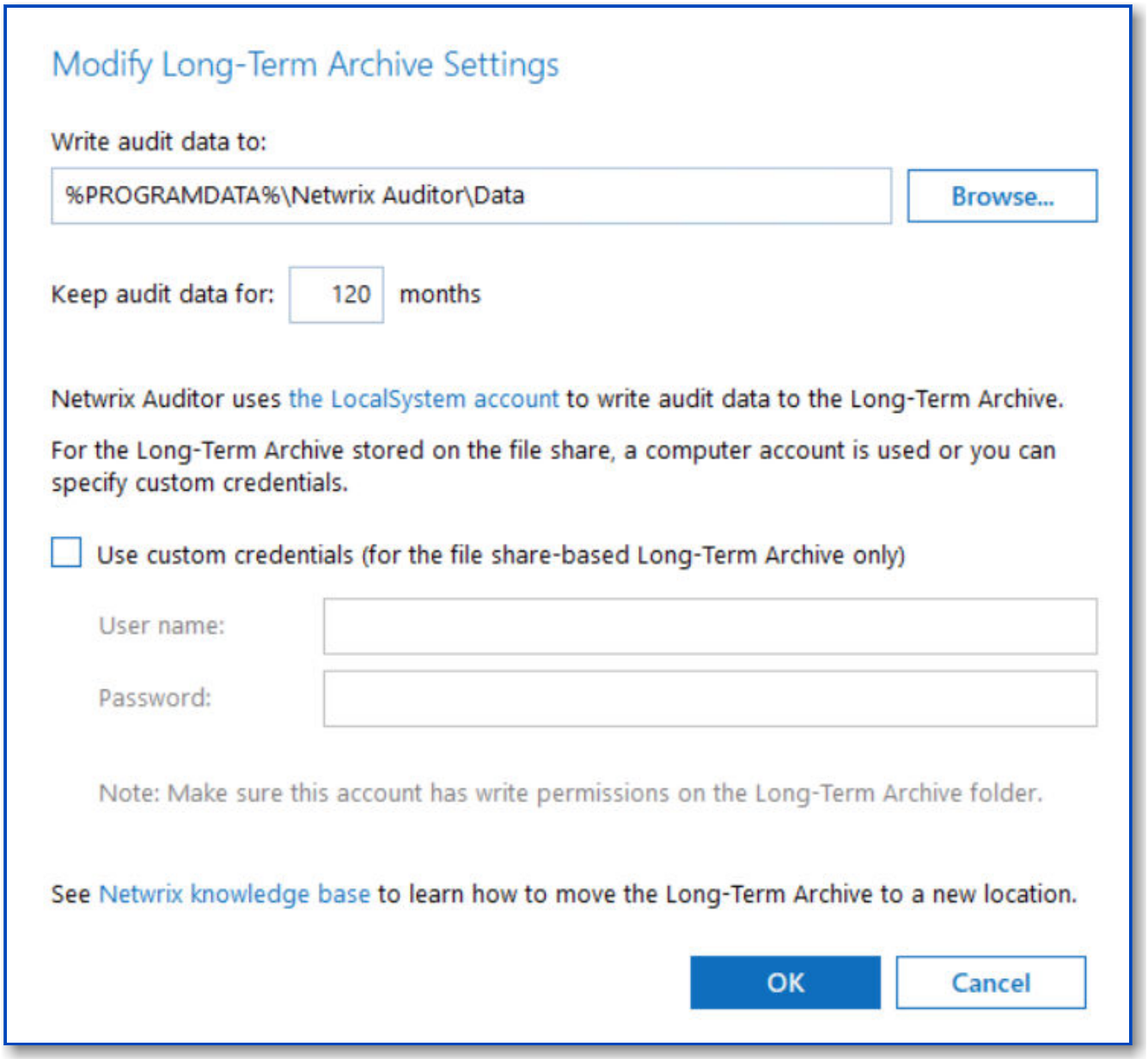
To reduce the impact on the system drive in large and extra-large environments, it is recommended to move Long-Term Archive to another disk. For that, you should estimate the required capacity using recommendations in the next section.

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.

Follow the steps to modify Long-Term Archive location and other settings.

Step 1 – In 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.

Step 2 – Click Modify.



Step 3 – Enter new path or browse for the required folder.

Step 4 – Provide retention settings and access credentials.

Step 5 – To move data from the old repository to the new location, take the steps described in the following Netwrix knowledge base article: How to Move Long-Term Archive to a New Location.

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

Retention

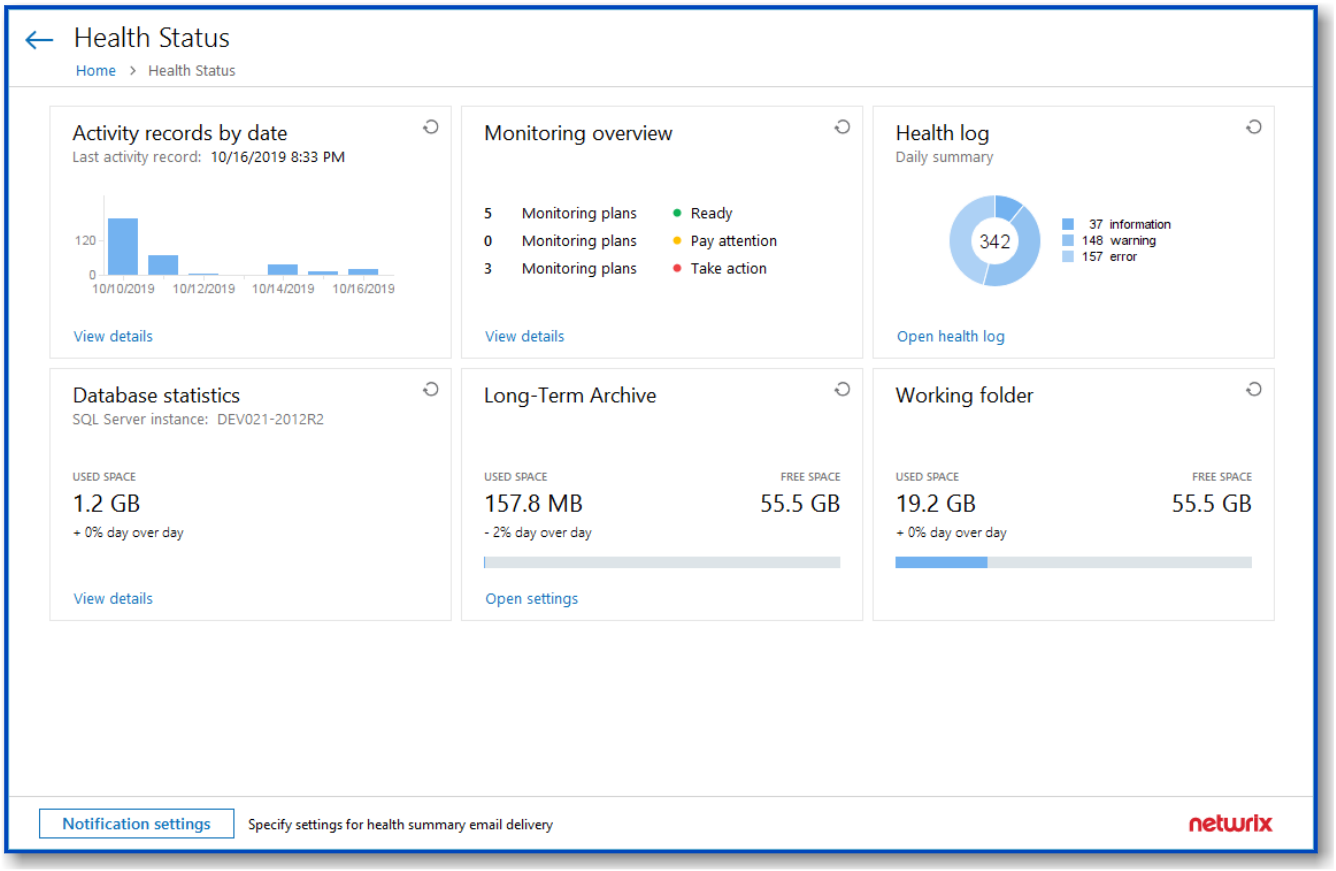
Default retention period for repository data is **120 months**. You can specify the value you need in the Long-Term Archive settings. When retention period is over, data will be deleted automatically.

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.

Capacity

To examine the repository capacity and daily growth, use the Long-Term Archive Capacity 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 Statistics 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.

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

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 Auditor.

Starting with version 9.96, you can use Group Managed Service Account (gMSA) as the account for accessing Long-term Archive.

The custom 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

  Subscriptions created in the Auditor client are uploaded to file servers under the Long-Term Archive service account as well. See the Subscriptions topic for additional information.

Assign Permissions on the Long-Term Archive Folder

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

Follow the steps to assign permissions on the Long-Term Archive folder:

Step 1 – Navigate to a folder where the Long-Term Archive will be stored, right-click it and select Properties.

Step 2 – In the **<Folder_name> Properties** dialog, select the **Security** tab and click **Advanced**.

Step 3 – In the Advanced Security dialog, select the Permissions tab and click Add.

Step 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

Assign Change and Create Files/Write Data Permissions to Upload Subscriptions to File Shares

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

Follow the steps to assign the **Change** and **Create Files/Write Data** permissions to upload subscriptions to file shares:

Step 1 – Navigate to a folder where report subscriptions will be stored, right-click it and select Properties.

Step 2 – In the **<Share_Name> Properties** dialog, select the **Sharing** tab and click **Advanced Sharing**.

Step 3 – In the Advanced Sharing dialog, click Permissions.

Step 4 – In the Permissions for <Share_Name> dialog, select a principal or add a new, then check the Allow flag next to Change.

Step 5 – Apply settings and return to the **<Share_Name> Properties** dialog.

Step 6 – In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

Step 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.

Step 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.

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 Auditor.

System Health

Long-Term Archive is a file-based storage where Auditor saves the collected activity records. By default, it is located on the system drive at *%PROGRAMDATA%\Netwrix Auditor\Data* and keeps data for 120 months. You may want to modify these settings, for example, move the storage from the system drive to another location. The Long-Term Archive widget will help you to monitor the Long-Term Archive capacity. The widget displays the current size and daily increase of the Long-Term Archive, and the remaining free space on the target drive.

To open the Long-Term Archive settings, click the corresponding link. Then you will be able to adjust the settings as necessary. See the Long-Term Archive topic for additional information.

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 *%ProgramData%\Netwrix Auditor*.

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.

If you want to change the working folder default location, run the specially designed utility. See the How to Migrate Netwrix Auditor Working Folder to a New Location Knowledge Base article for additional information.

Protocols and Ports Required

To ensure successful data collection and activity monitoring, Auditor has to communicate through firewall and requires some ports to be opened for inbound and outbound connections.

RECOMMENDED: Netwrix recommends reviewing your current port configuration after every re-installation or upgrade.

If you use...	Do the following...
Windows Firewall	If you are running Windows Firewall on the computer where Auditor Server is going to be installed, the 135, 9004, 9699, 9011, and one dynamic port will be opened automatically for inbound connections during Auditor installation. For outbound rules, create or enable predefined Windows Firewall rules. Before installing Auditor, make sure that the Windows Firewall service is started.
Third-party Firewall	If you use a third-party firewall, you must create rules manually.

Follow the steps to create Firewall rules manually.

The example below applies to Windows Firewall and explains how to create a rule for inbound connection.

Step 1 – Start the Windows Firewall service.

Step 2 – Navigate to **Start** > **Control Panel** and select **Windows Firewall**.

Step 3 – In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.

Step 4 – In the Windows Firewall with Advanced Security dialog, select Inbound Rules on the left.

Step 5 – Click New Rule. In the New Inbound Rule wizard, complete the following steps:

- On the Rule Type step, select Port.

- On the Protocol and Ports step, select TCP or UDP. In the Specific local ports field specify the port number.
- On the Action step, select the Allow the connection action.
- On the Profile step, make sure that the rule applies to all profiles (Domain, Private, Public).
- On the Name step, specify the rule's name, for example Netwrix Auditor TCP port_number Access.

In most cases, this configuration is enough to ensure successful data collection and processing. If your organization policy requires you to provide a justification for each particular port, review the following for a full list of ports to be opened on the computer where Auditor Server is going to be installed and on your target servers.

- Active Directory Ports
- AD FS Ports
- Microsoft Entra ID Ports
- Dell Data Storage Ports
- Exchange Ports
- Exchange Online Ports
- Group Policy Ports
- Integration API Ports
- Logon Activity Ports
- Nutanix Ports
- Oracle Database Ports
- Qumulo Ports
- SharePoint Ports
- SharePoint Online Ports
- SQL Server Ports
- Synology Ports
- Teams Ports
- User Activity Ports
- VMware Ports

- Windows File Server Ports
- Windows Server Ports

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	Netwrix Auditor Server	Netwrix Auditor internal components interaction.

Port	Protocol	Source	Target	Purpose
		Auditor client are installed		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
• **80 for http** • **443 for https**	TCP	SSRS	Netwrix Auditor Server	Reports **NOTE:** If your environment is configured differently, we recommend that you check with your DBA or the SSRS settings through the Configuration Manage.

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.

Configure Netwrix Auditor Service Accounts

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 Data Collecting Account for additional information.
Audit Database service account	An account used by Netwrix Auditor to write collected audit data to the Audit Database. See Requirements for SQL Server to Store Audit Data for additional information.
SSRS service account	An account used by Netwrix Auditor to upload data to the Report Server. See SQL Server Reporting Services for additional 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 File-Based Repository for Long-Term Archive for additional information.

Use Group Managed Service Account (gMSA)

Auditor supports using Group Managed Service Accounts (gMSA) for data collection and storage. This can help you to simplify product administration, providing the following benefits:

- There is no password to manage for this account: Windows handles the password management for it. User interaction for password update on a regular basis is not required.
- Using the gMSA also eliminates a need in service accounts with static passwords that are set upon creation and then never cycled.
- The gMSA also helps to ensure that service account is only used to run a service (gMSA accounts cannot be used to log on interactively to domain computers).

- The gMSA is allowed to audit trusted domains using configured and validated gMSA from the target domain.

Currently, gMSA is supported:

- As a data collecting account for the following data sources: Active Directory (also for Group Policy and Logon Activity), Windows Server, File Server (currently for Windows File Servers), SQL Server, SharePoint. See the Data Collecting Account topic for additional information.

  NOTE: If you are using a gMSA account for Active Directory collection consider that the Active Directory Object Restore tool will not work.

- As an account for accessing Long-Term archive. See the File-Based Repository for Long-Term Archive topic for additional information.

- As an account for accessing Audit Databases. See Requirements for SQL Server to Store Audit Data topic for additional information.

  CAUTION: In case of accessing Audit Databases using gMSA account, SSRS-based reports will not work.

RECOMMENDED: Prepare a dedicated gMSA for these purposes.

The gMSA would work only within one domain, the parent domain and NA also should be joined within the same domain. The reason is that gMSAs are designed to be scoped within a single Active Directory domain or subdomain.

See the following Microsoft article for more information: What's New for Managed Service Accounts

By default, the gMSA account is not a member of any domain groups. After creating gMSA account, you need to add this account to one of the domain groups (Domain admins or Doman users groups, depending on your security policies).

Check for a KDS Root Key

To generate password for gMSA accounts, domain controllers require a Key Distribution Services (KDS) root key. This key is created once, so if there are any gMSA accounts in your domain, this means the root key already exists.

Follow the steps to check whether the root key exists in your domain.

Step 1 – Open the **Active Directory Sites and Services** Console and select **View** > **Show Services Node**.

Step 2 – Browse to **Services** > **Group Key Distribution Services** > **Master Root Keys**.

Step 3 – Alternatively, you can run the `Get-KdsRootKey` cmdlet. If the key does not exist, it will not return any output.

Create a KDS Root Key

If the KDS root key does not exist, then you can create a KDS root key as described below, or contact your Active Directory administrator.

Follow the steps to create a KDS key (on a domain controller running Windows Server 2012 or later).

Step 1 – On the domain controller, run **Windows PowerShell**.

Step 2 – In the command prompt of Windows PowerShell Active Directory module, run the following cmdlet:

```
Add-KdsRootKey -EffectiveImmediately
```

Step 3 – A root key will be added to the target DC which will be used by the KDS service immediately.

NOTE: This requires waiting 10 hours, as other domain controllers will be able to use the root key only after a successful replication. See the Create the Key Distribution Services KDS Root Key Microsoft article for additional information.

Step 4 – Alternatively, you can use the following cmdlet:

```
Add-KdsRootKey -EffectiveTime MM/DD/YYYY
```

This cmdlet generates a KDS root key that will take effect on the specified date. Use the *mm/dd/yyyy* format, for example: `Add-KdsRootKey -EffectiveTime 02/27/21`

CAUTION: This approach, however, should be used with care. Waiting up to 10 hours is a safety measure to prevent password generation from occurring before all DCs in the environment are capable of answering gMSA requests. For more information, refer to the following microsoft article: Create the Key Distribution Services KDS Root Key.

To make the KDS Root Key work immediately you can use the following powershell command:

```
Add-KDSRootKey -Effectivetime ((get-date).addhours(-10))
```

This command will make the KDS Root Key work immediately.

NOTE: This is recommended only for small environments. In large environments, it is required to wait 10 hours for replication.

Create a gMSA

To create a new gMSA, you will need to specify:

- New account name and FQDN
- Computer account(s) that will be allowed to make use of that gMSA. Here it will be your Auditor Server
    - The account must be a member of the **Administrators** group on the Auditor Server.

For example, you can create a gMSA using the `New-ADServiceAccount` PowerShell cmdlet. If so, you should specify your Auditor Server account in the `-PrincipalsAllowedToRetrieveManagedPassword` attribute.

Make sure you specify a valid computer object in this attribute.

If you have multiple Auditor servers, you can specify the computer accounts using a comma separated list, or specify a security group and add the required computer accounts to that security group.

To create a new gMSA in the root domain using PowerShell:

- If you are using a single Netwrix Auditor Server, run the command as follows:

  ```
  New-ADServiceAccount -name nagmsa -DNSHostName nagmsa.mydomain.local
  -PrincipalsAllowedToRetrieveManagedPassword NASrv$
  ```

  here:

- *name* — new gMSA name, here **nagmsa**. Make sure the name refers to a valid computer objects.
- *DNSHostName* — FQDN of the new gMSA account, here **nagmsa.mydomain.local**
- *PrincipalsAllowedToRetrieveManagedPassword* — your Netwrix Auditor Server NETBIOS name ended with $, here **NASrv$**

- If you want to specify a security group that comprises multiple Auditor servers, run the command as follows:

```
New-ADServiceAccount -Name gmsagroup -DNSHostName
gmsagroup.mydomain.local -PrincipalsAllowedToRetrieveManagedPassword
NAServers
```

here **NAServers** — a security group with your Auditor servers.

Assign Required Roles and Permissions to a gMSA

Once a new gMSA account has been prepared, assign the required roles and permissions to this account, depending on what purpose a gMSA account will be used for.

- If you are going to use a gMSA as a data collecting account in Auditor, add this account to the Local Admins group on the Auditor Server and assign the following rights and permissions, depending on the data source you want to collect data from:
  - Permissions for Active Directory Auditing
  - Permissions for Group Policy Auditing
  - Permissions for Logon Activity Auditing
  - Permissions for Windows File Server Auditing
  - Permissions for SharePoint Auditing
  - Permissions for SQL Server Auditing
  - Permissions for Windows Server Auditing

    Remember, Permissions for Windows Server Auditing

- If you are going to use a gMSA to access Long-Term archive, assign the roles and permissions required for a custom account:

    - File-Based Repository for Long-Term Archive

      Remember, that you can use custom (gMSA) account only if your Long-Term archive stored on a file share.

- If you are going to use a gMSA to access Audit Database, assign the required roles:
    - Requirements for SQL Server to Store Audit Data

      Remember, that a gMSA account cannot access SSRS due to Microsoft restrictions.

Now you can use a gMSA account as one of the Auditor Service Account.

Apply a gMSA

This topic contains instructions on how to apply a gMSA as one of the Auditor Service Accounts.

- Apply a gMSA as a Data Collecting Account
- Apply gMSA to Access Long-Term Archive
- Apply gMSA to Access Audit Database

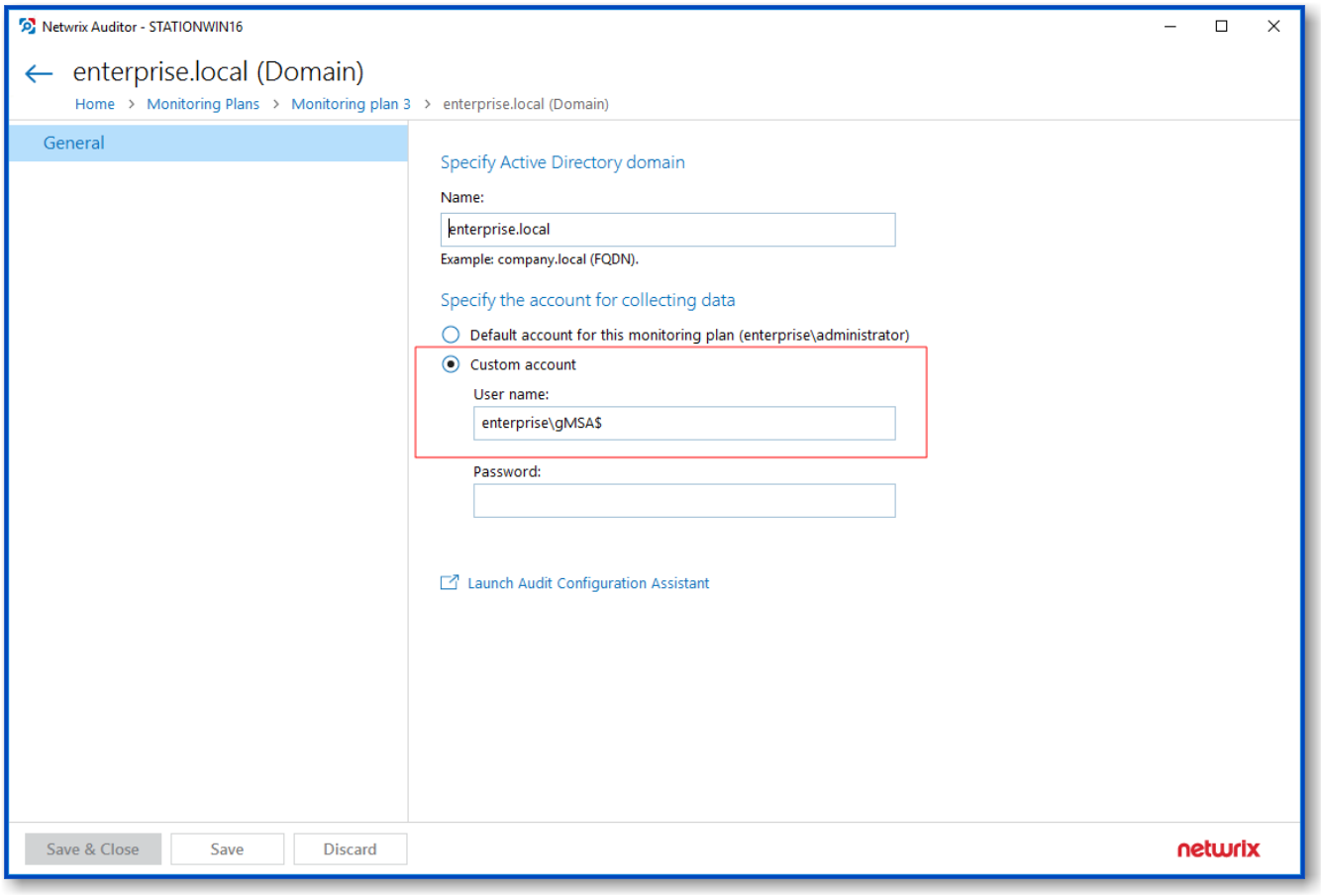
Apply a gMSA as a Data Collecting Account

To process the corresponding monitored items using gMSA, you can specify this account in the monitored plan properties. See the Create a New Monitoring Plan topic for additional information.

Follow the steps to set a custom account in the monitored item properties.

Step 1 – Open the monitored item properties for editing.

Step 2 – On the **General** tab, under **Specify account for collecting data**, select **Custom account**.



See the Add Items for Monitoring topic for additional information.

Apply gMSA to Access Long-Term Archive

To write data to the Long-Term Archive and upload report subscriptions to shared folders, you can specify this account as a custom account in the Long-Term Archive settings. See the Long-Term Archive topic for additional information.

NOTE: For a custom account or a gMSA one, consider that you can use the account for the Long-Term Archive based on a file share

Apply gMSA to Access Audit Database

To access Audit Database, generate reports and run interactive search queries, you can specify this account under the 'Specify custom connection parameters' in your monitoring plan settings. See the Fine-Tune Your Plan and Edit Settings topic for additional information.

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 are going to set up integration with Netwrix Data Classification, consider planning for 3 dedicated servers:

- Netwrix Auditor server
- Netwrix Data Classification server
- SQL server with 2 instances: for Netwrix Auditor databases and for NDC SQL Database

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

To learn more, see the How It Works and Deployment Planning topics in the Netwrix Data Classification Knowlege center: Netwrix Data Classification Documentation..

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

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

Hardware component	Requirement
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 the SQL Server Reporting Services topic for additional 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.

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.

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	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.

   Client-server connection requires user sign-in. You can automate this process, as described in Automate Sign-in to the Client of Online Help.

3. When prompted to configure the Audit database settings, proceed with installing SQL Server Express Edition with Advanced Services. See the SQL Server Reporting Services topic for additional 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.

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	8 cores
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 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.

   Client-server connection requires user sign-in. You can automate this process, as described in the Automate Sign-in to the Client section of Online Help.

3. Prepare Microsoft SQL Server meeting the following requirements:

Hardware component	Requirement
Processor	2-4 cores
RAM	16-32 GB

Hardware component	Requirement
Disk space	• 100 GB on system drive • 200-400 GB on data drive

Software component	Requirement
Microsoft SQL Server 2012 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.

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 Auditor Server, meeting the following requirements:

Hardware component	Requirement
Processor	16 cores (recommended)
RAM	32 - 64 GB
Disk space	• 300-500 GB on system drive • 1+ TB on data drive

Hardware component	Requirement
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.

   Client-server connection requires user sign-in. You can automate this process, as described in the Automate Sign-in to the 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 2012 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
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.

Data Source Configuration

With the Netwrix Auditor, the following Data Sources can be monitored:

- Active Directory
- AD FS
- Exchange
- File Servers
    - Dell Data Storage
    - Dell Isilon/PowerScale
    - NetApp Data ONTAP
    - Nutanix
    - Qumulo
    - Synology
    - Windows File Servers
- Group Policy
- Logon Activity
- Microsoft 365
    - Exchange Online
    - Microsoft Entra ID
    - SharePoint Online
    - MS Teams
- Network Devices
- Oracle Database
- SharePoint

- SQL Server
- User Activity
- VMware
- Windows Server

Active Directory

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - Configure the domain for auditing. See the Audit Configuration Assistant topic for information on configuring the domain.
    - On the Auditor console computer:
        - If you have enabled automatic log backup for the Security log of your domain controller, you can instruct Auditor to clear the old backups automatically. For that, use the **CleanAutoBackupLogs** registry key, as described in the Active Directory Registry Key Configuration topic.

          RECOMMENDED: Adjust retention period for the backup files accordingly (default is **50** hours). See the Adjust Security Event Log Size and Retention topic.

- To provide for event data collection, the Secondary Logon service must be up and running . Open **Administrative Tools** > **Services**, right-click the **Secondary Logon** service and on the **General** tab make sure that Startup type for this service is other than *Disabled*.

Monitored Objects

Netwrix Auditor tracks changes made to all object classes and attributes in the Active Directory Domain, Configuration and Schema partitions. It also tracks changes to new object classes and attributes added due to the Active Directory Schema extension. For detailed information, refer to Microsoft articles:

- A full list of Active Directory object classes
- A full list of Active Directory object attributes

Review the following limitations:

- Netwrix Auditor does not track changes to non-replicated attributes, such as badPwdCount, Last-Logon, Last-Logoff, etc. The non-replicated attributes pertain to a particular domain controller and are not replicated to other domain controllers.
- Changes made through the Exchange Management Console in the Organization Configuration node (Federation Trust, Organization Relationships and Hybrid Configuration tabs) are displayed in an internal Active Directory format that can be difficult to interpret.
- Netwrix Auditor tracks changes to membership in all groups inside the monitored domain (Domain local groups) and Universal and Global groups of domains in the same forest. Changes to Domain local groups of a different domain in the same forest are not reported.

State-in-time data collection is supported for Active Directory.

For AD domain monitoring with Netwrix Auditor, the domain should be configured as explained below.

Domain Audit Policy Settings

Effective domain controllers policy settings must be configured as listed in the table below.

Policy	Audit type
Audit account management	*"Success"*
Audit directory service access	*"Success"*
Audit logon events	*"Success"*

You can configure either **Basic domain audit policies**, or **Advanced domain audit policies**.

- To configure these settings automatically using Netwrix Auditor, refer to the Active Directory: Automatic Configuration topic.
- To configure them manually, refer to the Configure Basic Domain Audit Policies or Configure Advanced Audit Policies topics.

Audit Settings for AD Partitions

Required object-level audit settings for the Active Directory partition must be configured as described in the next sections.

Domain Partition

Object-level audit settings for the Domain partition must be configured to audit for *Success* of all access operations except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.

These settings must be configured for **Everyone** security principal and applied to **This object and all descendant objects**.

- You can configure these settings automatically using Netwrix Auditor, as described in the Active Directory: Automatic Configuration topic.
- To configure them manually, refer o the Configure Object-Level Auditing topic.

Configuration and Schema Partitions

Object-level audit settings for the Configuration and **Schema** partitions must be configured to audit for *Success* of all access operations except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*

These settings must be configured for **Everyone** security principal and applied to **This object and its descendant objects**.

- You can configure these settings automatically using Netwrix Auditor, as described in the Active Directory: Automatic Configuration topic.
- To configure them manually, refer to the Configure Object-Level Auditing topic.

Security Event Log Settings

Security event log settings for the domain controllers should be configured as follows:

Setting	Value
Max event log size	4 GB
Retention method	*Overwrite events as needed*
Auto-archiving	Enabled

- You can configure these settings automatically using Netwrix Auditor, as described in the Active Directory: Automatic Configuration topic.
- To configure them manually, refer to the Adjust Security Event Log Size and Retention topic.

Exchange Settings

If you have an on-premises Exchange server 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 the Exchange Administrator Audit Logging Settings topic.

- Make sure that the account used for data collection has the following:

    - Membership in the Organization Management or Records Management group

-OR-

- The Audit Logs management role.

Next Steps

- Configure Data Collecting Account, as described in the Additional Configuration to Review Changes Made via Exchange Server topic.
- Configure required protocols and ports, as described in the Active Directory Ports topic.
- If you plan to restore deleted Active Directory objects and their attributes using the Netwrix Auditor Object Restore for Active Directory tool (shipped with Netwrix Auditor,) it is recommended to set the **Active Directory tombstone lifetime** property to 730 days (default is 180 days). See the Adjust Active Directory Tombstone Lifetime (optional) topic for additional information.

Active Directory Ports

Review a full list of protocols and ports required for monitoring Active Directory.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to the local 389 TCP port.

Port	Protocol	Source	Target	Purpose
389	TCP\UDP	Netwrix Auditor Server	Domain controllers	LDAP Common queries

Port	Protocol	Source	Target	Purpose
3268	TCP	Netwrix Auditor Server	Domain controllers	LDAP Group membership GC search
3269	TCP	Netwrix Auditor Server	Domain controllers	Global catalog LDAP over SSL
88	TCP/UDP	Netwrix Auditor Server	Domain controllers	Kerberos authentication
135 **and dynamic range:** **1024 -65535**	TCP	Netwrix Auditor Server	Domain controllers	Windows Management Instrumentation. `gpupdate /force`
445	TCP	Netwrix Auditor Server	Domain controllers	SMB 2.0/3.0 Authenticated communication between Netwrix Auditor Server and domain controllers.
53	UDP	Netwrix Auditor Server	DNS Server	DNS Client

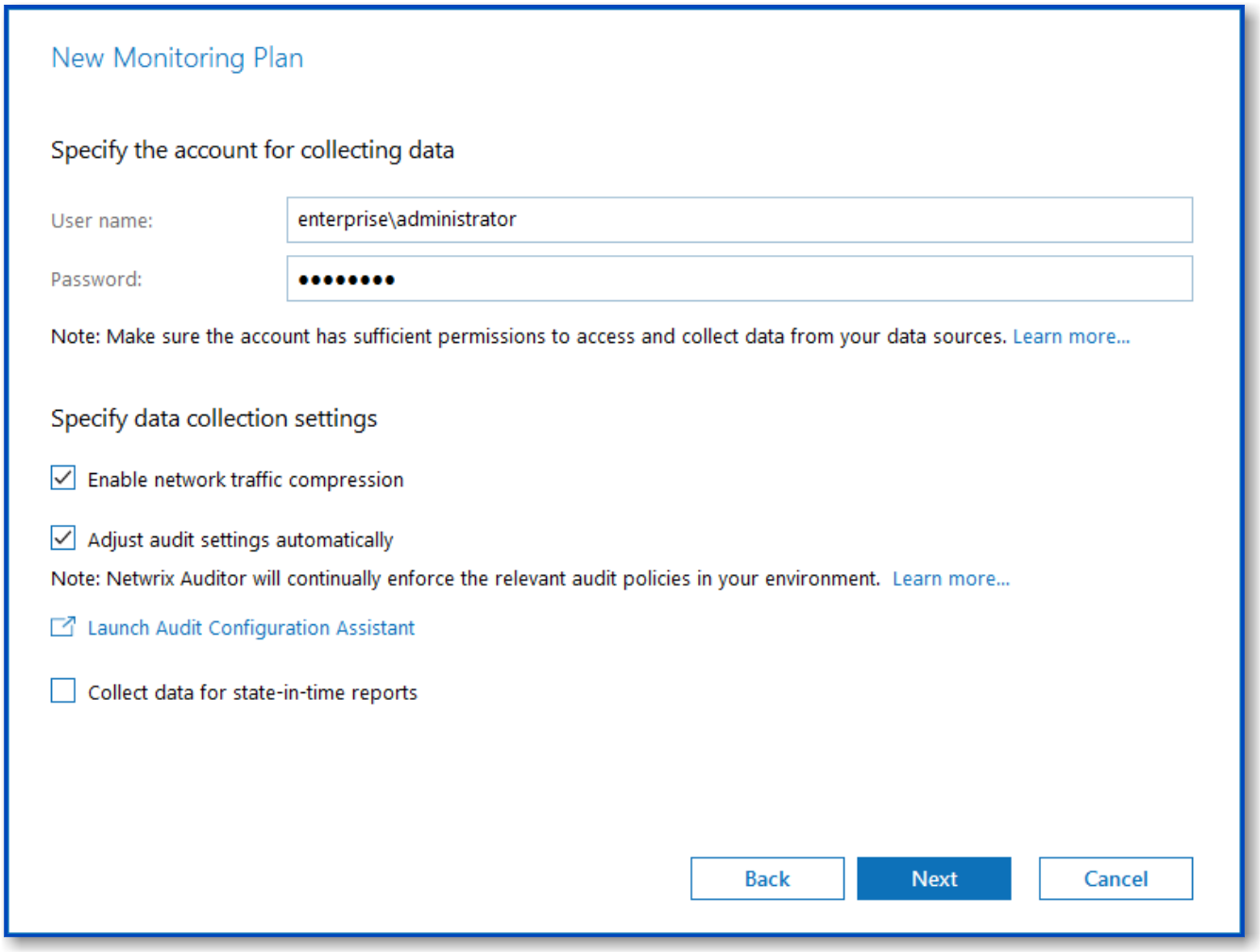
* - for Exchange 2010 only

Active Directory: Automatic Configuration

This is a recommended method of applying Active Directory audit settings required by Auditor to monitor your AD domain. With this approach, the program will check your current audit settings at each data collection session and adjust them if necessary.

To adjust audit settings automatically, do any of the following:

- When creating a new monitoring plan, at the first step of the wizard select the **Adjust audit settings automatically** option. See the Create a New Monitoring Plan topic for additional information.



- For the existing monitoring plan, modify data collection settings for Active Directory data source, selecting **Adjust audit settings automatically** option. See the Manage Data Sources and Active Directory topics for additional information.
- For both new and existing monitoring plans, you can click **Launch Audit Configuration Assistant** (in the wizard step or in the plan settings, respectively) to launch a special tool

that can detect current infrastructure settings and adjust them as needed for monitoring. See the Audit Configuration Assistant topic for additional information.

If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. For a full list of audit settings required for Netwrix Auditor to collect comprehensive audit data and instructions on how to configure them, refer to the Active Directory topic.

See also:

- Active Directory
- Audit Configuration Assistant
- Active Directory: Manual Configuration

Active Directory: Manual Configuration

To configure your domain for monitoring manually, you will need:

- Group Policy Management Console — Required if you plan to perform configuration steps from a domain controller

  -OR-

- ADSI Edit — Required if you plan to perform configuration steps from a server other than domain controller

NOTE: If these tools are not installed, refer to the following Microsoft articles:

- Group Policy Management Console
- ADSI Edit

Follow the steps to configure your domain for monitoring.

Step 1 – Configure effective domain controllers policy (by default, Default Domain Controllers Policy). See the Configure Basic Domain Audit Policies or Configure Advanced Audit Policies topics for additional information.

Step 2 – Configure object-level auditing. See the Configure Object-Level Auditing topic for additional information.

Step 3 – Adjust the security event log size and retention settings. See the Adjust Security Event Log Size and Retentiontopic for additional information.

Step 4 – If you have an on-premises Exchange server in your Active Directory domain, consider that some changes to AD can be made via that Exchange server. To be able to audit and report

who made those changes, perform configuration steps as described in the Exchange Administrator Audit Logging Settings topic.

Optionally, you can adjust the Active Directory Tombstone Lifetime. See the Adjust Active Directory Tombstone Lifetime (optional) topic for additional information.

Also, remember to perform the following steps for AD auditing:

Step 1 – Configure Data Collecting Account, as described in the Additional Configuration to Review Changes Made via Exchange Server topic.

Step 2 – Configure required protocols and ports, as described in the Active Directory Ports topic.

Step 3 – Enable Secondary Logon Service on the computer where Netwrix Auditor Server resides.

Enable Secondary Logon Service

Follow the steps to Enable Secondary Logon Service.

Step 1 – On the computer where Auditor Server resides, navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Services**.

Step 2 – In the **Services** dialog, locate the **Secondary Logon** service.

Step 3 – Right-click the service and on the **General** tab make sure that **Startup type** for this service is other than *Disabled*. The startup type can be either *Automatic* or *Manual*.

Additional Configuration to Review Changes Made via Exchange Server

If you have an on-premises Exchange server in your Active Directory domain, consider that some changes can be made through this Exchange server. To be able to audit and report who made those changes, make sure that the account used for data collection meets one of the following requirements:

- Membership in the Organization Management or Records Management group

OR

- The Audit Logs management role (see the Assign Management Roles topic for additional information)

You will also need to configure Exchange Administrator Audit Logging (AAL) settings. See the Exchange Administrator Audit Logging Settings topic for additional information.

Additional Configuration for Domain Controller's Event Logs Auto-backup

The following is required if auto-backup is *enabled* for the domain controller event logs:

- Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See the Assign Permission to Read the Registry Key topic for additional information.
- Membership in one of the following groups: Administrators, Print Operators, or Server Operators
- Read/Write share permission and Full control security permission on the logs backup folder.

Considerations for gMSA Account

If you are using gMSA for data collection, consider that AAL event data collection from your on-premise Exchange server will not be possible.

Thus, changes made to your Active Directory domain via that Exchange server will be reported with *domain\Exchange_server_name$* instead of the initiator (user) name in the "*Who*" field of reports, search results and activity summaries.

Configure Manage Auditing and Security Log Policy

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

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

Step 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.

Step 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.**

Step 4 – On the right, double-click the **User Rights Assignment** policy.

Step 5 – Locate the **Manage auditing and security log** policy and double-click it.

Step 6 – In the Manage auditing and security log Properties**anage auditing and security log Properties** dialog, click **Add User or Group**, specify the user that you want to define this policy for.

Step 7 – Run the following command to update group policy: `gpupdate /force`

Step 8 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 9 – Ensure that new GPO settings applied on any audited domain controller.

Grant Permissions for Deleted Objects Container

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

Step 1 – Log on to any domain controller in the target domain with a user account that is a member of the **Domain Admins** group.

Step 2 – Navigate to **Start > Run** and type **cmd**.

Step 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`

Step 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.

Define Log On As a Batch Job Policy

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

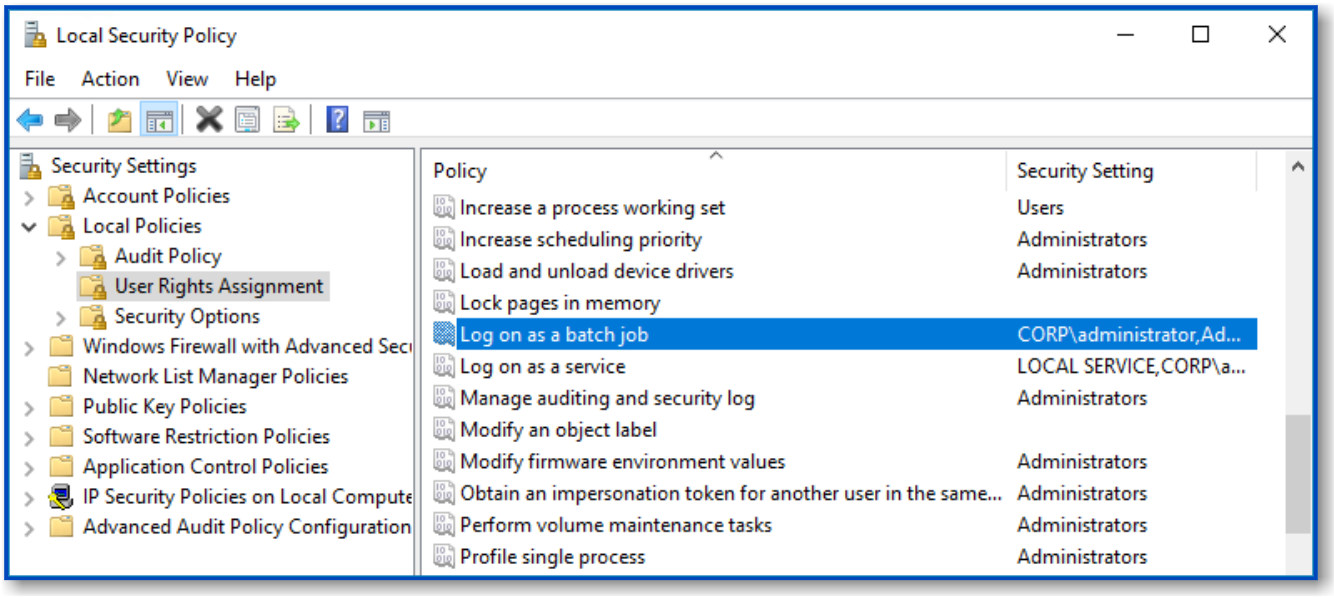
You can configure this policy via the Local Security Policy snap-in or using the Group Policy Management console.

Configure the Log On As a Batch Job policy via Local Security Policy Snap-in

Follow the steps to configure the Log On As a Batch Job policy via Local Security Policy snap-in.

Step 1 – On any domain controller in the target domain, open the Local Security Policy snap-in: navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** and select Local Security Policy.

Step 2 – In the Local Security Policy snap-in, navigate to **Security Settings** > **Local Policies > User Rights Assignment** and locate the **Log on as a batch job** policy.



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

Configure the Log On As a Batch Job Policy Using the Group Policy Management Console

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

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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.

Step 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.

Step 4 – On the right, double-click the User Rights Assignment policy.

Step 5 – Locate the Log on as a batch job policy and double-click it.

Step 6 – In the Log on as a batch job Properties dialog, click Add User or Group and specify the user that you want to define this policy for.

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

Step 8 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 9 – Ensure that new GPO settings applied on any audited domain controller.

Assign Permission to Read the Registry Key

This permission is required 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, it is recommended to assign permissions through Group Policy, or automatically using Audit Configuration Assistant.

To assign permissions manually, use the Registry Editor snap-in or the Group Policy Management console.

Assign Permission Via the Registry Editor Snap-in

Follow the steps to assign permission via the Registry Editor snap-in:

Step 1 – On your target server, open Registry Editor: navigate to **Start > Run** and type *"regedit"*.

Step 2 – In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\EventLog\Security*.

Step 3 – Right-click the **Security** node and select **Permissions** from the pop-up menu.

Step 4 – Click **Add** and enter the name of the user that you want to grant permissions to.

Step 5 – Check **Allow** next to the **Read** permission.

Step 6 – For auditing Logon Activity, you also need to assign the Read permission to the *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv* registry key.

To assign permission using the Group Policy Management console

Assign Permission Using the Group Policy Management Console

Follow the steps to assign permission using the Group Policy Management console:

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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 .

Step 3 – In the Group Policy Management Editor dialog, expand the Computer Configuration node on the left and navigate to Policies > Windows Settings > Security Settings > Registry.

Step 4 – Right-click in the pane and select Add Key.

Step 5 – Navigate to `HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv` and click OK.

Step 6 – Click Add and enter the name of the user that you want to grant permissions to and press Enter.

Step 7 – Check Allow next to the *"Read"* permission and click OK

Step 8 – In the pop-up window, select Propagate inheritable permissions to all subkeys and click OK.

Step 9 – Repeat the steps 4-8 for keys below:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`;
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\EventLog\Security`.

Step 10 – Close the Group Policy Management console.

Step 11 – Navigate to Start > Run and type **cmd**. Input the `gpupdate /force` command and press Enter. The group policy will be updated.

Step 12 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 13 – Ensure that new GPO settings were applied to the domain controllers.

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 the Configure Advanced Audit Policiestopic for additional information.

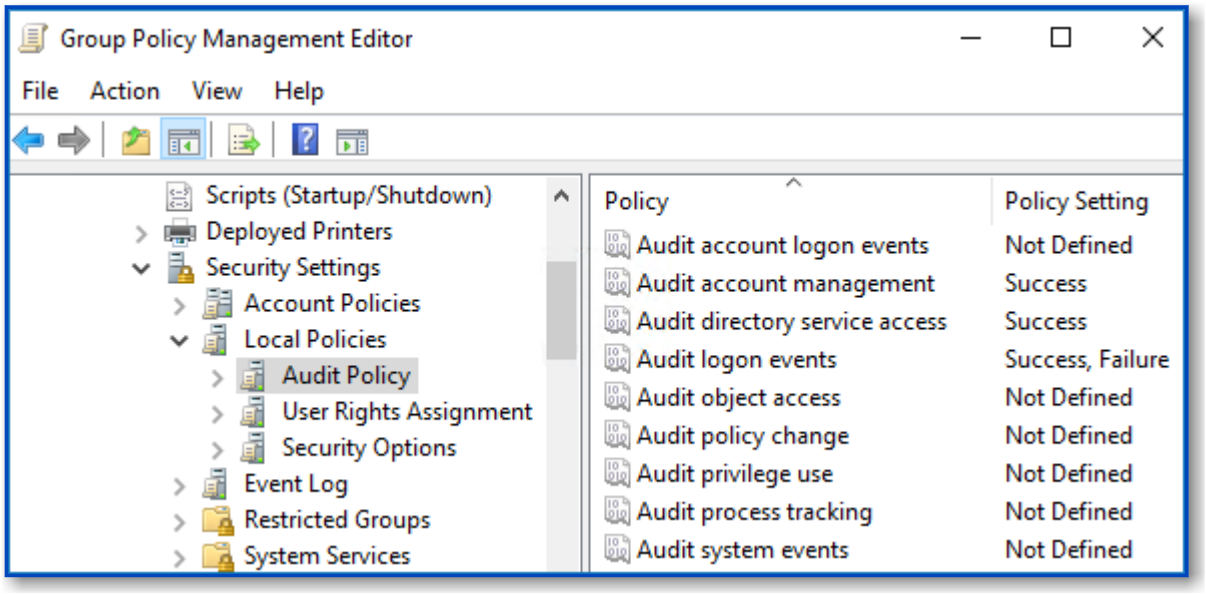
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016 and higher) or Administrative Tools (Windows 2012) **Group Policy Management.**

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"*



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.

5. Run the following command to update group policy: `gpupdate /force`

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

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.

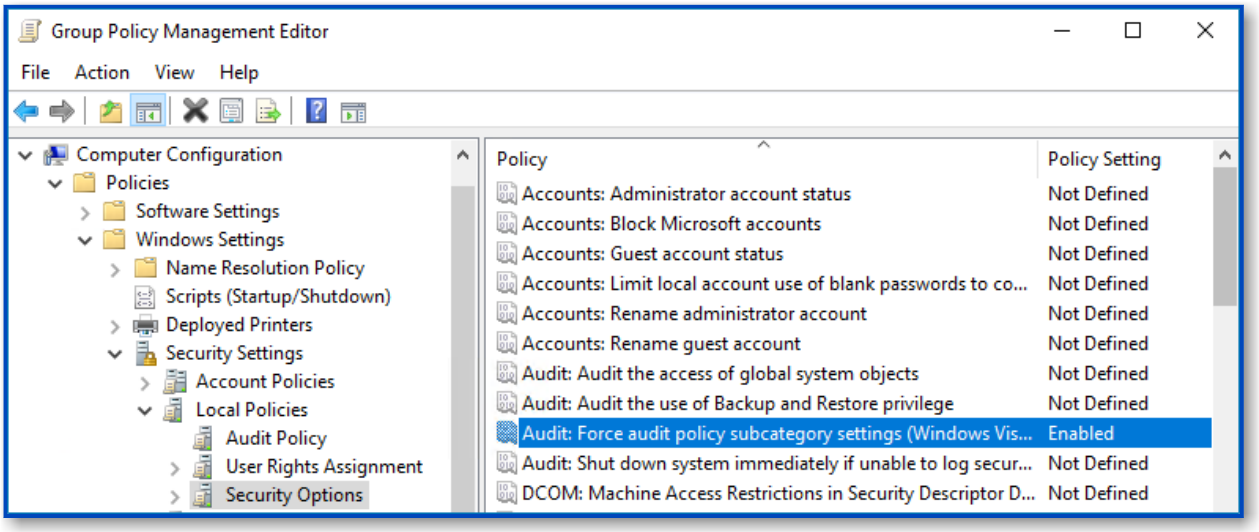
To do it, perform the following steps:

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016 and higher) or Administrative Tools (Windows 2012) **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. Run the following command to update group policy: `gpupdate /force`

To configure advanced audit policies

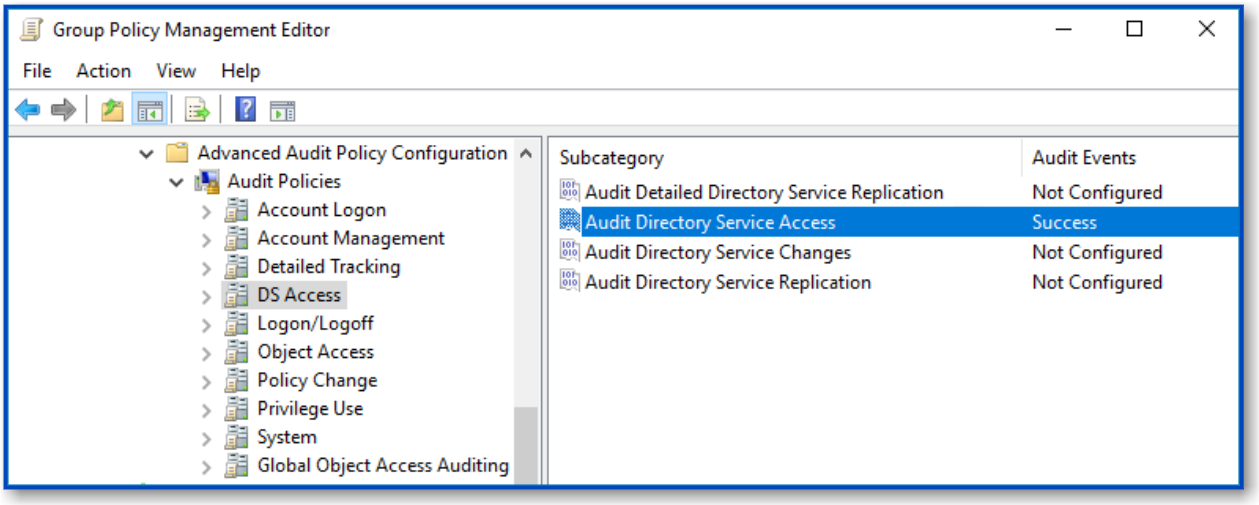
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016 and higher) or Administrative Tools (Windows 2012) **Group Policy Management.**

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 These policies are only required to collect the information on the originating workstation, i.e., the computer from which a change was made.	*"Success"*



5. Run the following command to update group policy: `gpupdate /force`

Configure Object-Level Auditing

Object-level auditing must be configured for the **Domain** partition if you want to collect information on user activity in the domain. If you also want to audit changes to AD configuration and schema, you must enable object-level auditing for **Configuration** and **Schema** partitions.

Auditing of the Configuration partition is enabled by default. See the Active Directory topic for detailed instructions on how to enable monitoring of changes to the Schema partition in the target AD domain.

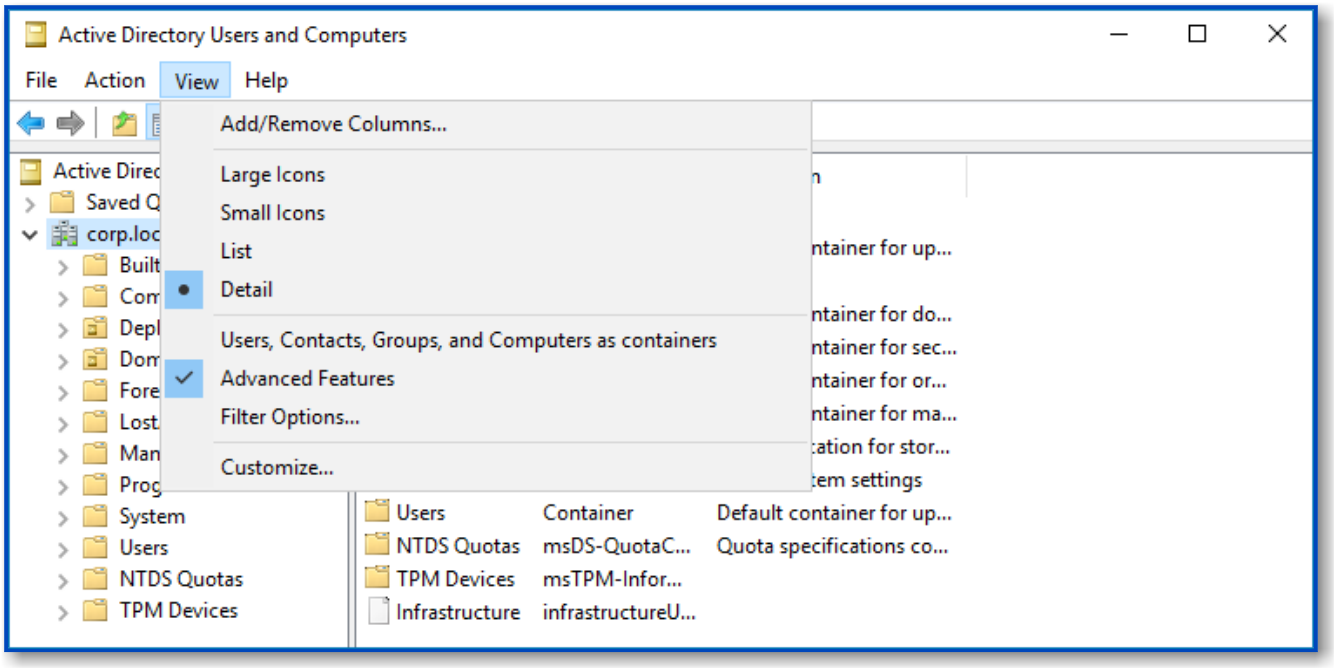
Perform the following procedures to configure object-level auditing for the Domain, Configuration and Schema partitions:

- Configuring object-level auditing for the Domain partition
- Enabling object-level auditing for the Configuration and Schema partitions

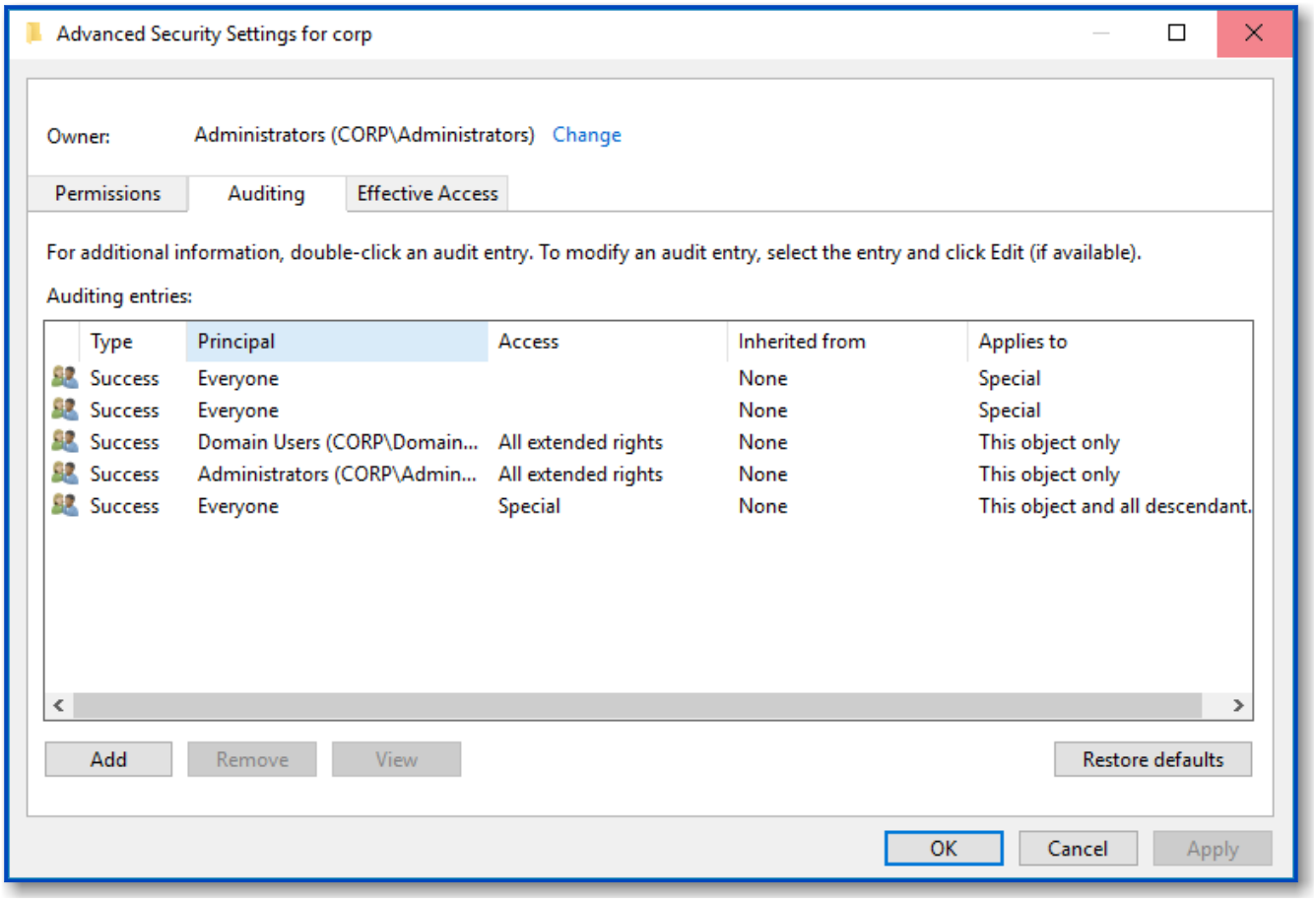
Configuring object-level auditing for the Domain partition

Step 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 and higher) or** Administrative Tools **(Windows 2012)** → **Active Directory Users and Computers**.

Step 2 – In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** are enabled.

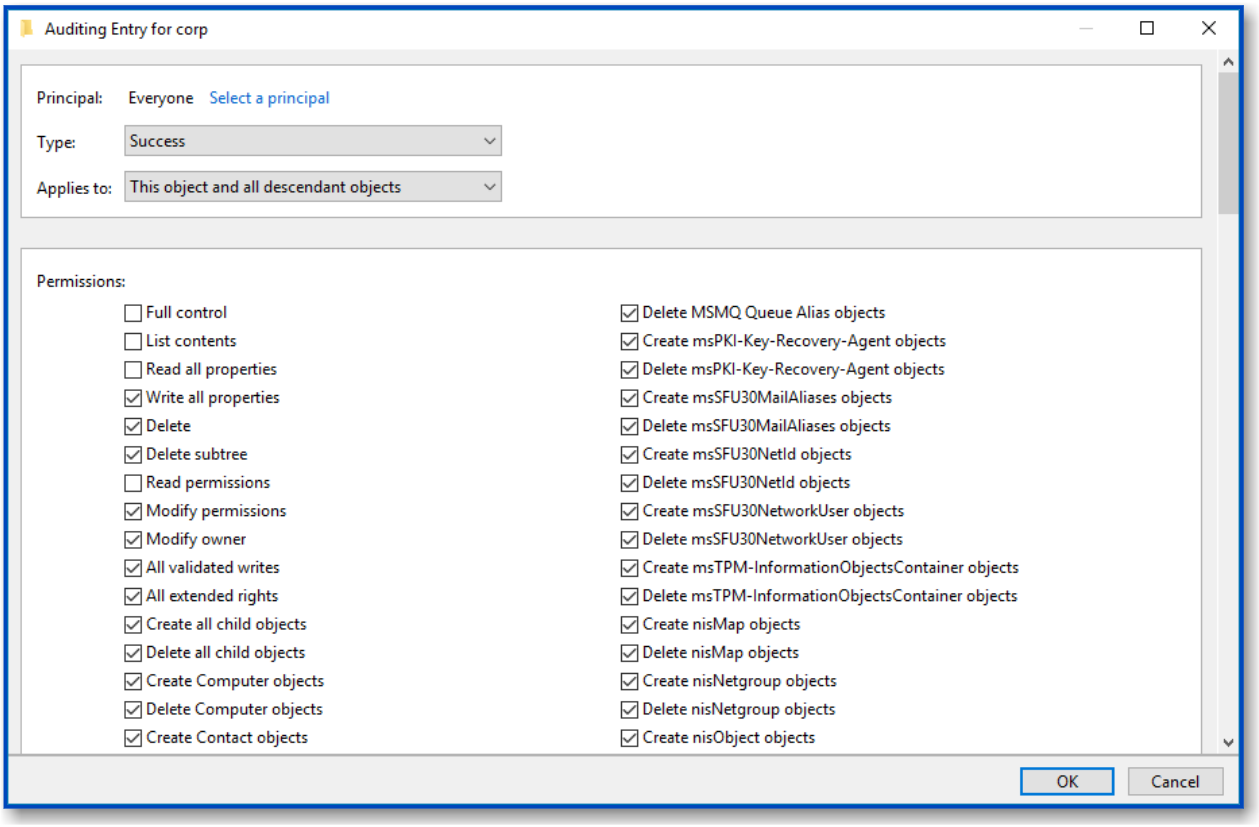


Step 3 – Right-click the **<domain_name>** node and select **Properties.** Select the **Security** tab and click **Advanced**. In the **Advanced Security Settings for <domain_name>** dialog, select the **Auditing** tab.



Step 4 – Perform the following actions on the Windows Server 2012 and above:

1. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.
2. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.
3. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.
4. Under **Permissions**, select all checkboxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.
5. 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.

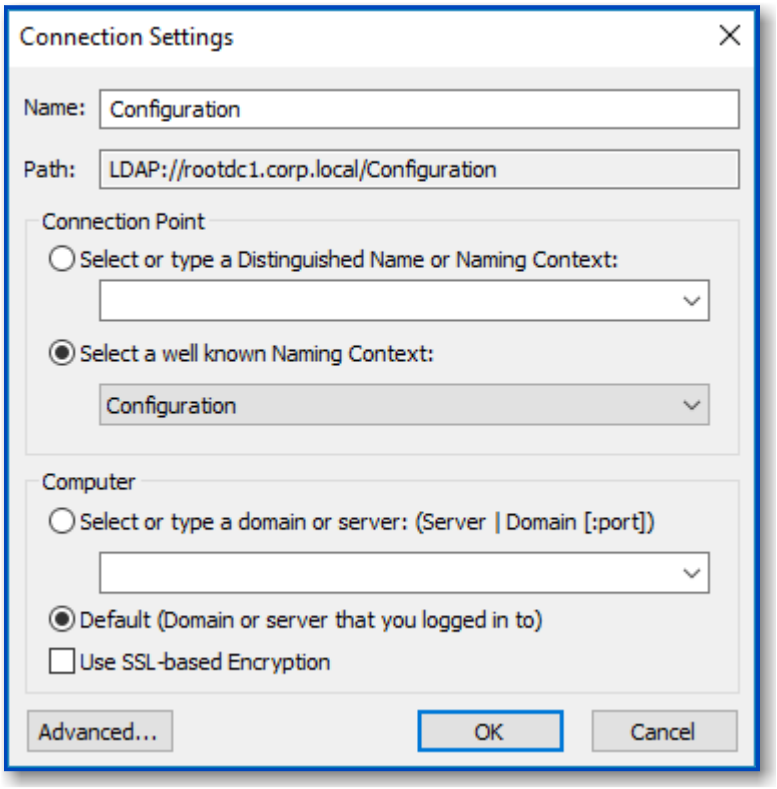


Enabling object-level auditing for the Configuration and Schema partitions

To perform this procedure, you will need the ADSI Edit utility.utility. Follow the steps to enable object-level auditing for the Configuration and Schema partitions.

Step 1 – On any domain controller in the target domain, navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012) > ADSI Edit**.

Step 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.

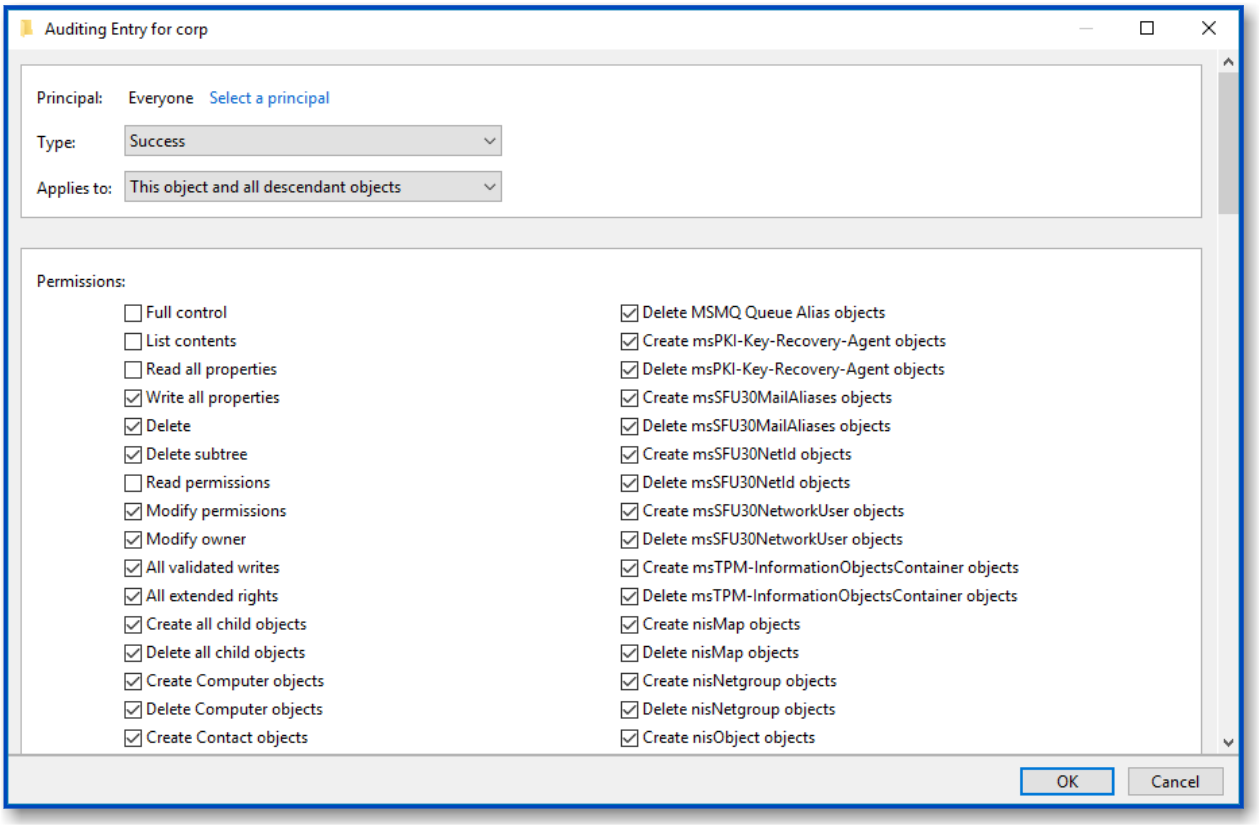


Step 3 – Expand the **Configuration <Your_Root_Domain_Name>** node. Right-click the **CN=Configuration, DC=<name>,DC=<name>...** node and select **Properties.**

Step 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.

Step 5 – Perform the following actions on the Windows Server 2012 and above:

1. Click **Add**. In the **Auditing Entry** dialog, click the **Select a principal** link.
2. In the **Select user, Computer, Service account, or Group** dialog, type *"Everyone"* in the **Enter the object name to select** field.
3. Set **Type** to *"Success"* and **Applies to** to *"This object and all descendant objects"*.
4. Under **Permissions**, select all checkboxes except the following: *Full Control*, *List Contents*, *Read All Properties* and *Read Permissions*.
5. 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.



Repeat these steps for the Schema container if necessary.

Adjust Security Event Log Size and Retention

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.

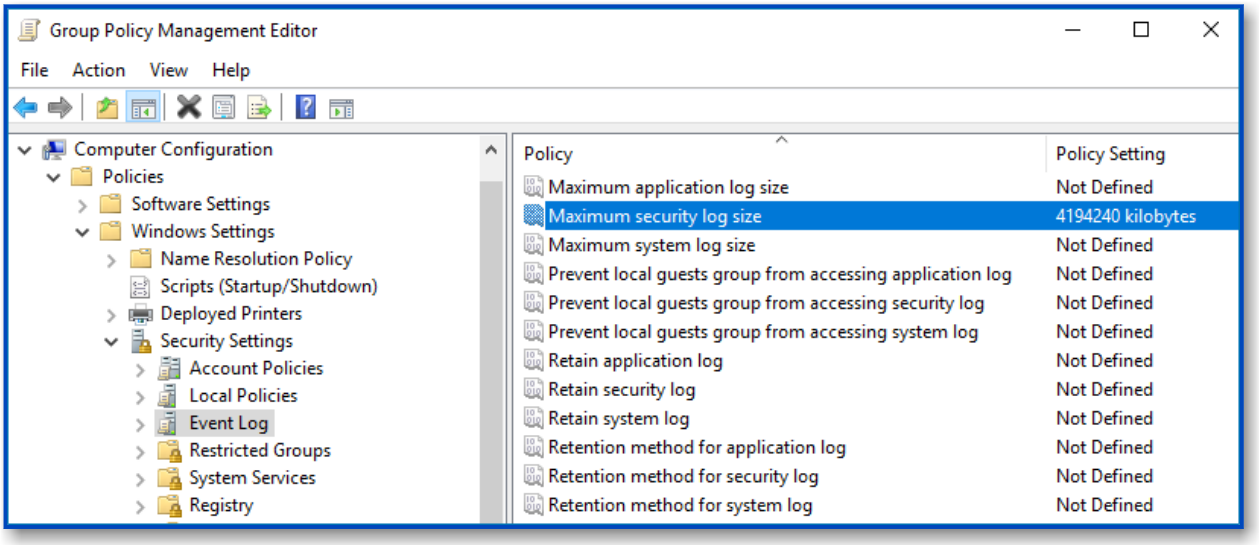
To read about event log settings recommended by Microsoft, refer to the following article: Event Log.

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 and higher) or Administrative Tools (Windows 2012) **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. Run the following command to update group policy: `gpupdate /force`

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. With that option enabled, you may want to adjust the retention settings for log archives (backups). Related procedures are described in the Auto-archiving Windows Security log Netwrix Knowledge Base article.

Adjust Active Directory Tombstone Lifetime (optional)

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.

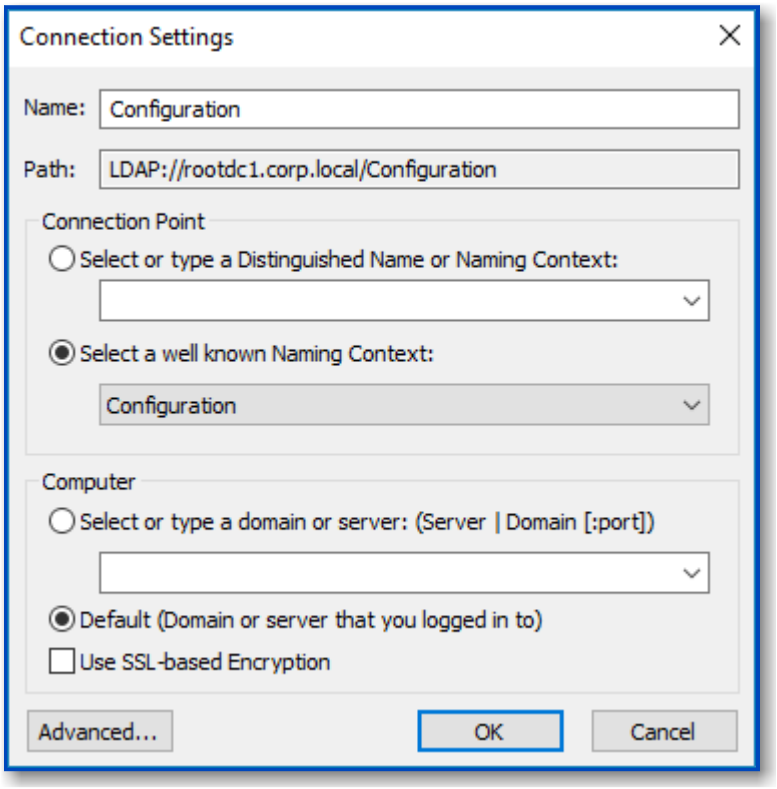
Take into consideration that increasing tombstone lifetime may affect Active Directory performance and operability.

To perform this procedure, you will need the ADSI Edit utility.utility.

Follow the steps to change the tombstone lifetime attribute.

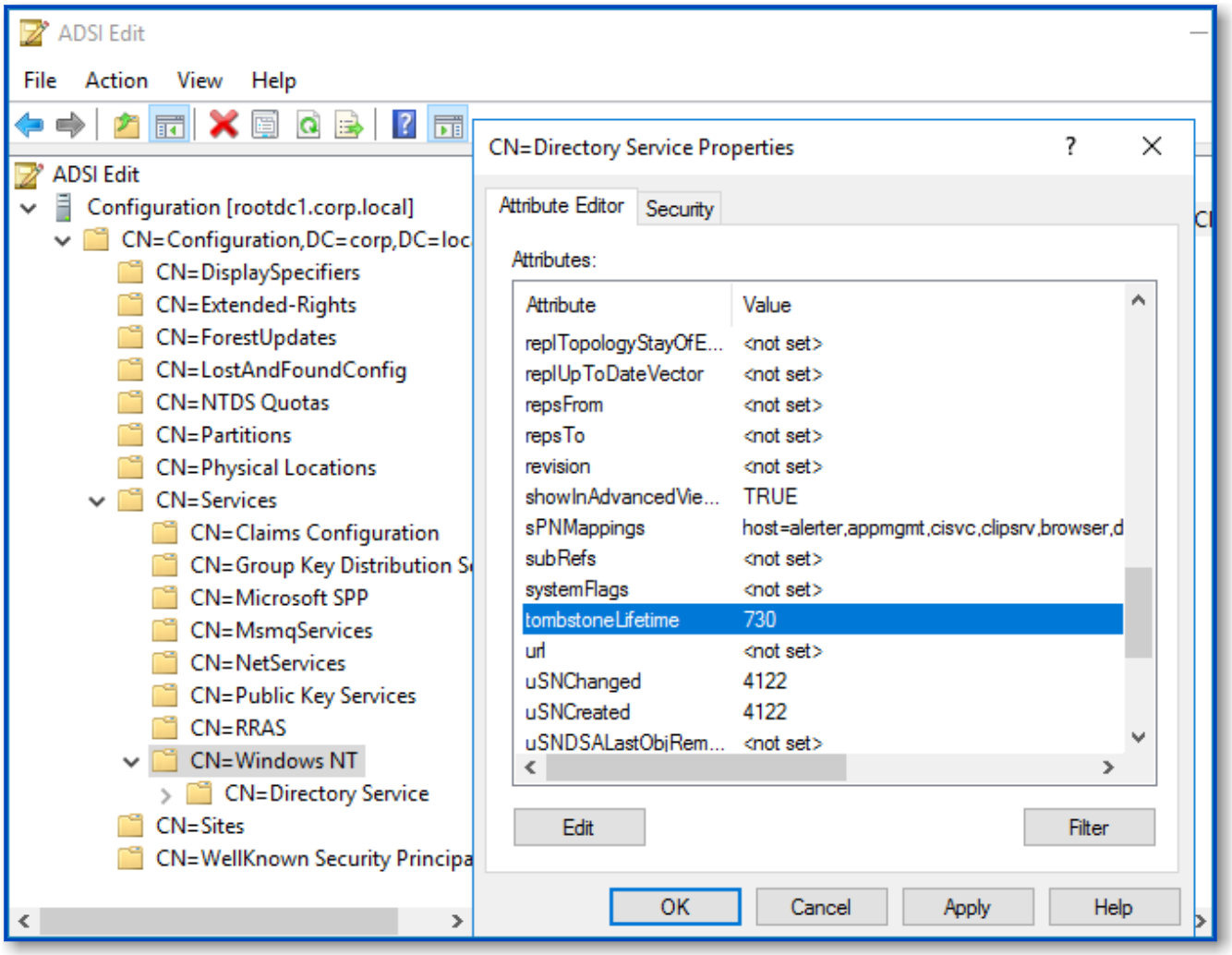
Step 1 – On any domain controller in the target domain, navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012) > ADSI Edit**.

Step 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.



Step 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.

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



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

Active Directory Registry Key Configuration

Review the basic registry keys that you may need to configure for monitoring Active Directory with Netwrix Auditor. On the computer whereNetwrix Auditor Server is installed, navigate to **Start** > **Run** and type **regedit**.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	

Registry key (REG_DWORD type)	Description / Value
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
IgnoreRootDCErrors	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
MonitorModifiedAndRevertedBack	Defines whether the Activity Summary must display the attributes whose values were modified and then restored between data collections: • 0—These attributes are not displayed • 1—These attributes are displayed as "modified and reverted back"
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes

Registry key (REG_DWORD type)	Description / Value
	Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the CleanAutoBackupLogs key.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter\<monitoring plan name>	
CollectLogsMaxThreads	Defines the number of Domain Controllers to simultaneously start log collection on.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Management Console\Database settings	
SqlOperationTimeout	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).
timeout	Defines the Audit Database connection timeout (in seconds).

Permissions 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 in this topic. Then you will provide this account in the monitoring plan wizard (or in the monitored item settings).

Account Requirements

The account used for data collection must meet the following requirements:

- Member of the Domain Admins group on the target server.

NOTE: This covers all the required permissions below and is a mandatory setting if you want to use network traffic compression for data collection.

- The combination of the following rights and permissions if you plan to disable network traffic compression for your monitoring plan or, for some reasons, do not want to add this account to the Domain Admins group:
  - The "Manage auditing and security log" policy must be defined for this account. See the Configure the Manage Auditing and Security Log Policy topic for additional information.
  - If you plan to process the Active Directory Deleted Objects container, Read permission on this container are required. See the Grant Permissions for the Deleted Objects Container topic for additional information.

If the account selected for data collection is not a member of the Domain Admins group, see the Assign Permission To Read the Registry Key topic.

Additional Configuration to Review Changes Made via Exchange Server

If you have an on-premises Exchange server 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 make sure that the account used for data collection has any of the following:

- Membership in the **Organization Management** or **Records Management** group.
- The **Audit Logs** management role (see the Assign Management Roles topic for additional information).

You will also need to configure Exchange Administrator Audit Logging (AAL) settings. See the Exchange Administrator Audit Logging Settings topic for additional information.

Additional Configuration for Domain Controller's Event Logs Auto-backup

The following is required if auto-backup is enabled for the domain controller event logs:

- Permissions to access the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security registry key on the domain controllers in the target domain. See the Assign Permission To Read the Registry Key topic for additional information.
- Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**.
- Read/Write share permission and Full control security permission on the logs backup folder.

Considerations for gMSA Account

If you are using gMSA for data collection, consider that AAL event data collection from your on-premise Exchange server will not be possible.

Thus, changes made to your Active Directory domain via that Exchange server will be reported with *domain\Exchange_server_name$* instead of the initiator (user) name in the "*Who*" field of reports, search results and activity summaries.

Target Domain

If you plan to use network traffic compression for data processing, consider the following:

- If network traffic compression will be *enabled*, then the account must belong to the Domain Admins group

  If you need granular rights to be assigned instead, please contact Netwrix Technical support.
- If network traffic compression will be *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 for more information.

If you need to process Active Directory **Deleted Objects** container, consider the following:

- Read permission on this container is required. See the Grant Permissions for the Deleted Objects Container topic for additional information.
- Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group.

If auto-backup is *enabled* for the domain controller event logs:

- Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See the Assign Permission To Read the Registry Key topic for additional information.
- Membership in any of the following groups: Administrators, Print Operators, Server Operators
- 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.

If you have an on-premises Exchange server 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 make sure that the account used for data collection has any of the following:

- Membership in the **Organization Management** or **Records Management** group.
- The **Audit Logs** management role (see the Assigning Management Roles topic for additional information).

You will also need to configure Exchange Administrator Audit Logging (AAL) settings. See the Exchange Administrator Audit Logging Settings topic for additional information.

If you are using gMSA for data collection, consider that AAL event data collection from your on-premise Exchange server will not be possible.

Thus, changes made to your Active Directory domain via that Exchange server will be reported with *domain\Exchange_server_name$* instead of the initiator (user) name in the "*Who*" field of reports, search results and activity summaries.

Configure the Manage Auditing and Security Log Policy

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

Follow the steps to configure the Manage Auditing and Security Log Policy.

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

Step 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.

Step 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.**

Step 4 – On the right, double-click the **User Rights Assignment** policy.

Step 5 – Locate the **Manage auditing and security log** policy and double-click it.

Step 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.

Step 7 – Run the following command to update group policy: `gpupdate /force`

Step 8 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 9 – Ensure that new GPO settings applied on any audited domain controller.

Grant Permissions for the Deleted Objects Container

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

Follow the steps to grant permissions for the Deleted Objects Container.

Step 1 – Log on to any domain controller in the target domain with a user account that is a member of the **Domain Admins** group.

Step 2 – Navigate to **Start > Run** and type *"cmd"*.

Step 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`

Step 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.

Define the Log On As a Service Policy

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

Follow the steps to define the Log On As a Service policy.

Step 1 – On the computer where Auditor Server is installed, open the **Local Security Policy** snap-in: navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** and select Local Security Policy.

Step 2 – Navigate to **Security Settings > Local Policies > User Rights Assignment** and locate the **Log on as a service** policy.

Step 3 – Double-click the **Log on as a service** policy, and click **Add User or Group**.

Step 4 – Specify the account that you want to define this policy for.

Define the Log On As a Batch Job Policy

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

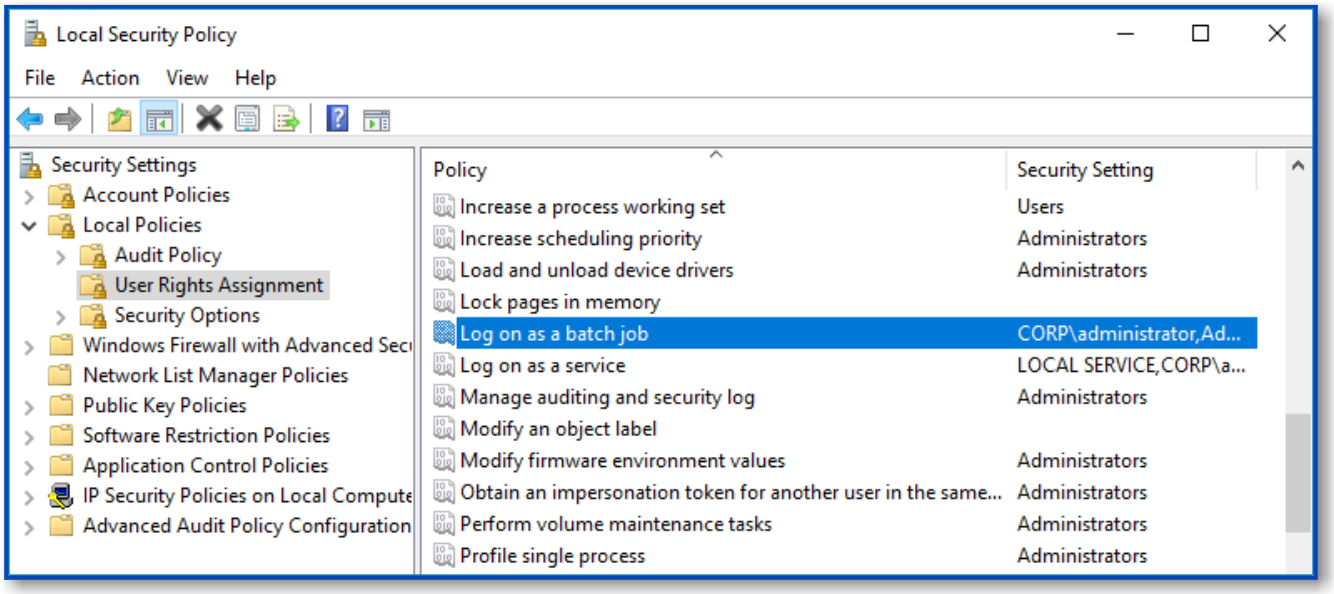
You can configure this policy via the **Local Security Policy** snap-in or using the Group Policy Management console.

Configure the Log On As a Batch Job policy via Local Security Policy Snap-in

Follow the steps to configure the Log On As a Batch Job policy via Local Security Policy snap-in.

Step 1 – On any domain controller in the target domain, open the **Local Security Policy** snap-in: navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** and select Local Security Policy.

Step 2 – In the **Local Security Policy** snap-in, navigate to **Security Settings** > **Local Policies > User Rights Assignment** and locate the **Log on as a batch job** policy.



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

Configure the Log On As a Batch Job Policy Using the Group Policy Management Console

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

Follow the steps to configure the Log On As a Batch Job policy using the Group Policy Management Console.

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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.

Step 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.

Step 4 – On the right, double-click the User Rights Assignment policy.

Step 5 – Locate the Log on as a batch job policy and double-click it.

Step 6 – In the Log on as a batch job Properties dialog, click Add User or Group and specify the user that you want to define this policy for.

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

Step 8 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 9 – Ensure that new GPO settings applied on any audited domain controller.

AD FS

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

Active Directory Federation Services (AD FS) server role can be assigned:

- to a domain controller
- to a Windows server joined in the domain

Multiple AD FS federation servers can be included in a **farm**, a group of connected servers with configuration replicated between them. The first AD FS federation server you set up in the farm becomes the **primary** server. Other federation servers you add to the farm will become **secondary** servers.

Make sure you have Windows Remote Management properly configured on your Auditor console computer. See the Software Requirements topic for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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. See the Configure AD FS farm audit settings automatically topic for additional information.
- Manually – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
  - AD FS audit settings must be configured on the primary AD FS server, i.e. on the first server you have set up in the farm:
    - To configure audit of AD FS 4.0 on Windows Server 2016 or AD FS 5.0 on Windows Server 2019, use the following PowerShell cmdlets:

      ```
      Set-AdfsProperties -LogLevel Errors,FailureAudits,Verbose,SuccessAudits,WarningsSet-AdfsProperties –AuditLevel Verbose
      ```

    - To configure audit of AD FS 3.0 on Windows Server 2012 R2, use the following PowerShell cmdlet

      ```
      Set-AdfsProperties -LogLevel Errors,FailureAudits,Verbose,SuccessAudits,Warnings
      ```

  - Windows Audit policy must be configured on each server in the farm. For all Windows server versions Run the *auditpol* utility with the following parameters:

        - `auditpol.exe /set /subcategory:"Application Generated" /failure:enable /success:enable`

    - Adjust log size and retention settings for **Security** log and for **AD FS Admin** log (under **Applications and Service logs**). See Adjusting Event Log Size and Retention Settings for details.

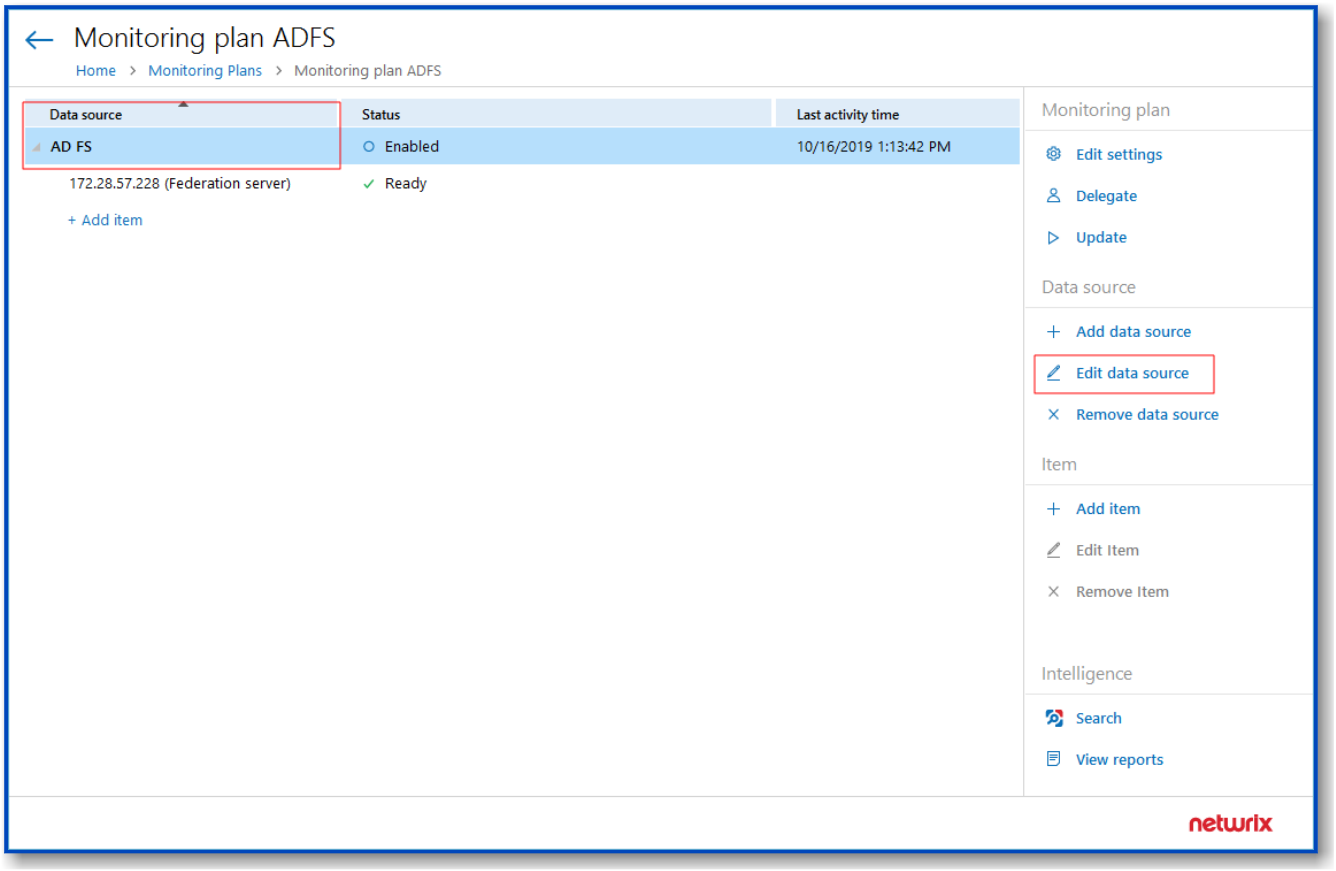
    - If AD FS Admin logging is disabled, you should enable it.

    - See the Configure AD FS farm manually topic for additional information.

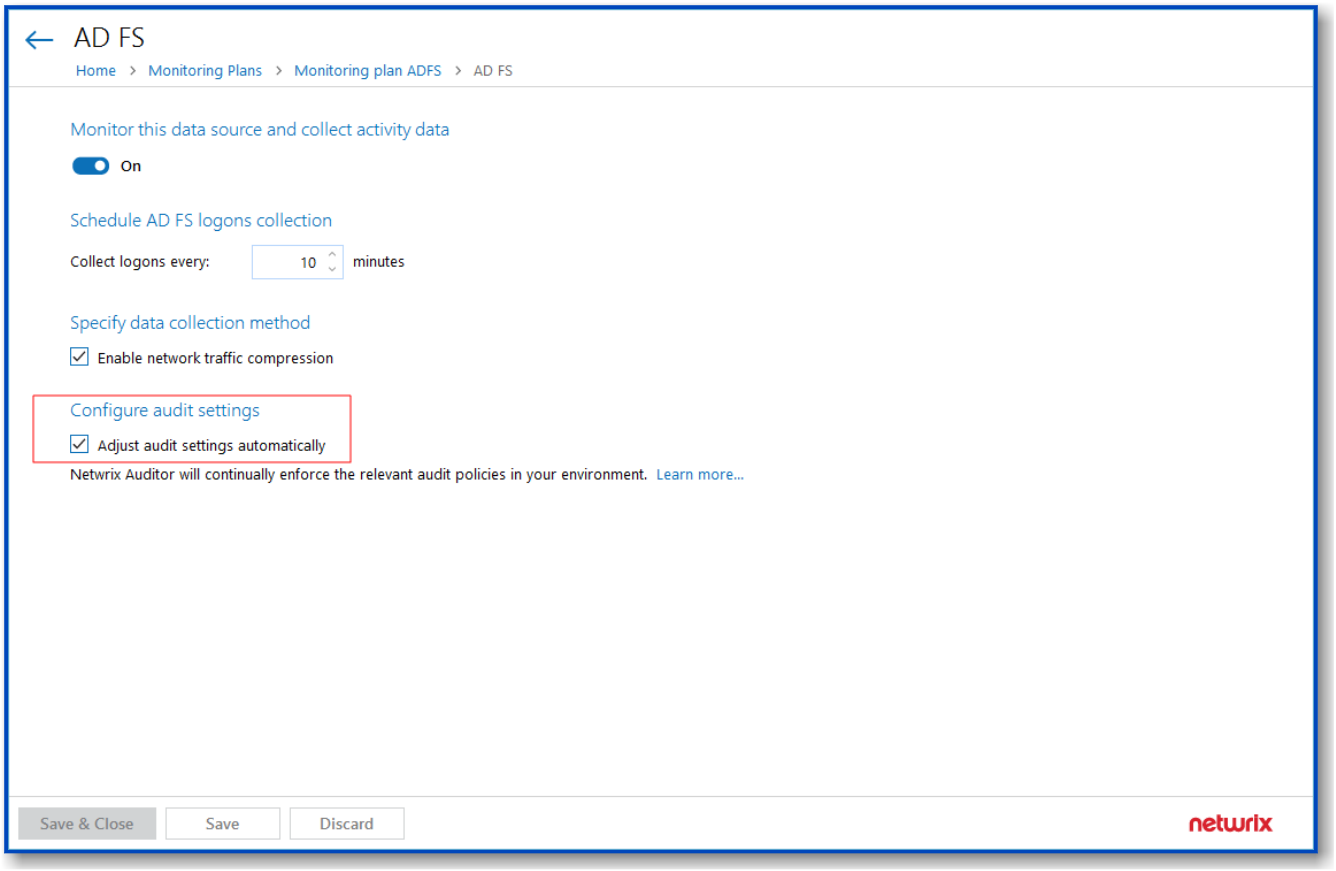
Configure AD FS farm audit settings automatically

Audit settings can be applied automatically if your monitoring plan has the primary AD FS federation server included as an item. If it has only secondary AD FS federation servers included, you will need to configure audit settings manually, as described later in this section.

Step 1 – Select the AD FS data source in this monitoring plan (top row under the header), click **Edit data source** to open its settings.



Step 2 – In the **Configure audit settings** section, select **Adjust audit settings automatically** check box.



Step 3 – Save the settings.

Auditor will automatically configure audit settings on all servers in the AD FS farm and adjust the necessary log settings on these servers.

Configure AD FS farm manually

Follow the steps to enable AD FS audit settings and set up Windows audit policy.

Step 1 – AD FS audit settings must be configured on the primary AD FS server, i.e. on the first server you have set up in the farm:

- To configure audit of AD FS 3.0 on Windows Server 2012 R2, use the following PowerShell cmdlet:

```
Set-AdfsProperties -LogLevel
Errors,FailureAudits,Verbose,SuccessAudits,Warnings
```

- To configure audit of AD FS 4.0 on Windows Server 2016 or AD FS 5.0 on Windows Server 2019, use the following PowerShell cmdlets:

```
Set-AdfsProperties -LogLevel
Errors,FailureAudits,Verbose,SuccessAudits,Warnings

Set-AdfsProperties –AuditLevel Verbose
```

Step 2 – Windows Audit policy must be configured on each server in the farm. For all Windows server versions

- Run the *auditpol* utility with the following parameters:

  ```
  auditpol.exe /set /subcategory:"Application Generated" /
  failure:enable /success:enable
  ```

Step 3 – Adjust log size and retention settings for **Security** log and for **AD FS Admin** log (under **Applications and Service logs**). See the Adjusting Event Log Size and Retention Settings topic for additional information.

If AD FS Admin logging is disabled, you should enable it.

Remember, do the following:

- Configure Data Collecting Account as described in the Permissions for AD FS Auditing topic.
- Configure ports as described in the AD FS Ports topic.

AD FS Servers Data Collection

For Active Directory Federation Services (AD FS) servers, Netwrix Auditor can collect audit data on the events and configuration objects listed below.

Event type	Action	Details
AD FS logon (intranet)	Failed Logon	Cause (for failed attempts)
AD FS logon (extranet)	Successful Logon	Authentication methods (for Successful attempts)

Configuration information can be collected for the following objects:

- AD FS servers included in the farm
- Application Groups settings
- Authentication Method names

- Relying Party Trusts settings
- Scope Descriptions

AD FS Ports

Review a full list of protocols and ports required for monitoring logon activities performed using Active Directory Federation Services (AD FS).

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to local 389 TCP port.

Port	Protocol	Source	Target	Purpose
389	TCP	Netwrix Auditor Server	Domain controllers	LDAP DC query Account resolve
53	TCP	Netwrix Auditor Server	DNS Server	DNS Client
135 + Dynamic: 1024 -65535	TCP	Netwrix Auditor Server	Domain controllers	Windows Management Instrumentation Firewall configuration
135	TCP	Netwrix Auditor Server	Domain controllers	Service Control Manager Remote Protocol (RPC)

Port	Protocol	Source	Target	Purpose
				Core Service installation
137 through 139	UDP	Netwrix Auditor Server	Domain controllers	Service Control Manager Remote Protocol (RPC) Core Service installation
445	TCP	Netwrix Auditor Server	Domain controllers	SMB 2.0/3.0
5985 (for HTTP) 5986 (for HTTPS)	TCP	Netwrix Auditor Server	AD FS servers	Windows Remote Management (WinRM)

Permissions for AD FS Auditing

Before you start creating a monitoring plan to audit your AD FS federation 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:

- If the target AD FS federation server is a domain controller, then the account must belong to the **Administrators** or **Domain Admins** group
- Otherwise, if the server is not a domain controller, the account must belong to the **Local Administrators** group.

Exchange

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - In the Exchange environment:
        - Install the ADSI Edit utility to the server from which configuration is performed if it is not a domain controller
        - 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.”*
        - 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"*.
        - If you have an on-premises Exchange server 2019, 2016, 2013 or 2010 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 in the Exchange Administrator Audit Logging Settings topic.

- The Administrator Audit Logging settings must be configured (only required for Exchange 2019, 2016, 2013 or 2010). See the Exchange Administrator Audit Logging Settings topic for additional information.
- 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
- If you want to track non-owner access, configure mailbox monitoring. See the Configure Exchange for Monitoring Mailbox Access topic for additional information.

◦ On the Auditor console computer:

- If you have enabled automatic log backup for the Security log of your domain controller, you can instruct Auditor to clear the old backups automatically. For that, use the **CleanAutoBackupLogs** registry key, as described in the Active Directory Registry Key Configuration topic.

  RECOMMENDED: Adjust retention period for the backup files accordingly (default is **50** hours). See the Adjust Security Event Log Size and Retention topic.
- To provide for event data collection, the Secondary Logon service must be up and running . Open **Administrative Tools** > **Services**, right-click the **Secondary Logon** service and on the **General** tab make sure that Startup type for this service is other than *Disabled*.

Remember, for Exchange auditing, do the following:

1. Configure Data Collecting Account, as described in the Data Collecting Account topic.
2. Configure required protocols and ports, as described in the Exchange Ports topic.

Monitored Object Types, Actions, and Attributes

Netwrix Auditor tracks changes that have been made to all Exchange server object classes and attributes. The list of Exchange object classes is version-dependent.

- The list of schema changes for Exchange 2013 can be found in the following Microsoft article: https://learn.microsoft.com/en-us/exchange/exchange-2013-active-directory-schema-changes-exchange-2013-help
- The list of schema changes for Exchange 2016 can be found in the following Microsoft article: https://learn.microsoft.com/en-us/exchange/plan-and-deploy/active-directory/ad-schema-changes?view=exchserver-2016
- The list of schema changes for Exchange 2019 can be found in the following Microsoft article: https://learn.microsoft.com/en-us/exchange/plan-and-deploy/active-directory/ad-schema-changes?view=exchserver-2019

Non-Owner Mailbox Access

Netwrix Auditor can monitor non-owner access to mailboxes in on-premises Exchange organization. The following mailbox types will be monitored by default:

- UserMailbox
- EquipmentMailbox
- LinkedMailbox
- RoomMailbox

Here is the list of actions captured:

Item	Action	Audited	How this change is reported by the product
Emails and Folders	New email	Yes	The message was created in \Drafts folder with subject <...>

Item	Action	Audited	How this change is reported by the product
	A user with Send as or Send on behalf permissions tried to send an email	Yes	Message located in Root with subject <...> was queued for delivery to IPM.Message.
	Delete email	Yes	Message with subject <...> was moved from folder \Drafts to folder \Deleted Items.
	Move email to another folder	Yes	Message with subject <...> was moved from folder <...> to folder <...>.
	Create rules for emails	No	—
	Email read attempt	No	—
	New folder	No	—
	Open folder	Yes	The folder <...> was opened.
	Delete folder	Yes	Folder <...> was moved from folder <...> to folder \Deleted Items.

Item	Action	Audited	How this change is reported by the product
	Empty folder	Yes	The folder <...> was opened.
	Edit folder permissions	No	—
Calendar	New event	Yes	Message was created in \Calendar with subject <...>.
	Event read attempt	No	—
	Edit event	Yes	Message located in \Calendar with subject <...> was modified.
	Delete event	Yes	Message with subject <...> was moved from folder \Calendar to folder \Deleted Items.
People	New contact	Yes	Message was created in \Contacts\Recipient Cache with subject <*contact name*>.
	Contact read attempt	Yes	Folder \Contacts\Recipient Cache was opened.

Item	Action	Audited	How this change is reported by the product
	Edit contact	No	—
	Delete contact	Yes	Message with subject <...> was moved from folder \Contacts to folder \Deleted Items.
Tasks	New task	Yes	Message was created in \Tasks with subject <...>.
	Task read attempt	No	—
	Edit task	Yes	Message located in \Tasks with subject <...> was modified.
	Delete task	Yes	Message with subject <...> was moved from folder \Tasks to folder \Deleted Items.

Exchange Ports

Review a full list of protocols and ports required for monitoring Exchange.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to the local 389 TCP port.

Port	Protocol	Source	Target	Purpose
135 and dynamic range: 1024 -65535	TCP	Netwrix Auditor Server	Exchange Server	• Windows Management Instrumentation. • Retrieve Exchange Server configuration settings* • Run `gpupdate /force *`
5985 5986	TCP	Netwrix Auditor Server	Exchange server	• Windows Remote Management. • PowerShell connections: ◦ 5985 - for HTTP ◦ 5986 - for HTTPS
80 443	TCP	Netwrix Auditor Server	Exchange server	PowerShell connections

* - for Exchange 2010 only

Exchange Administrator Audit Logging Settings

To be able to audit and report who made changes to the Exchange servers in your on-premises infrastructure, or to Active Directory via the Exchange, ensure the Exchange Administrator Audit Logging (AAL) settings are configured as follows:

Setting	Value	Comment
AdminAuditLogEnabled	True	Enables audit logging
AdminAuditLogAgeLimit	30	Determines how long audit log entries will be retained (default is 90 days)
AdminAuditLogCmdlets	*	Instructs the program to create a log entry for every cmdlet that is run.
LogLevel	Verbose	Sets logging level.
ExcludedCmdlets	*-InboxRule, *-MailboxAutoReplyConfiguration, Set-MailboxAuditBypassAssociation, Set-MailboxAutoReplyConfiguration, Set-MailboxCalendarConfiguration, Set-MailboxCalendarFolder, Set-MailboxFolderPermission, Set-MailboxJunkEmailConfiguration, Set-MailboxMessageConfiguration, Set-MailboxRegionalConfiguration, Set-MailboxSpellingConfiguration	This list of exclusions is set up as explained in step 3 of the procedure below.

You can configure these settings automatically using Netwrix Auditor, as described in the Active Directory: Automatic Configuration topic.

To configure them manually, refer to the procedure described below.

You can perform this procedure on any of the Exchange servers, and these settings will then be replicated to all Exchange servers in the domain.

To configure Exchange Administrator Audit Logging settings

Step 1 – On the computer where the monitored Exchange server is installed, navigate to **Start → Programs → Exchange Management Shell**.

Step 2 – Execute the following command depending on your Exchange version:

- Exchange 2019, 2016 and 2013

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

- Exchange 2010

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

Step 3 – To reduce server load, you can exclude the cmdlets listed in the table above from Exchange logging. For that:

- On the computer where Netwrix Auditor is installed, browse to the *%Netwrix Auditor Server installation folder%/Active Directory Auditing* folder, locate the **SetAALExcludedCmdlets.ps1** PowerShell script file and copy it to Exchange server.
- In **Exchange Management Shell**, run this script using the command line:

```
<Path_To_SetAALExcludedCmdlets_File>.\SetAALExcludedCmdlets.ps1
```

  Make sure your policies allow script execution.

Configure Exchange for Monitoring Mailbox Access

Netwrix Auditor allows tracking non-owner mailbox access in your Exchange organization.

It is recommended to select **Adjust audit settings automatically** option when setting up Exchange monitoring in Netwrix Auditor. See the Create a New Monitoring Plan topic for additional information.

However, in some scenarios users may need to apply required audit settings manually. For that, review the following procedures:

- Configuring mailbox access tracking for Exchange 2019, 2016 and 2013 manually
- Configuring mailbox access tracking for Exchange 2010 manually

Configuring mailbox access tracking for Exchange 2019, 2016 and 2013 manually

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 mailboxes (User, Linked, Equipment, and Room mailbox)
- 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,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*). If you are going to audit multiple Exchange servers, repeat these steps for each audited Exchange server.
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:

Track...	Steps...
	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, • User Principal Name. Example: MJones@enterprise.local If you are going to audit multiple individual mailboxes, repeat these steps for each mailbox on each Exchange server.

Configuring mailbox access tracking for Exchange 2010 manually

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

Step 1 – On the computer where the monitored Exchange server is installed, navigate to **Start** → **Programs** → **Exchange Management Shell**.

Step 2 – Execute the following command:

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

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

Exchange Registry Keys

Review the basic registry keys that you may need to configure for monitoring Exchange with Netwrix Auditor. Navigate to Start → Run and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
IgnoreRootDCErrors	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
MonitorModifiedAndRevertedBack	Defines whether the Activity Summary must display the attributes whose values were modified and then restored between data collections: • 0—These attributes are not displayed • 1—These attributes are displayed as "modified and reverted back"
ProcessBackupLogs	Defines whether to process security log backups: • 0—No

Registry key (REG_DWORD type)	Description / Value
	• 1—Yes Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the CleanAutoBackupLogs key.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter\<monitoring plan name>	
CollectLogsMaxThreads	Defines the number of Domain Controllers to simultaneously start log collection on.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Management Console\Database settings	
overwrite_datasource	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the monitoring plan: • 0—No • 1—Yes
SqlOperationTimeout	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).
timeout	Defines the Audit Database connection timeout (in seconds).

Assign Permission To Read the Registry Key

This permission is required 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, it is recommended to assign permissions through Group Policy, or automatically using Audit Configuration Assistant. To assign permissions manually, use the Registry Editor snap-in or the Group Policy Management console. See the Permissions for Group Policy Auditing topic for additional information.

Assign Permission Via the Registry Editor Snap-in

Follow the steps to assign permission via the Registry Editor snap-in.

Step 1 – On your target server, open Registry Editor: navigate to **Start > Run** and type *"regedit"*.

Step 2 – In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\EventLog\Security*.

Step 3 – Right-click the **Security** node and select **Permissions** from the pop-up menu.

Step 4 – Click **Add** and enter the name of the user that you want to grant permissions to.

Step 5 – Check **Allow** next to the **Read** permission.

Step 6 – For auditing Logon Activity, you also need to assign the Read permission to the *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv* registry key.

Assign Permission Using the Group Policy Management Console

Follow the steps to assign permission using the Group Policy Management console.

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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 .

Step 3 – In the Group Policy Management Editor dialog, expand the Computer Configuration node on the left and navigate to Policies > Windows Settings > Security Settings > Registry.

Step 4 – Right-click in the pane and select Add Key.

Step 5 – Navigate to `HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv` and click OK.

Step 6 – Click Add and enter the name of the user that you want to grant permissions to and press Enter.

Step 7 – Check Allow next to the *Read* permission and click OK

Step 8 – In the pop-up window, select Propagate inheritable permissions to all subkeys and click OK.

Step 9 – Repeat the steps 4-8 for keys below:

- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlSet\Control\SecurePipeServers\winreg`;
- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlSet\services\EventLog\Security`.

Step 10 – Close Group Policy Management console.

Step 11 – Navigate to Start > Run and type `cmd`. Input the `gpupdate /force` command and press Enter. The group policy will be updated.

Step 12 – Type `repadmin/syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 13 – Ensure that new GPO settings were applied to the domain controllers.

Permissions for Exchange Auditing

Before creating a monitoring plan to audit your Exchange server, you need to plan for the account that will be used for data collection. This account should meet the requirements listed below. You will specify this account in the monitoring plan wizard (or in the monitored item settings).

Account Requirements

The account used for data collection must meet the following requirements:

- Member of the Domain Admins group on the target server.

  NOTE: This covers all the required permissions below and is a mandatory setting if you want to use network traffic compression for data collection.

  OR

- The combination of the following rights and permissions if you plan to disable network traffic compression for your monitoring plan or, for some reasons, do not want to add this account to the Domain Admins group:
  - The Manage auditing and security log policy must be defined for this account. See the Permissions for Active Directory Auditing topic for additional information.
  - If you plan to process the Active Directory Deleted Objects container, Read permission on this container is required. See the Permissions for Active Directory Auditing topic for additional information.
  - The account must belong to the Organization Management or Records Management group. See the Add Account to the Organization Management Group topic for additional information.
  - Several management roles assigned: Audit Logs role, View-only Configuration role, Mail Recipients role, and Monitoring role. See the Add Account to the Organization Management Group topic for additional information on how to perform role assignment.
  - Additional configuration if auto-backup is *enabled* for the domain controller event logs (see below).

Additional Configuration for Domain Controller's Event Logs Auto-backup

The following is required if auto-backup is *enabled* for the domain controller event logs:

- Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See the Assign Permission to Read the Registry Key topic for additional information.
- Membership in one of the following groups: Administrators, Print Operators, Server Operators
- Read/Write share permission and Full control security permission on the logs backup folder

Add Account to the Organization Management Group

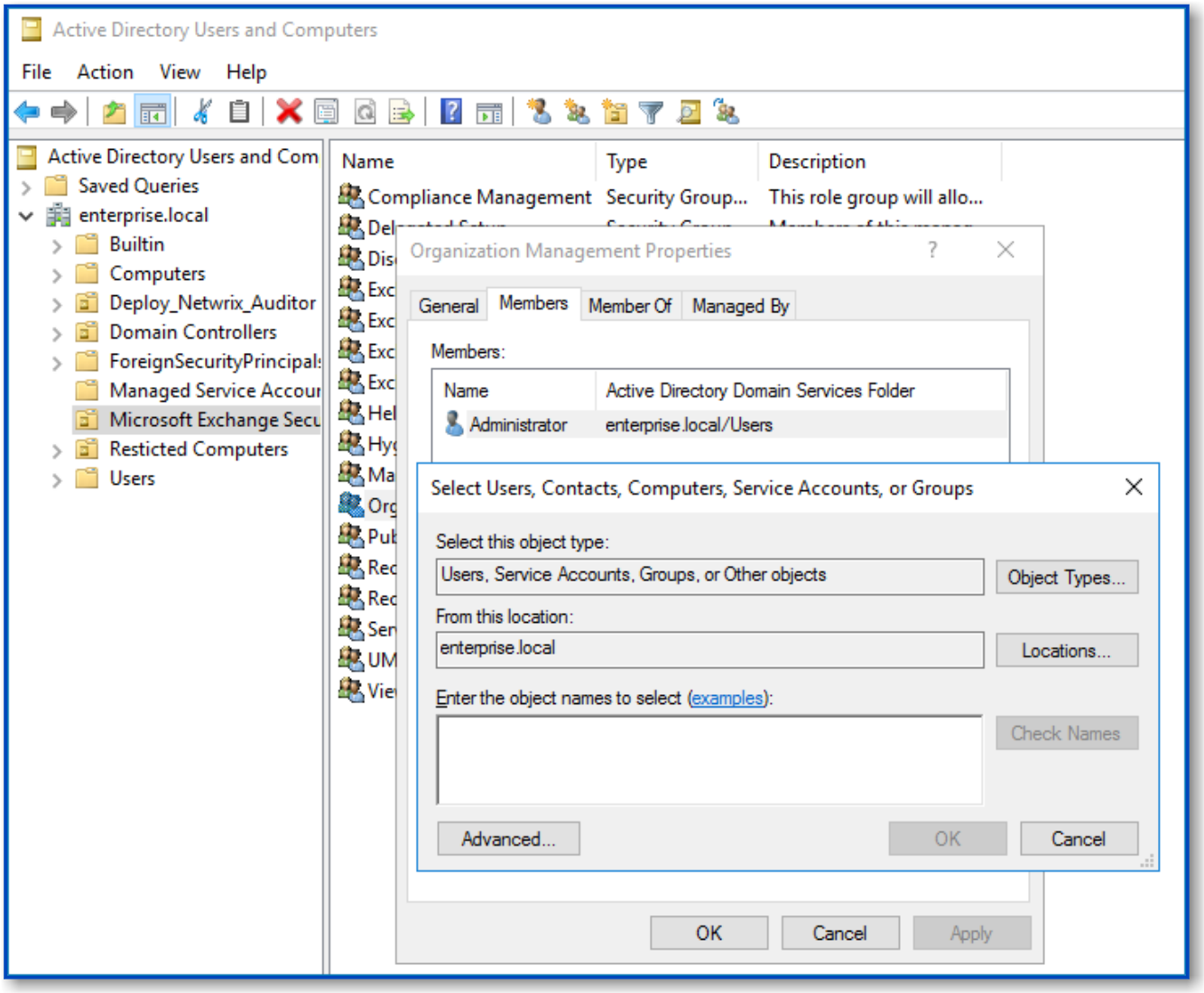
Follow the steps to add account to the Organization Management group.

Step 1 – Navigate to **Start > Active Directory Users and Computers** on any domain controller in the root domain of the forest where Microsoft Exchange 2019, 2016, or 2013 is installed.

Step 2 – In the left pane, navigate to **<domain_name> > Microsoft Exchange Security Groups**.

Step 3 – On the right, locate the **Organization Management** group and double-click it.

Step 4 – In the **Organization Management Properties** dialog that opens, select the **Members** tab and click **Add**.



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.

Assign Management Roles

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

Follow the steps to assign management roles.

Step 1 – On the computer where Microsoft Exchange 2019, 2016, 2013 or is installed, open the **Exchange Management Shell** under an account that belongs to the **Organization Management** group.

Step 2 – Use the following syntax to assign the required management 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.

Assign Permission to Read the Registry Key

This permission is required 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, it is recommended to assign permissions through Group Policy, or automatically using Audit Configuration Assistant.

To assign permissions manually, use the Registry Editor snap-in or the Group Policy Management console.

Assign Permission Via the Registry Editor Snap-in

Follow the steps to assign permission via the Registry Editor snap-in.

Step 1 – On your target server, open Registry Editor: navigate to **Start > Run** and type *"regedit"*.

Step 2 – In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\EventLog\Security*.

Step 3 – Right-click the **Security** node and select **Permissions** from the pop-up menu.

Step 4 – Click **Add** and enter the name of the user that you want to grant permissions to.

Step 5 – Check **Allow** next to the **Read** permission.

Step 6 – For auditing Logon Activity, you also need to assign the Read permission to the *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv* registry key.

Assign Permission Using the Group Policy Management Console

Follow the steps to assign permission using the Group Policy Management console.

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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 .

Step 3 – In the Group Policy Management Editor dialog, expand the Computer Configuration node on the left and navigate to Policies > Windows Settings > Security Settings > Registry.

Step 4 – Right-click in the pane and select Add Key.

Step 5 – Navigate to `HKEY_LOCAL_MACHINE\sECURITY\Policy\PolAdtEv` and click OK.

Step 6 – Click Add and enter the name of the user that you want to grant permissions to and press Enter.

Step 7 – Check Allow next to the *"Read"* permission and click OK

Step 8 – In the pop-up window, select Propagate inheritable permissions to all subkeys and click OK.

Step 9 – Repeat the steps 4-8 for keys below:

- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlSet\Control\SecurePipeServers\winreg;`

- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlSet\services\EventLog\Security`.

Step 10 – Close Group Policy Management console.

Step 11 – Navigate to Start > Run and type "*cmd*". Input the `gpupdate /force` command and press Enter. The group policy will be updated.

Step 12 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 13 – Ensure that new GPO settings were applied to the domain controllers.

File Servers

Netwrix Auditor can monitor for operations with files and folders on the storage systems, collect state-in-time snapshots and track changes to the object attributes. This section provides detailed information on these activities.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

Supported File Servers and Devices

The following topics list the operations with files and folders that can be monitored and reported by Auditor on these supported storage systems.:

- Dell Data Storage
- Dell Isilon/PowerScale
- NetApp Data ONTAP
- Nutanix
- Qumulo
- Synology
- Windows File Servers

State-in-Time Data

State-in-time data collection is supported for files, folders and shares on Windows-based file servers, Dell and NetApp storage systems, and Nutanix File Servers. Remember to select the corresponding option in the data source settings within the monitoring plan.

Sensitive Data

Starting with the version 10, the product is able to report about sensitive data in your IT infrastructure. Pay attention to the "*Data categories*" column in search and reports (for the "*File*" object types only). See the Sensitive Data Discovery topic for additional information on how to enable monitoring of sensitive data in Auditor.

Monitored Object Attributes

The table below lists the object types and attributes that can be monitored by Auditor.

For more information on the attributes marked with (*) , refer to the following Microsoft article: File Attribute Constants.

Object type	Attributes
File	• Attributes* • Location • Name • Ownership • Permissions: ◦ Group Permissions ◦ User Permissions • Primary Group • Security descriptor control flags • Size • Data categories

Object type	Attributes
Folder	• Attributes* The Reparse point attribute content is available for reviewing only when State-In-Time snapshot collection is enabled. Mind that reparse point content changes cannot be audited. • Location • Name • Ownership • Permissions: ◦ Group Permissions ◦ User Permissions • Primary Group • Security descriptor control flags
Share	• Access-based Enumeration • Caching • Continuous Availability • Description • Enable BranchCache • Encrypt Data Access • Local Path • User Limit

CAUTION: File and folder attributes marked with the (*) are not monitored by default. Please contact Netwrix Technical Support team to monitor these file and folder attributes.

In addition to general object attributes, Auditor generates the following attributes associated with the object and reserved for internal use:

- **Session ID** — This attribute is based on the user's logon ID and timestamp of the related logon event. Being unique for a user's logon session, it usually helps to distinguish the events and changes that occurred within that session.
- **Statement ID** — This attribute appears if an object was moved/renamed due to its root object modifications.

Dell Data Storage

NOTE: Dell VNX, VNXe, Celerra, and Unity NAS devices are collectively referred to as Dell Data Storage.

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - On the Dell Data Storage device:
        - 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 Dell VNX/VNXe/Unity/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 Auditor console computer:
        - 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 Auditor Server.

First, you should decide on the objects and actions you want to track. Consider the following:

- Actions reported by Auditor vary depending on the file server type and the audited object (file, folder, or share).
- Besides, monitoring and reporting of the Dell Data Storage systems may not provide the results you expect — due to native Dell audit peculiarities. See the File Servers topic for additional information.

For example, the *change* operation (in Auditor terminology) includes creation, modification, and deletion.

Manual Configuration

To collect comprehensive audit data, you must configure your file shares for monitoring. Consider the following:

Step 1 – 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). Auditor does not clean Dell Unity logs automatically, the log will start overwriting when it goes beyond the limit. See the Unity

Family Security Configuration Guide for additional information on how to set logs roll over manually.

Step 2 – 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.

Step 3 – Configure Audit Object Access Policy. Set the Audit object access policy to "Success" and "Failure" in the Group Policy of the OU where your Dell VNX/VNXe/Unity/Celerra appliance belongs to. For more information on VNX/VNXe/Unity/Celerra GPO support, refer to documentation provided by Dell.

Step 4 – Configure Audit Settings for CIFS File Shares on Dell Data Storage

Dell Data Storage Ports

Review a full list of Dell Data Storage protocols and ports required for Netwrix Auditor for File Servers.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to local 389 TCP port.

Port	Protocol	Source	Target	Purpose
Dell Isilon				
8080	TCP	Netwrix Auditor Server	Isilon cluster	HTTPS Used to connect to the Isilon Management Server

Configure Security Event Log Maximum Size

Follow the steps to configure Event Log maximum size:

Step 1 – On your file server, create a new file system where the security log will be stored.

Step 2 – Mount this file system on a mount point, e.g., **/events**.

Step 3 – Make sure that it is accessible via the **\\<file_server_name>\C$\events** UNC path.

Step 4 – On the computer where Auditor Server is installed, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.

Step 5 – Navigate to **File** → **Connect Network Registry** and specify the file server name.

Step 6 – Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security** and set the **File** value to *"C:\events\security.evt"*.

Step 7 – Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.

Configure Audit Object Access Policy

Netwrixrecommends 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.

Follow the steps to configure Audit Object Access Policy:

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

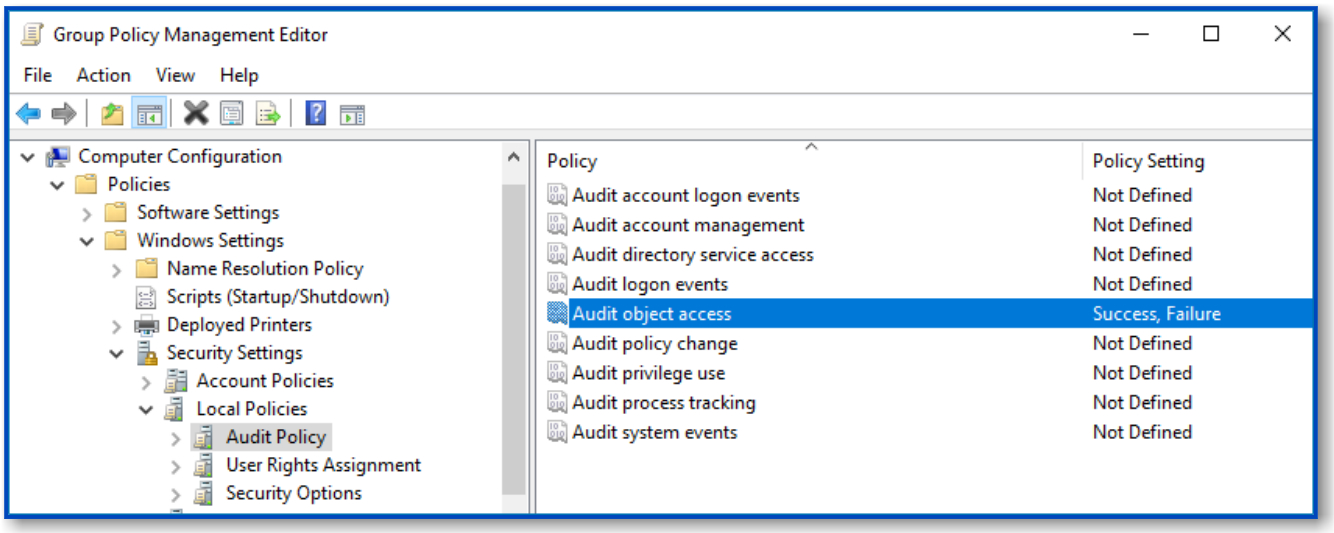
Step 2 – In the left pane, navigate to **Forest: <forest_name>** → **Domains** → **<domain_name>**, right-click <OU_name> and select **Create a GPO in this domain and Link it here**.

Step 3 – Enter the name for the new GPO.

Step 4 – Right-click the newly created GPO and select **Edit**.

Step 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"*



Step 6 – To update the group policies, execute the following command:

- For Dell Unity:

  ```
  svc_cifssupport <NAS Server Name> -gpo -update
  ```

  where <NAS server Name> is the name of the target Unity\VNX server.

- For Dell VNX:

  ```
  server_security <NAS Server Name> -update -policy gpo
  ```

  where <NAS server Name> is the name of the target Unity\VNX server.

  To update group policies for Dell VNX you must be logged in as the 'nasadmin' user.

You can configure advanced audit policy to narrow the range of events tracked and recorded by the product, thus preventing your AuditArchive and the Security event log from overfilling. See the Configure Security Event Log Maximum Size topic for additional information.

Configure Audit Settings for CIFS File Shares on Dell Data Storage

Dell VNX, VNXe, Celerra, and Unity NAS devices are collectively referred to as Dell Data Storage.

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. 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 Audit Archive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification.

Option		Description
		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 Audit Archive.

Actions reported by 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. See the Dell Data Storage topic for additional information.

Configure Audit Settings for the CIFS File Shares Pre-Windows Server 2012

Perform the following steps:

Step 1 – Navigate to the target file share, right-click it and select **Properties**.

Step 2 – In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

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

Step 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**.

Step 5 – 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 Auditor client and the product will only audit user accounts that belong to the selected group.

Step 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 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: • **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.**
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 container only checkbox is cleared.**

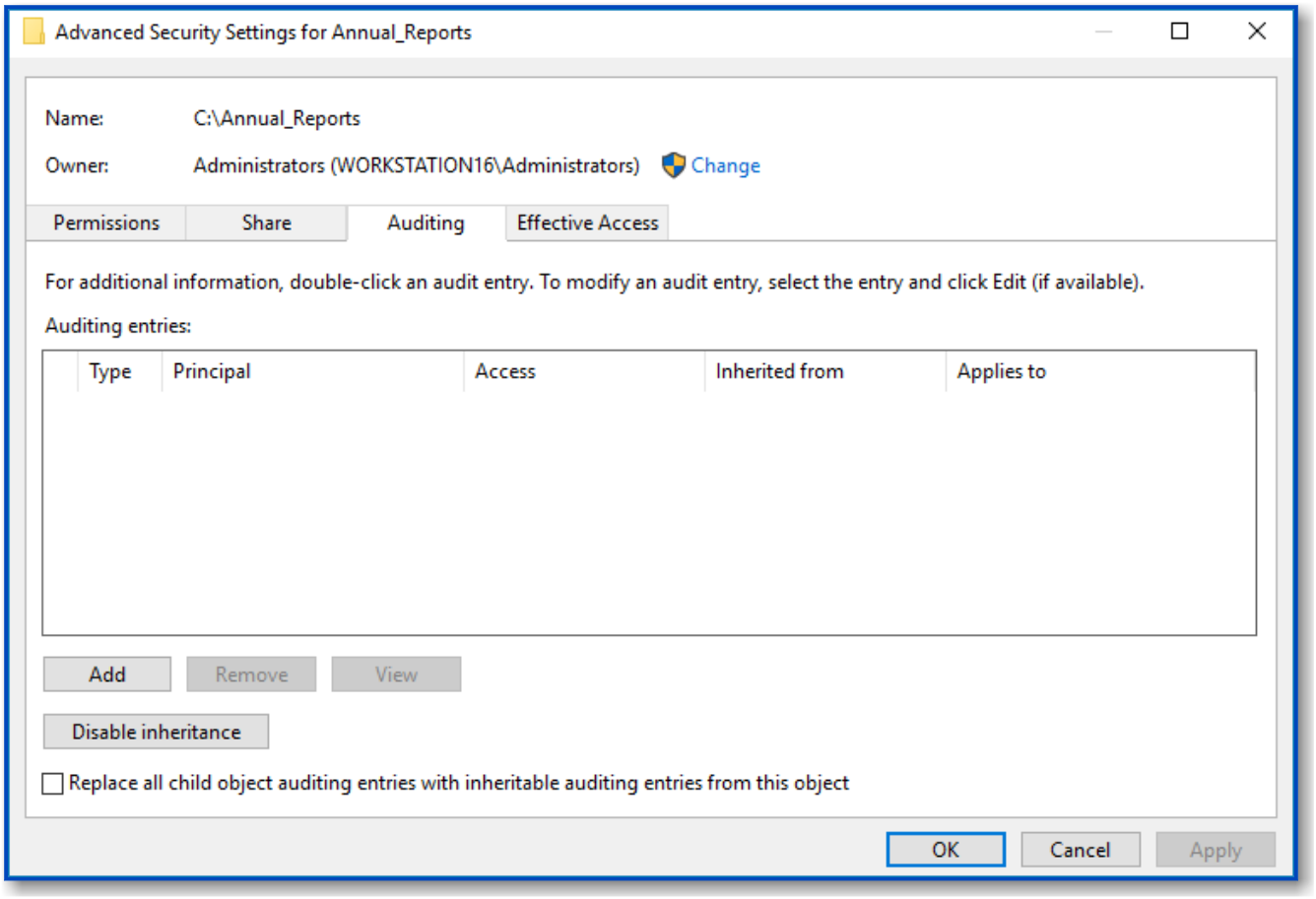
Configure Audit Settings for the CIFS File Shares Windows Server 2012 and Above

Follow the steps to configure audit settings.

Step 7 – Navigate to the target file share, right-click it and select **Properties**.

Step 8 – In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

Step 9 – In the **Advanced Security Settings for <Share_Name>** dialog, navigate to the **Auditing** tab.



Step 10 – 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.

Step 11 – In the Auditing Entry for <Folder_Name> dialog, click the Select a principal link and specify Everyone.

Step 12 – 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.

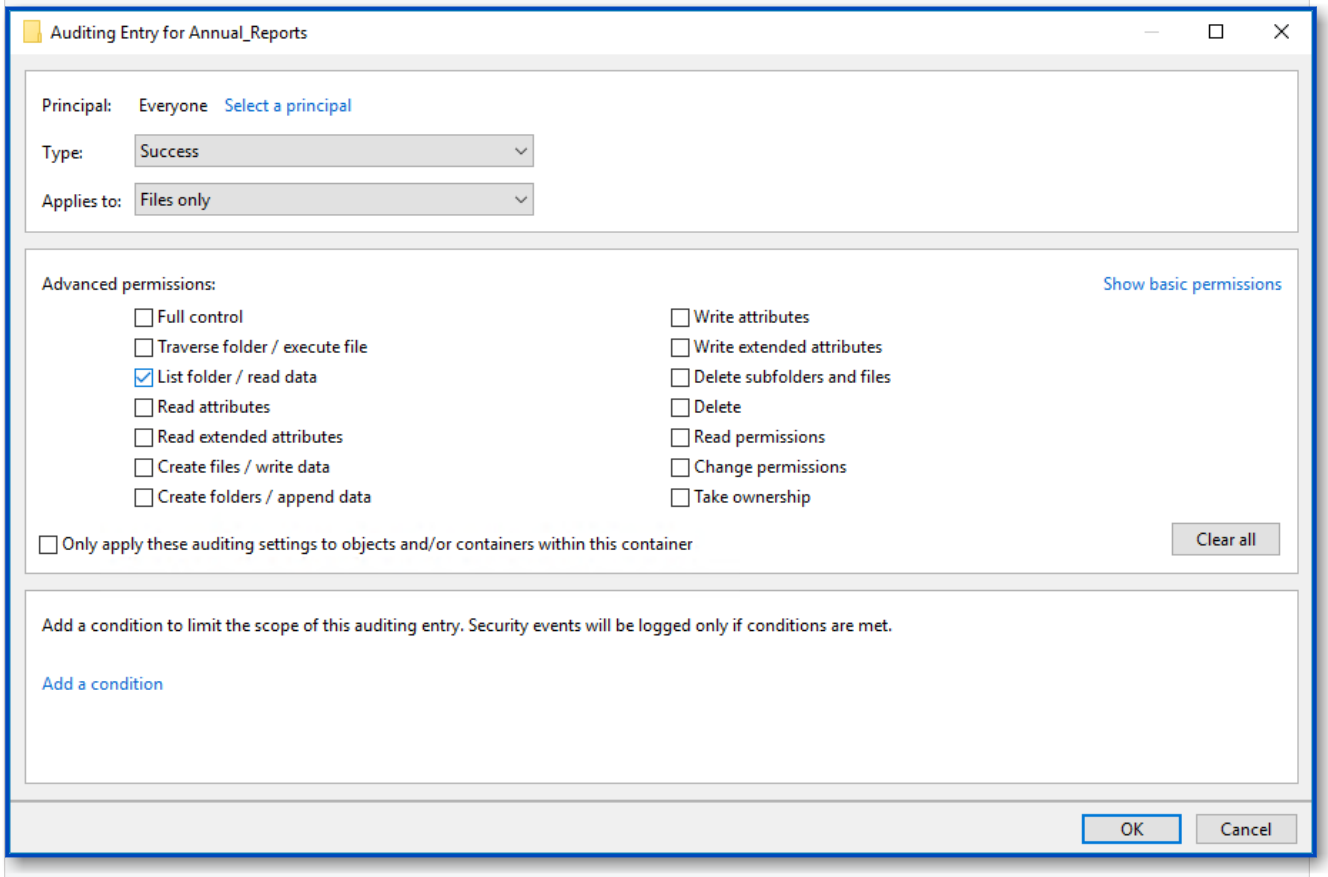
Step 13 – Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports 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:

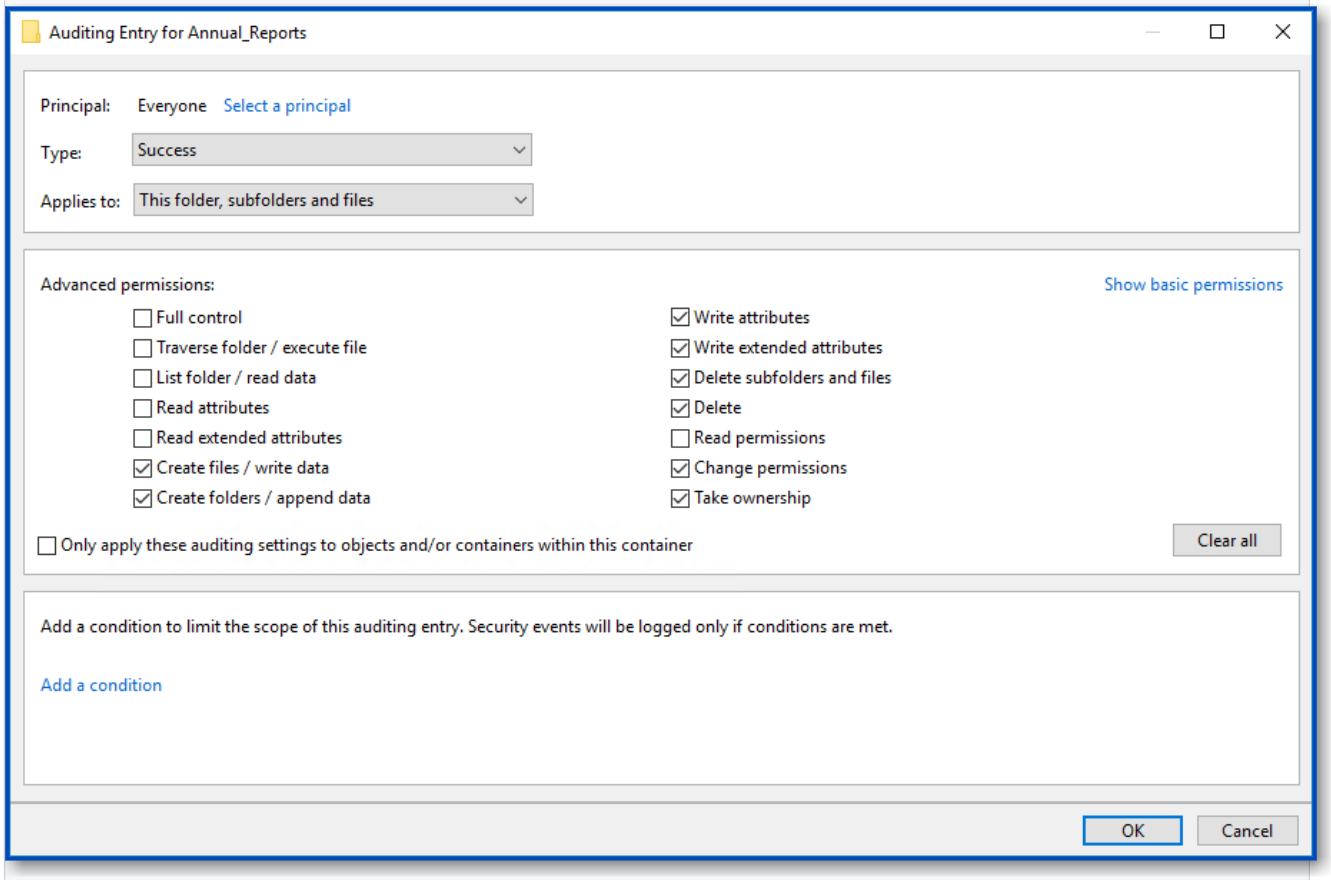


- **Type—Set to *"Success"*.**
- **Applies to—Set to *"Files only"*.**
- **Advanced permissions—Select List folder / read data.**
- **Make sure that the Only apply these auditing settings to objects and/or containers within this container checkbox is cleared.**

Successful changes

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

Auditing Entry	

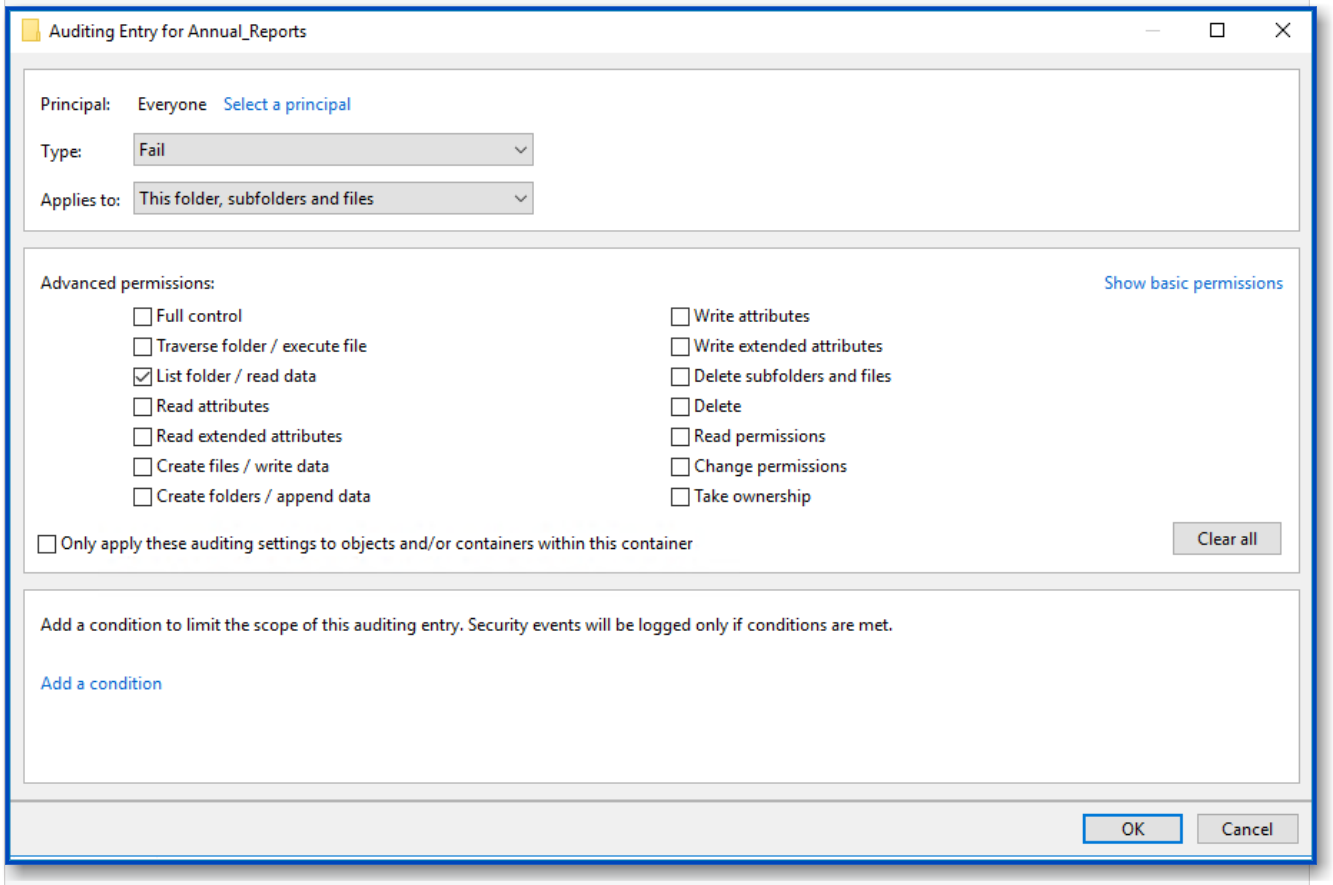


- **Type—Set to *"Success"*.**
- **Applies to—Set to *"This folder, subfolders and files"*.**
- **Advanced permissions:**
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**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



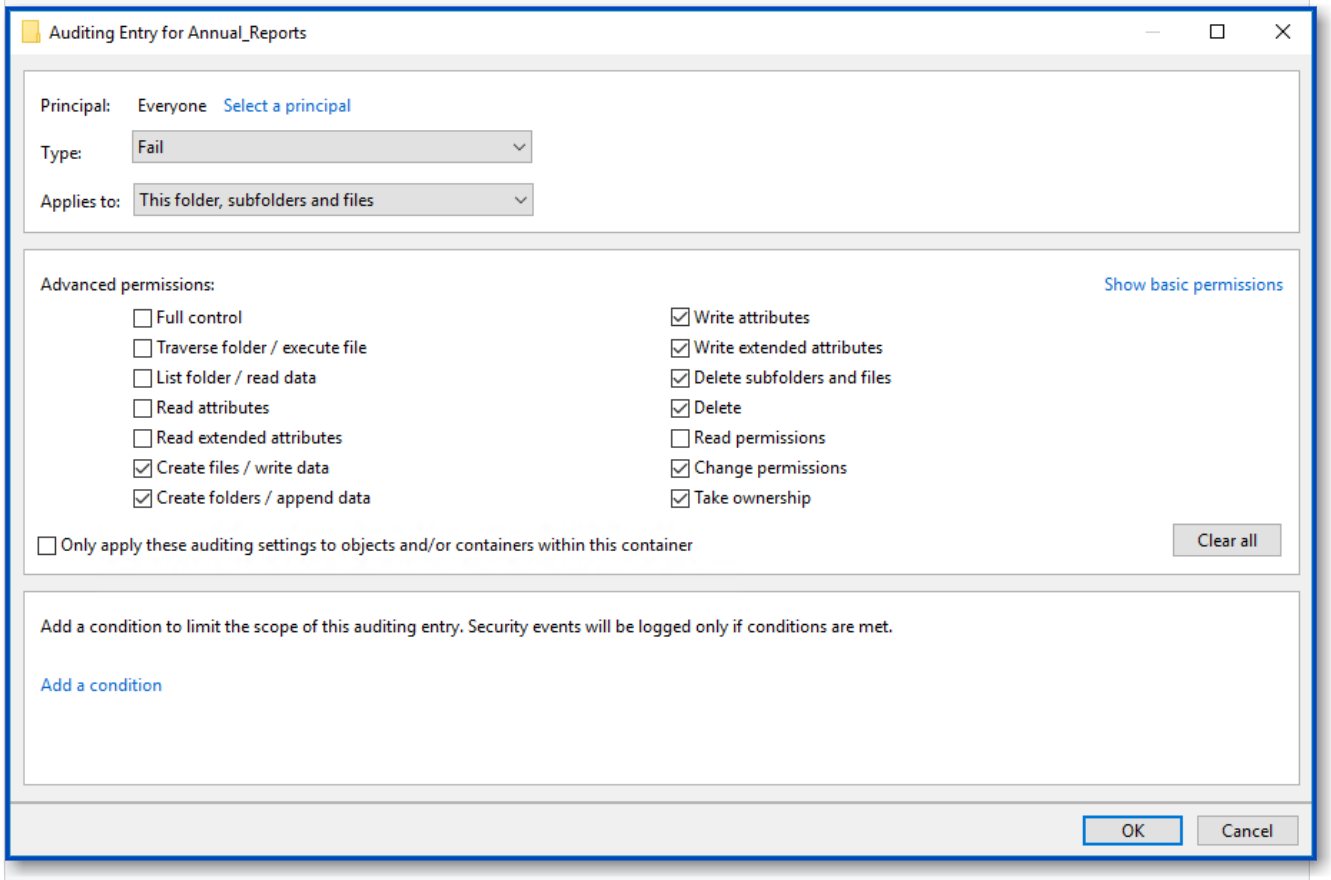
- **Type—Set to *"Fail"*.**
- **Applies to—Set to *"This folder, subfolders and files"*.**
- **Advanced permissions—Select List folder / read data.**

- **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.**

Auditing Entry			
Successful reads	**Successful modifications**	**Failed read attempts**	**Failed modifications attempts**
Applies to			
Files only	**This folder, subfolders and files**	**This folder, subfolders and files**	**This folder, subfolders and files**
Type			
Success	**Success**	**Fail**	**Fail**
Advanced permissions			
• List Folder / Read Data	• Create Files / Write Data • Create Folders / Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Change Permissions • Take Ownership	• List Folder / Read Data	• Create Files / Write Data • Create Folders / Append Data • Write Attributes • Write Extended Attributes • Delete Subfolders and Files • Delete • Change Permissions • Take Ownership

Permissions for Dell Data Storage Auditing

Dell VNX, VNXe, Celerra, and Unity NAS devices are collectively referred to as Dell Data Storage.

Before you start creating a monitoring plan to audit your Dell VNX/VNXe/Unity 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.

Dell Isilon/PowerScale

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - CIFS Network Protocol support is required.
    - Create a shared directory */ifs/.ifsvar/audit/* on your cluster.

      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:

      For EMC Isilon/PowerScale 7x:

        - Audit Success: read, write, delete, set_security, rename
        - Audit Failure: read, create, write, delete, set_security, rename

For EMC Isilon/PowerScale 8.2 and above:

- Audit Success: read, create, write, delete, set_security, rename
- Audit Failure: read, create, write, open, delete, set_security, rename

To configure your Dell Isilon/PowerScale appliance for monitoring perform the following procedures:

- Normal and Enterprise Modes for Clusters
- Compliance Mode

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 AuditorServer.

The following table lists actions that can be performed on Dell Isilon/PowerScale:

Added	+	+	+
Add (failed attempt)	+*	+*	–
Modified	+	+	+
Modify (failed attempt)	+	+	–
Moved	+*	+*	–
Move (failed attempt)	+*	+*	–
Read	+	–	–
Read (failed attempt)	+	+*	–
Renamed	+*	+*	–
Renamed (failed attempt)	+*	+*	–
Removed	+	+	+
Remove (failed attempt)	+*	+*	–
Copied	–	–	–

NOTE: For Dell Isilon/PowerScale storage, auditing of *System* zone is not supported. As stated by Dell, this zone should be reserved for configuration access only. Current data should be stored in other access zones. See the Dell Upsilon CLI Administration Guide for additional information.

Actions marked with an asterisk (*) are reported for Dell Isilon/PowerScale only. Consider that monitoring and reporting of other Dell Data Storage systems may not provide the results you expect due to native Dell audit peculiarities.

Dell Isilon/PowerScale Ports

Review a full list of protocols and ports required for Netwrix Auditor for Dell Isilon/PowerScale:

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Port	Protocol	Source	Target	Purpose
8080	TCP	Netwrix Auditor Server	Isilon/PowerScale cluster	HTTPS Used to connect to the Isilon/PowerScale Management Server

Normal and Enterprise Modes for Clusters

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 the Configure Dell Isilon/PowerScale Cluster in Normal or Enterprise Mode via Shell Script topic for additional information.
- Manual configuration. See the Configure Dell Isilon/PowerScale Cluster in Normal or Enterprise Mode Manually topic for additional information.

Configure Dell Isilon/PowerScale Cluster in Normal or Enterprise Mode via Shell Script

Follow the steps to configure Dell Isilon/PowerScale cluster in Normal or Enterprise mode using shell script:

Step 1 – On the computer where 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.

Step 2 – Navigate to your cluster command prompt through the SSH connection.

Step 3 – Log in to your cluster as a root user.

Step 4 – Run the shell script by executing the following command:

```
sh /ifs/data/configure_ifs.sh -z zone1 -a 1
```

where

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

`1` 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

Configure Dell Isilon/PowerScale Cluster in Normal or Enterprise Mode Manually

Follow the steps to configure Dell Isilon/PowerScale cluster in Normal or Enterprise mode manually:

Step 1 – Navigate to your cluster command prompt through the SSH connection.

Step 2 – Log in to your cluster as a root user.

Step 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/

chmod +a user root allow dir_gen_read /ifs/.ifsvar/audit/
```

Step 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
```

Starting from Dell Isilon/PowerScale 9.2.0 and above, the `lwnet` command is considered as deprecated. When configuring audit manually, you see the following warning:

WARNING: lwnet has been deprecated.

Please use `isi smb ...` equivalents instead.

See `isi smb --help` for more information.

This command is required to create a shared folder pointed to */ifs/.ifsvar/audit/*. Please ignore the warning.

Step 5 – Add the BUILTIN\Administrators group in the share permissions for the 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
```

Step 6 – Enable protocol auditing for a selected zone (for example, *"zone1"*). Do one of the following, depending on your Dell Isilon/PowerScale storage version:

Dell Isilon/PowerScale 7.x	Dell Isilon/PowerScale 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.

Dell Isilon/PowerScale 7.x	Dell Isilon/PowerScale 8.2 and above
Successful changes	

Dell Isilon/PowerScale 7.x	Dell Isilon/PowerScale 8.2 and above
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, create
Failed change attempts	
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,open
Successful reads	
isi zone zones modify zone1 --audit-success=read	isi audit settings modify -- zone=zone1 --audit-success=read
Failed read attempts	
isi zone zones modify zone1 --audit-failure= create,read	isi audit settings modify --zone=zone1 --audit-failure=create,read, open

Step 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"
```

Considerations and Recommendations

When preparing to audit your Dell Isilon/PowerScale storage system, consider the following:

- If you plan to configure audit settings for Dell Isilon/PowerScale storage below the version 8.2 manually (without using the**configure_ifs.sh** script), make sure that auditing of the `success create` events is **disabled**.

  For Dell Isilon/PowerScale storage below the version 8.2, the storage system logging will become too verbose, which may lead to data collector overload with excessive events, decrease its performance and result in data collection errors with the "*Timeout expired*" message issued.

  For Dell Isilon/PowerScale storage 8.2 and above, this option for manual audit configuration can be safely enabled.

- Auditing of the *System* zone is not supported. As stated by Dell, this zone should be reserved for configuration access only. Current data should be stored in other access zones. See the Isilon OneFS 8.2.1 CLI Administration Guide for additional information.

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 the Configure Dell Isilon/PowerScale Cluster in Compliance Mode Via Shell Script topic for additional information.
- Manual configuration. See the Configure Dell Isilon/PowerScale Cluster in Compliance Mode Manually topic for additional information.

Configure Dell Isilon/PowerScale Cluster in Compliance Mode Via Shell Script

Follow the steps to configure Dell Isilon/PowerScale cluster in Compliance mode via the shell script:

Step 1 – On the computer where 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.

Step 2 – Navigate to your cluster command prompt through the SSH connection.

Step 3 – Log in to your cluster as a **compadmin** user.

Step 4 – Run the shell script by executing the following command:

```
sh /ifs/data/configure_ifs.sh -z zone1 -a 1
```

where

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

`1` 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

Step 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
```

Step 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
```

Step 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.

Configure Dell Isilon/PowerScale Cluster in Compliance Mode Manually

Follow the steps to configure Dell Isilon/PowerScale cluster in Compliance mode manually:

Step 1 – Navigate to your cluster command prompt through the SSH connection.

Step 2 – Log in to your cluster as a **compadmin** user.

Step 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
```

Step 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
```

Step 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.

Step 6 – Enable protocol auditing for a selected zone (for example, *"zone1"*). Do one of the following, depending on your Dell Isilon/PowerScale version:

EMC Isilon/PowerScale 7.x	EMC Isilon/PowerScale 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/PowerScale 7.x	EMC Isilon/PowerScale 8.2 and above
Successful changes	
`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, create`
Failed change attempts	
`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,open`
Successful reads	
`isi zone zones modify zone1 --audit-success=read`	`isi audit settings modify -- zone=zone1 --audit-success=read`
Failed read attempts	
`isi zone zones modify zone1 --audit-failure= create,read`	`isi audit settings modify --zone=zone1 --audit-failure=create,read, open`

Step 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"
```

Permissions for Dell Isilon/PowerScale Auditing

Before you start creating a monitoring plan to audit your Dell Isilon/PowerScale file storage system, plan for the account that will be used for data collection. See the Configuring Your Dell Isilon/PowerScale Cluster for Auditing section for additional information. The following scenarios are possible:

- Automatic configuration: you can use a special shell script for configuring an audited Dell Isilon/PowerScale cluster and granting necessary privileges to the account used to collect audit data. See the following topics for additional information:
  - Configure Dell Isilon/PowerScale Cluster in Compliance Mode Manually
  - Configure Dell Isilon/PowerScale Cluster in Normal or Enterprise Mode via Shell Script
- Manual configuration: you can grant all the necessary permissions to data collecting account manually. See the following topics for additional information:
  - Configure Dell Isilon/PowerScale Cluster in Compliance Mode Via Shell Script
  - Configure Dell Isilon/PowerScale Cluster in Normal or Enterprise Mode Manually

For manual configuration, 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 **Dell Isilon/PowerScale** 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

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

Configuring Your Dell Isilon/PowerScale Cluster for Auditing

A Dell Isilon/PowerScale cluster can operate in one of the following modes:

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

For your convenience, Netwrixprovides a special shell script for configuring an audited Dell Isilon/PowerScale cluster and granting necessary privileges to the account that is used to collect audit data.

To grant the necessary permissions to Isilon/PowerScale data collecting account manually, you need to perform all steps for manual audit configuration, otherwise the product will not function properly.

See the Normal and Enterprise Modes for Clusters topic for additional information.

NetApp Data ONTAP

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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.

    - To use this option for NetApp Clustered Data ONTAP 8 or ONTAP 9, make sure that audit configuration has been created (with `vserver audit create` command) for the target system enabling audit configuration is optional.

- Manually – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - On the NetApp device:
        - 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 Clustered Data ONTAP 8 and ONTAP 9:
            - `External Web Services: true`.

              RECOMMENDED: For security reasons, enable only SSL access.

            - Firewall policy for data interfaces must be configured to allow ONTAPI protocol connections.
            - Audit settings must be configured as follows:

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

        - On Data ONTAP 7 and Data ONTAP 8 in 7-mode:

- The `httpd.admin.enable` or the `httpd.admin.ssl.enable` option must be set to *"on"*. For security reasons, it is recommended to configure SSL access and enable the `httpd.admin.ssl.enable` option.
- The `cifs.audit.liveview.enable` option must be set to *"off"*.
- The `cifs.audit.enable` and the `cifs.audit.file_access_events.enable` options must be set to *"on"*.
- Unless you are going to audit logon events, the `cifs.audit.logon_events.enable` and the `cifs.audit.account_mgmt_events.enable` options must be set to *"off"*.
- The Security log must be configured:
  - `cifs.audit.logsize 300 000 000 (300 MB)`
  - `cifs.audit.autosave.onsize.enable on`
  - `cifs.audit.autosave.file.extension timestamp`

- 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 Extended Attributes
  - Delete Subfolders and Files
  - Delete
  - Change Permissions
  - Take Ownership

◦ On the Auditor console computer:

- 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 Auditor Server.

See the following topics for additional information:

- Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring
- Configure Audit Settings for CIFS File Shares

The following table lists the actions that can be performed on NetApp:

Added	+	+	+
Add (failed attempt)	–	–	–
Modified	+	+	+
Modify (failed attempt)	+	+	–
Moved	+*	+*	–
Move (failed attempt)	+*	+*	–
Read	+	-	–
Read (failed attempt)	+	+	–
Renamed	+*	+*	–
Renamed (failed attempt)	+*	+*	–
Removed	+	+	+
Remove (failed attempt)	+	+	–
Copied	–	–	–

Actions marked with an asterisks (*) are reported for NetApp Clustered Data ONTAP 8 and ONTAP 9 only.

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\RESTAPI Web Access
- Configure System Service Firewall Policies
- Configure Service Policy
- Configure Event Categories and Log

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 - 9.10	• ONTAP 9 Documentation Center

Perform the following steps before proceeding with the audit configuration.

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

NOTE: NFS file shares are not supported.

Step 2 – Configure System Access Control List (SACL) on your file share. See Configure Audit Settings for CIFS File Shares topic for additional information.

Step 3 – Set the Security Style for Volume or Qtree where the audited file shares are located to the *"ntfs"* or *"mixed"*.

Step 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.

Configure ONTAPI\RESTAPI 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 management 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

   where `'cluster1'` is the name of your NetApp ONTAP cluster.

External Web Services:	true
Status:	online
HTTP Protocol Port:	80
HTTPs Protocol Port:	443
TLSv1 Enabled:	true
SSLv3 Enabled:	true
SSLv2 Enabled:	false

   If the result of the `External Web Services` command is `'false'`, execute the following:

```
cluster1::> system services web modify -external true
```

3. Enable ONTAPI access on the 'Storage VM' (SVM) where CIFS server is installed. Run the following command where svm1 is the name of your SVM:

```
cluster1::> vserver services web modify -vserver svm1 -name ontapi
-enabled true

cluster1::> vserver services web show -vserver svm1.
```

Vserver	Type	Service Name	Description	Enabled
svm1	data	ontapi	Remote Administrative API	true
			Support	
svm1	data	rest	Remote Administrative API	true
			Support	

4. To display the current settings of web services for SVM svm1, use the following command:

   ```
   cluster1::> vserver services web show -vserver svm1
   ```

   Review the Permissions for NetApp Auditing topic for additional information on how to create the role and enable AD user access.

   Enable HTTP/HTTPS access. For example:

   ONTAPI

   ```
   cluster1::> vserver services web modify -vserver svm1 -name ontapi
   -enabled true
   ```

   RESTAPI

   ```
   cluster1::> vserver services web modify -vserver svm1 -name rest
   -enabled true
   ```

   Enable only SSL access (HTTPS in Netwrix Auditor). For example:

   ONTAPI

   ```
   cluster1::> vserver services web modify -vserver svm1 -name ontapi
   -enabled true -ssl-only true
   ```

   RESTAPI

   ```
   cluster1::> vserver services web modify -vserver svm1 -name rest
   -enabled true -ssl-only true
   ```

5. Make sure that the custom role (e.g., netwrix_role for ONTAPI or netwrix_rest_role for RESTAPI) assigned to your account specified for data collection can access ONTAPI or RESTAPI. See Permissions for NetApp Auditing topic for additional information.

```
cluster1::> vserver services web access show -name ontapi -vserver
svm1

cluster1::> vserver services web access show -name rest -vserver svm1
```

Vserver	Type	Service Name	Role
svm1	data	ontapi	netwrix_role
svm1	data	ontapi	vsadmin
svm1	data	ontapi	vsadmin-protocol
svm1	data	ontapi	vsadmin-readonly
svm1	data	ontapi	vsadmin-volume
5 entries were displayed.			

Configure System Service Firewall Policies

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:

NOTE: For NetApp ONTAP 9.10.1 and higher, the command context system services firewall policy is deprecated and might be removed in a future ONTAP release. Review the NetApp ONTAP 9.10.1 commands article for additional information.

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`

To...	Execute...
	netwrix_policy -service http -vserver svm1 -action allow -ip-list 192.168.1.0/24 cluster1::> system services firewall policy create -policy netwrix_policy -service https -vserver svm1 -action allow -ip-list 192.168.1.0/24
Modify existing policy	cluster1::> system services firewall policy modify -policy netwrix_policy -service http -vserver svm1 -action allow -ip-list 192.168.1.0/24 cluster1::> system services firewall policy modify -policy netwrix_policy -service https -vserver svm1 -action allow -ip-list 192.168.1.0/24
NetApp Clustered Data ONTAP 8.3, ONTAP 9.0 - 9.10	
Create a policy	cluster1::> system services firewall policy create -policy netwrix_policy -service http -vserver svm1 -allow-list 192.168.1.0/24 cluster1::> system services firewall policy create -policy netwrix_policy -service https -vserver svm1 -allow-list 192.168.1.0/24
Modify existing policy	cluster1::> system services firewall policy modify -policy netwrix_policy -service http -vserver svm1 -allow-list 192.168.1.0/24 cluster1::> system services firewall policy modify -policy

To...	Execute...
	`netwrix_policy -service https -vserver svm1 -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 svm -lif vs1-cifs-lif1 -firewall-policy netwrix_policy
   ```

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

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

Configure Service Policy

NOTE: This paragraph only applies to NetApp ONTAP version 9.10.1 and higher.

By default, the 'default-data-files' policy is applied to the SVM CIFS/SMB interface and HTTP/HTTPS options are not available. To make the ONTAPI available through HTTP/HTTPS ports on your SVM interface for Netwrix Auditor Server, configure the 'interface service'-policy. Below is an example of the configuration:

1. Navigate to your cluster command prompt through the SSH/Telnet connection.
2. Log in as a cluster administrator and review your current service-policy configuration. Run the following command:

   ```
   cluster1::> network interface show -vserver svm1 -fields service-policy
   ```

   Example output:

   ```
   vserver lif service-policy

   ---------- ---------------- ------------------

   svm1 lif_svm1_126 default-data-files

   svm1 lif_svm1_349 default-data-files
   ```

Where `svm1` – is the name of your SVM,

The `lif_svm1_126` and `lif_svm1_349` parameter is the `svm1` logical interface.

The `default-data-files` parameter is the service-policy applied to lif-s.

3. To display the services available through the '`default-data-files`' policy, run the following command:

```
cluster1::> network interface service-policy show -vserver svm1
-policy default-data-files
```

Example output:

```
Vserver: svm1

Policy Name: default-data-files

Included Services: data-core, data-cifs, data-fpolicy-client, data-
dns-server

Service: Allowed Addresses: data-core: 0.0.0.0/0

data-cifs: 0.0.0.0/0

data-fpolicy-client: 0.0.0.0/0

data-dns-server: 0.0.0.0/0
```

4. Set the advanced privilege level to be able to create and modify the service-policy. Run the following command:

```
cluster1::> set -privilege advanced
```

Remember, The command prompt should be changed to "`cluster1::*>`"

5. Clone the existing '`default-data-files`' LIF policy to be able using shares with a new service-policy. Run the following command:

```
cluster1::*> network interface service-policy clone -vserver svm1
-policy default-data-files -target-policy netwrix-policy -target-
vserver svm1
```

Where the '`netwrix-policy`' parameter is the name of new service-policy.

6. Modify the new service-policy by adding services to access over http\https protocols. Run the following command:

```
cluster1::*> network interface service-policy add-service -vserver
svm1 -policy netwrix-policy -service management-http

cluster1::*> network interface service-policy add-service -vserver
svm1 -policy netwrix-policy -service management-https
```

7. Return to the administrator privilege level. Run the following command:

```
cluster1::*> set -privilege admin
```

8. Apply a new service-policy to the SVM LIFs. Run the following command:

```
cluster1::> network interface modify -vserver svm1 -lif lif_svm1_126
-service-policy netwrix-policy

cluster1::> network interface modify -vserver svm1 -lif lif_svm1_349
-service-policy netwrix-policy
```

   NOTE: For better security, specify the allowed ip-addresses when adding the service. Double-check that your subnet is configured on the machine where Netwrix Auditor Server resides. Allowed-addresses are: 192.168.1.0/24.

9. Check the current interface service-policy using command from the step 2:

```
cluster1::> network interface show -vserver svm1 -fields service-
policy
```

   Example output:

```
vserver lif service-policy

---------- ---------------- -------------

svm1 lif_svm1_126 netwrix-policy

svm1 lif_svm1_349 netwrix-policy
```

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 (SVM). 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 `svm1`:

   ```
   cluster1::> vserver context -vserver svm1
   ```

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

   ```
   svm1::>
   ```

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

   ```
   svm1::> vserver audit create -destination <path to the volume>
   ```

   In the example above, the `vserver audit create -destination /audit` command executed on the `svm1` SVM creates and enables audit on the volume `/audit`.

   Netwrix Auditor accesses audit logs via file shares. Make sure the volume you specified is mounted on SVM and shared (e.g., `audit$` is a share name and its path is `/audit`).

4. Enable audit:

   ```
   svm1::> vserver audit enable
   ```

5. Add categories of events to be audited:

   - For ONTAPI 9.0 or later

     ```
     svm1::> vserver audit modify -events file-ops, file-share
     ```

   - For ONTAPI 8.3 and below

     svm1::> vserver audit modify -events file-ops

6. Check the following options:

Option	Setting
`Auditing State`	`true`
`Categories of Events to Audit`	`file-ops` 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-policy-change`. For ONTAP 8.3, just check `file-ops`.
Log Format	"XML" or "EVTX"

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

   svm1::> 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 the Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS.

8. After configuration, double-check your settings.

   ```
   svm1::> 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-policy-change`.

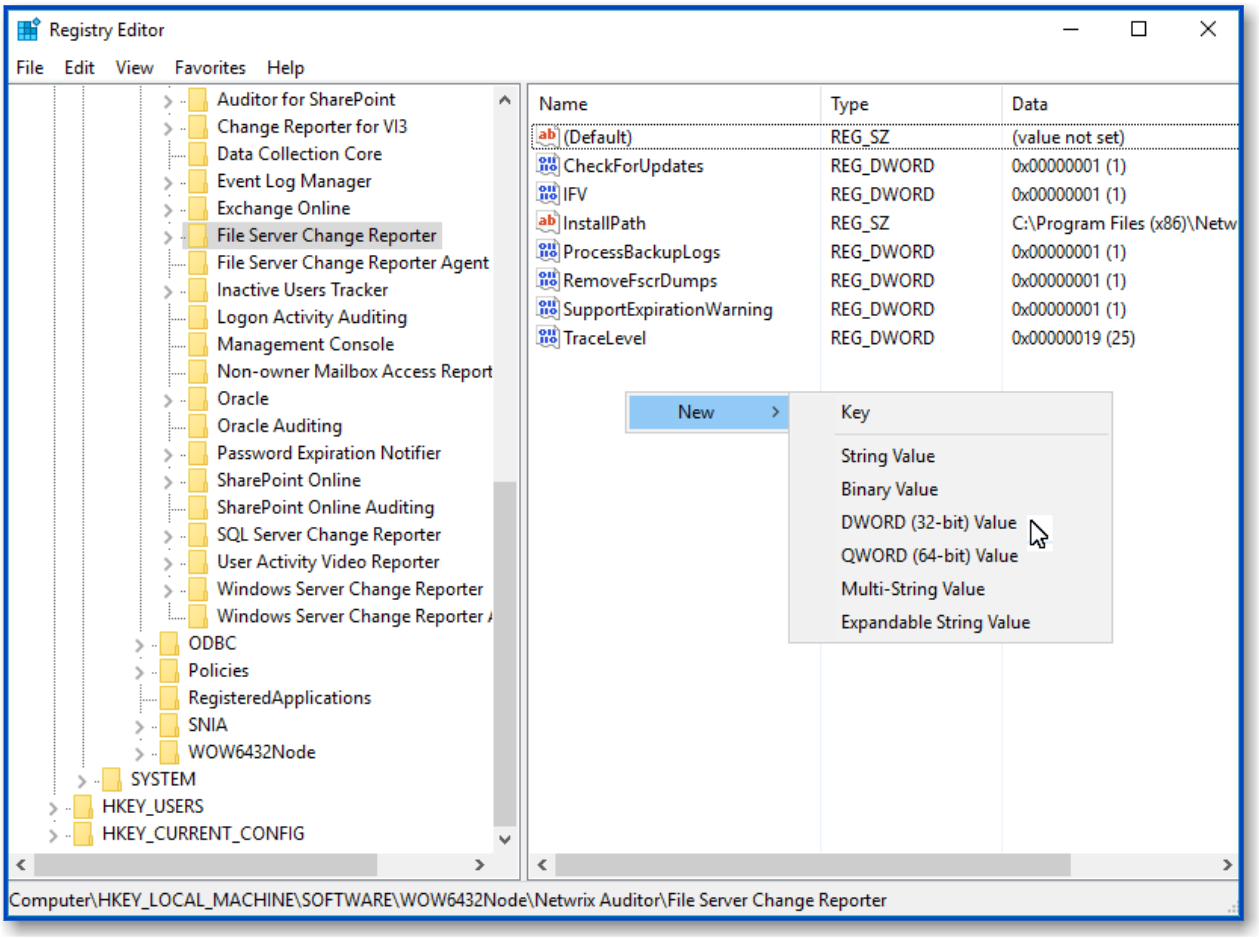
For ONTAP 8.3, just check `file-ops`.

To configure logs retention period

NOTE: This instruction is only effective for NetApp versions older than 8.2.1.

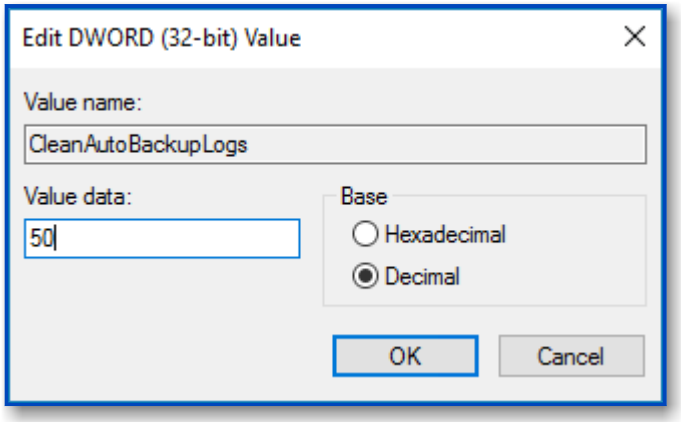
1. On the computer where Auditor Server resides, open Registry Editor: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File Server Change Reporter**.
3. In the right-pane, right-click and select New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

   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.

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. 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. 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.

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. See File Servers topic for additional information.

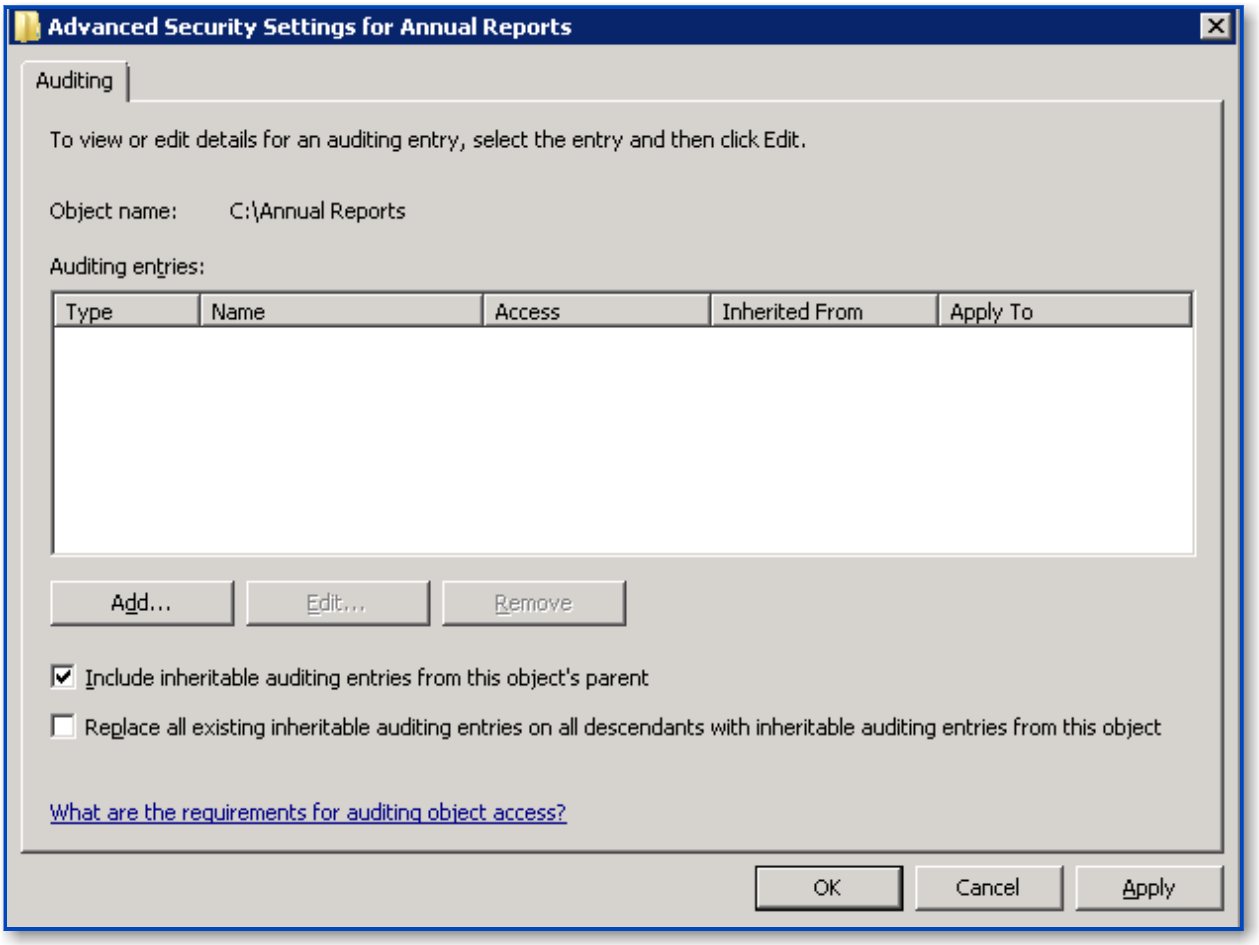
Do one of the following depending on the OS:

- 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**.

   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**.

   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.

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

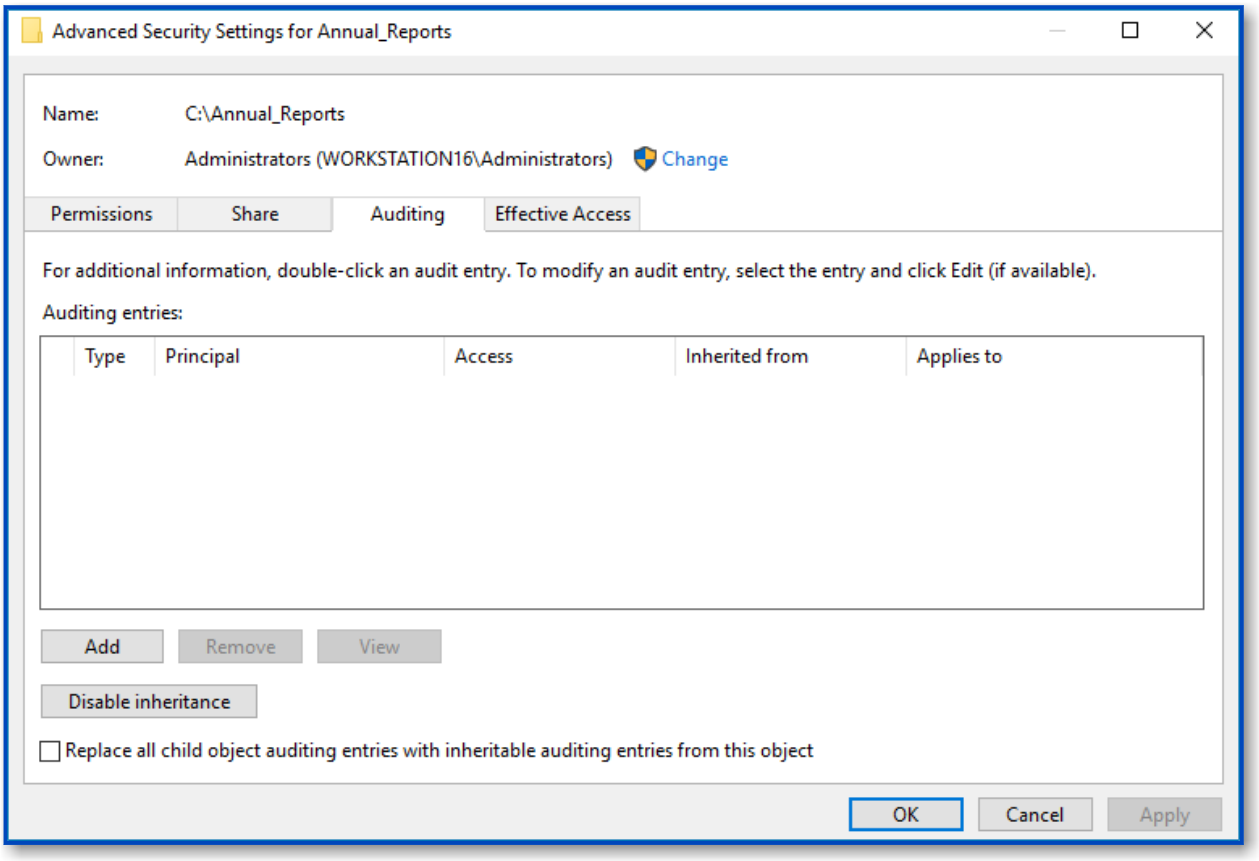
Auditing Entry
• Apply onto—Select *"Files only"*. • Check *"Successful"* and *"Failed"* next to List folder / read data. • Make sure that the **Apply these auditing entries to objects and/or containers within this container only** checkbox is cleared.
Successful changes
The Auditing Entry below shows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

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

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

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

   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. 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.

   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.

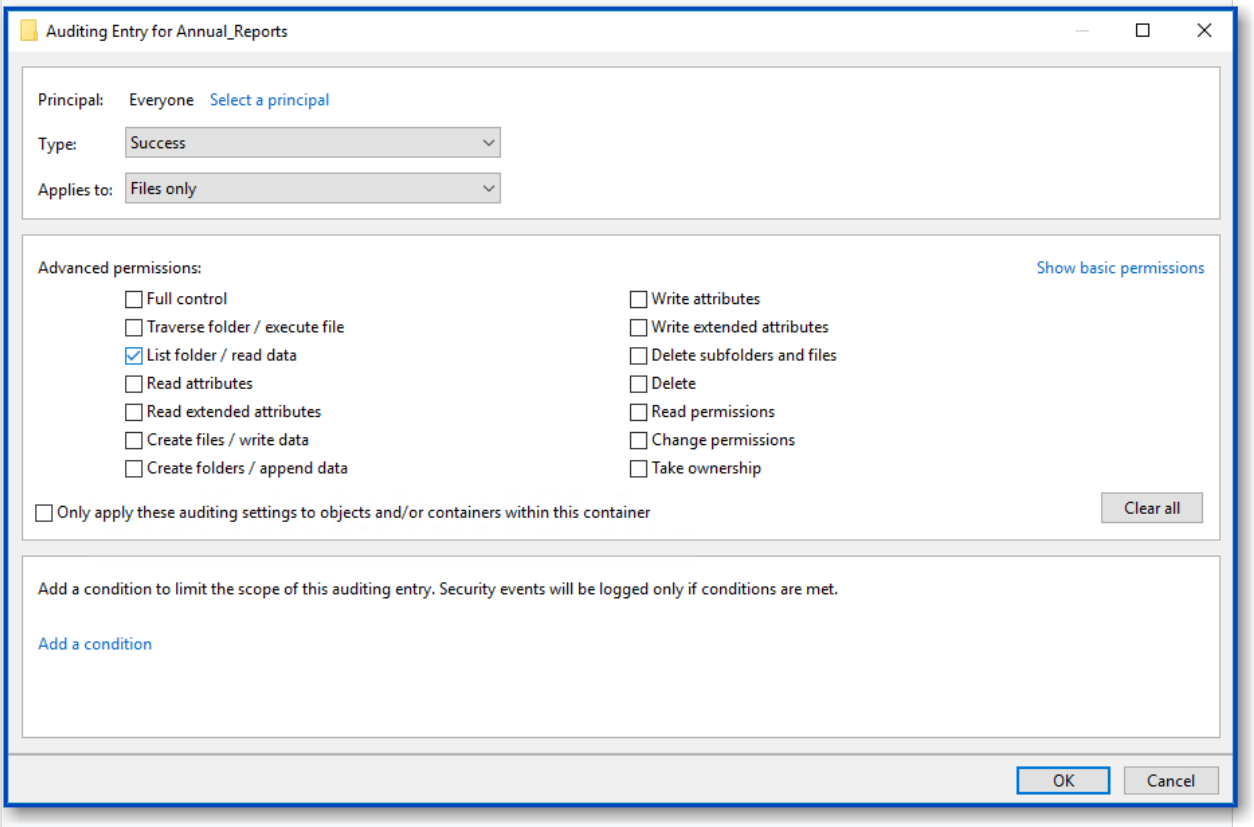
6. Apply settings to your Auditing Entries depending on actions that you want to audit. If you want to audit all actions (successful reads and changes as well as failed read and change attempts), you need to add three separate Auditing Entries for each file share. Otherwise, reports will contain limited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

   - Successful reads
   - Successful changes
   - Failed read attempts
   - Failed change attempts

Auditing Entry	

Successful reads

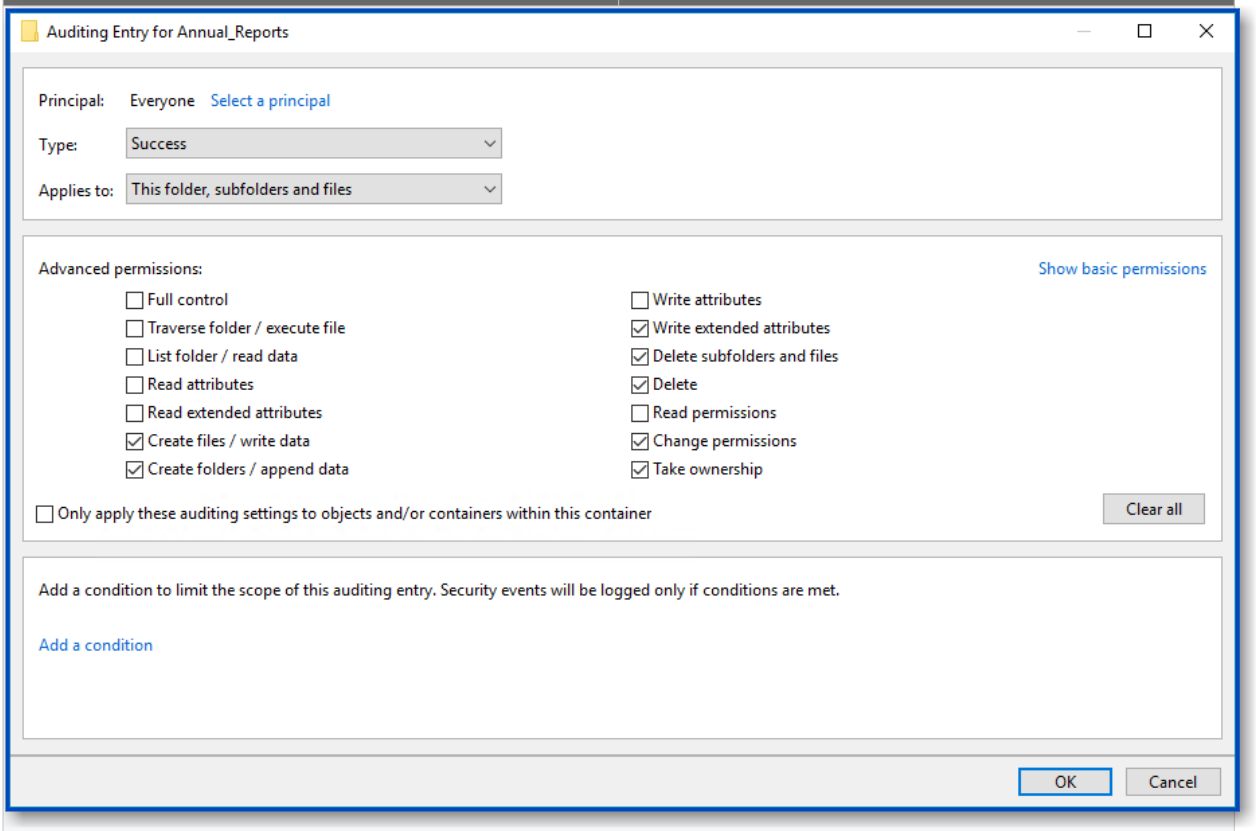
The Auditing Entry below shows Advanced Permissions for auditing successful reads only:

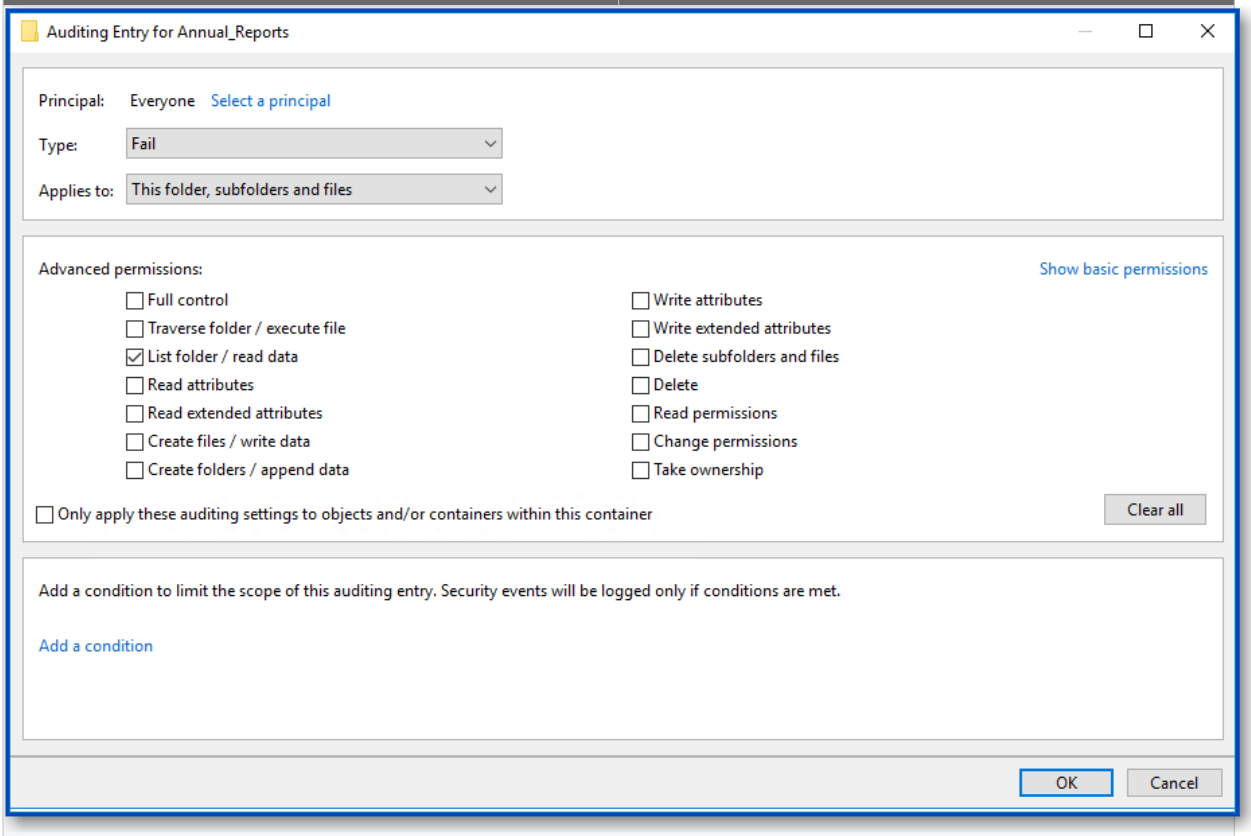


- Type—Set to*"Success"*.
- Applies to—Set to*"Files only"*.
- Advanced permissions—SelectList folder / read data.
- Make sure that theOnly apply these auditing settings to objects and/or containers within this containercheckbox is cleared.

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 theOnly apply these auditing settings to objects and/or containers within this containercheckbox is cleared.	
Failed read attempts	
The Auditing Entry below shows Advanced Permissions for auditing failed read attempts:	

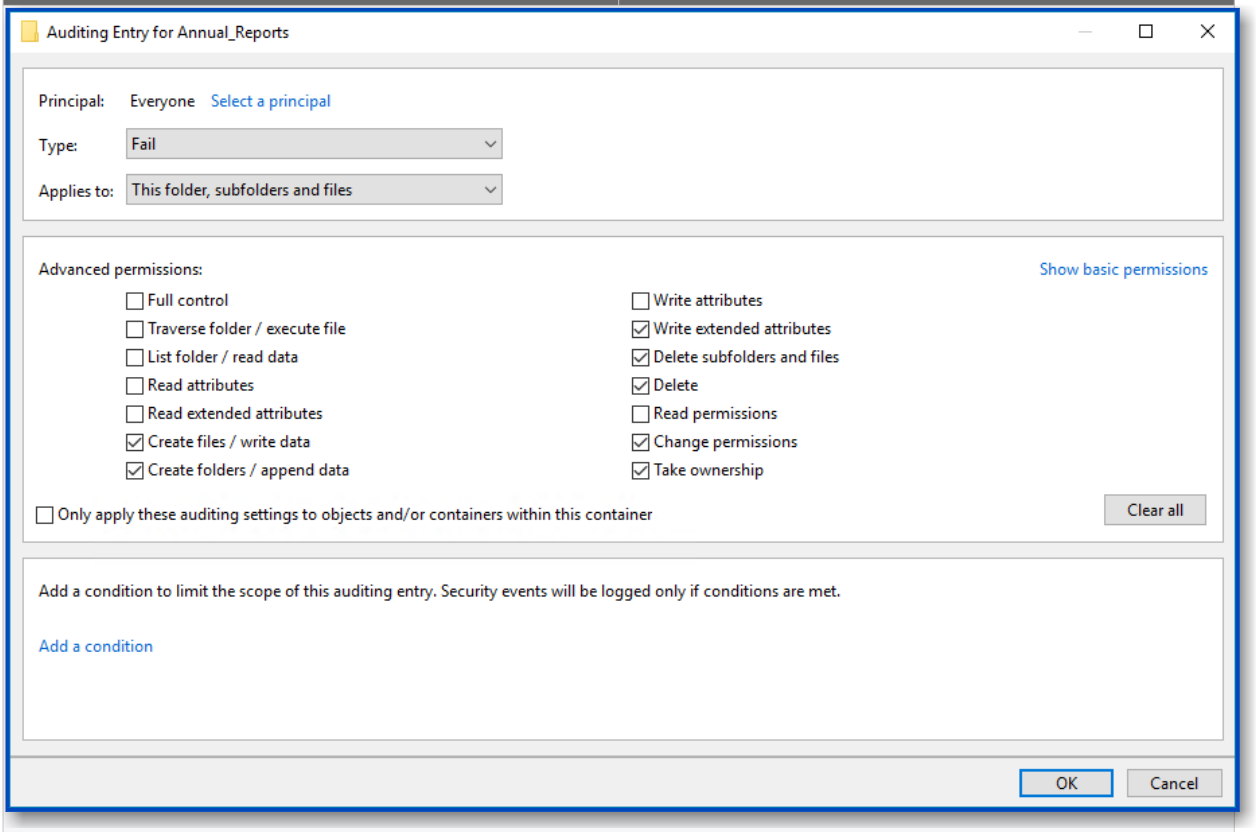
Auditing Entry	
	

- Type—Set to*"Fail"*.
- Applies to—Set to*"This folder, subfolders and files"*.
- Advanced permissions—SelectList folder / read data.
- Make sure that theOnly apply these auditing settings to objects and/or containers within this containercheckbox 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 theOnly apply these auditing settings to objects and/or containers within this containercheckbox is cleared.

To audit successful changes on NetApp 8.x or earlier, also selectWrite Attributesin the**Advanced permissions**list in the auditing entry settings.

Permissions 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.

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

The following permissions are required for the account on the target server:

- The account must be a member of the Local Administrators group.
- The account must be a member of the BUILTIN\Administrators group.
- The account requires the following **NTFS** permissions:
  - List folder / read data
  - Read attributes
  - Read extended attributes
  - Read permissions
- The account requires the following share permissions:
  - Read
- The account requires the following NTFS and share permissions:
  - Read permission on the audit logs folder and its content.
  - Delete permission on the audit log folder content.
- 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 ◦ volume ◦ vserver audit ◦ vserver audit rotate-log ◦ vserver cifs	readonly readonly all all

	readonly

The following permissions are required for the account on the Netwrix Auditor server:

- The account must be a member of the Local Administrators group.

See Create Role on NetApp Clustered Data ONTAP 8 or ONTAP 9 and Enabling AD User Access section for additional information.

Remember, that you can also assign the built-in *vsadmin* role instead of the permissions above.

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

NOTE: This article applies to NetApp 8.3.2 and later. You must be a **cluster administrator** to run the commands below.

Follow the steps to create a role for enabling AD user access:

Step 1 – Create a new role (e.g., netwrix_role for ONTAPI and netwrix_rest_role for RESTAPI) on your SVM (e.g., svm1). For example:

Create ONTAPI role:

```
security login role create -role netwrix_role -cmddirname version -acces
s readonly -vserver svm1security login role create -role netwrix_role -c
mddirname volume -access readonly -vserver svm1security login role creat
e -role netwrix_role -cmddirname "vserver audit" -access all -vserver sv
m1security login role create -role netwrix_role -cmddirname "vserver aud
it rotate-log" -access all -vserver svm1
```

NOTE: This option is required for auto audit configuration.

```
security login role create -role netwrix_role -cmddirname "vserver cifs"
 -access readonly -vserver svm1
```

Create RESTAPI role:

```
security login rest-role create -role netwrix_rest_role -api /api/svm/sv
ms -access read_create_modify -vserver svm1 security login rest-role cre
ate -role netwrix_rest_role -api /api/protocols/audit -access read_creat
e_modify -vserver svm1 security login rest-role create -role netwrix_res
t_role -api /api/storage/volumes -access readonly -vserver svm1 security
 login rest-role create -role netwrix_rest_role -api /api/protocols/cifs
/shares -access readonly -vserver svm1
```

NOTE: The commands in the first two lines above can be used on NetApp versions 9.11+. In earlier versions, use the following commands:

```
security login rest-role create -role netwrix_rest_role -api /api/svm/sv
ms -access all -vserver svm1security login rest-role create -role netwri
x_rest_role -api /api/protocols/audit -access all -vserver svm1
```

Step 2 – The capabilities must be assigned one by one. To review currently applied capabilities, you can use the following command:

ONTAPI role:

```
security login role show -vserver svm1 -role netwrix_role
```

RESTAPI role:

```
security login rest-role show -vserver svm1 -role netwrix_rest_role
```

Step 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:

NOTE: In ONTAP 9.10 and higher, it is not possible to assign ONTAPI role (e.g. netwrix_role) and RESTAPI role (e.g. netwrix_rest_role) to one AD user. To allow a user access to both the ONTAPI and RESTAPI, you can use different AD groups by assigning roles to them and including the user in these groups.

Create login for ONTAPI role:

```
security login create -vserver svm1 -user-or-group-name domain\user -app
lication ontapi -authmethod domain -role netwrix_role
```

Create login for RESTAPI role:

```
security login create -vserver svm1 -user-or-group-name domain\user -app
lication http -authmethod domain -role netwrix_rest_role
```

where `domain\user` is your data collecting account.

Remember, that 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 (required for the product to adjust audit settings automatically)
- vserver audit rotate-log all
- vserver cifs readonly

The role you set up for working with RESTAPI must have the following attributes:

- /api/svm/svms read_create_modify
- /api/protocols/audit read_create_modify
- /api/storage/volumes readonly
- /api/protocols/cifs/shares readonly

Nutanix

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - To allow inbound connections to Netwrix Auditor server from Nutanix File Server, a TCP port must be open:

    - For the first Nutanix File Server you configure for auditing, the **TCP 9898** port will be used.
    - For each subsequent server, a new TCP port must be open.
  - Target Nutanix File Server must be located in the same subnet as Netwrix Auditor Server and must be configured as described in the Nutanix section.

Manual Configuration

To configure your Nutanix File Server for monitoring SMB shares, you will need to do the following:

Step 1 – Create a user account to access the Nutanix REST API. See the Create User Account to Access Nutanix REST API topic for additional information.

Step 2 – Open a port for inbound connections. See the Nutanix Ports topic for additional information.

In addition, configure the Auditor console server as a partner server for Nutanix Files, and create a notification policy to make Netwrix Auditor aware of the Nutanix events. These operations can be performed in any of the following ways:

- Automatically when creating a monitoring plan. For that, you should select the **Adjust audit settings automatically** option in the monitoring plan wizard. See the Settings for Data Collection topic for additional information.
- Manually, as described in the corresponding topics:
  - Configure Partner Server
  - Create a Notification Policy

Remember that in both cases (automatic or manual configuration) you will need to complete the steps above to ensure that the user account for accessing REST API is created and the listening port on Netwrix Auditor Server is open for inbound connections.

Nutanix Files

The following table lists the actions that can be performed with Nutanix Files:

Added	+	+	+
Add (failed attempt)	+	+	–
Modified	+	+	+

Modify (failed attempt)	+	+	–
Moved	+	+	–
Move (failed attempt)	–	–	–
Read	+	+	–
Read (failed attempt)	+	+	–
Renamed	+	+	–
Renamed (failed attempt)	–	–	–
Removed	+	+	+
Remove (failed attempt)	+	+	–
Copied	–	–	–

The following considerations refer to Nutanix Files auditing and reporting:

- All changes performed on Nutanix File Shares initiated from the machine(s) where Auditor Server resides, will not displayed in Netwrix search and reports because Nutanix Files unable to generate such Activity Records for Auditor.
- Auditing of NFS file shares in not supported due to known limitations.
- Currently, not every detail about permission and attribute changes may be provided by Nutanix Files, so they cannot be reported by Auditor.
- As for the state-in-time data collection, note that effective permissions (as a combination of NTFS and Shared permissions) are not calculated properly for the local Administrator group members.

Nutanix Ports

Follow the steps to open Nutanix port for inbound connections.

Step 1 – On a target computer navigate to **Start** > **Control Panel** and select **Windows Firewall.**

Step 2 – In the Help Protect your computer with Windows Firewall page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select Inbound Rules on the left.

Step 4 – Click New Rule. In the New Inbound Rule wizard, complete the steps as described below.

Option	Setting
Rule Type	Port
Protocols and Ports	• Does this rule applies to TCP or UDP—Select TCP • Specific local ports—Type required port, e.g., 9898.
Action	Select Allow the connection
Profile	Applies to Domain
Rule name	Rule name, for example Nutanix Files inbound rule.

When you add the first item (*Nutanix SMB shares*) to the Nutanix monitoring plan, you will be suggested to use port **9898**. For the next *Nutanix SMB shares* added as an item, you should specify a different TCP port and configure it for inbound connections, as described above.

Protocols and Ports Required for Monitoring Nutanix Files

Review a full list of protocols and ports required for Netwrix Auditor for Nutanix Files.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to the remote ports on the computer where Netwrix Auditor Server resides.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 9898 TCP port.

Port	Protocol	Source	Target	Purpose
9898	TCP	Monitored Nutanix Files devices	Netwrix Auditor Server	Getting events from monitored devices

NOTE: You need to open the 9898 TCP port for inbound connections manually.

Later, you can specify any custom TCP port when editing your Nutanix Files monitoring plan. See the File Servers (Nutanix section) for more information.

Create User Account to Access Nutanix REST API

To create a user account using the ncli utility:

1. Download and install the *ncli* (Nutanix command-line interface) on any server in your infrastructure, as described here.
2. Start the utility and establish a *ncli* session by the following command:

   ```
   ncli -s management_ip_addr -u 'username' -p 'user_password'
   ```

   here:

   - `management_ip_addr` - the IP address of any Nutanix Controller VM in the cluster
   - `username` - user name to access that VM; if not specified, *admin* (default name) will be used
   - `user_password` - password to access that VM
3. Run the `fs list` command in *ncli* to get the list of Nutanix Files servers.
4. Locate the name of Nutanix Files server you want to audit; locate and save the following server parameters to a text file:
   - **Uuid** - Nutanix Files server ID
5. Finally, create a new user and specify credentials that will be used to access this Nutanix Files server. For that, run the following command in *ncli* :

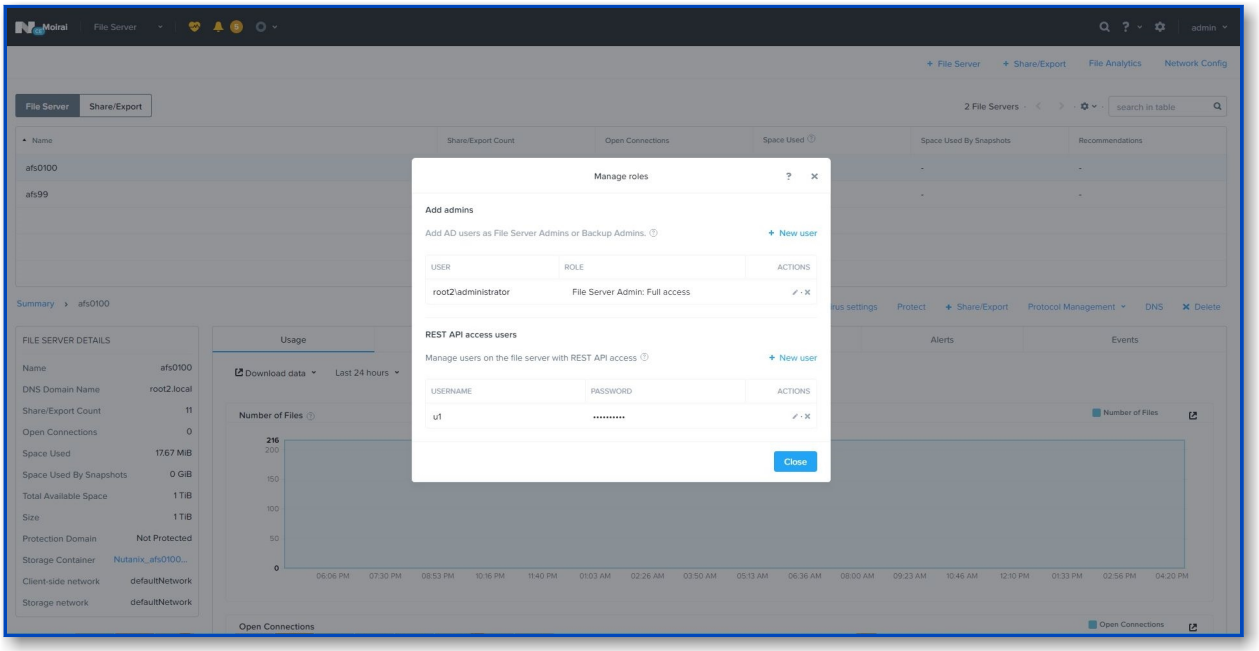
   ```
   fs add-user uuid=<fs_uuid> user=<username> password=<password>
   ```

   here:

   - `<fs_uuid>` - Nutanix Files server ID (Uuid)
   - `<username>` - user name
   - `<password>` - password

To create a new user account with Nutanix Prism:

1. Open Nutanix Prism web portal.
2. Select **File Server** category. In the list of servers, select the server you want to audit.
3. Click **Manage roles**.
4. In the **Manage roles** dialog locate the **REST API access user** section and click **+New user**.



5. Enter local user account name and password, then click **Save** next to them to save the settings.
6. Click the **Close** button to close the **Manage roles** dialog.

Configure Partner Server

To start monitoring files and folders on Nutanix File Server, you should configure Netwrix Auditor Server as a partner server for Nutanix File Server.

This configuration procedure involves creation of API requests and assumes that you have an good understanding of REST API concept, as well as experience in working with JSON-formatted requests in some API client. To get acquainted with Nutanix REST API Explorer client, refer to Nutanix documentation

To create a partner server for Nutanix File Server via API:

1. Open the **File Server REST API Explorer** REST API client using the following URL: `https://<fileserver_ip>:9440/api/nutanix/v3/api_explorer/index.html#/` here `<fileserver_ip>` - IP address of the Nutanix File Server to be audited.

If you select to launch the RestAPI Explorer from the Prism menu, the **RestAPI Explorer for Prism** server will be opened.

2. In the **username** and **password** fields, enter the credentials of the Create User Account to Access Nutanix REST API you have created.
3. Click **Explore**.
4. Locate the POST request for **partner_servers** endpoint: `POST /partner_servers`

5. In the request body, enter the following JSON-formatted structure:

```
{
"spec": {
"name": "<NAME_OF_PARTNER_SERVER>",
"resources": {
"usage_type": "NOTIFICATION",
"vendor_name": "netwrix",
"server_info": {
"server_type": "PRIMARY",
"address": {
"ip": "<IP_OF_THE_NETWRIX_AUDITOR>",
"port": 9898
}
}
}
},
"api_version": "3.0",
```

"metadata": {

"kind": "partner_server"

}

}

here:

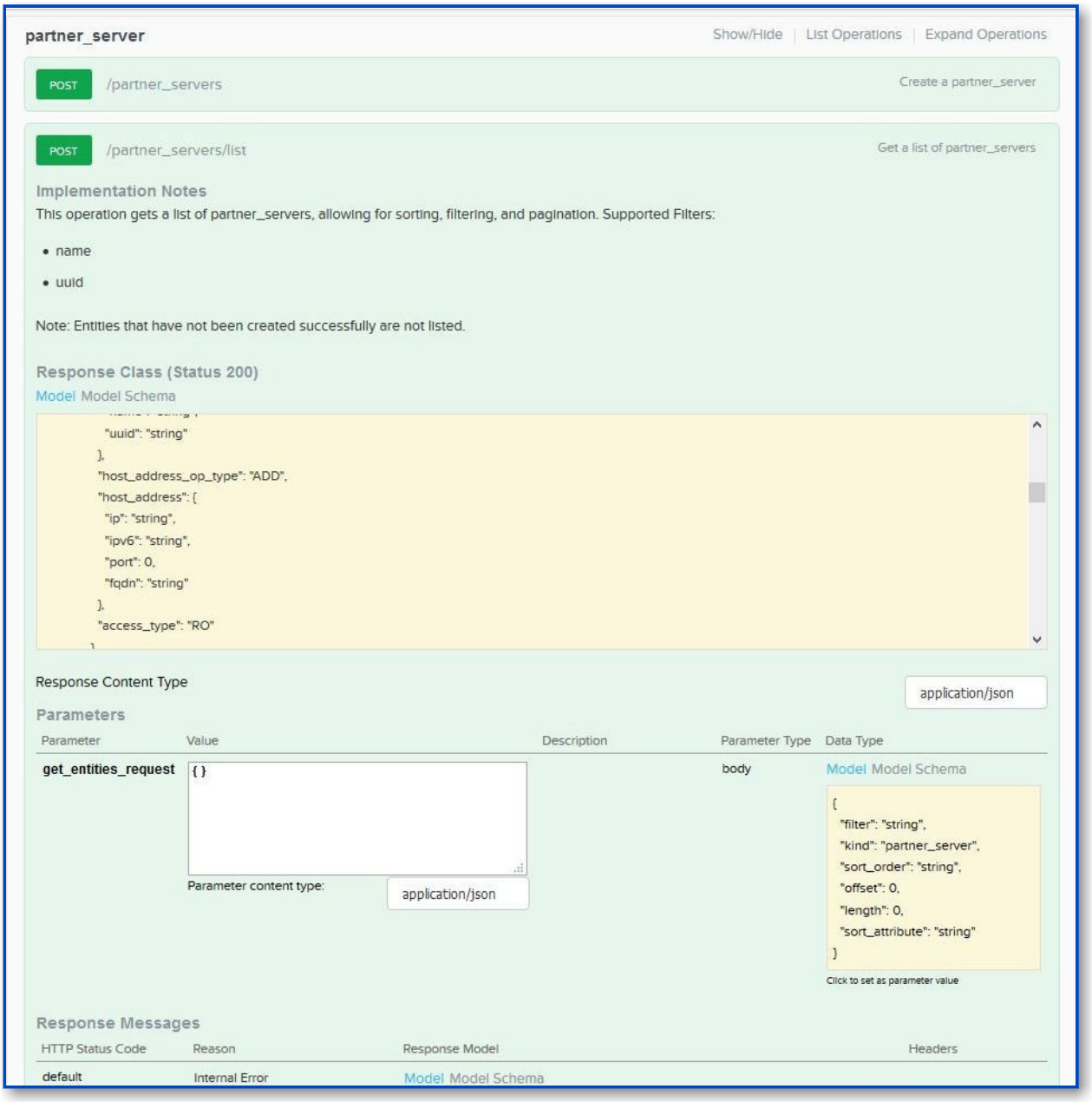
<*NAME_OF_PARTNER_SERVER*> - enter the Netwrix Auditor server name

<*IP_OF_NETWRIX_AUDITOR*> - enter the Netwrix Auditor server IP address

This address must be visible from the Nutanix File Server network.

6. Send the request, clicking **Try it out**.
7. Get the response - `Response Code` should be *200*. In the response body, locate the `uuid` of the created partner server.
8. To check that a new partner server was included in the list of existing partner servers, retrieve the list of servers, sending the POST request to the following endpoint: `POST /partner_servers/list`

   The request body must be empty - for that, enter empty brackets as the **value** for *get_entities_request* parameter: { }



9. The response body should contain the list of servers, including new partner server name and other settings.

Create a Notification Policy

To monitor operations with files and folders on Nutanix File Server, you should configure a notification policy for the related events.

Monitored Operations

The list of supported operations is provided in the table below. Your notification policy can include any of them.

To audit...	Operation name to specify at policy creation
Successful *create* operations	FILE_CREATE DIRECTORY_CREATE
Successful *read* operations	FILE_READ
Successful *modify* operations	FILE_WRITE RENAME SECURITY
Successful *delete* operations	FILE_DELETE DIRECTORY_DELETE
Failed *read/modify/delete* attempts*	FILE_OPEN

* - Failed attempt to move/rename file are not audited.

Configuration Procedure

Notification policy creation procedure involves API requests usage. It is assumed that you have a good understanding of REST API concepts, as well as enough experience in working with JSON-formatted requests in any API client. To get acquainted with Nutanix REST API Explorer client, refer to Nutanix documentation.

To create a notification policy for Nutanix File Server via API:

1. Open the **File Server REST API Explorer** client using the following URL: `https://<fileserver_ip>:9440/api/nutanix/v3/api_explorer/index.html#/here` < `fileserver_ip` > - IP address of the Nutanix File Server to be audited.

   If you select to launch the RestAPI Explorer from the Prism menu, the **RestAPI Explorer for Prism** client will be opened.

2. In the **username** and **password** fields, enter the credentials of the Create User Account to Access Nutanix REST API you have created.
3. Click **Explore**.
4. In the **File Server REST API Explorer** REST API client, locate the POST request for `notification_policies` : `POST /notification_policies`
5. In the request body, enter the following JSON-formatted structure:

   ```
   {

   "spec": {

   "name": "<NAME_OF_NOTIFICATION_POLICY> ",

   "resources": {

   "all_mount_targets" : true,

   "protocol_type_list" : ["SMB"],

   "file_operation_list" : [<LIST_OF_FILE_OPERATIONS>],

   "partner_server_reference_list" : [{

   "kind" : "partner_server",

   "uuid" : "<UUID_OF_PARTNER_SERVER>"

   }]

   },

   "description": "<optional_string>"

   },

   "api_version": "3.0",

   "metadata": {

   "kind": "notification_policy"

   }
   ```

}

here:

"all_mount_targets" : true - instructs to notify on changes to all shares

"protocol_type_list" : ["SMB"] - instructs to track SMB shares (the only currently supported)

<*NAME_OF_NOTIFICATION_POLICY*> – enter the name of notification policy you want to create

<*UUID_OF_PARTNER_SERVER*> - enter the `uuid` of Configure Partner Server

<*LIST_OF_FILE_OPERATIONS*> - enter the list of operations to be audited.

6. Send the request, clicking **Try it out**.
7. Get the response - `Response Code` should be *200*. In the response body, locate the `uuid` of the created notification policy.
8. To check that a new policy was included in the list of existing policies, retrieve the list of policies, sending the POST request to the following endpoint: `POST /notification_policies/list`. The request body must be empty - for that, enter empty brackets as the **value** for *get_entities_request* parameter : { }

Auditing Specific Folders

If you want to audit only the certain folders on Nutanix File Server (mount targets), then do the following:

1. Retrieve the list of existing mount targets using the `mount_target POST /mount_targets/list` request with empty body, as described above.
2. In the response, locate the `uuids` of the target folders you want to audit.
3. In the notification policy creation request (described above) instead of `"all_mount_targets" : true` in the request body enter the following JSON-formatted structure:

"mount_target_reference_list": [

{

"kind" : "mount_target",

"uuid" : "<UUID_OF_MOUNT_TARGET1>"

},

```
{

"kind" : "mount_target",

"uuid" : "<UUID_OF_MOUNT_TARGET2>"

},

]
```

here:

<UUID_OF_MOUNT_TARGET> – enter the uuid of target you want to audit.

Example

The JSON-formatted structure below is an example of the request body that can be used to create a notification policy named *MOUNT_POINT_POLICY* to audit the mount a share on Nutanix File Server with the *uuid=378896fd-e829-4869-84a2-6c29268acfff*. The following operations will be audited:

- "FILE_READ",
- "FILE_CREATE",
- "FILE_DELETE",
- "DIRECTORY_CREATE",
- "DIRECTORY_DELETE",
- "FILE_WRITE",
- "RENAME",
- "SECURITY",
- "FILE_OPEN"

JSON structure is as follows:

```
{

"spec": {

"name": "MOUNT_POINT_POLICY ",

"resources": {

"mount_target_reference_list": [

{

"kind" : "mount_target",
```

"uuid" : "378896fd-e829-4869-84a2-6c29268acfff”

}

],

"protocol_type_list" : ["SMB"],

"file_operation_list" :[

"FILE_READ",

"FILE_CREATE",

"FILE_DELETE",

"DIRECTORY_CREATE",

"DIRECTORY_DELETE",

"FILE_WRITE",

"RENAME",

"SECURITY",

"FILE_OPEN"

],

"partner_server_reference_list" : [

{

"kind" : "partner_server",

"uuid" : " d0bfb952-924b-459e-bd32-44c8b5a62838"

}

]

},

"description": "<optional_string>"

},

"api_version": "3.0",

"metadata": {

"kind": "notification_policy"

}

}

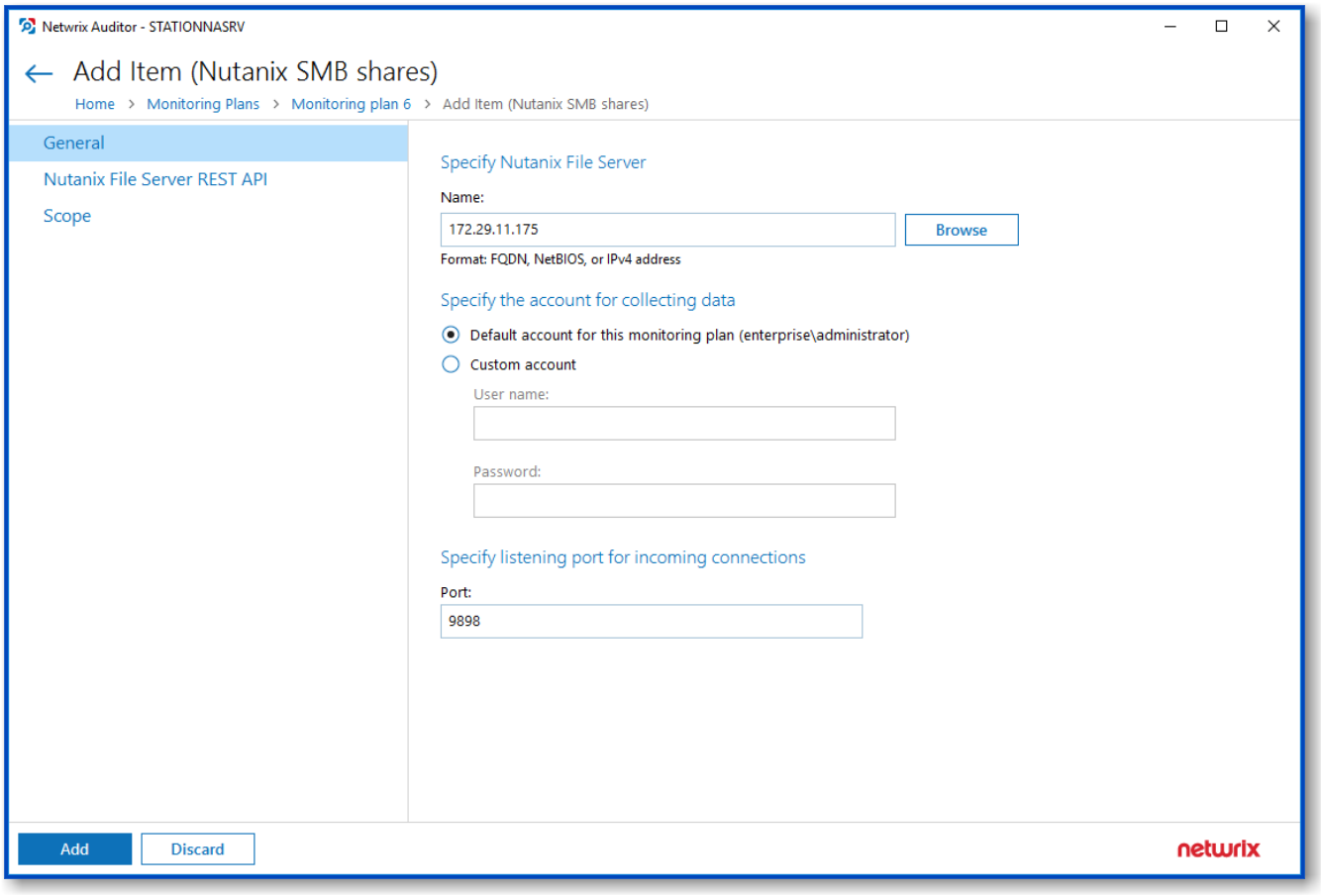
Permissions for Nutanix Files Auditing

Before you start creating a monitoring plan to audit Nutanix Files, plan for the accounts that will be used for data collection. They should meet the requirements listed below.

Account for Accessing Nutanix File Server

First, you need an account that Netwrix Auditor will use to access Nutanix File Server. This account requires at least *Read* permission for the target SMB shares on the Nutanix File Server.

This is the account you will provide in the monitoring plan wizard at the Create a New Monitoring Plan step; it can be modified in the **General** tab of the monitored item settings.

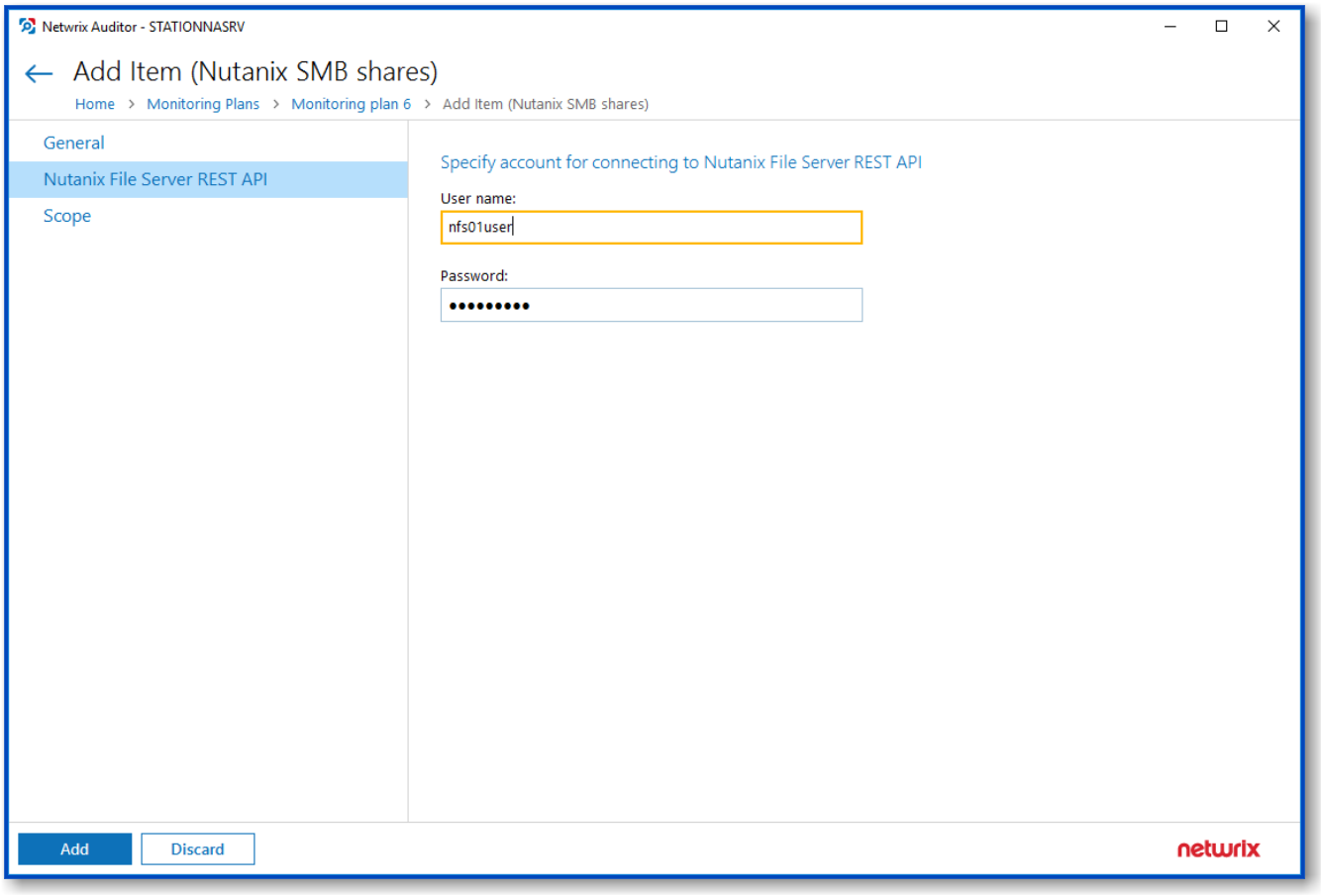


This account must have a role with sufficient privileges on that server: **File Server Admin** (recommended) or **Backup Admin** role.

Account for Accessing REST API

You will also need an account that will be used to connect to Nutanix File Server REST API.

This account should be provided in the **Nutanix File Server REST API** tab of the monitored item (*Nutanix SMB shares*) settings.



This account must be assigned the **REST API access users** role for Nutanix File Server you want to audit.

See the section below for the instructions on user role assignment.

Role Assignment Procedure

Before starting the role assignment, make sure your Nutanix File Server is included in the AD domain.

Follow the steps to assign the required roles to the corresponding accounts using Nutanix Prism.

Step 1 – Open Nutanix Prism web portal.

Step 2 – Select **File Server** category. In the list of servers, select the server you want to audit.

Step 3 – Click **Manage roles**.

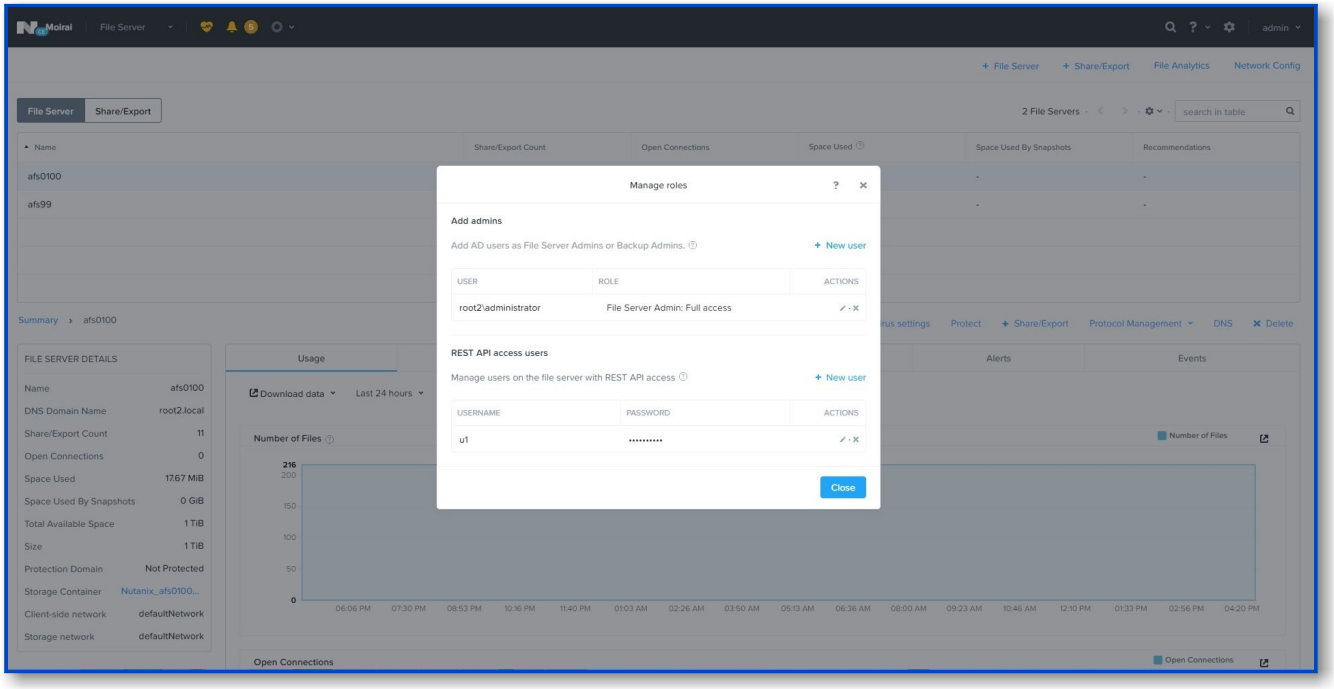
Step 4 – In the **Manage roles** dialog locate the **Add admins** section and click **+New user**.

Step 5 – Enter the AD user account (to be used as data collection account) in the *domain\name* format and select the **File Server Admin** or **Backup Admin** role to assign

Step 6 – Click **Save** next to these cells to save the settings.

Step 7 – Next, in the **REST API access users** section click **+New user**.

Step 8 – Enter the local user account and password, then click **Save** next to these cells to save the settings.



Step 9 – When finished, click **Close**.

See the following topics for additional information.

- Add Items for Monitoring
- Create User Account to Access Nutanix REST API.

Qumulo

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - The Remote Syslog Address and port number must be configured as described in the Configure Core Audit for Qumulo File Servers topic.

Review a full list of object types Netwrix Auditor can collect on Qumulo network devices.

Action	File	Folder	Share
Added	+	+	-
Add (failed attempt)	+	+	-
Modified	+	+	-
Modify (failed attempt)	-	-	-
Moved	+	+	-
Move (failed attempt)	-	-	-
Read	+	+	-
Read (failed attempt)	-	-	-
Renamed	+	+	-
Rename (failed attempt)	-	-	-

Action	File	Folder	Share
Removed	+	+	-
Remove (failed attempt)	-	-	-
Copied	-	-	-

NOTE: For Qumulo system Auditor displays the actual time when the event occurred. The 'When' column shows the time when the syslog message arrived.

If an object has been moved between file shares, the product reports the following actions:

- Read + Removed for the initial object;
- Added + Modified for the object to a new location.

Qumulo Ports

Review a full list of protocols and ports required for Netwrix Auditor for Qumulo.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 514 UDP port.

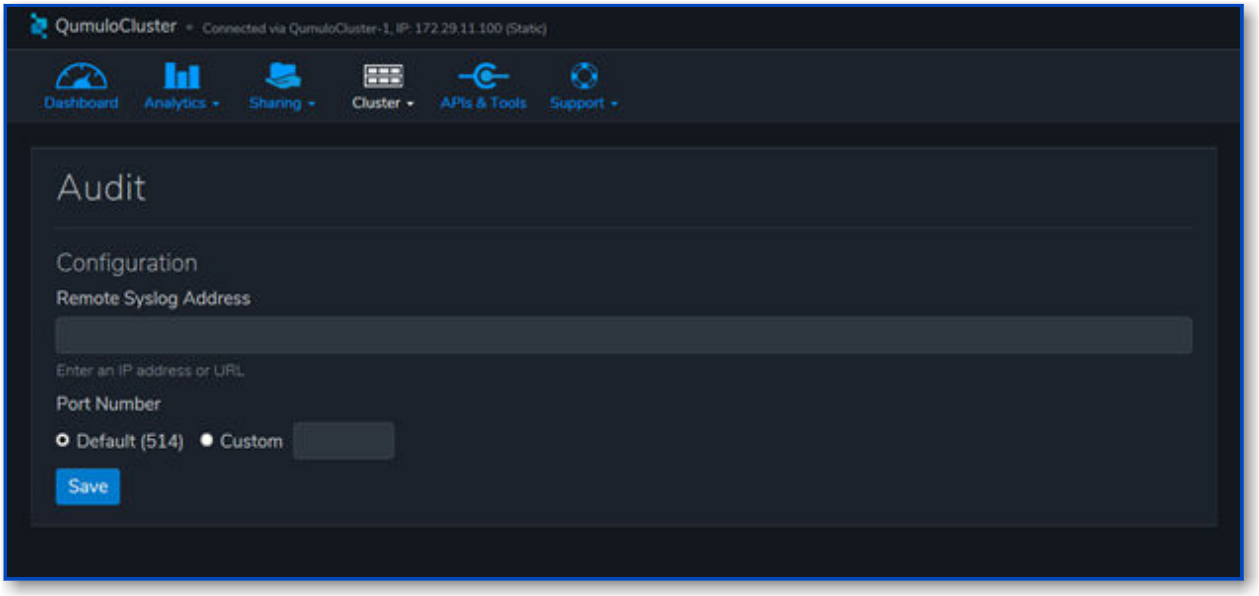
Port	Protocol	Source	Target	Purpose
514	UDP / TCP	Monitored file servers	Netwrix Auditor Server	Getting events from monitored file servers

Configure Core Audit for Qumulo File Servers

To configure your Qumulo file servers for auditing, you need to connect your device to Active Directory or LDAP (local names are supported) and then configure Remote Syslog Address and port number via Web UI.

To configure Core Audit for Qumulo file servers

1. Log in to the Web UI.
2. Navigate to Cluster and click Audit.
3. Under the Configuration, provide the following:
    - Remote Syslog Address – Provide the IP address or the computer listened by Syslog. It should be a third-party Syslog forward service or the machine where Netwrix Auditor is installed.
    - Port Number – use the default value (*514*).



When you see the green line "*Connected*", the environment is ready.

For detailed information about Qumulo Web UI. refer to the following Qumulo how-to article: Qumulo Core Audit Logging.

Permissions for Qumulo Auditing

Before you start creating a monitoring plan to audit your Qumulo or Synology 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 (or monitored item settings).

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

See the Use Group Managed Service Account (gMSA) topic and the Group Managed Service Accounts Overview Microsoft article for additional information.

These group Managed Service Accounts should meet the related requirements, as listed below.

On the target server:

1. The account requires Read share permission on the audited shared folders.
2. The account requires Read NTFS permission on all objects in the audited folders.

Synology

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - The log sending must be configured as described in the Configure Synology File Servers for Audit topic.

Review a full list of object types Netwrix Auditor can collect on Synology NAS network devices.

Monitored Objects

Action	File	Folder	Share
Added	+	+	-
Add (failed attempt)	-	-	-
Modified	+	-	-
Modify (failed attempt)	-	-	-
Moved	+	+	-
Move (failed attempt)	-	-	-
Read	+	-	-
Read (failed attempt)	-	-	-
Renamed	+	+	-
Rename (failed attempt)	-	-	-

Action	File	Folder	Share
Remove (failed attempt)	-	-	-
Copied	-	-	-

NOTE: For Synology system Auditor displays the actual time when the event occurred. The 'When' column shows the time when the syslog message arrived.

If an object has been moved between file shares, the product reports the following actions:

- Read + Removed for the initial object
- Added + Modified for the object to a new location

Configure Synology File Servers for Audit

Follow the steps to configure your Synology NAS devices to transmit the local system logs for monitoring.

Step 1 – Log in to the Synology Web Administration Console.

Step 2 – Navigate to Log Center > Log Sending and configure the following:

- Server – Provide the IP address or the computer listened by Syslog. It should be a running Netwrix Syslog service or a third-party Syslog forward service.
- Port – Use the default value (*514*).
- Transfer protocol – select TCP or **UDP**.
- Log format – Set to "*IETF (RFC 5424)*".
- Enable secure connection – Use the default value.
- Import certificate – Use the default value.

Step 3 – Click Apply.

NOTE: Currently, Netwrix Auditor cannot collect activities using a local Synology user. Data collection only supported via a domain user with the necessary access privileges to the Synology file server.

Synology Ports

Review a full list of protocols and ports required for Netwrix Auditor for Synology.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 514 UDP port.

Port	Protocol	Source	Target	Purpose
514	UDP / TCP	Monitored file servers	Netwrix Auditor Server	Getting events from monitored file servers

Permissions for Synology Auditing

Before you start creating a monitoring plan to audit your Qumulo or Synology 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 (or monitored item settings).

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

See the Use Group Managed Service Account (gMSA) topic and the Group Managed Service Accounts Overview Microsoft article for additional information.

These group Managed Service Accounts should meet the related requirements, as listed below.

On the target server:

1. The account requires Read share permission on the audited shared folders.

2. The account requires Read NTFS permission on all objects in the audited folders.

Windows File Servers

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

Configuration Overview

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - On the Windows file server:
        - For a security principal (e.g., Everyone), the following options must be configured in the Advanced Security > Auditing settings for the audited shared folders:

Advanced Security Option	Setting
List Folder / Read Data (Files only)	"Success" and "Fail"

Advanced Security Option	Setting
List Folder / Read Data (This folder, subfolders and files)	"Fail"
Create Files / Write Data*	"Success" and "Fail"
Create Folders / Append Data*	"Success" and "Fail"
Write 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"

* Select "Fail" only if you want to track failure events, it is not required for success events monitoring.

NOTE: 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.

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

Advanced Audit Policy	Setting
Object Access > Audit File Share	"Success"
Object Access > Audit Handle Manipulation	"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)
  - 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.

        - 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 Auditor console computer:
        - 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 Auditor Server.

Consider the following:

- 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.
- Scale-Out File Server (SOFS) cluster is not supported.
- Auditing of files and folders placed directly into the DFS namespace root is not supported, as such configuration is not recommended by Microsoft. (See the Microsoft Placing files directly in the namespace share article for additional information.) Make sure the UNC path of a shared folder is placed within a share targeted by a DFS folder.

Configuration Steps

Follow the steps to configure Windows File Servers for auditing:

Step 1 – Check requirements. Make sure the Windows File Servers you want to monitor meet the requirements.

Step 2 – Decide on audit data to collect.

- Review the list of objects and attributes that can be monitored by Auditor: See the File Serverstopic for additional information.
- Plan for the file servers and shares you want to audit:
-
    - 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.
    - Audit flags must be set on every file share you want to audit.
    - 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.
    - By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings.
    - Administrative hidden shares like default system root or Windows directory (*ADMIN$*), default drive shares (*D$, E$*), etc. will not be monitored.

Step 3 – Review considerations and limitations:

The following considerations and limitations refer to data collection:

- 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.
- Scale-Out File Server (SOFS) cluster is not supported.
- Several constraints apply to DFS auditing. See the DFS-Related Constraints topic for additional information.

The following considerations and limitations refer to reporting:

- In the reports and search results, in some cases, Auditor displays not the actual time when the event occurred but data collection time.
- Auditor may report on several unexpected changes with *who* (initiator's account) reported as *system* due to the native Windows File Servers audit peculiarities. If you do not want to see these changes, exclude them from the audit. See the File Servers topic for additional

information. For example - mass file removals, when target Windows server generates too many events at a time and the product is unable to parse their sequences correctly.
- Due to Windows limitations, the *copy/rename/move* actions on remote file shares may be reported as two sequential actions: copying – as adding a new file and reading the initial file; renaming/moving – as removing the initial file and adding a new file with the same name.
- To report on *copy* actions on remote file shares, make sure that audit of successful read operations is enabled. See the Configure Object-Level Access Auditing topic for additional information.

Step 4 – Apply required audit settings.

Depending on your auditing requirements, you may need to audit your file server objects for:

- Successful read attempts
- Successful modifications
- Failed read and modification attempts
- Failed modification attempts

For that, object-level audit settings and appropriate audit policies should be set up. Besides, the following should be configured for your Windows file servers:

- Windows Event log size and retention settings
- Remote registry service
- Inbound connection rules for Windows firewall

You can apply required audit settings to your Windows file servers in one of the following ways:

- **Automatically** when creating a monitoring plan.

  In this case, the audit settings will be applied automatically, then they will be periodically checked and adjusted if necessary. See the Create a New Monitoring Plan topic for additional information.

- **Manually.** To configure your Windows 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
  - Windows File Server Ports

With automatically applied settings, initial SACL configuration for DFS replication links may take longer than with manual configuration — however, automatic configuration will help to minimize the impact on the DFS backlog and replication process in general.

Step 5 – Configure Data Collecting Account. See the Data Collecting Account topic for additional information.

Step 6 – Configure required protocols and ports. Set up protocols and ports. See the Dell Data Storage Ports topic for additional information.

DFS-Related Constraints

Perform the following steps if planning to audit DFS files and folders:

Step 1 – Auditor supports auditing of DFS and clustered file servers if Object Access Auditing is enabled on DFS file shares or on every cluster node.

Step 2 – When adding a cluster file server for auditing, it is recommended to specify a server name of the **Role** server or a UNC path of the shared folder located on the **Role** server.

Step 3 – When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path of the whole namespace or UNC path of the DFS link (folder). For example:

- *"\\domain\dfsnamespace\"* (domain-based namespace)
- *"\\server\dfsnamespace\"* (in case of stand-alone namespace);

Auditing of files and folders placed directly into the DFS namespace root is not supported, as such configuration is not recommended by Microsoft. See the Placing files directly in the namespace share section of the Microsoft article for additional information. Make sure the UNC path of a shared folder is placed within a share targeted by a DFS folder.

For recommendations on configuring DFS replication, refer to the following Netwrix knowledge base article: Why did loss of performance occur when configuring audit settings for Windows File Servers?. Remember that replication of namespace roots is not supported.

File Servers and Antivirus

It is strongly recommended that you add the following executables to the list of exclusions for your antivirus:

- C:\Windows\SysWOW64\NwxExeSvc\NwxExeSvc.exe
- C:\Windows\SysWOW64\NwxExeSvc\NwxEventCollectorAgent.exe
- C:\Windows\SysWOW64\NwxExeSvc\NwxFsAgent.exe
- C:\Windows\SysWOW64\NwxExeSvc\NwxSaclTunerAgent.exe

Otherwise, significant delays and performance issues may occur while collecting data.

This happens because these executables access a large number of file server objects (files, folders), fetching audit data — and your antivirus may treat this as a suspicious behavior.

For some antiviruses (for example, Trend Micro) you may need to specify the folders to exclude, that is, **C:\Windows\SysWOW64\NwxExeSvc**. Refer to your antivirus documentation for details.

Monitored Objects

The following table lists the actions that can be performed with Windows-Based File Shares:

Added	+	+	+
Add (failed attempt)	+	+	–
Modified	+	+	+
Modify (failed attempt)	+	+	+
Moved	+	+	–
Move (failed attempt)	–	–	–
Read	+	–	–
Read (failed attempt)	+	+	+
Renamed	+	+	–
Renamed (failed attempt)	–	–	–
Removed	+	+	+
Remove (failed attempt)	+	+	–
Copied	+	–	–

Windows File Server Ports

Review a full list of Windows File Server protocols and ports required for Netwrix Auditor for File Servers.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to local 389 TCP port.

Port	Protocol	Source	Target	Purpose
Windows File Servers				
389	TCP/UDP	Netwrix Auditor Server	Domain controllers	LDAP DC query Account resolve
135 **+ Dynamic:** **1024 -65535**	TCP	Netwrix Auditor Server	Monitored computer	Windows Management Instrumentation Firewall configuration Core Service communication
135	TCP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol Core Service installation
137	UDP	Netwrix Auditor Server	Monitored computer	File and Printer Sharing (NetBIOS Name Resolution)
138	UDP	Netwrix Auditor Server	Monitored computer	File and Printer Sharing (NetBIOS Datagram Service)

Port	Protocol	Source	Target	Purpose
139	TCP	Netwrix Auditor Server	Monitored computer	File and Printer Sharing (NetBIOS Session Service)
445	TCP	Netwrix Auditor Server	Monitored computer	SMB 2.0/3.0
3268	TCP	Netwrix Auditor Server	Domain controllers	LDAP Group membership GC search

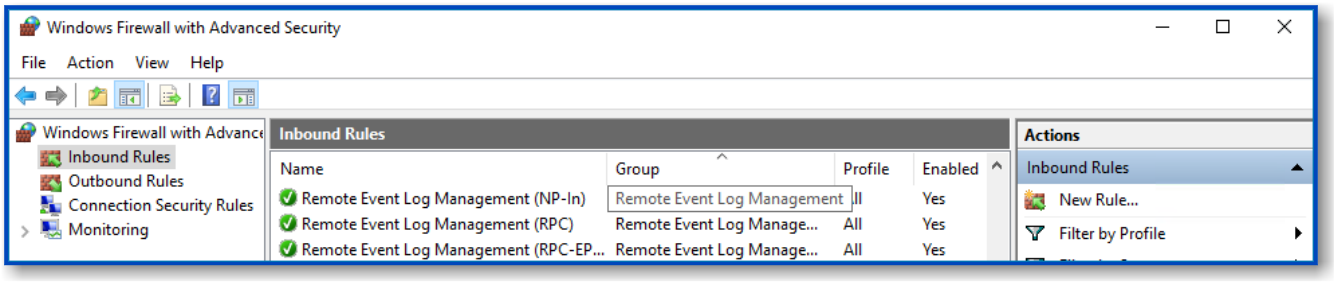
Configure Windows Firewall Inbound Connection Rules

You can also 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.

Step 1 – On each audited server, navigate to **Start** > **Control Panel** and select **Windows Firewall**.

Step 2 – In the Help Protect your computer with Windows Firewall page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select **Inbound Rules** on the left.



Step 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)
- Remote Service Management (NP-In)
- Remote Service Management (RPC)
- Remote Service Management (RPC)
- Performance Logs and Alerts (DCOM-In)
- Performance Logs and Alerts (Tcp-In)

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

Option		Description
		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. 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. 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.

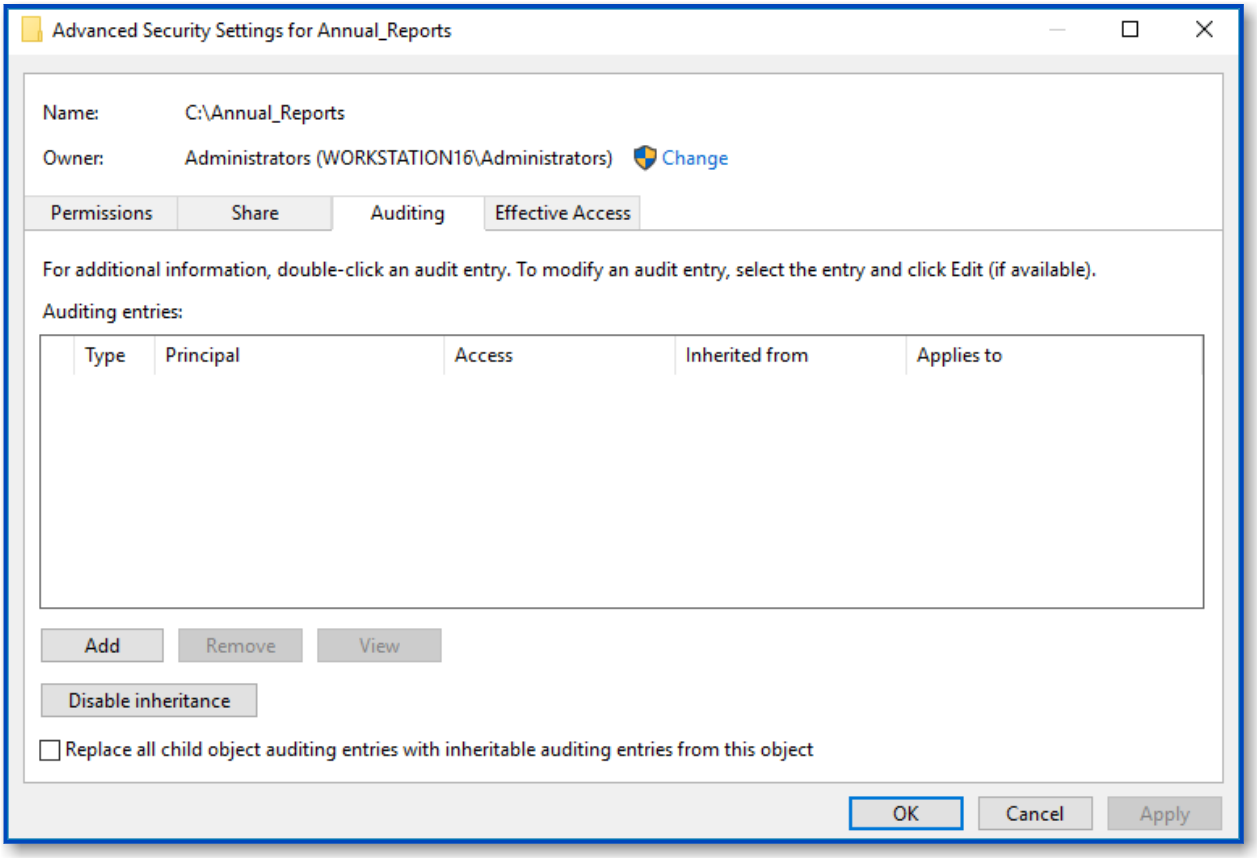
Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, renaming, and copying. To track the copy action, enable successful read access and change auditing. See File Servers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

Perform one of the following procedures depending on the OS:

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

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.

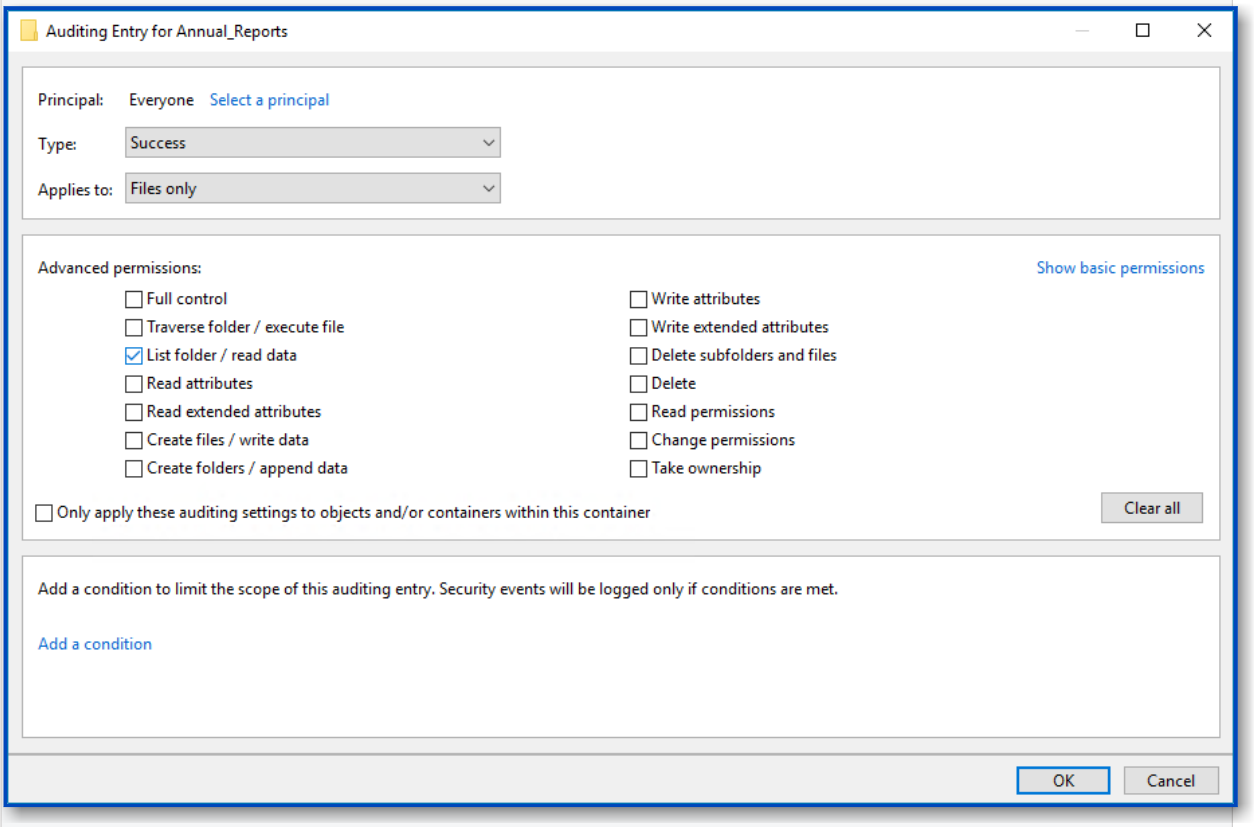


4. Click Add to add a new principal. You can select Everyone (or another user-defined group containing users that are granted special permissions) and click Edit.
5. In the Auditing Entry for <Folder_Name> dialog, click the Select a principal link and specify Everyone.

   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.

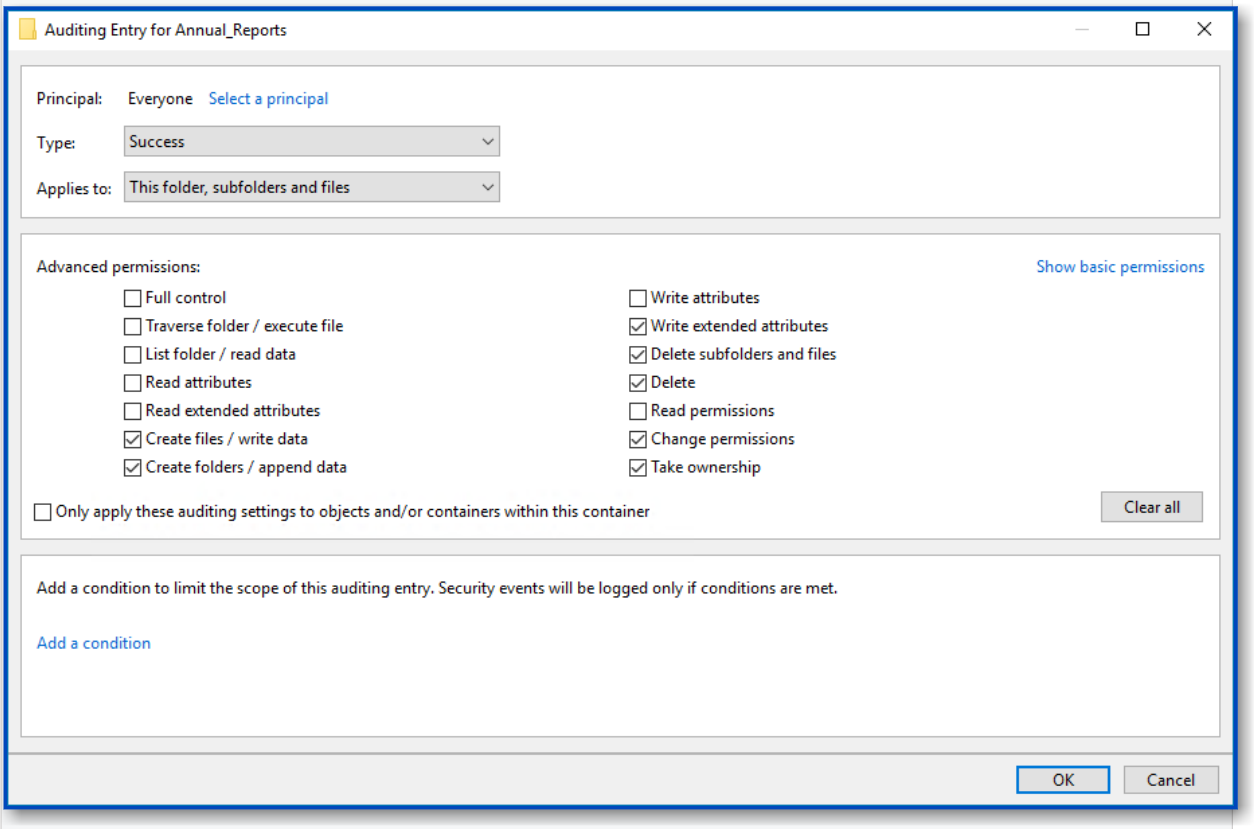
6. Apply settings to your Auditing Entries depending on the access types that you want to audit. If you want to audit all access types (successful reads, modification as well as failed read and modification attempts), you need to add separate Auditing Entries for each file share. Otherwise, reports will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

Auditing Entry	

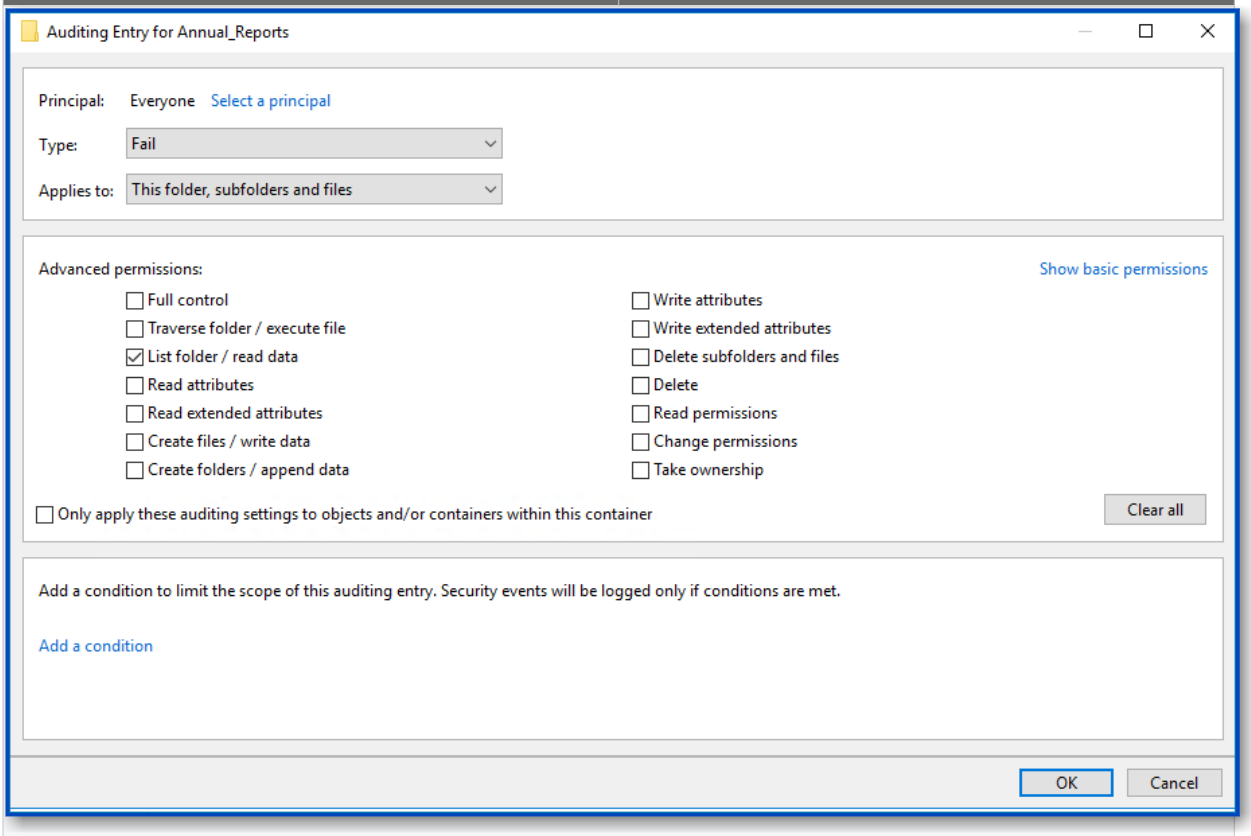
The Auditing Entry below shows Advanced Permissions for auditing successful changes only:



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

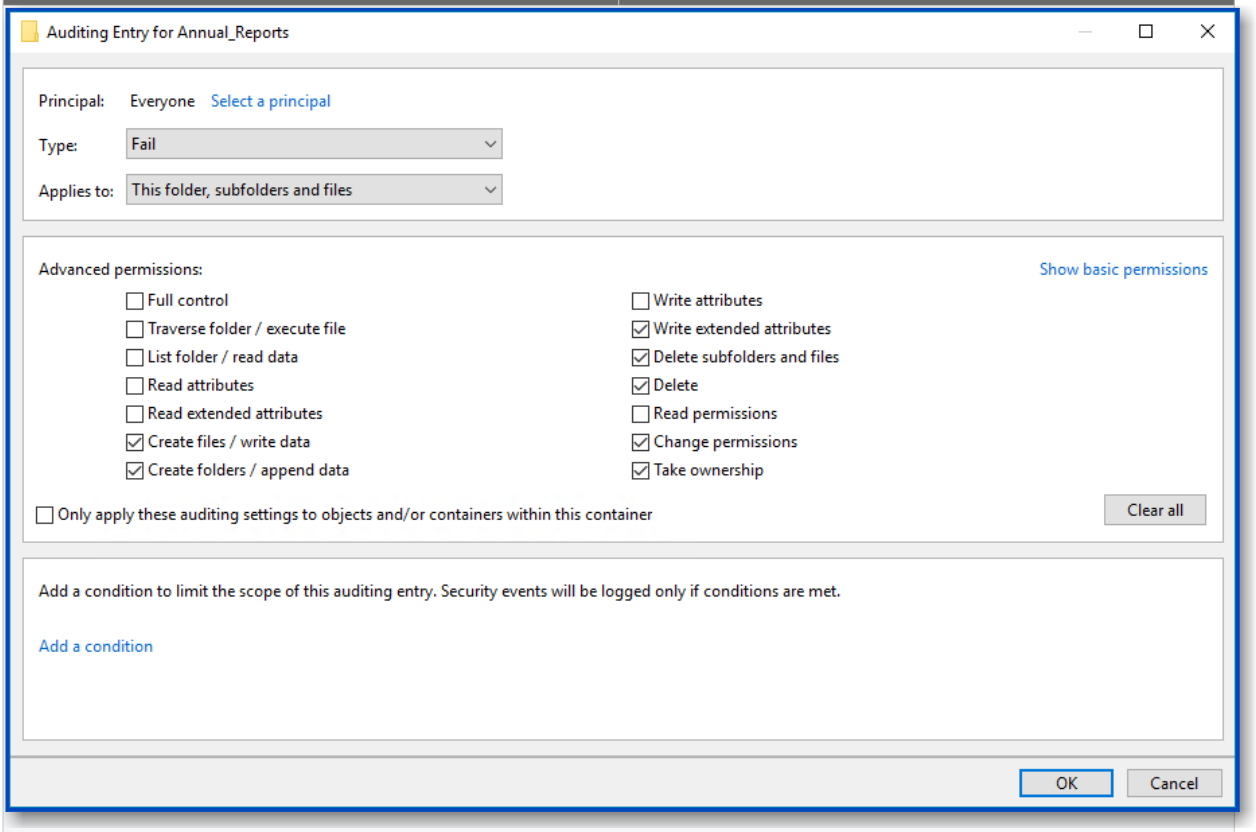
Auditing Entry	
	

- 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.

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

Step 1 – Navigate to the target file share, right-click it and select **Properties**.

Step 2 – In the **<Share_Name> Properties** dialog, select the **Security** tab and click **Advanced**.

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

Step 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**.

Step 5 – 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 Auditor client and the product will only audit user accounts that belong to the selected group.

Step 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 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: • **Apply onto—Select *"This folder, subfolders and files"*.** • **Check *"Successful"* next to the following permissions:**

Auditing Entry
◦ 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.
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: • 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.

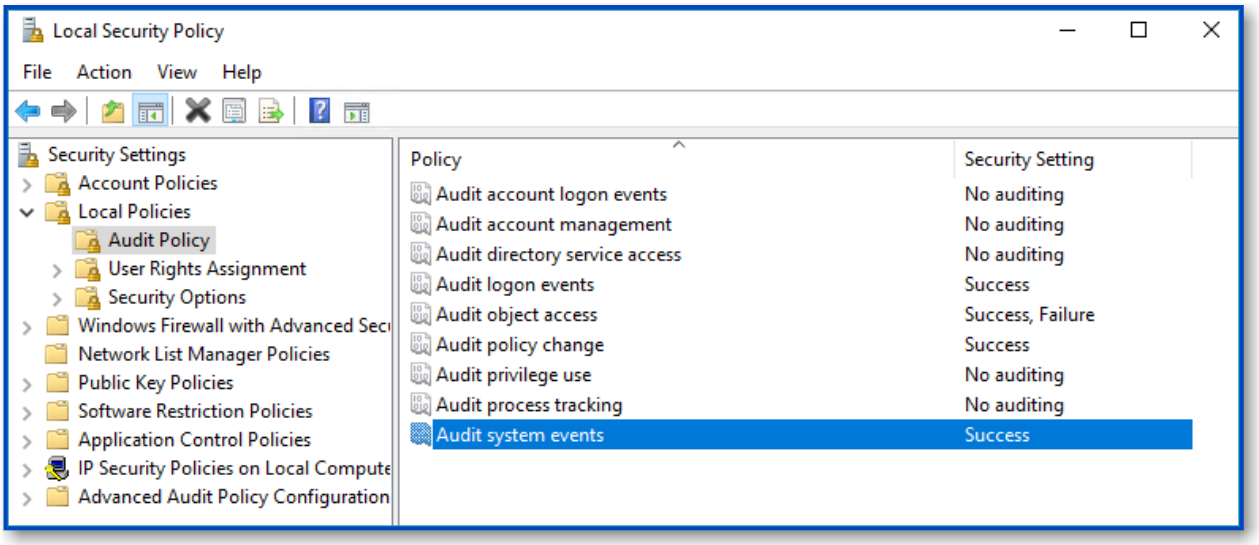
Configure Local Audit Policies

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

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



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.

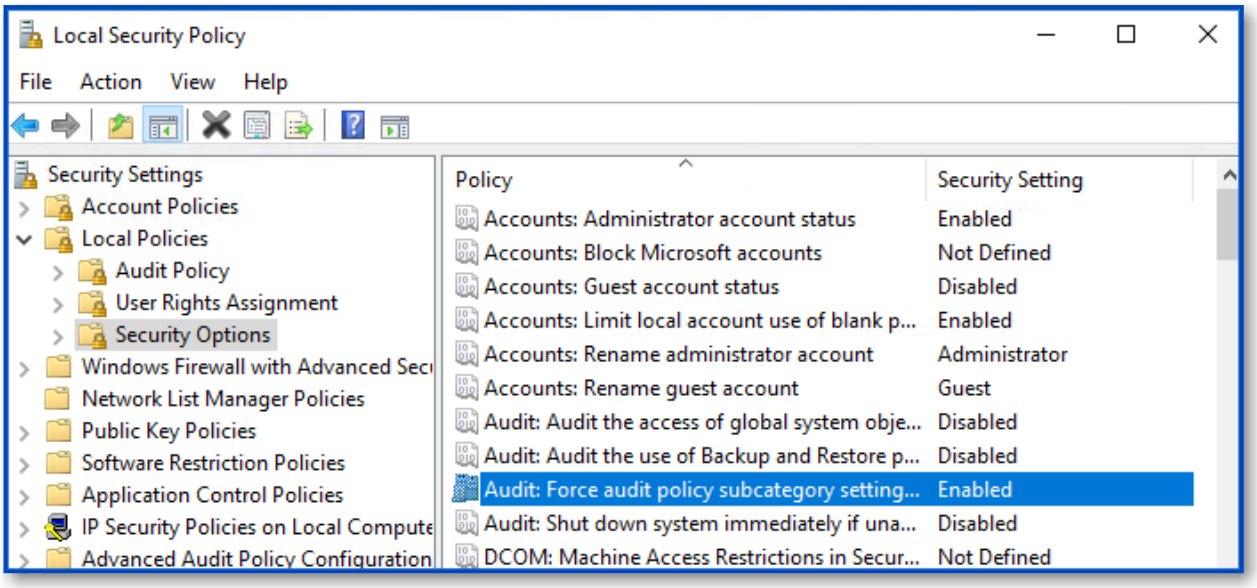
To configure security options

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 and higher) or** Administrative Tools **(Windows 2012)** → 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.

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`

Audit subcategory	Command
Logoff	`auditpol /set /subcategory:"Logoff" /success:enable`

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"`.

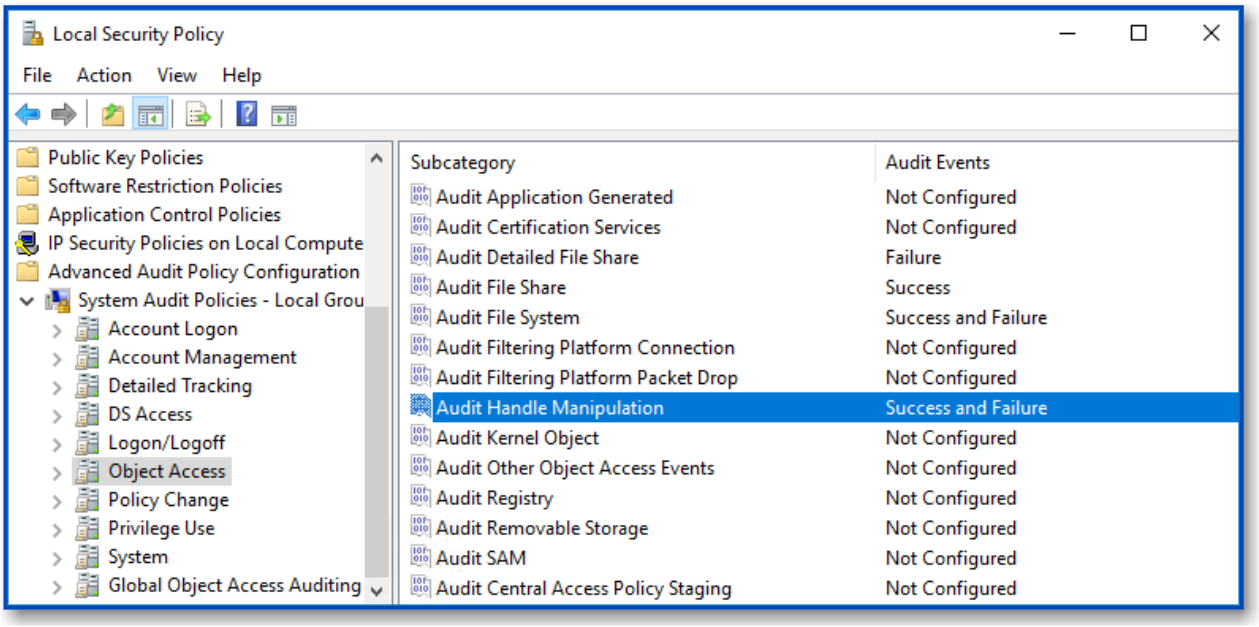
To configure advanced audit policy on Windows Server 2008 R2 / Windows 7 and above

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 and higher) or** Administrative Tools **(Windows 2012)** → Local Security Policy.
2. In the left pane, navigate to **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies**.
3. Configure the following audit policies.

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

Policy Subnode	Policy Name	Audit Events
Policy Change	• Audit Audit Policy Change	*"Success"*
Logon/Logoff	• Logon	*"Success"*
	• Logoff	*"Success"*
System	• Security State Change	*"Success"*



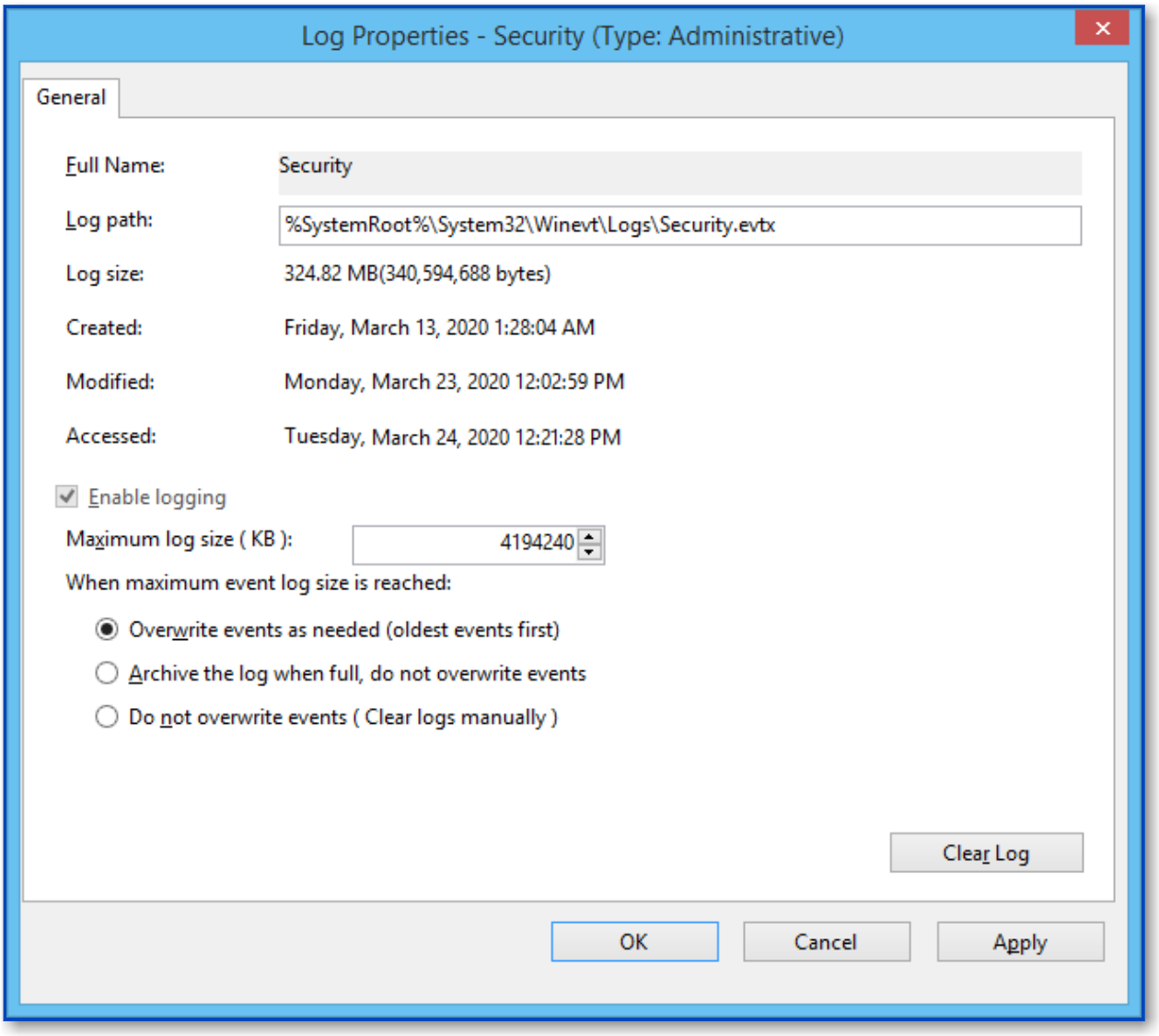
Configure Event Log Size and Retention Settings

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.

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 and higher) or** Administrative Tools **(Windows 2012)** → **Event Viewer**.

2. Navigate to **Event Viewer tree** → **Windows Logs**, right-click **Security** and select **Properties**.



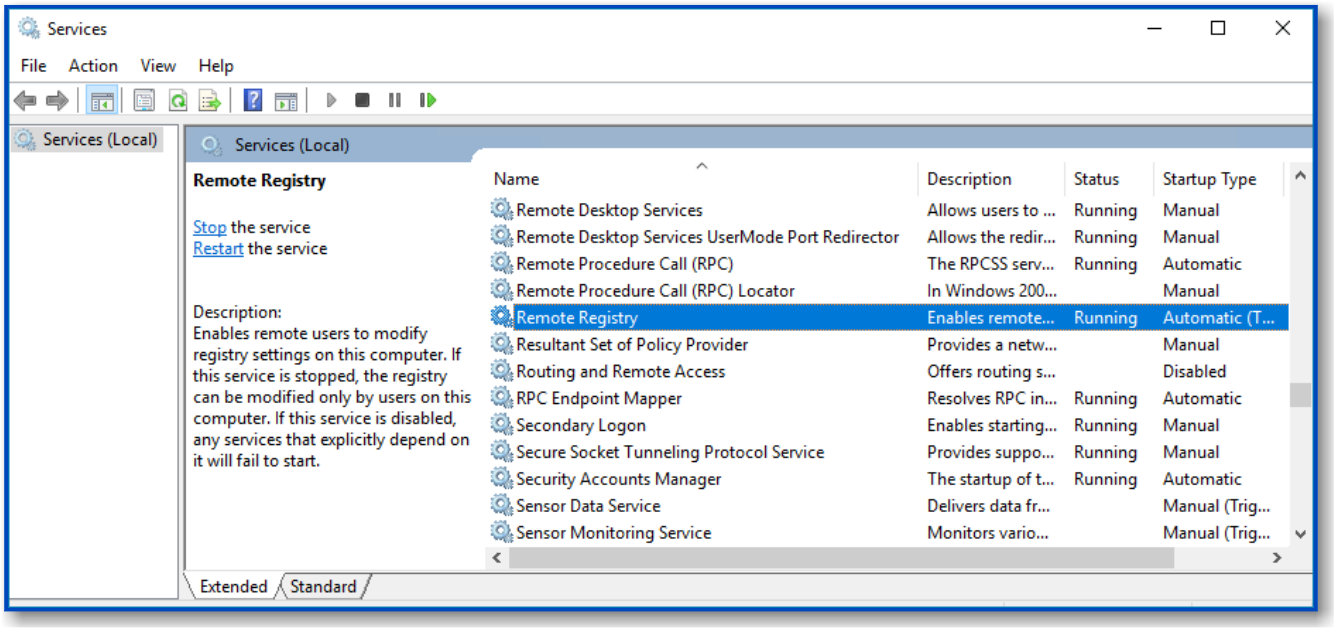
3. Make sure **Enable logging** is selected.
4. In the **Maximum log size** field, specify the size you need.
5. Make sure **Do not overwrite events (Clear logs manually)** is cleared. If selected, change the retention method to **Overwrite events as needed (oldest events first)**.

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**.

Enable Remote Registry Service

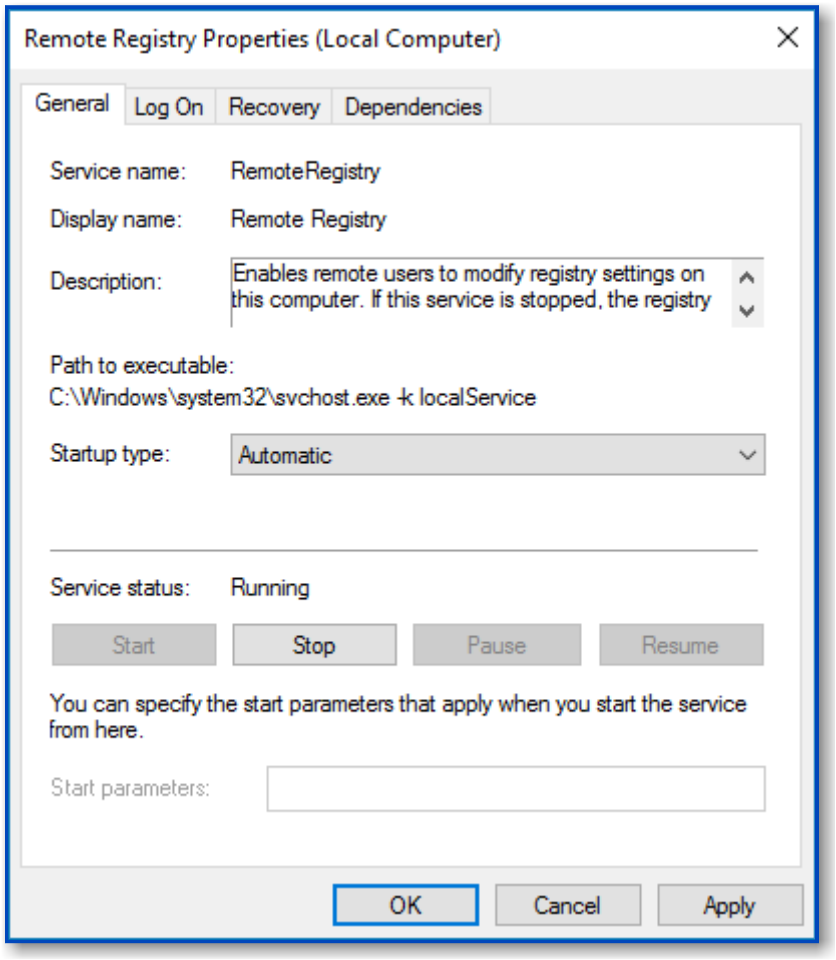
Follow the steps to enable the Remote Registry service.

Step 1 – Navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Services**.



Step 2 – In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.

Step 3 – In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



Step 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.

NOTE: The Remote Registry should be enabled on the target server.

Permissions for Windows File Server Auditing

Before creating a monitoring plan to audit your Windows file servers, plan for the account that will be used for data collection . This account should meet the requirements listed below. You will provide this account in the monitoring plan wizard or monitored item settings.

Data Collection Accounts should meet the following policies and permissions:

- Data collecting account on the target server must be a member of the local Administrators group.

- The **Manage auditing and security log** and Backup files and directories policies must be defined for this account. See the Permissions for Active Directory Auditing and topics for additional more information.
- The **Read** share permission on the audited shared folders.
- The Read NTFS permission on all objects in the audited folders.

Considerations for gMSA Account

You can use group Managed Service Accounts (gMSA) as data collecting accounts.

NOTE: On the Netwrix Auditor Server, the gMSA account must be a member of the local Administrators group.

For more information on gMSA, see the following:

- Use Group Managed Service Account (gMSA)
- Microsoft article: Group Managed Service Accounts Overview

Configure the Back up Files and Directories Policy

Configure this Back up Files and Directories policy via the Local Security Policy Snap-in or using the Group Policy Management Console.

Follow the steps to configure the Back up Files and Directories policy via the Local Security Policy Snap-in.

Step 1 – On any domain controller in the target domain, open the Local Security Policy snap-in: navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > Local Security Policy.

Step 2 – Navigate to **Security Settings** > **Local Policies** > **User right Assignment**.

Step 3 – Locate the Back up files and directories policy and double-click it.

Step 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.

The policy is now configured.

Follow the steps to configure the Back up Files and Directories policy using the Group Policy Management Console.

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

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to **Start** > **Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below)** > **Group Policy Management**.

Step 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**.

Step 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**.

Step 4 – On the right, double-click the User Rights Assignment policy.

Step 5 – Locate the Back up files and directories policy and double-click it.

Step 6 – In the Back up files and directories Properties dialog, click Add User or Group and specify the user that you want to define this policy for.

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

Step 8 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 9 – Ensure that new GPO settings applied on any audited domain controller.

The policy is now configured.

Group Policy

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - Configure the domain for auditing. See the Audit Configuration Assistant topic for information on configuring the domain.
    - On the Auditor console computer:
        - If you have enabled automatic log backup for the Security log of your domain controller, you can instruct Auditor to clear the old backups automatically. For that, use the **CleanAutoBackupLogs** registry key, as described in the Active Directory Registry Key Configuration topic.

          RECOMMENDED: Adjust retention period for the backup files accordingly (default is **50** hours). See the Adjust Security Event Log Size and Retention topic.
        - To provide for event data collection, the Secondary Logon service must be up and running . Open **Administrative Tools** > **Services**, right-click the **Secondary Logon** service and on the **General** tab make sure that Startup type for this service is other than *Disabled*.

Group Policy Ports

Review a full list of protocols and ports required for monitoring Active Directory, Exchange, and Group Policy.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to the local 389 TCP port.

Port	Protocol	Source	Target	Purpose
389	TCP/UDP	Netwrix Auditor Server	Domain controllers	LDAP Common queries
3268	TCP	Netwrix Auditor Server	Domain controllers	LDAP Group membership GC search
3269	TCP	Netwrix Auditor Server	Domain controllers	Global catalog LDAP over SSL
88	TCP/UDP	Netwrix Auditor Server	Domain controllers	Kerberos authentication
135 **and dynamic range:** **1024 -65535**	TCP	Netwrix Auditor Server	Domain controllers	Windows Management Instrumentation. `gpupdate /force`
445	TCP	Netwrix Auditor Server	Domain controllers	SMB 2.0/3.0 Authenticated communication between Netwrix Auditor Server and domain controllers.

Port	Protocol	Source	Target	Purpose
53	UDP	Netwrix Auditor Server	DNS Server	DNS Client

Group Policy Registry Keys

Review the basic registry keys that you may need to configure for monitoring Group Policy with Netwrix Auditor. Navigate to Start → Run and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
GPOBackup	Defines whether to backup GPOs during data collection: • 0—No • 1—Yes
GPOBackupDays	Defines the backup frequency: • 0—Backup always • X—Once in X days GPOBackup must be set to *"1"*.
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Activity Summary footer: • 0—Display errors • 1—Do not display errors

Registry key (REG_DWORD type)	Description / Value
IgnoreRootDCErrors	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the CleanAutoBackupLogs key.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter\<monitoring plan name>	
CollectLogsMaxThreads	Defines the number of Domain Controllers to simultaneously start log collection on.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\ AD Change Reporter\<monitoring plan name>\Database settings	
SessionImportDays	Defines the frequency of a full snapshot upload: • X—Once in X days
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Management Console\Database settings	
overwrite_datasource	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the monitoring plan: • 0—No • 1—Yes

Registry key (REG_DWORD type)	Description / Value
SqlOperationTimeout	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).
timeout	Defines the Audit Database connection timeout (in seconds).

Permissions 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 (or in the monitored item settings).

You can use group Managed Service Accounts (gMSA) as data collecting accounts.

See the Use Group Managed Service Account (gMSA) topic and the following Microsoft article: Group Managed Service Accounts Overview for additional information about gMSA.

Account Requirements

NOTE: These group Managed Service Accounts should also meet the related requirements. See the Use Group Managed Service Account (gMSA) topic and the following Microsoft article: Group Managed Service Accounts Overview for additional information about gMSA.

The account used for data collection must meet the following requirements:

- Member of the local Administrators group on the target server.
- Member of the Domain Admins group on the target server.

  NOTE: This covers all the required permissions below and is a mandatory setting if you want to use network traffic compression for data collection.

  OR

- The combination of the following rights and permissions if you plan to disable network traffic compression for your monitoring plan or, for some reasons, do not want to add this account to the **Domain Admins** group:

- **Manage auditing and security log** policy must be defined for this account. See the Permissions for Active Directory Auditing topic for additional information.
- If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See the Permissions for Active Directory Auditing topic for additional information.

Additional Configuration for Domain Controller's Event Logs Auto-backup

The following is required if auto-backup is *enabled* for the domain controller event logs:

- Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See the Assign Permission to Read the Registry Key topic for additional information.
- Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**.
- Read/Write share permission and Full control security permission on the logs backup folder.

Assign Permission to Read the Registry Key

This permission is required 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, it is recommended to assign permissions through Group Policy, or automatically using Audit Configuration Assistant.

To assign permissions manually, use the Registry Editor snap-in or the Group Policy Management console.

Assign Permission Via the Registry Editor Snap-in

Follow the steps to assign permission via the Registry Editor snap-in:

Step 1 – On your target server, open Registry Editor: navigate to **Start > Run** and type *"regedit"*.

Step 2 – In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\EventLog\Security*.

Step 3 – Right-click the **Security** node and select **Permissions** from the pop-up menu.

Step 4 – Click **Add** and enter the name of the user that you want to grant permissions to.

Step 5 – Check **Allow** next to the **Read** permission.

Step 6 – For auditing Logon Activity, you also need to assign the Read permission to the *HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv* registry key.

To assign permission using the Group Policy Management console

Assign Permission Using the Group Policy Management Console

Follow the steps to assign permission using the Group Policy Management console:

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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 .

Step 3 – In the Group Policy Management Editor dialog, expand the Computer Configuration node on the left and navigate to Policies > Windows Settings > Security Settings > Registry.

Step 4 – Right-click in the pane and select Add Key.

Step 5 – Navigate to `HKEY_LOCAL_MACHINE\sECURITY\Policy\PolAdtEv` and click OK.

Step 6 – Click Add and enter the name of the user that you want to grant permissions to and press Enter.

Step 7 – Check Allow next to the *"Read"* permission and click OK

Step 8 – In the pop-up window, select Propagate inheritable permissions to all subkeys and click OK.

Step 9 – Repeat the steps 4-8 for keys below:

- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlset\Control\securePipeservers\winreg`;
- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlset\services\EventLog\security`.

Step 10 – Close Group Policy Management console.

Step 11 – Navigate to Start > Run and type "*cmd*". Input the `gpupdate /force` command and press Enter. The group policy will be updated.

Step 12 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 13 – Ensure that new GPO settings were applied to the domain controllers.

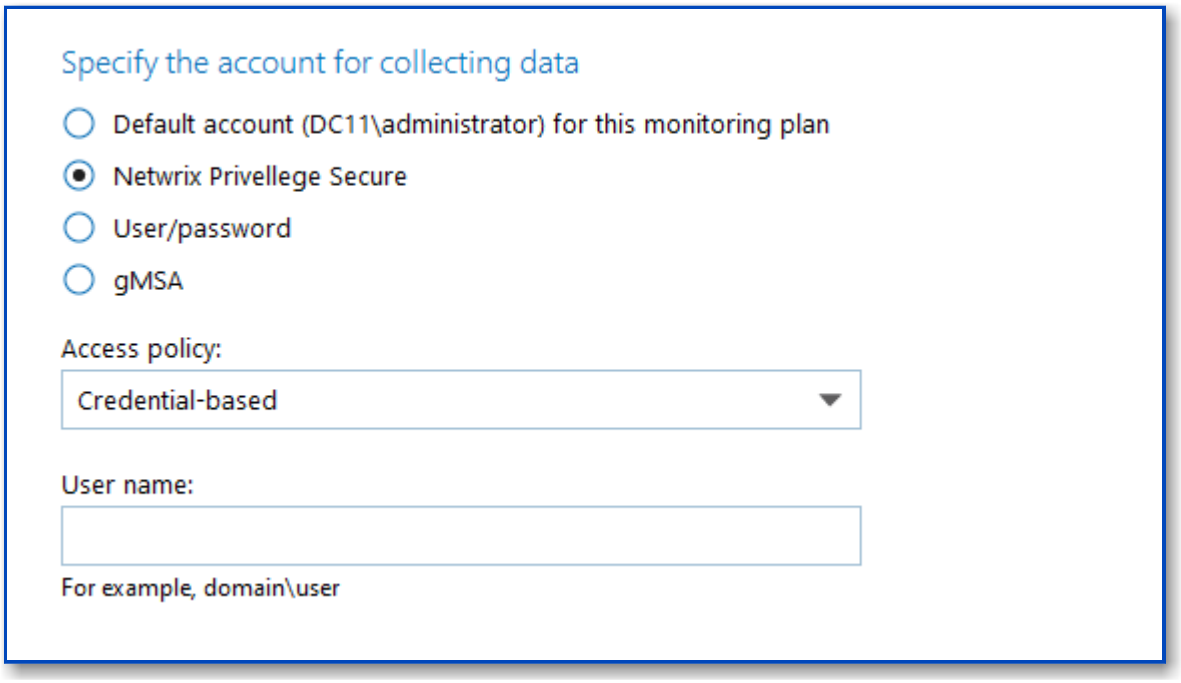
Considerations for Netwrix Privilege Secure Integration

Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

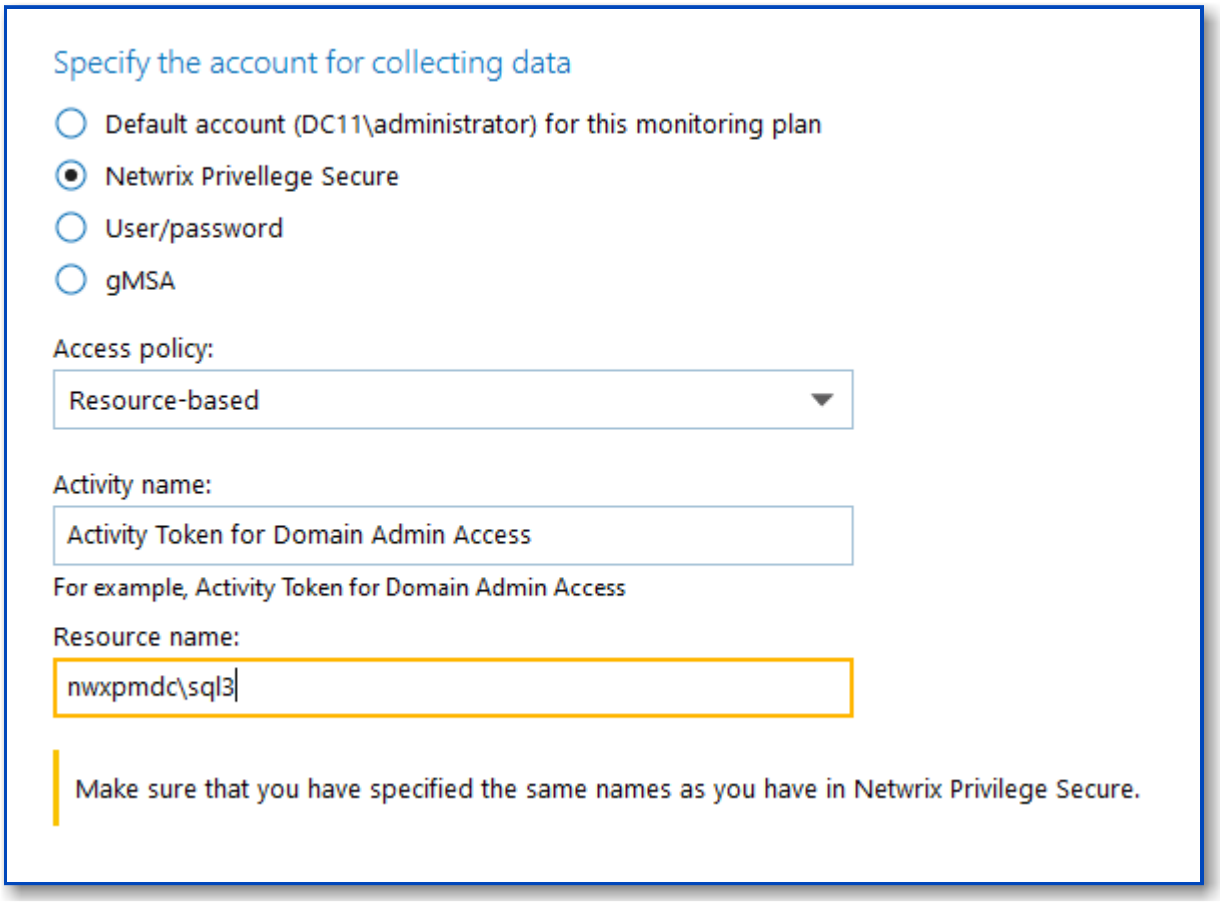
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

Logon Activity

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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.
    - For both new and existing monitoring plans, you can click **Launch Audit Configuration Assistant** (in the wizard step or in the plan settings, respectively) to launch a special tool that can detect current infrastructure settings and adjust them as needed for monitoring. See the Audit Configuration Assistant topic for additional information.
- Manually – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - 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)
- Remote Event Log Management (RPC-EPMAP)

See the following topics for additional information:

- Configure Basic Domain Audit Policies
- Configure Advanced Audit Policies
- Configure Security Event Log Size and Retention Settings
- Logon Activity Ports

Logon Activity Actions

Review a full list of actions captured when monitoring Logon Activity with Netwrix Auditor.

NOTE: Please consider the following:

- Logon activity by local accounts is not reported
- Logoff activity from workstations is not reported
- Logoff activity from Domain Controllers is reported

For the attributes marked with asterisk (*) *what* changed is not reported.

Action	Object Type	Attributes
Successful Logon	Logon	—
	Interactive Logon	A session was reconnected.
Failed Logon	Logon*	Cause description.

Action	Object Type	Attributes
	Interactive Logon	The number of matching events if the logon attempt failed several times during a short period of time.
Logoff	Interactive Logon	A session was disconnected. Session duration (if the corresponding logon was found).

Logon Activity Ports

Review a full list of protocols and ports required for monitoring Logon Activity.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 389 TCP port. On domain controllers in your domain (target), allow inbound connections to local 389 TCP port.

Port	Protocol	Source	Target	Purpose
389	TCP	Netwrix Auditor Server	Domain controllers	LDAP DC query Account resolve
53	TCP	Netwrix Auditor Server	DNS Server	DNS Client

Port	Protocol	Source	Target	Purpose
135 **+ Dynamic:** **1024 -65535**	TCP	Netwrix Auditor Server	Domain controllers	Windows Management Instrumentation Firewall configuration
135	TCP	Netwrix Auditor Server	Domain controllers	Service Control Manager Remote Protocol (RPC) Core Service installation
137 through 139	UDP	Netwrix Auditor Server	Domain controllers	Service Control Manager Remote Protocol (RPC) Core Service installation
445	TCP	Netwrix Auditor Server	Domain controllers	SMB 2.0/3.0

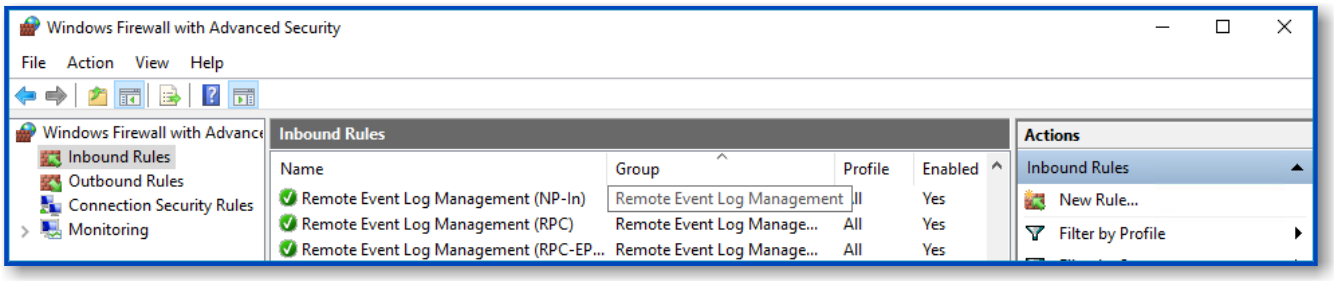
Configure Windows Firewall Inbound Connection Rules

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.

Step 1 – On every domain controller, navigate to **Start** → **Control Panel** and select **Windows Firewall**.

Step 2 – In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select Inbound Rules on the left.



Step 4 – Enable the following inbound connection rules:

- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

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 the Configure Advanced Audit Policies topic for additional information.

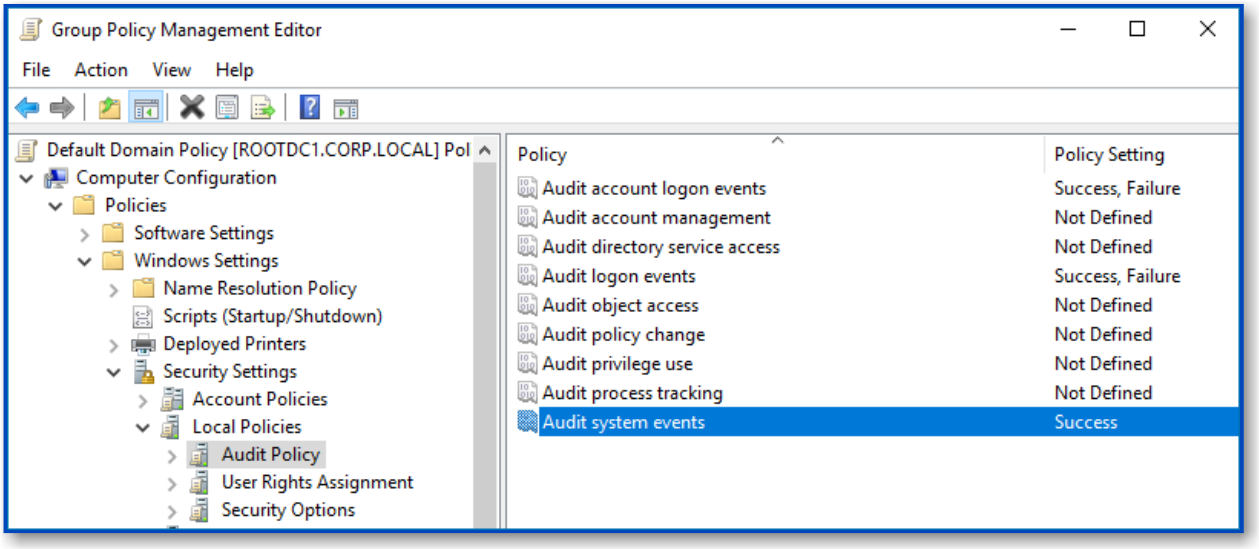
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016 and higher) or Administrative Tools (Windows 2012) **Group Policy Management.**

2. In the left pane, navigate to **Forest: <forest_name> > Domains > <domain_name> > Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.

3. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy.**

4. Configure the following audit policies.

Policy	Audit Events
Audit logon events	*"Success"* and *"Failure"*
Audit account logon events	*"Success"* and *"Failure"*
Audit system events	*"Success"*



5. Run the following command to update group policy: `gpupdate /force`

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:

- Configuring security options
- Configuring advanced audit policies

Configuring security options

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.

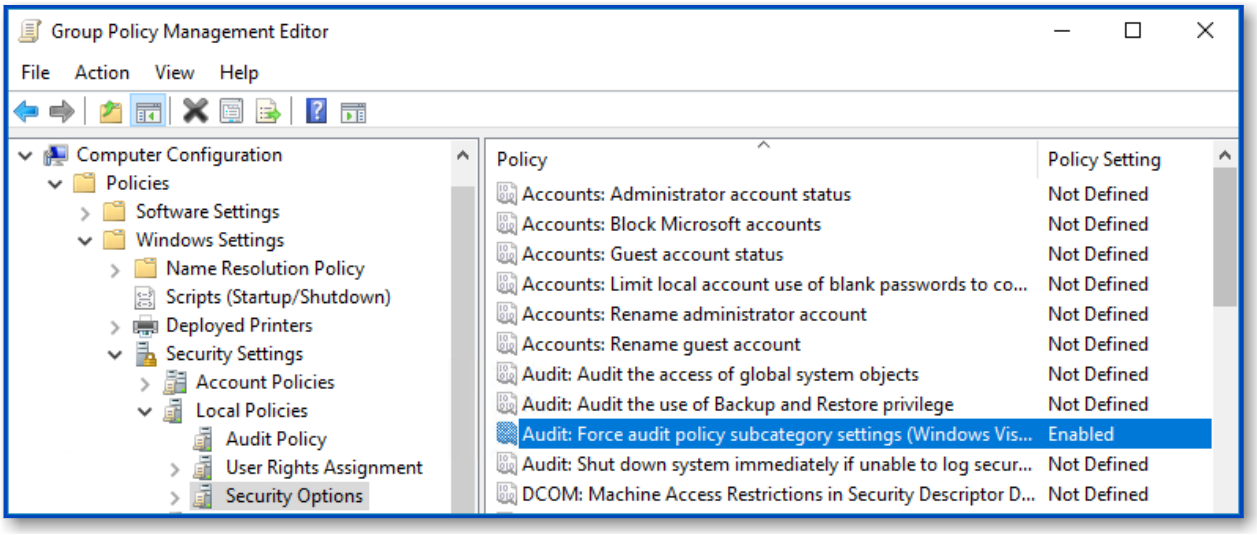
To do it, perform the following steps:

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016 and higher) or Administrative Tools (Windows 2012) **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. Run the following command to update group policy: `gpupdate /force`

Configuring advanced audit policies

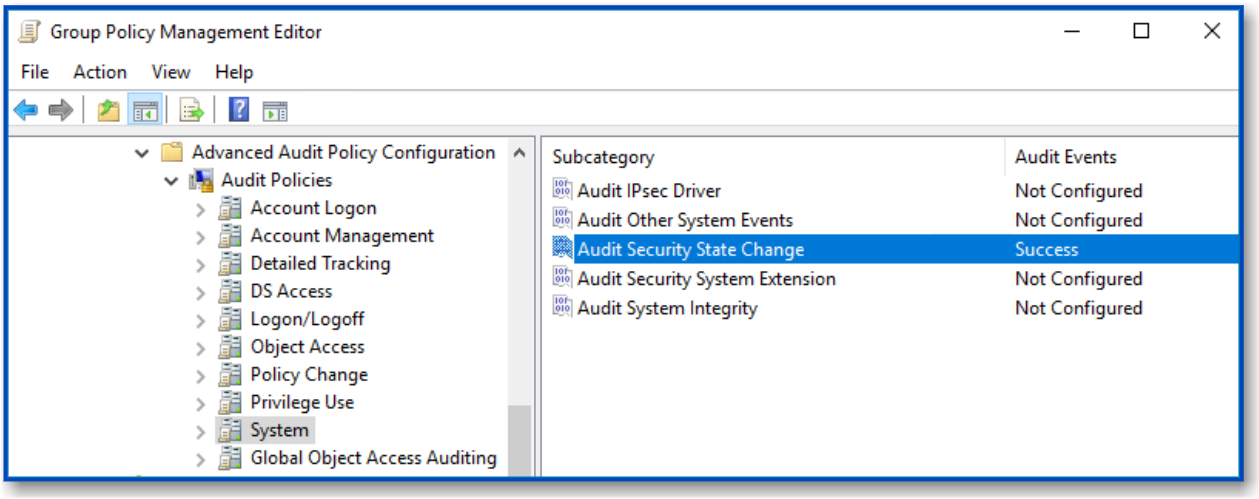
1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016 and higher) or Administrative Tools (Windows 2012) **Group Policy Management.**

2. In the left pane, navigate to **Forest: <forest_name> > Domains > <domain_name> > Domain Controllers**. Right-click the effective domain controllers policy (by default, it is the **Default Domain Controllers Policy**), and select **Edit** from the pop-up menu.

3. In the Group Policy Management Editor dialog, expand the Computer Configuration node on the left and navigate to Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies .

4. Configure the following audit policies.

Policy Subnode	Policy Name	Audit Events
Account Logon	• Audit Kerberos Service Ticket Operations • Audit Kerberos Authentication Service • Audit Credential Validation	*"Success"* and *"Failure"*
	• Audit Other Account Logon Events	*"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. Run the following command to update group policy: `gpupdate /force`

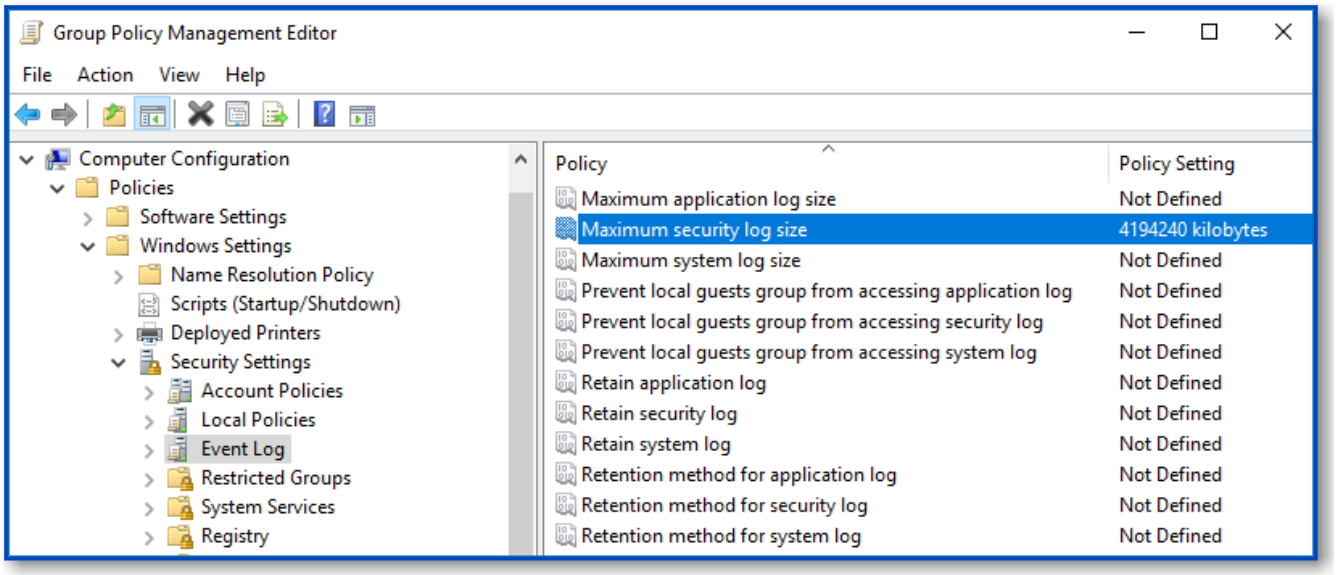
Configure Security Event Log Size and Retention Settings

Follow the steps to configure Security Event Log settings:

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

Step 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.

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



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

Step 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**.

Step 6 – Run the following command to update group policy: `gpupdate /force`

NOTE: After configuring security event settings via Group Policy, you may notice that the log size on a specific computer is not set correctly. In this case, follow the resolution steps from the Netwrix Knowledge base article to fix the issue: Security log settings do not apply via GPO.

Permissions for Logon Activity Auditing

Before you start creating a monitoring plan to audit the logon activity in your domain, plan for the domain 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.

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, then you can choose between account which belongs to the Domain Admins group or non-administrative account. See the Configure Non-Administrative Account to Collect Logon Activity topic for additional information.

NOTE: Data collecting account on the target server must be a member of the local Administrators group.

Configure Non-Administrative Account to Collect Logon Activity

This section contains instructions on how to configure an account to collect Logon Activity with minimum rights assignment. The instructions below apply only if you are going create a monitoring plan with disabled network traffic compression and do not want to adjust audit settings automatically.

Before creating an account, grant the *Read* permission on the SECURITY registry key (`HKEY_LOCAL_MACHINE\SECURITY`) for an admin account under which you will make changes in Group Policy.

Follow the steps to configure non-administrative account to collect logon activity:

Step 1 – Create a domain user with the following privileges:

- Back up files and directories. See the Configure the Back up Files and Directories Policy topic for additional information.
- Log on as a batch job. See the Permissions for Active Directory Auditing topic for additional information.
- Manage auditing and security log. See the Configure the Manage Auditing and Security Log Policy topic for additional information.

Step 2 – Grant the *Read* permission on the following registry keys to this user:

- `HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\EventLog\Security`

See the Assign Permission To Read the Registry Key topic for additional information on how to do it using Registry Editor.

Microsoft 365

Microsoft 365 audit configuration will cover the following components:

- Exchange Online
- Microsoft Entra ID
- MS Teams
- SharePoint Online

Microsoft Entra ID

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - Unified audit log must be enabled for a Tenant. See the Microsoft Turn auditing on or off article for additional information.
    - While no special settings are required. Remember to do the following:
        - Prepare a Data Collecting Account as described in Permissions for Microsoft Entra ID Auditing topic
        - Configure required protocols and ports, as described in the Microsoft Entra ID Ports topic

Microsoft Entra ID Ports

Review a full list of protocols and ports required for Netwrix Auditor for Microsoft Entra ID (formerly Azure AD).

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to the remote ports on the computer where Netwrix Auditor Server resides.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 80 TCP port.

Port	Protocol	Source	Target	Purpose
80	TCP/UDP	Netwrix Auditor Server	For a full list of Microsoft Entra ID URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	login.windows.net graph.windows.net manage.office.com
443	TCP/UDP	Netwrix Auditor Server	For a full list of Microsoft Entra ID URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	login.windows.net graph.windows.net manage.office.com

Permissions for Microsoft Entra ID Auditing

Auditor allows you to audit Office 365 organizations that have established modern authentication as their identity management approach, including support for multi-factor authentication (MFA). To learn more about modern authentication, refer to the following Microsoft article: What is modern authentication.

In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID (formerly Azure AD) application with appropriate access permissions. So, you should register an Microsoft Entra ID app and provide its settings to Auditor when configuring a monitored item.

For Microsoft Entra ID Auditing

To collect audit data in your cloud-based environment, Netwrix uses a dedicated Microsoft Entra ID application and leverages APIs access permissions granted to that app. To register such application and assign required permissions, a Microsoft Entra ID account with an administrative role will be required:

- If Basic Authentication is used:
  - A Microsoft Entra ID application named **Netwrix Auditor for Microsoft Entra ID** will be created automatically when Netwrix Auditor connects to the monitored item (Office 365 tenant) for the first time. Thus, you will need to prepare a Microsoft Entra ID user account with an administrative role in Microsoft Entra ID —to create an app and perform initial data collection.
  - Provide this user name and password in the monitored item properties. See the Microsoft Entra ID topic for additional information.

See the Using Basic Authentication with Microsoft Entra ID topic for additional information.

- If Modern Authentication is used:
  - Microsoft Entra ID application should be created manually by user with administrative role and assigned required permissions. See the Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID topic for additional information.
  - You will need to provide the Microsoft Entra ID app settings in the monitored item (Office 365 tenant) properties. See the Microsoft Entra ID topic for additional information.

See the Using Modern Authentication with Microsoft Entra ID topic for additional information.

Permissions for ongoing data collection will depend on data you plan to collect:

- To collect activity (event-based) data including logon attempts, the administrative role will be needed.
- To collect activity data without logons, the privileged role can be revoked from the specified account after the initial data collection.

Grant Admin Consent to a Tenant

Go back to the **Microsoft Entra ID admin center** > **Applications** > **App registrations** > **API permissions** and click **Grant admin consent for** <*tenant name*>. When prompted to confirm, click **Yes**.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra application and service principal that can access resources.

Configure Client Secret

Follow the steps to create a new client secret to be used by the app.

Step 1 – Go to **Manage** > **Certificates & secrets** and click **New client secret**.

Step 2 – Enter the description. From the expiration options select **24 months**.

Step 3 – Click **Add**.

Step 4 – The new secret will be displayed in the list. Click **Copy to clipboard** icon on the "Value" parameter on the right side of the screen.

See the following Microsoft article for more information on how to add a client secret: Add a client secret.

Obtain Tenant Name

Follow the steps to obtain the tenant name.

Step 1 – Go to **Microsoft Entra ID** > **Overview**.

Step 2 – In the Tenant Information section, locate the **Primary domain** field, copy its value and store to a safe location.

Using Basic Authentication with Microsoft Entra ID

With basic authentication, your Microsoft Entra ID organization will be accessed on behalf of a user. You will need to provide user name and password in the monitored item properties. Auditor will use this account to access the Microsoft Entra ID organization, automatically create

an Microsoft Entra ID app with required permissions, and perform initial data collection. For that, the user account will need an administrative role in the cloud-based infrastructure.

Further permission assignment will depend on the data you plan to collect:

- To collect activity data including **logon attempts**, the administrative role is required, as well as the Premium Plan license.
- To collect activity data without logons, the privileged role can be revoked from the specified account after the initial data collection. Ongoing audit data collection will leverage Microsoft APIs access permissions granted to Microsoft Entra ID app and, therefore, requires no tenant-level administrative permissions.

Required Roles and Permissions

To...	Requirement	Comment
Create Microsoft Entra ID application, run initial data collection, and perform Auditor upgrade from previous version	Any of the following role combinations: • Application Administrator & Privileged Role Administrator OR • Cloud Application Administrator & Privileged Role Administrator OR • *Global Admin*	Prepare a user account and specify it in the monitored item properties. See the and Microsoft Entra ID topics for additional information.
Collect audit data, including *Successful Logons* and/or *Failed Logons*	• *Security Reader* OR • *Security Administrator* OR • *Application Administrator* OR	To assign the non-privileged role, see

To...	Requirement	Comment
	• *Cloud Application Administrator* OR • *Global Administrator*	
Collect audit data (without logons)	Any of the following roles: • *Security Reader* OR • *Application Administrator* OR • *Cloud Application Administrator* OR • *Global Admin*	Assign the role you need, as explained above.

Assigning a Privileged Role for Microsoft Entra ID and Office 365

When configuring a monitored item for Microsoft Entra ID (formerly Azure AD) or Office 365 auditing with basic authentication, specify a data collecting account that has sufficient privileges in Microsoft Entra ID. This account should be able to create a dedicated application in your Microsoft Entra ID domain. Depending on your requirements and company policies, you can select one of the following approaches:

- Assign a privileged role (for example, *Application Administrator* & *Privileged Role Administrator*) to the account, then revoke it after the application creation and initial data collection, and assign a less-privileged role to this account (for example, *Security Reader*).
- Use the account with a privileged role on a regular basis. Any additional role assignments will not be necessary in this case. If you select this method, contact your security administrator to avoid violations of security policies in your organization.

NOTE: If you previously used a non-privileged account for Microsoft Entra ID data collection in your Netwrix Auditor, consider that after the upgrade you will have to perform the role assignment procedure again, selecting one of these approaches. Until then, data collection will not be performed.

Follow the steps to assign a privileged role to the account.

Step 1 – Sign in to Microsoft Entra ID portal using your Microsoft account.

Step 2 – Select Microsoft Entra ID on the left.

Step 3 – Select the account that you want to use as data collecting account, or create a new user.

Step 4 – Make sure you have disabled multi-factor authentication for this account.

Step 5 – Expand Directory role and select the role you need (for example, Global admin or any other privileged role).

Remember, In Microsoft Graph API, Microsoft Entra ID Graph API, and Microsoft Entra ID PowerShell, the Global admin role is identified as *Company Administrator* .

Step 6 – Click OK.

Step 7 – In Auditor, create a monitoring plan for auditing Microsoft Entra ID and specify this account with this privileged role on the Specify the account for collecting data step.

Step 8 – Wait until initial data collection completes.

Step 9 – Open Microsoft Entra ID portal and remove the privileged role from the account.

Step 10 – Assign a less-privileged role to this account.

A less privileged role has now been assigned to the account.

Assigning 'Security Administrator' or 'Security Reader' Role

To audit *Successful* and/or *Failed Logons* in Microsoft Entra ID, the Security Administrator or Security Reader role is required. Follow the steps to assign the role you need:

Step 1 – Sign in to Microsoft Entra ID portal using your Microsoft account.

Step 2 – Select Microsoft Entra ID portal on the left.

Step 3 – Navigate to Roles and administrators.

Step 4 – Click the Security administrator or Security Reader role.

Step 5 – Click Add member and select the account that you want to assign the role to.

Refer to the following Microsoft article: Microsoft Entra built-in roles for additional information on the Administrator role permissions.

Using Modern Authentication with Microsoft Entra ID

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario, Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID application with appropriate access permissions.

If you plan to implement this scenario, you should register an Microsoft Entra ID app manually and provide its settings to Auditor when configuring a monitored item.

Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID

Follow the steps to use a data collecting account with modern authentication.

Step 1 – Create and Register a New App in Microsoft Entra ID app that will be used for modern authentication. See the Create and Register a New App in Microsoft Entra ID section for additional information.

Step 2 – Grant required permissions to that application using Microsoft Entra ID app manifest. See the Grant Required Permissions section for additional information.

Step 3 – Configure client secret for that application. See the Configure Client Secret topic for additional information.

Step 4 – Obtain tenant ID – you will need it when configuring a monitored item (Office 365 tenant) settings. See the Obtain Tenant Name section for additional information.

Create and Register a New App in Microsoft Entra ID

You will need to create a dedicated app for each cloud-based data source you plan to audit: Microsoft Entra ID (formerly Azure AD), Exchange Online or SharePoint Online, or MS Teams. That is, if you plan to audit all of them, you should create 4 apps.

Follow the steps to register a new Microsoft Entra ID application.

Step 1 – Sign into the **Microsoft 365 Admin Center** with your *Global Administrator*, *Application Administrator* or *Cloud Application Administrator* account and go to the **Microsoft Entra ID admin center**.

Step 2 – Under the **App registrations** section, select **New registration**.

Step 3 – In the **Name** field, enter the application name.

Step 4 – In the **Supported account types** select who can use this application – use the **Accounts in this organizational directory only** option.

Step 5 – Click the **Register** button. Application **Redirect URI** is optional, you can leave it blank.

Step 6 – Your **Application (client) ID** is now available in the **Overview** section. Copy it to a safe location.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra ID application and service principal that can access resources.

Grant Required Permissions

You need to grant your new application the required API permissions. Microsoft Entra ID applications can be assigned *Delegated* or *Application* permissions:

- *Delegated* permissions require a signed-in user present who consents to the permissions every time an API call is sent.
- *Application* permissions are consented by an administrator once granted.

For the newly created app, you should use the *Application* permissions.

Follow the steps to grant required permissions.

Step 1 – Assign granular *Application* permissions required for Netwrix Auditor to collect data from the application. To do so, perform the following steps:

- Go to the **App registrations** and open the app you created to assign Auditor permissions.

- Go to **Manage > API permissions** and click **Add a permission** button.
- Assign the required permissions.

Permission assignment will depend on the data you plan to collect: activity data only or both activity and state-in-time data.

Requirement	Comment
Microsoft Entra ID app requires the following Application permissions: **1. Microsoft Graph** • **Directory.Read.All** • **AuditLog.Read.All** **2. Office 365 Management APIs** • **ActivityFeed.Read**	To learn how to assign required permissions, see the Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID section for additional information.

NOTE: You can also assign application permissions by editing Microsoft Entra app manifest. See the Using Modern Authentication with Microsoft Entra ID topic for additional information on how to assign the required permissions. Information about manifest is also described in the following Microsoft article: Microsoft Entra app manifest.

Step 2 – Grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app).

See the following Microsoft article for additional information: Grant admin consent in App registrations.

Grant Admin Consent to a Tenant

Go back to the **Microsoft Entra ID admin center** > **Applications** > **App registrations** > **API permissions** and click **Grant admin consent for** <*tenant name*>. When prompted to confirm, click **Yes**.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra application and service principal that can access resources.

Configure Client Secret

Follow the steps to create a new client secret to be used by the app.

Step 1 – Go to **Manage** > **Certificates & secrets** and click **New client secret**.

Step 2 – Enter the description. From the expiration options select **24 months**.

Step 3 – Click **Add**.

Step 4 – The new secret will be displayed in the list. Click **Copy to clipboard** icon on the "Value" parameter on the right side of the screen.

See the following Microsoft article for more information on how to add a client secret: Add a client secret.

Add Microsoft Entra ID monitoring plan

Follow the steps to add Microsoft Entra ID monitoring plan in the Netwrix Auditor.

Step 1 – In the Monitoring Plans, click **Add Plan** button.

Step 2 – Create a monitoring plan with the Microsoft Entra ID data source.

Step 3 – Add the Office 365 tenant item.

Step 4 – Click **Select**.

Step 5 – Enter your **tenant name**.

Step 6 – Choose modern authentication.

Step 7 – Enter the **Application ID** and **Application secret** you have created before.

Step 8 – Click **Add**.

Microsoft Entra ID monitoring plan has been added to Auditor and initial data collection has begun.

Obtain Tenant Name

Follow the steps to obtain the tenant name.

Step 1 – Navigate to **Microsoft Entra ID** > **Overview**.

Step 2 – In the Tenant Information menu, locate the **Primary domain** field and copy its value.

Step 3 – Store the tenant to a safe location.

Assign Application Permissions Using Manifest

Follow the steps to assign application permissions using manifest.

Step 1 – Under App registrations, select the newly created app.

Step 2 – Select **Manifest** on the left.

Step 3 – Locate the **requiredResourceAccess** property in the manifest and edit it with the following in the square brackets ([]).

Step 4 – Click **Save**.

Optionally, you can select **Download** to edit the manifest locally, and then use Upload to reapply it to your application.

The following Application permissions will be added:

- Microsoft Graph
  - Directory.Read.All
  - AuditLog.Read.All
- Office 365 Management APIs
  - ActivityFeed.Read

To add the required permissions, do one of the following:

- For the clear installation of Auditor 10.5, add roles as described below.
- If you upgraded Auditor from the version 10.0, replace all existing content under the **requiredResourceAccess** property.

```
{    "resourceAppId": "00000003-0000-0000-c000-000000000000",    "resour
ceAccess": [        {            "id": "b0afded3-3588-46d8-8b3d-9842eff7
78da",            "type": "Role"        },        {            "id": "7a
b1d382-f21e-4acd-a863-ba3e13f7da61",            "type": "Role"        }
   ]},{    "resourceAppId": "c5393580-f805-4401-95e8-94b7a6ef2fc2",    "
```

```
resourceAccess": [        {            "id": "594c1fb6-4f81-4475-ae41-0c
394909246c",            "type": "Role"         }    ]}
```

Exchange Online

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - Unified audit log must be enabled for a Tenant. See the Microsoft Turn auditing on or off article for additional information.
    - If you plan to audit non-owner mailbox access within your Exchange Online organization, 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
    - Perform the following configuration procedures:
        - Prepare a Data Collecting Account as described in the Permissions for Exchange Online Auditing topic
        - Configure required protocols and ports, as described in the Exchange Online Ports topic

Monitored Object Types and Attributes

See the full list of object types and attributes monitored by Exchange Online.

Mailboxes:

- UserMailbox
- SharedMailbox
- EquipmentMailbox
- LinkedMailbox
- RoomMailbox

Users:

- MailUser
- GuestMailUser
- User (Entity under UserMailbox or MailUser)

Groups:

- Role Group \ RoleGroup
- Mail-enabled security\MailUniversalSecurityGroup
- Dynamic distribution list\DynamicDistributionGroup
- Distribution list\MailUniversalDistributionGroup
- Microsoft 365 \ GroupMailbox
- ExchangeSecurityGroup

Folders:

- MailFolder
- Permissions:
- SendAs
- FullAccess

- ChangeOwner
- DeleteItem
- ExternalAccount
- ChangePermission
- ReadPermission

Azure:

- Group

Properties

Refer to the table to see Properties used in the Snapshot collection.

Type	Properties
User Mailbox **Shared Mailbox** **Equipment Mailbox** **Room Mailbox** **Linked Mailbox** **Mail-enabled security** **Dynamic distribution list** **Distribution list** **Microsoft 365**	Identity Name DisplayName DistinguishedName PrimarySmtpAddress Guid ArchiveGuid ExternalDirectoryObjectId ExchangeObjectId AuditEnabled AuditAdmin AuditDelegate

Type	Properties
	AuditLogAgeLimit Type OwnerUPN ExchangeSecurityDescriptorSddl SendOnBehalfPrincipals Sid IsDirSynced SerializationData ForwardingAddress ForwardingSMTPAddress DeliverToMailboxAndForward
ExchangeSecurityGroup	RecipientTypeDetails ExchangeObjectId ExternalDirectoryObjectId ExternalDirectoryObjectId Name
RoleGroup	ExchangeObjectId Name Sid UserFriendlyName

Type	Properties
	UserPrincipalName
MailUser **GuestMailUser** **User**	Identity Name DisplayName DistinguishedName SamAccountName UserPrincipalName ObjectCategory Id ExchangeObjectId ExternalDirectoryObjectId OrganizationId OriginatingServer RecipientType RecipientTypeDetails IsDirSynced Sid
MailFolder	ObjectType ObjectId DisplayName

Type	Properties
	MailboxGuid SecurityDescriptorSddl ParentFolderId ChildFolderCount UnreadItemCount TotalItemCount WellKnownName Childs
SendAs permissions	Trustee AccessControlType AccessRights IsInherited InheritanceType IsValid ObjectState
Permissions: **FullAccess** **ChangeOwner** **DeleteItem** **ExternalAccount**	MailboxIdentity User UserSid IsOwner AccessRights

Type	Properties
ChangePermission **ReadPermission**	IsInherited Deny InheritanceType

Refer to the table to see Properties used in membership collection.

Type	Properties
Azure group	Id Classification CreatedDateTime Description DisplayName GroupTypes Mail MailEnabled MailNickname OnPremisesLastSyncDateTime OnPremisesSecurityIdentifier OnPremisesSyncEnabled ProxyAddresses RenewedDateTime

Type	Properties
	SecurityEnabled Visibility ResourceProvisioningOptions

Monitored Actions

See the full list of actions monitored by Exchange Online.

Monitored Sign-In types:

- Delegate
- Admin

Delegate:

- A user who's been assigned the SendAs, SendOnBehalf, or FullAccess permission to another mailbox.
- An admin who's been assigned the FullAccess permission to a user's mailbox.

Admin:

- The mailbox is searched with one of the following Microsoft eDiscovery tools:
  - Content Search in the compliance portal.
  - eDiscovery or eDiscovery (Premium) in the compliance portal.
  - In-Place eDiscovery in Exchange Online.

• The mailbox is accessed by using the Microsoft Exchange Server MAPI Editor.

• The mailbox is accessed by an account impersonating another user. This occurs when the ApplicationImpersonation role is assigned to an account, such as an application, which is now actively accessing the data.

Sign-In types	Action Types	Description
Delegate **Admin**	Update	A message or any of its properties was changed.
Admin	Copy	A message or any of its properties was changed.
Delegate **Admin**	Move	A message was moved to another folder.
Delegate **Admin**	MoveToDeletedItems	A message was deleted and moved to the Deleted Items folder.
Delegate **Admin**	SoftDelete	A message was permanently deleted or deleted from the Deleted Items folder. Soft-deleted items are moved to the Recoverable Items folder.
Delegate **Admin**	FolderBind	A mailbox folder was accessed. This action is also logged when the admin or delegate opens the mailbox. **NOTE:** Audit records for folder bind actions performed by delegates are consolidated. One audit record is generated for individual folder access within a 24-hour period.

Sign-In types	Action Types	Description
Delegate **Admin**	SendAs	A message was sent using the SendAs permission. This permission allows another user to send the message as though it came from the mailbox owner.
Delegate **Admin**	SendOnBehalf	A message was sent using the SendOnBehalf permission. This permission allows another user to send the message on behalf of the mailbox owner. The message indicates to the recipient who the message was sent on behalf of and who actually sent the message.
Delegate **Admin**	Create	An item was created in the Calendar, Contacts, Draft, Notes, or Tasks folder in the mailbox (for example, a new meeting request is created). Creating, sending, or receiving a message isn't audited. Also, creating a mailbox folder isn't audited.

Exchange Online Ports

Review a full list of protocols and ports required for Netwrix Auditor for Office 365.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to the remote ports on the computer where Netwrix Auditor Server resides.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 80 TCP port.

Port	Protocol	Source	Target	Purpose
Exchange Online				
80	TCP	Netwrix Auditor Server	For a full list of Office 365 URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	outlook.office365.com graph.windows.net manage.office.com
443	TCP	Netwrix Auditor Server	For a full list of Office 365 URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	outlook.office365.com graph.windows.net manage.office.com

Permissions for Exchange Online Auditing

Auditor allows you to audit Office 365 organizations that have established modern authentication as their identity management approach, including support for multi-factor authentication (MFA). To learn more about modern authentication, refer to the following Microsoft article: What is modern authentication.

In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID (formerly Azure AD) application with appropriate access permissions. So, you should register an Microsoft Entra ID app and provide its settings to Auditor when configuring a monitored item.

Configure the Microsoft Entra ID App for Auditing Exchange Online

Follow the steps to use a data collecting account with modern authentication.

Step 1 – Create a Microsoft Entra ID app that will be used for modern authentication. See the Create and Register a New App in Microsoft Entra ID topic for additional information.

NOTE: After you start a new monitoring plan and select a data source in the first step, you will be asked to enter a default data collection account. However, this step is not needed for Exchange Online as it cannot be used. Thus, there is no need to grant any permissions to this account. Instead, you will need to configure a modern authentication app and give the necessary permissions there.

Step 2 – Grant required permissions to that application. See the Grant Required Permissions topic for additional information.

Step 3 – Grant required roles to that application. See the Grant Required Roles topic for additional information.

Step 4 – Configure client secret for that application. See the Configure Client Secret topic for additional information.

Step 5 – Obtain tenant ID – you will need it when configuring a monitored item (Office 365 tenant) settings. See the Obtain the Tenant Name topic for additional information.

Non-owner Mailbox Access Audit: Automatic Configuration

To prepare for non-owner mailbox access auditing in the Exchange Online organization, you will need to take several configuration steps, creating a Microsoft Entra ID app with the required permissions and instructing this app to automatically apply the necessary audit settings.

Follow the steps to configure a non-owner mailbox access audit.

Step 1 – Install the **Exchange Online PowerShell V3** module. There are three versions in the repository: 3.0.0, 3.1.0 and 3.2.0.

NOTE: Make sure you are using the version specified in the App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell Microsoft article.

Step 2 – In the **Microsoft Entra ID admin center**, create and register an Microsoft Entra ID app, as described in the related Connect to Exchange Online PowerShell Microsoft article.

Step 3 – At the top of the **Request API permissions** pane, click the **APIs my organization uses** tab and search for *Office 365 Exchange Online*.

Step 4 – Click on the *Office 365 Exchange Online* entry in the list of apps found.

Step 5 – Proceed with adding the permissions for this app: select **Application permissions** and then select **Exchange.ManageAsApp**.

Step 6 – Grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app). Go to the **new app settings > API permissions** and click **Grant admin consent for***<tenant name>*. When prompted to confirm granting, click **Yes**.

Step 7 – Go to **Azure Active Directory** — **Roles and administrators** and assign **Exchange Administrator** role.

Step 8 – Download the PowerShell script for certificate creation, as provided in the Generate a self-signed certificate Microsoft article.

Step 9 – To create a self-signed certificate to be used by the app, run the following command:

```
 .\Create-SelfSignedCertificate.ps1 -CommonName "MyCompanyName" -StartDat
e 2020-04-01 -EndDate 2022-04-01
```

where:

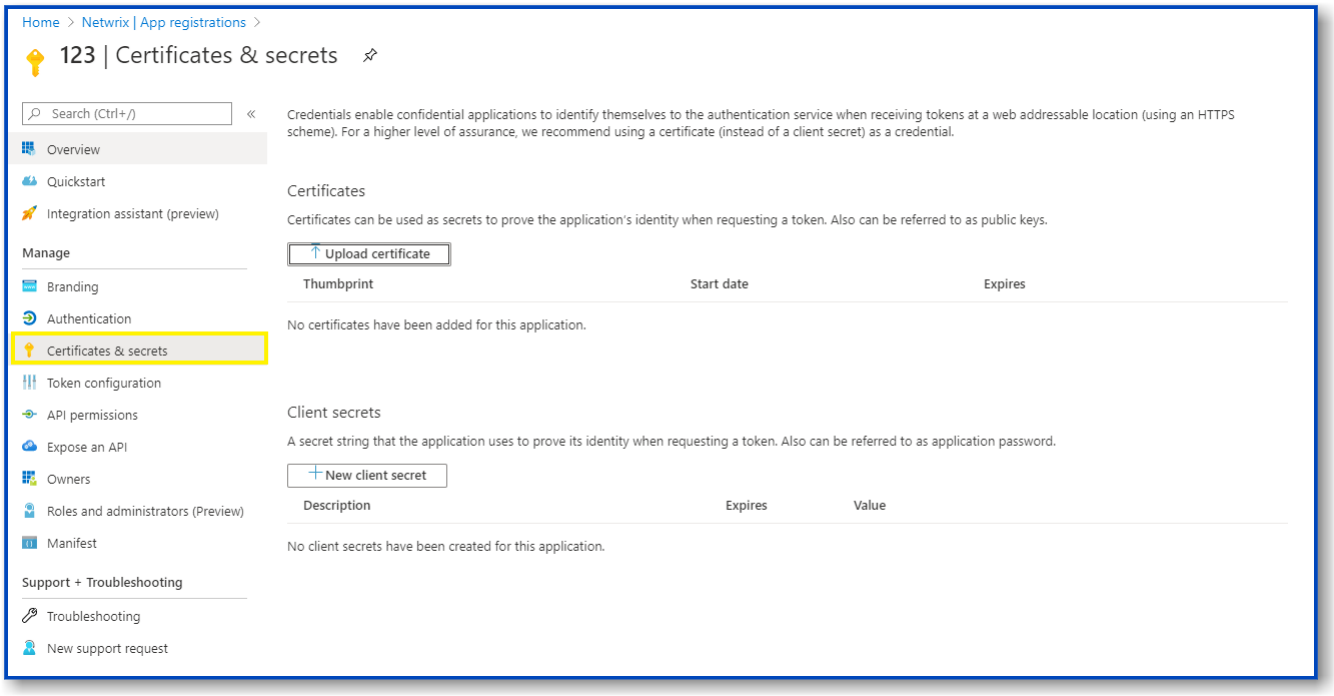
CommonName — specify *"Netwrix Auditor"*

StartDate — set to current date

EndDate — set to 2 years from now

Step 10 – When prompted to specify a password, click **Enter**.

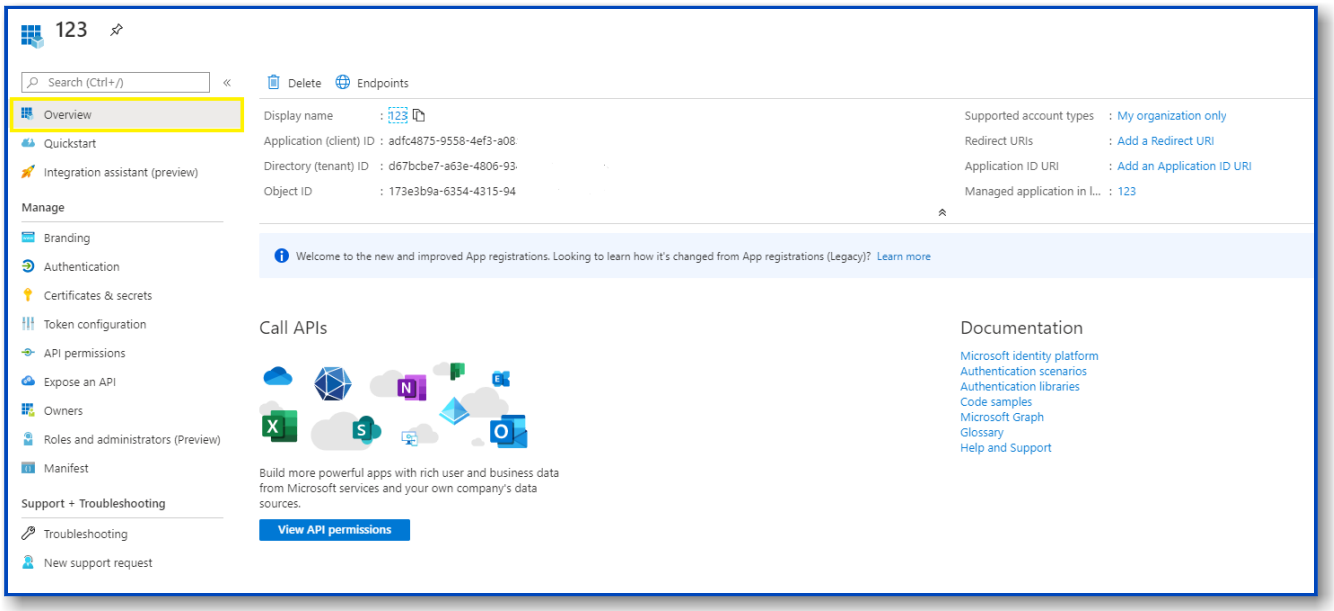
Step 11 – Go to **Manage > Certificates & secrets**, click **Upload certificate** and upload the*.crt* file you have just created.



Step 12 – To create Exchange Online connection session, you can provide certificate file path or thumbprint. If you want to use a file path, run the following command:

```
Connect-ExchangeOnline -CertificateFilePath "full_path_to_certificate" -AppID "yourAppId" -Organization "Office365_tenant_name"
```

Application (client ID) can be found in the **Overview** page.



For example:

```
Connect-ExchangeOnline -CertificateFilePath "C:\Path\MyCompanyName1.pfx"
-AppId "402b12a2-fb2b-4222-8f54-5596def1" -Organization "myorganization1
23.onmicrosoft.com"
```

You can use certificate thumbprint instead of file path. For that, import the certificate to the local certificate store, using the following command:

```
Import-PfxCertificate -FilePath "path_to_pfx_certificate" -CertStoreLocati
on Cert:\CurrentUser\My
```

Then run the command like following:

```
Connect-ExchangeOnline -CertificateThumbprint 6AEA5A82911AAA3F76FEE149B7B
52A70DDFD88 -AppId a14a 822d-f228-412b-9222-281de23 -Organization myorga
nization123.onmicrosoft.com
```

Finally, run the following command to end the session:

```
Disconnect-ExchangeOnline -Confim:$false
```

To automate the process described above, you can create a a script comprising the corresponding commands and schedule its launch.

Non-owner mailbox access audit: manual configuration

If you plan to manually apply the audit settings required to audit non-owner mailbox access in Exchange Online organization, you will need to create a remote PowerShell session to Exchange Online. Follow the steps to do so.

Step 1 – Install the Exchange Online PowerShell V2 module as described in the About the Exchange Online PowerShell module Microsoft article.

Make sure to install the latest version.

Step 2 – Launch PowerShell and connect to Exchange Online, as described in the About the Exchange Online PowerShell module Microsoft article.

Step 3 – Run the cmdlet, depending on the mailboxes you plan to audit (all mailboxes or selected individual mailbox):

For	Command
All	Execute the following cmdlet: `Get-ExoMailbox -PropertySets Minimum -RecipientTypeDetails UserMailbox,SharedMailbox,EquipmentMailbox,LinkedMailbox,RoomMailbox | Set-Mailbox -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create`
Selected	Execute the following cmdlet: `Set-Mailbox -Identity {0} -AuditEnabled $true -AuditAdmin Update,Copy,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create -AuditDelegate Update,Move,MoveToDeletedItems,SoftDelete,HardDelete,FolderBind,SendAs,SendOnBehalf,Create` Where the *{0}* character must be replaced with any 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=97da560450c942aba81b2da46c60858a-analyst • SamAccountName. Example: MANAG58792-1758064122

For	Command
	• (DN) Distinguished name. Example: CN=MJones,CN=Users,DC=enterprisedc1,DC=enterprise,DC=lo • User ID or User Principal Name. Example: MJones@enterprise.onmicrosoft.com If you are going to audit multiple individual mailboxes, run the cmdlet for each mailbox you need.

Access Exchange Online Using Modern Authentication

Support for modern authentication will allow you to audit the organizations where MFA is enabled for all users, including service accounts.

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID application with appropriate access permissions.

If you plan to implement this scenario, you should register an Microsoft Entra ID app manually and provide its settings to Netwrix Auditor when configuring a monitored item.

Create and Register a New App in Microsoft Entra ID

You will need to create a dedicated app for each cloud-based data source you plan to audit: Microsoft Entra ID (formerly Azure AD), Exchange Online or SharePoint Online, or MS Teams. That is, if you plan to audit all of them, you should create 4 apps.

Follow the steps to register a new Microsoft Entra ID application.

Step 1 – Sign into the **Microsoft 365 Admin Center** with your *Global Administrator*, *Application Administrator* or *Cloud Application Administrator* account and go to the **Microsoft Entra ID admin center**.

Step 2 – Under the **App registrations** section, select **New registration**.

Step 3 – In the **Name** field, enter the application name.

Step 4 – In the **Supported account types** select who can use this application – use the **Accounts in this organizational directory only** option.

Step 5 – Click the **Register** button. Application **Redirect URI** is optional, you can leave it blank.

Step 6 – Your **Application (client) ID** is now available in the **Overview** section. Copy it to a safe location.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra ID application and service principal that can access resources.

Grant Required Permissions

You need to grant your new application the required API permissions. Microsoft Entra ID applications can be assigned *Delegated* or *Application* permissions:

- *Delegated* permissions require a signed-in user present who consents to the permissions every time an API call is sent.
- *Application* permissions are consented by an administrator once granted.

For the newly created app, you should use the *Application* permissions.

Follow the steps to grant required permissions.

Step 1 – Assign granular *Application* permissions required for Netwrix Auditor to collect data from the application. To do so, perform the following steps:

- Go to the **App registrations** and open the app you created to assign Auditor permissions.
- Go to **Manage > API permissions** and click **Add a permission** button.
- Assign the required permissions.

Permission assignment will depend on the data you plan to collect: activity data only or both activity and state-in-time data.

To...	Requirement	Comment
Collect audit data	Microsoft Entra ID app requires the following **Application** permissions: 1. **Microsoft Graph**	To learn how to assign required permissions, see the Access Exchange Online Using Modern Authentication section for additional information.

To...	Requirement	Comment
	• Directory.Read.All • Application.ReadWrite.All • **Mail.ReadBasic.All** • **MailboxSettings.Read** 2. **Office 365 Management APIs** • **ActivityFeed.Read** 3. **Office 365 Exchange Online** • **Exchange.ManageAsApp**	
Roles	*Exchange Administrator* (*Exchange Service Administrator*) assigned to application service principal OR *Global Administrator* assigned to application service principal	

NOTE: You can also assign application permissions by editing Microsoft Entra app manifest. See the Access Exchange Online Using Modern Authentication topic for additional information on how to assign the required permissions. Information about manifest is also described in the following Microsoft article: Microsoft Entra app manifest.

Step 2 – Grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app).

See the following Microsoft article for additional information: Grant admin consent in App registrations.

Grant Admin Consent to a Tenant

Follow the steps to grant Admin consent to a tenant.

Go back to the **Microsoft Entra ID admin center** > **Applications** > **App registrations** > **API permissions** and click **Grant admin consent for** <*tenant name*>. When prompted to confirm, click **Yes**.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra application and service principal that can access resources.

Grant Required Roles

Follow the steps to grant the required Microsoft Entra ID (formerly Azure AD) roles to the new application.

Step 1 – In the Entra portal, click View under Manage Azure Active Directory.

Step 2 – Select **Roles and administrators** under Manage.

Step 3 – Select the Exchange Administrator or Global Administrator role.

Step 4 – On the Assignments page that appears, click Add assignments.

Step 5 – In the Add assignments flyout that appears, find and select the created application, and click Add.

See the following Microsoft article for additional information on how to create an application and service principal using Azure AD Admin portal: Create an Azure Active Directory application and service principal that can access resources.

Configure Client Secret

Follow the steps to create a new client secret to be used by the app.

Step 1 – Go to **Manage** > **Certificates & secrets** and click **New client secret**.

Step 2 – Enter the description. From the expiration options select **24 months**.

Step 3 – Click **Add**.

Step 4 – The new secret will be displayed in the list. Click **Copy to clipboard** icon on the "Value" parameter on the right side of the screen.

See the following Microsoft article for more information on how to add a client secret: Add a client secret.

Add an Exchange Online Monitoring Plan

Follow the steps to add Exchange Online monitoring plan in the Netwrix Auditor:

Step 1 – In the Monitoring Plans, click **Add Plan** button.

Step 2 – Create a monitoring plan with the Exchange Online data source.

Step 3 – Add the "Office 365 tenant" item.

Step 4 – Click **Select**.

Step 5 – Enter your tenant name.

Step 6 – Choose modern authentication.

Step 7 – Enter Application ID and Application secret you have created before.

Step 8 – Click **Add**.

Exchange Online monitoring plan has been added to Auditor and initial data collection has begun.

Obtain the Tenant Name

Follow the steps to obtain the tenant name.

Step 1 – Navigate to **Microsoft Entra ID** > **Overview**.

Step 2 – In the **Tenant information** locate the **Primary domain** field, copy its value and store to a safe location.

See the following Microsoft article for additional information on how to obtain tenant name: Locate important IDs for a user.

Then, create a corresponding monitoring plan in Netwrix Auditor and add an item (Office 365 tenant) to it. See the Microsoft Entra ID topic for additional information.

Configure Exchange Online State-in-Time Modern Authentication Manually

This topic contains general requirements for Exchange Online State-in-Time and Auto Audit for mailboxes Modern Authentication, configuration steps, including the ExchangeOnlineManagement PowerShell module installation.

Review the following:

- Requirements for Exchange Online Modern Authentication
- Install the ExchangeOnlineManagement PowerShell Module
- Configure Exchange Online Modern Authentication Manually

Requirements for Exchange Online Modern Authentication

General Requirements

- Windows Management Framework for your OS: Windows Management Framework 5.1
- .NET Framework 4.7.1 and above: Download .NET Framework 4.7.1

NOTE: If you have the FIPS option enabled you should proceed to Manual Exchange Online pre-configuration. See the Configure Exchange Online Modern Authentication Manuallysection for additional information.

Follow the steps to enable Exchange Online Auto Audit for mailboxes with Modern Authentication (automatic mode).

Step 1 – Install the ExchangeOnlineManagement Powershell module and dependencies (Nget package provider). Refer to the following Microsoft article for more information: About the Exchange Online PowerShell V2 module.

Step 2 – Generate the self-signed certificate.

Step 3 – Install the certificate to the *CurrentUser/My certificate* folder for the Local System account.

Step 4 – Install the certificate to the Microsoft Entra ID cloud application

Install the ExchangeOnlineManagement PowerShell Module

This section will be helpful for any case below:

- You encountered errors related to the ExchangeOnlineManagement PowerShell module
- You have the FIPS policy enabled
- You want to install the module manually

Follow the steps to install the module.

Step 1 – Install the Windows Management Framework for your OS: Windows Management Framework 5.1

Step 2 – Install **Nuget Package Provider** version 3.1 and above. Open **Windows PowerShell** and execute the following command:

```
Install-PackageProvider Nuget -MinimumVersion 2.8.5.201 -Scope AllUsers
```

Step 3 – Install the ExchangeOnlineManagement Powershell module. Open **Windows PowerShell** and execute the following command:

```
Install-Module ExchangeOnlineManagement
```

Review the following Microsoft technical article for more information: About the Exchange Online PowerShell V2 module

See next: Configure Exchange Online Modern Authentication Manually

NOTE: If you encountered errors executing the `Install-PackageProvider` cmdlet try to force PowerShell into TLS 1.2 mode and try again:

```
[System.Net.ServicePointManager]:SecurityProtocol = [System.Net.SecurityProtocolType] 'Ssl3 , Tls12'
```

NOTE: If you getting *"No match was found for the specified search criteria..."* message on the `Install-Module ExchangeOnlineManagement` execution, try to register default repository:

```
Register-PSRepository -Default
```

Configure Exchange Online Modern Authentication Manually

If you encountered errors from Netwrix Auditor during the automatic configuration of the certificate, complete the following steps.

Step 1 – In Netwrix Auditor, find your Exchange Online monitoring plan.

Step 2 – Click Update to force data collection.

If the error still persists, or you want to pre-configure the work with certificate, follow the instructions below:

Follow the steps to install a certificate.

Step 1 – Get your certificate or generate a self-signed certificate. The name must be *Netwrix_Auditor_MFA_<your_tenant_name>*

Step 2 – Save the certificate to the *CurrentUser/My certificate* folder for the Local System account.

Step 3 – Upload the certificate to the application selected in your monitoring plan or configure it automatically with Netwrix Auditor.

Follow the steps to generate a self-signed certificate.

Step 1 – Open Windows PowerShell as an Administrator and run the following commands:

```
# Create certificate$mycert = New-SelfSignedCertificate -DnsName "example.com" -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(1) -KeySpec KeyExchange# Export certificate to .pfx file$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $(ConvertTo-SecureString -String "your_password" -Force -AsPlainText)# Export certificate to .cer file$mycert | Export-Certificate -FilePath mycert.cer
```

Step 2 – Replace the `DnsName` parameter value with your certificate name (Netwrix_Auditor_MFA_<your_tenant_name>).

Follow the steps to install the certificate to the CurrentUser/My certificate folder.

Step 1 – Download PsExec to run Windows PowerShell session under the LocalSystem account;

Step 2 – Run Windows PowerShell as an Administrator, navigate to to PsExec.exe installation directory (use the 'CD' command), if necessary, and run the following command:

```
.\PsExec.exe -i -s powershell.exe
```

Step 3 – Verify that you are logged in as a Local System account. Run the following command:

```
whoami
```

Step 4 – Import the certificate. Run the following command:

```
Import-PfxCertificate -FilePath <path to your certificate> -CertStoreLocat
ion 'Cert:\CurrentUser\My' -Password (ConvertTo-SecureString -String "yo
ur_password" -AsPlainText -Force)
```

Where `path_to_certificate` is the full path to the certificate file.

You can also install the certificate with the '.cer' extension to the Microsoft Entra ID Portal or Netwrix Auditor will set it automatically during establishing a PowerShell connection with Exchange Online.

Assigning Application Permissions Using Manifest

Follow the steps to assign Exchange Online application permissions using manifest.

Step 1 – Under App registrations, select the newly created app.

Step 2 – Select **Manifest** on the left.

Step 3 – Locate the **requiredResourceAccess** property in the manifest and edit it with the following in the square brackets ([]).

Step 4 – Click **Save**.

Optionally, you can select **Download** to edit the manifest locally, and then click **Upload** to reapply it to your application.

Do one of the following:

- For the clear installation of Netwrix Auditor, add roles as described below.
- If you upgraded Netwrix Auditor from the version 10.0, replace all existing content under the **requiredResourceAccess** property.

```
{    "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",    "resour
ceAccess": [        {            "id": "dc50a0fb-09a3-484d-be87-e023b12c
6440",            "type": "Role"        }    ]},{    "resourceAppId": "0
0000003-0000-0000-c000-000000000000",    "resourceAccess": [        {
        "id": "693c5e45-0940-467d-9b8a-1022fb9d42ef",            "type"
: "Role"        },        {            "id": "1bfefb4e-e0b5-418b-a88f-73
c46d2cc8e9",            "type": "Role"        },        {            "id
```

```
": "7ab1d382-f21e-4acd-a863-ba3e13f7da61",            "type": "Role"
    },        {            "id": "40f97065-369a-49f4-947c-6a255697ae91",
                        "type": "Role"        }    ]},{    "resourceAppI
d": "c5393580-f805-4401-95e8-94b7a6ef2fc2",    "resourceAccess": [
  {            "id": "594c1fb6-4f81-4475-ae41-0c394909246c",
"type": "Role"        }    ]}
```

SharePoint Online

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in the following way:

- Manually – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
  - Unified audit log must be enabled for a Tenant. See the Microsoft Turn auditing on or off article for additional information.
  - Prepare a Data Collecting Account as described in the Permissions for SharePoint Online Auditing topic.
  - Configure required protocols and ports, as described in the SharePoint Online Ports topic.

Review a full list of object types and attributes Netwrix Auditor can collect on SharePoint Online. OneDrive for Business changes are reported as SharePoint Online.

Object type	Attributes
Site Collection	• Site Collection administrators

Object type	Attributes
Document	• Name • Permissions • URL • Data categories
Site	• Permissions
Site Collection Sharing Policy	• Sharing with external users • Sharing using anonymous access links
Sharing Policy	• Sharing with external users • Sharing using anonymous access links • External users must accept sharing invitations using the same account that the invitations were sent to • Sharing Domain Restriction mode • Allow domain list • Deny domain list • Require anonymous links expire in days
Group	• Members • Name
Folder	• Permissions
Sharing Invitation	• Expiration date • Shared with

Object type	Attributes
Access Request	• Expiration date

Sensitive data

Starting with the version 10, Netwrix Auditor is able to report about sensitive data in your IT infrastructure. Pay attention to the "*Data categories*" column in search and reports (for the "*Document*" object types only). See the Sensitive Data Discovery topic for additional information on how to enable monitoring of sensitive data in Netwrix Auditor.

SharePoint Online Ports

Review a full list of protocols and ports required for Netwrix Auditor for Office 365.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to the remote ports on the computer where Netwrix Auditor Server resides.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 80 TCP port.

Port	Protocol	Source	Target	Purpose
80	TCP	Netwrix Auditor Server	For a full list of Office 365 URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	login.windows.net graph.windows.net manage.office.com
443	TCP	Netwrix Auditor Server	For a full list of Office 365 URLs, refer to the following Microsoft support	login.windows.net graph.windows.net

Port	Protocol	Source	Target	Purpose
			article: Office 365 URLs and IP address ranges	manage.office.com

Permissions for SharePoint Online Auditing

Auditor allows you to audit Office 365 organizations that have established modern authentication as their identity management approach, including support for multi-factor authentication (MFA). To learn more about modern authentication, refer to the following Microsoft article: What is modern authentication.

In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID (formerly Azure AD) application with appropriate access permissions. So, you should register an Microsoft Entra ID app and provide its settings to Auditor when configuring a monitored item.

Authentication for SharePoint Online Auditing

To collect audit data from your SharePoint Online and OneDrive for Business, Netwrix Auditor uses a dedicated Microsoft Entra ID application and leverages APIs access permissions granted to that app. To register this application and assign required permissions, an Microsoft Entra ID account with an administrative role will be required:

- If Modern Authentication is used:
  - Microsoft Entra ID application should be created manually by user with administrative role and assigned required permissions. This app will allow you to collect both activity and state-in-time data. See the Configuring Microsoft Entra ID App for Auditing SharePoint Online section for additional information.
  - You will need to provide the Microsoft Entra ID app settings in the monitored item (Office 365 tenant) properties. See the Microsoft Entra ID topic for additional information.

See the Using Modern Authentication with SharePoint Online topic for additional information.

- If Basic Authentication is used:
  - Microsoft Entra ID application named **Netwrix Auditor for Microsoft Entra ID** will be created automatically when Netwrix Auditor connects to the monitored item

(Office 365 tenant) for the first time. Thus, you will need to prepare an Office 356 user account with an administrative role in Microsoft Entra ID — to create an app and perform initial data collection.
- Provide this user name and password in the monitored item properties. See the Microsoft Entra ID topic for additional information.

- Permissions for ongoing data collection will depend on data you plan to collect:

  - To collect both activity (event-based) and state-in-time data, the administrative role will be still needed.
  - To collect activity data only, the privileged role can be revoked from the specified account after the initial data collection.

See the Using Basic Authentication with SharePoint Online topic for additional information.

Using Modern Authentication with SharePoint Online

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario,Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID application with appropriate access permissions.

If you plan to implement such scenario, you should register an Microsoft Entra ID app manually and provide its settings to Auditor when configuring a monitored item.

Support for modern authentication will allow you to audit the organizations where MFA is enabled for all users, including service accounts.

Required configuration procedure includes several manual steps, as described in the corresponding section:

Configuring Microsoft Entra ID App for Auditing SharePoint Online

To collect data with modern authentication, you should do the following:

Step 1 – Create an Microsoft Entra ID app that will be used for modern authentication. See the Creating and registering a new app in Microsoft Entra ID topic for additional information.

Step 2 – Grant required permissions to that application using Microsoft Entra ID app manifest. See the Granting required permissions topic for additional information.

Step 3 – Configure client secret for that application. See the Configuring client secret topic for additional information.

Step 4 – Obtain tenant ID – you will need it when configuring a monitored item (Office 365 tenant) settings. See the Obtaining tenant name topic for additional information.

Creating and registering a new app in Microsoft Entra ID

You will need to create a dedicated app for each cloud-based data source you plan to audit: Microsoft Entra ID (formerly Azure AD), Exchange Online or SharePoint Online, or MS Teams. That is, if you plan to audit all of them, you should create 4 apps.

Follow the steps to register a new Microsoft Entra ID application.

Step 1 – Sign into the **Microsoft 365 Admin Center** with your *Global Administrator*, *Application Administrator* or *Cloud Application Administrator* account and go to the **Microsoft Entra ID admin center**.

Step 2 – Under the **App registrations** section, select **New registration**.

Step 3 – In the **Name** field, enter the application name.

Step 4 – In the **Supported account types** select who can use this application – use the **Accounts in this organizational directory only** option.

Step 5 – Click the **Register** button. Application **Redirect URI** is optional, you can leave it blank.

Step 6 – Your **Application (client) ID** is now available in the **Overview** section. Copy it to a safe location.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra ID application and service principal that can access resources.

Granting required permissions

You need to grant your new application the required API permissions. Microsoft Entra ID applications can be assigned *Delegated* or *Application* permissions:

- *Delegated* permissions require a signed-in user present who consents to the permissions every time an API call is sent.

- *Application* permissions are consented by an administrator once granted.

For the newly created app, you should use the *Application* permissions.

Follow the steps to grant required permissions.

Step 1 – Assign granular *Application* permissions required for Netwrix Auditor to collect data from the application. To do so, perform the following steps:

- Go to the **App registrations** and open the app you created to assign Auditor permissions.
- Go to **Manage > API permissions** and click **Add a permission** button.
- Assign the required permissions.

Permission assignment will depend on the data you plan to collect: activity data only or both activity and state-in-time data.

To...	Requirement	Comment
Collect activity and State-in-Time data	Microsoft Entra ID app requires the following **Application** permissions: 1. **Office 365 Management APIs** • **ActivityFeed.Read** 2. Microsoft Graph • Application.ReadWrite.All • Directory.Read.All 3. SharePoint • Sites.FullControl.All	To learn how to assign required permissions, see the Configuring Microsoft Entra ID App for Auditing SharePoint Online section for additional information.

NOTE: You can also assign application permissions by editing Microsoft Entra app manifest. See the Using Modern Authentication with SharePoint Online topic for additional information on how to assign the required permissions. Information about manifest is also described in the following Microsoft article: Microsoft Entra app manifest.

Step 2 – Grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app).

See the following Microsoft article for additional information: Grant admin consent in App registrations.

Granting Admin consent to a tenant

Go back to the **Microsoft Entra ID admin center** > **Applications** > **App registrations** > **API permissions** and click **Grant admin consent for** <*tenant name*>. When prompted to confirm, click **Yes**.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra application and service principal that can access resources.

Configuring client secret

Follow the steps to create a new client secret to be used by the app.

Step 1 – Go to **Manage** > **Certificates & secrets** and click **New client secret**.

Step 2 – Enter the description. From the expiration options select **24 months**.

Step 3 – Click **Add**.

Step 4 – The new secret will be displayed in the list. Click **Copy to clipboard** icon on the "Value" parameter on the right side of the screen.

See the following Microsoft article for more information on how to add a client secret: Add a client secret.

Obtaining tenant name

Follow the steps to obtain the tenant name.

Step 1 – Navigate to **Microsoft Entra ID** > **Overview**.

Step 2 – In the **Tenant information** locate the **Primary domain** field, copy its value and store to a safe location.

See the following Microsoft article for additional information on how to obtain tenant name: Locate important IDs for a user.

Then, create a corresponding monitoring plan in Netwrix Auditor and add an item (Office 365 tenant) to it. See the Microsoft Entra ID topic for additional information.

Assigning Application Permissions Using Manifest

Follow the steps to assign application permissions using Manifest.

Step 1 – Under **App registrations**, select the newly created app.

Step 2 – Select **Manifest** on the left.

Step 3 – Locate the **requiredResourceAccess** property in the manifest and edit it with the following in the square brackets ([]). Then click **Save**.

Optionally, you can select **Download** to edit the manifest locally, and then use Upload to reapply it to your application.

Do one of the following:

- For the clear installation of Netwrix Auditor, add roles as described in the Using Modern Authentication with SharePoint Online topic.
- If you upgraded Netwrix Auditor from the version 10.0, replace all existing content under the **requiredResourceAccess** property.

```
{    "resourceAppId": "00000003-0000-0ff1-ce00-000000000000",    "resour
ceAccess": [        {            "id": "678536fe-1083-478a-9c59-b99265e6
b0d3",            "type": "Role"        }    ]},{    "resourceAppId": "0
0000003-0000-0000-c000-000000000000",    "resourceAccess": [        {
        "id": "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",            "type"
: "Role"        },        {            "id": "7ab1d382-f21e-4acd-a863-ba
3e13f7da61",            "type": "Role"        }    ]},{"resourceAppId":
"c5393580-f805-4401-95e8-94b7a6ef2fc2","resourceAccess": [        {
       "id": "594c1fb6-4f81-4475-ae41-0c394909246c",            "type":
"Role"        }    ]}
```

Using Basic Authentication with SharePoint Online

With basic authentication, your SharePoint Online will be accessed on behalf of a user. You will need to provide Office 365 user name and password in the monitored item properties. To access the Microsoft Entra ID (formerly Azure AD)/Office 365 organization and perform initial data collection, the user account will need an administrative role in the cloud-based infrastructure.

The user account should be a *Cloud-only* account.

Further permission assignment will depend on the data you plan to collect:

- To collect both activity and state-in-time data, the administrative role will be still needed. See the table below for details.
- To collect activity data only, the privileged role can be revoked from the specified account after the initial data collection.

Required Roles and Permissions

To...	Requirement	Comment
Collect activity and state-in-time data	Any of the following role combinations: • Application Administrator & Privileged Role Administrator OR • Cloud Application Administrator & Privileged Role Administrator OR • *Global Admin* (*Company Administrator* in Microsoft Entra ID PowerShell terms)	Prepare a **Cloud-only** user account and specify it in the monitored item properties. See the SharePoint Online topic for additional information.
Collect activity data only	1. For initial connection to SharePoint Online, initial data collection, and Netwrix Auditor upgrade from previous version — any of the role combinations listed above. 2. After the initial data collection, the privileged roles can be revoked from this account.	

Assigning a Privileged Role for SharePoint and Office 365

When configuring a monitored item for Microsoft Entra ID (formerly Azure AD) or Office 365 auditing with basic authentication, specify a data collecting account that has sufficient privileges in Microsoft Entra ID. This account should be able to create a dedicated application in your Microsoft Entra ID domain. Depending on your requirements and company policies, you can select one of the following approaches:

- Assign a privileged role (for example, *Application Administrator* & *Privileged Role Administrator*) to the account, then revoke it after the application creation and initial data collection, and assign a less-privileged role to this account (for example, *Security Reader*).
- Use the account with a privileged role on a regular basis. Any additional role assignments will not be necessary in this case. If you select this method, contact your security administrator to avoid violations of security policies in your organization.

NOTE: If you previously used a non-privileged account for Microsoft Entra ID data collection in your Netwrix Auditor, consider that after the upgrade you will have to perform the role assignment procedure again, selecting one of these approaches. Until then, data collection will not be performed.

Follow the steps to assign a privileged role to the account.

Step 1 – Sign in to Microsoft Entra ID portal using your Microsoft account.

Step 2 – Select Microsoft Entra ID on the left.

Step 3 – Select the account that you want to use as data collecting account, or create a new user.

Step 4 – Make sure you have disabled multi-factor authentication for this account.

Step 5 – Expand Directory role and select the role you need (for example, Global admin or any other privileged role).

Remember, In Microsoft Graph API, Microsoft Entra ID Graph API, and Microsoft Entra ID PowerShell, the Global admin role is identified as *Company Administrator* .

Step 6 – Click OK.

Step 7 – In Auditor, create a monitoring plan for auditing Microsoft Entra ID and specify this account with this privileged role on the Specify the account for collecting data step.

Step 8 – Wait until initial data collection completes.

Step 9 – Open Microsoft Entra ID portal and remove the privileged role from the account.

Step 10 – Assign a less-privileged role to this account.

A less privileged role has now been assigned to the account.

MS Teams

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - Unified audit log must be enabled for a Tenant. See the Microsoft Turn auditing on or off article for additional information.
    - Prepare a Data Collecting Account as described in the Permissions for Teams Auditing topic.
    - Configure required protocols and ports, as described in the Teams Ports topic.

Auditor can monitor for operations with MS Teams entities, collect state-in-time snapshots and track changes to the object attributes. This section provides detailed information on these activities.

Starting with the version 10.5, AUDITOR is able to report about sensitive data in your IT infrastructure. Pay attention to the "*Data categories*" column in search and reports (for the "*Document*" object types only). Refer to Sensitive Data Discovery for detailed instructions on how to enable monitoring of sensitive data in AUDITOR .

Review a full list of object types and attributes Auditor can collect on SharePoint Online. OneDrive for Business changes are reported as SharePoint Online.

Object type	Attributes
Document	• Name • Permissions • URL • Data categories
Team	• Members • Name
Folder	• Permissions

Teams Ports

Review a full list of protocols and ports required for Netwrix Auditor for Microsoft Teams.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to the remote ports on the computer where Netwrix Auditor Server resides.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 80 TCP port.

Port	Protocol	Source	Target	Purpose
80	TCP	Netwrix Auditor Server	For a full list of Office 365 URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	outlook.office365.com graph.windows.net manage.office.com

Port	Protocol	Source	Target	Purpose
443	TCP	Netwrix Auditor Server	For a full list of Office 365 URLs, refer to the following Microsoft support article: Office 365 URLs and IP address ranges	outlook.office365.com graph.windows.net manage.office.com

Permissions for Teams Auditing

Auditor allows you to audit Office 365 organizations that have established modern authentication as their identity management approach, including support for multi-factor authentication (MFA). To learn more about modern authentication, refer to the following Microsoft article: What is modern authentication.

In this scenario, Netwrix Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a pre-configured Microsoft Entra ID (formerly Azure AD) application with appropriate access permissions. So, you should register an Microsoft Entra ID app and provide its settings to Auditor when configuring a monitored item.

NOTE: In some scenarios multi-factor authentication cannot be enabled for Auditor service account. If so, you will need to configure an account with basic authentication to access Microsoft Entra ID/Office 365 tenant.

For Microsoft Teams

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 in this topic. Then you will provide this account in the monitoring plan wizard (or in the monitored item settings).

Refer to the following topics to access Microsoft teams:

- Using Basic Authentication with MS Teams
- Using Modern Authentication with MS Teams

Using Basic Authentication with MS Teams

With basic authentication, your MS Teams organization will be accessed on behalf of a user. You will need to provide user name and password in the monitored item properties. Auditor will use this account to access the Microsoft Entra ID (formerly Azure AD) organization, automatically create a Microsoft Entra ID app with required permissions, and perform initial data collection. For that, the user account will need an administrative role in the cloud-based infrastructure.

Required Roles and Permissions

To...	Requirement	Comment
Create Microsoft Entra ID application, run initial data collection, and perform Auditor upgrade from previous version	Any of the following role combinations: • Application Administrator & Privileged Role Administrator & *Teams Administrator* OR • Cloud Application Administrator & Privileged Role Administrator & *Teams Administrator* OR • *Global Admin*	Prepare a user account and specify it in the monitored item properties. See the MS Teams topic for additional information.
Collect activity data	Any of the following roles: *Application Administrator* & *Teams Administrator* OR *Cloud Application Administrator* & *Teams Administrator* OR	

To...	Requirement	Comment
	Global Admin	

Assigning a Privileged Role for Microsoft Entra ID and Office 365

When configuring a monitored item for Microsoft Entra ID (formerly Azure AD) or Office 365 auditing with basic authentication, specify a data collecting account that has sufficient privileges in Microsoft Entra ID. This account should be able to create a dedicated application in your Microsoft Entra ID domain. Depending on your requirements and company policies, you can select one of the following approaches:

- Assign a privileged role (for example, *Application Administrator* & *Privileged Role Administrator*) to the account, then revoke it after the application creation and initial data collection, and assign a less-privileged role to this account (for example, *Security Reader*).
- Use the account with a privileged role on a regular basis. Any additional role assignments will not be necessary in this case. If you select this method, contact your security administrator to avoid violations of security policies in your organization.

NOTE: If you previously used a non-privileged account for Microsoft Entra ID data collection in your Netwrix Auditor, consider that after the upgrade you will have to perform the role assignment procedure again, selecting one of these approaches. Until then, data collection will not be performed.

Follow the steps to assign a privileged role to the account.

Step 1 – Sign in to Microsoft Entra ID portal using your Microsoft account.

Step 2 – Select Microsoft Entra ID on the left.

Step 3 – Select the account that you want to use as data collecting account, or create a new user.

Step 4 – Make sure you have disabled multi-factor authentication for this account.

Step 5 – Expand Directory role and select the role you need (for example, Global admin or any other privileged role).

Remember, In Microsoft Graph API, Microsoft Entra ID Graph API, and Microsoft Entra ID PowerShell, the Global admin role is identified as *Company Administrator* .

Step 6 – Click OK.

Step 7 – In Auditor, create a monitoring plan for auditing Microsoft Entra ID and specify this account with this privileged role on the Specify the account for collecting data step.

Step 8 – Wait until initial data collection completes.

Step 9 – Open Microsoft Entra ID portal and remove the privileged role from the account.

Step 10 – Assign a less-privileged role to this account.

A less privileged role has now been assigned to the account.

See the Permissions for Microsoft Entra ID Auditing topic for additional information.

Using Modern Authentication with MS Teams

Modern authentication allows you to audit MS Teams environments without using an account with basic authentication. The configuration procedure includes several manual steps, as described below.

Access MS Teams Using Modern Authentication

This option is recommended for organizations that use modern authentication as the identity management approach, having multi-factor authentication (MFA) enabled for their user accounts. In this scenario, Auditor will access the cloud-based infrastructure via Microsoft Graph and other modern APIs, being authenticated through a preconfigured Microsoft Entra ID (formerly Azure AD) application with appropriate access permissions.

If you plan to implement this scenario, you should register an Microsoft Entra ID app manually and provide its settings to Netwrix Auditor when configuring a monitored item.

Configure the Microsoft Entra ID App for Auditing MS Teams

Follow the steps to use a data collecting account with modern authentication:

Step 1 – Create an Microsoft Entra ID app that will be used for modern authentication. See the Create and Register a New App in Microsoft Entra ID section for additional information.

Step 2 – Grant required permissions to that application using Microsoft Entra ID app manifest. See the Grant Required Permissions topic for additional information.

Step 3 – Configure client secret for that application. See the Configure Client Secret section for additional information.

Step 4 – Obtain the tenant ID. You will need it when configuring a monitored item (Office 365 tenant) settings. See the Obtain Tenant Name topic for additional information.

Create and Register a New App in Microsoft Entra ID

You will need to create a dedicated app for each cloud-based data source you plan to audit: Microsoft Entra ID (formerly Azure AD), Exchange Online or SharePoint Online, or MS Teams. That is, if you plan to audit all of them, you should create 4 apps.

Follow the steps to register a new Microsoft Entra ID application.

Step 1 – Sign into the **Microsoft 365 Admin Center** with your *Global Administrator*, *Application Administrator* or *Cloud Application Administrator* account and go to the **Microsoft Entra ID admin center**.

Step 2 – Under the **App registrations** section, select **New registration**.

Step 3 – In the **Name** field, enter the application name.

Step 4 – In the **Supported account types** select who can use this application – use the **Accounts in this organizational directory only** option.

Step 5 – Click the **Register** button. Application **Redirect URI** is optional, you can leave it blank.

Step 6 – Your **Application (client) ID** is now available in the **Overview** section. Copy it to a safe location.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra ID application and service principal that can access resources.

Grant Required Permissions

You need to grant your new application the required API permissions. Microsoft Entra ID applications can be assigned *Delegated* or *Application* permissions:

- *Delegated* permissions require a signed-in user present who consents to the permissions every time an API call is sent.
- *Application* permissions are consented by an administrator once granted.

For the newly created app, you should use the *Application* permissions.

Follow the steps to grant required permissions.

Step 1 – Assign granular *Application* permissions required for Netwrix Auditor to collect data from the application. To do so, perform the following steps:

- Go to the **App registrations** and open the app you created to assign Auditor permissions.
- Go to **Manage > API permissions** and click **Add a permission** button.
- Assign the required permissions.

Permission assignment will depend on the data you plan to collect: activity data only or both activity and state-in-time data.

-

Requirement	Comment
Microsoft Entra ID app requires the following Application permissions: • **Microsoft Graph** ◦ **Application.ReadWrite.All** ◦ **AuditLog.Read.All** ◦ **Directory.Read.All** ◦ **Sites.Read.All** ◦ **TeamMember.Read.All** • **Office 365 Management APIs** ◦ **ActivityFeed.Read** • **SharePoint** ◦ **Sites.FullControl.All**	To learn how to assign required permissions, see the Configure the Microsoft Entra ID App for Auditing MS Teams topic for additional information.

NOTE: You can also assign application permissions by editing Microsoft Entra app manifest. See the Using Modern Authentication with MS Teams topic for additional information on how to

assign the required permissions. Information about manifest is also described in the following Microsoft article: Microsoft Entra app manifest.

Step 2 – Grant admin consent to the tenant (that is, for the Office 365 organization whose audit data will be collected by the newly registered app).

See the following Microsoft article for additional information: Grant admin consent in App registrations.

Grant Admin Consent to a Tenant

Content/EnterpriseAuditor/Solutions/ActiveDirectoryPermissionsAnalyzer/Computers/Overview.htm

Go back to the **Microsoft Entra ID admin center** > **Applications** > **App registrations** > **API permissions** and click **Grant admin consent for** <*tenant name*>. When prompted to confirm, click **Yes**.

See the following Microsoft article for additional information on how to create an application and service principal using Microsoft Entra ID Admin portal: Create an Microsoft Entra application and service principal that can access resources.

Configure Client Secret

Follow the steps to create a new client secret to be used by the app.

Step 1 – Go to **Manage** > **Certificates & secrets** and click **New client secret**.

Step 2 – Enter the description. From the expiration options select **24 months**.

Step 3 – Click **Add**.

Step 4 – The new secret will be displayed in the list. Click **Copy to clipboard** icon on the "Value" parameter on the right side of the screen.

See the following Microsoft article for more information on how to add a client secret: Add a client secret.

Add MS Teams monitoring plan

Follow the steps to add MS Teams monitoring plan in the Netwrix Auditor.

Step 1 – In the Monitoring Plans, click **Add Plan** button.

Step 2 – Create a monitoring plan with the MS Teams data source.

Step 3 – Add the "Office 365 tenant" item.

Step 4 – Click **Select**.

Step 5 – Enter your tenant name.

Step 6 – Choose modern authentication.

Step 7 – Enter Application ID and Application secret you have created before.

Step 8 – Click **Add**.

MS Teams monitoring plan has been added to Auditor and initial data collection has begun.

Obtain Tenant Name

Follow the steps to obtain the tenant name.

Step 1 – Navigate to **Microsoft Entra ID** > **Overview**.

Step 2 – In the **Tenant information** locate the **Primary domain** field, copy its value and store to a safe location.

See the following Microsoft article for additional information on how to obtain tenant name: Locate important IDs for a user.

Then, create a corresponding monitoring plan in Netwrix Auditor and add an item (Office 365 tenant) to it. See the Microsoft Entra ID topic for additional information.

Assign Application Permissions Using Manifest

Follow the steps to assign application permissions using manifest.

Step 1 – Under **App registrations**, select the newly created app.

Step 2 – Select **Manifest** on the left.

Step 3 – Locate the **requiredResourceAccess** property in the manifest and edit it with the following in the square brackets ([]).

Step 4 – Click **Save**.

Optionally, you can select **Download** to edit the manifest locally, and then use Upload to reapply it to your application.

Depending on your installation type, do one of the following:

- For the clear installation, add roles as described below.
- If you upgraded Auditor from previous version, replace all existing content under the requiredResourcdAccess property.


```
{    "resourceAppId": "00000003-0000-0000-c000-000000000000",    "resour
ceAccess": [        {            "id": "332a536c-c7ef-4017-ab91-33697092
4f0d",            "type": "Role"        },        {            "id": "b0
afded3-3588-46d8-8b3d-9842eff778da",            "type": "Role"        },
        {            "id": "1bfefb4e-e0b5-418b-a88f-73c46d2cc8e9",
      "type": "Role"        },        {            "id": "7ab1d382-f21e-
4acd-a863-ba3e13f7da61",            "type": "Role"        },        {
         "id": "660b7406-55f1-41ca-a0ed-0b035e182f3e",            "type"
: "Role"        }    ]},{    "resourceAppId": "00000003-0000-0ff1-ce00-0
00000000000",    "resourceAccess": [        {            "id": "678536fe
-1083-478a-9c59-b99265e6b0d3",            "type": "Role"        }    ]},
{    "resourceAppId": "c5393580-f805-4401-95e8-94b7a6ef2fc2",    "resour
ceAccess": [        {            "id": "594c1fb6-4f81-4475-ae41-0c394909
246c",            "type": "Role"        }    ]}
```


Network Devices

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

- Configure Cisco ASA Devices
- Configure Cisco IOS Devices
- Cisco Meraki Dashboard
- Configure Cisco Meraki Devices
- Configure Fortinet FortiGate Devices
- Configure PaloAlto Devices
- Configure Juniper Devices
- Configure SonicWall Devices
- Configure HPE Aruba Devices
- Configure Pulse Secure Devices

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

Network Devices Ports

Review a full list of protocols and ports required for Netwrix Auditor for Network Devices.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to the remote ports on the computer where Netwrix Auditor Server resides.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 514 UDP port.

Port	Protocol	Source	Target	Purpose
514	UDP	Monitored network devices	Netwrix Auditor Server	Getting events from monitored devices
443	TCP	Netwrix Auditor Server	Cisco Meraki Dashboard	*.meraki.com

Configure Cisco ASA Devices

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - On the Cisco ASA Device:
        - 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.

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>

   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. Configure the devices to show username for failed logons:

   hostname(config)# no logging hide username

Cisco ASA Devices

Review a full list of object types Netwrix Auditor can collect on Cisco ASA network devices.

Object type	Actions	Event ID
Cisco ASA devices		
Authentication	• Successful logon	• 716038 • 611101 • 113012
	• **Failed logon**	• 716039 • 611102 • 113021 • 113020 • 113015 • 109031 • 109025 • 109024 • 109022 • 109017 • 109010 • 109008

Object type	Actions	Event ID
		• 109006 • 107001 • 107002
Configuration	• Modified / Modify (Failed attempt)	• 111004 • 111010 • 612001 • 612002 • 612003
	• **Read / Read (Failed attempt)**	• 111007
	• **Removed / Remove (Failed attempt)**	• 111003 • 112001 • 208005
CPU	• Modified / Modify (Failed attempt)	• 211003
Device state	• Modified / Modify (Failed attempt)	• 199009
Environment (IPMI)	• Modified / Modify (Failed attempt)	• 735002 • 735004 • 735006

Object type	Actions	Event ID
		• 735007 • 735008 • 735012 • 735014 • 735016 • 735018 • 735019 • 735022 • 735023 • 735025 • 735027 • 735028 • 735029
GroupPolicy	• Add / Added (Failed attempt)	• 502111
	• **Removed / Remove (Failed attempt)**	• 502112
Logon	• Successful logon	• 605005
	• **Failed logon**	• 308001 • 605004

Object type	Actions	Event ID
RAM	• Modified / Modify (Failed attempt)	• 211004
Session	• Successful Logon	• 716001 • 713228 • 722033 • 722022 • 725001 • 725002 • 725003 • 606001
	• **Logoff**	• 725007 • 722023 • 722030 • 722031 • 716002 • 713259 • 606002 • 302014 • 302304 • 302016
	• **Failed Logon**	• 722056

Object type	Actions	Event ID
		• 725006 • 725014
Rule	• Activated	• 733101
URL	• Read / Read (Failed attempt)	• 716003 • 716004
User	• Add / Added (Failed attempt)	• 502101
	• **Modified / Modify (Failed attempt)**	• 502103 • 113006 • 113007
	• **Removed / Remove (Failed attempt)**	• 502102

Configure Cisco IOS Devices

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
  - 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.

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# logging 192.168.1.5

Cisco IOS Devices

Review a full list of object types Netwrix Auditor can collect on Cisco IOS network devices.

Object type	Actions	Event ID
Cisco IOS		
Attribute	• Read	• INFO: AAA/ATTR
Authentication	• Successful logon	• IKEv2:
	• **Failed logon**	• IKEv2-ERROR:
Configuration	• Modified	• CONFIG_I
Device state	• Modified	• UPDOWN • CHANGED
Environment	• Modified	• FAN_FAULT • OVER_TEMP
Logon	• Successful logon	• LOGIN_SUCCESS
	• **Failed logon**	• LOGIN_FAILED

Object type	Actions	Event ID
Session	• Successful Logon	• IKEv2:
	• **Logoff**	• %FW-6-SESS_AUDIT_TRAIL
	• **Failed Logon**	• IKEv2-ERROR:

Cisco Meraki Dashboard

Before creating a monitoring plan to audit your Cisco Meraki devices, plan for the account that will be used for data collection. See the Data Collecting Account topic for additional information. You will provide this account in the monitoring plan wizard.

Changes that are collected with the basic authorization:

- Add/Modify/Remove User
- Configuration
- Successful logon
- Failed logon

Changes that are collected with the API:

- Add/Modify/Remove User
- Configuration

Configure Cisco Meraki Dashboard Account

Before you start creating a monitoring plan to audit your Cisco Meraki devices, plan for the data collection should meet the requirements listed below. Then you will provide this account in the item.

For Basic Authorization

Since accounts with multi-factor authentication are not supported, you need to create a special cloud account with read-only permissions and disabled multi-factor authentication.

Follow the steps to configure Cisco Meraki Dashboard item.

Step 1 – Sign in to the Cisco Meraki Dashboard.

Step 2 – Create a dashboard account as described in the following Cisco Meraki article: Getting Started

Step 3 – Make sure that the read-only permissions assigned to the account. For more information about Meraki permissions, refer to the following Cisco Meraki article: Managing Dashboard Administrators and Permissions.

Step 4 – Log in to this account and navigate to **My Profile** at the top of the dashboard.

Step 5 – Find the section labeled SMS authentication.

Step 6 – Make sure that the SMS authentication parameter is set to **OFF**. For more information about authentication, refer to the following Cisco Meraki article: Two-Factor Authentication.

NOTE: This account is for Netwrix Auditor purposes. Do not forget to switch back to your account.

To Collect Data via API Key

To work with multi-factor authentication (MFA) accounts, you need to generate an API key during authorization.

Follow the steps to create an API key for the Meraki Dashboard API.

Step 1 – Log in to your Cisco Meraki Dashboard account.

Step 2 – Click on your username in the top-right corner of the dashboard to open the drop-down menu.

Step 3 – Select **My profile**.

Step 4 – In the **My profile** page, scroll down to the **API access** section.

Step 5 – Click on the **Generate new API key** button. You may be prompted to enter your account password for security verification.

Once generated, the API key will be displayed on the screen. Make sure to copy and save the API key in a secure location, as it won't be displayed again for security reasons.

NOTE: Logons are not collected on the board due to technical limitations from the Meraki API.

Configure Cisco Meraki Devices

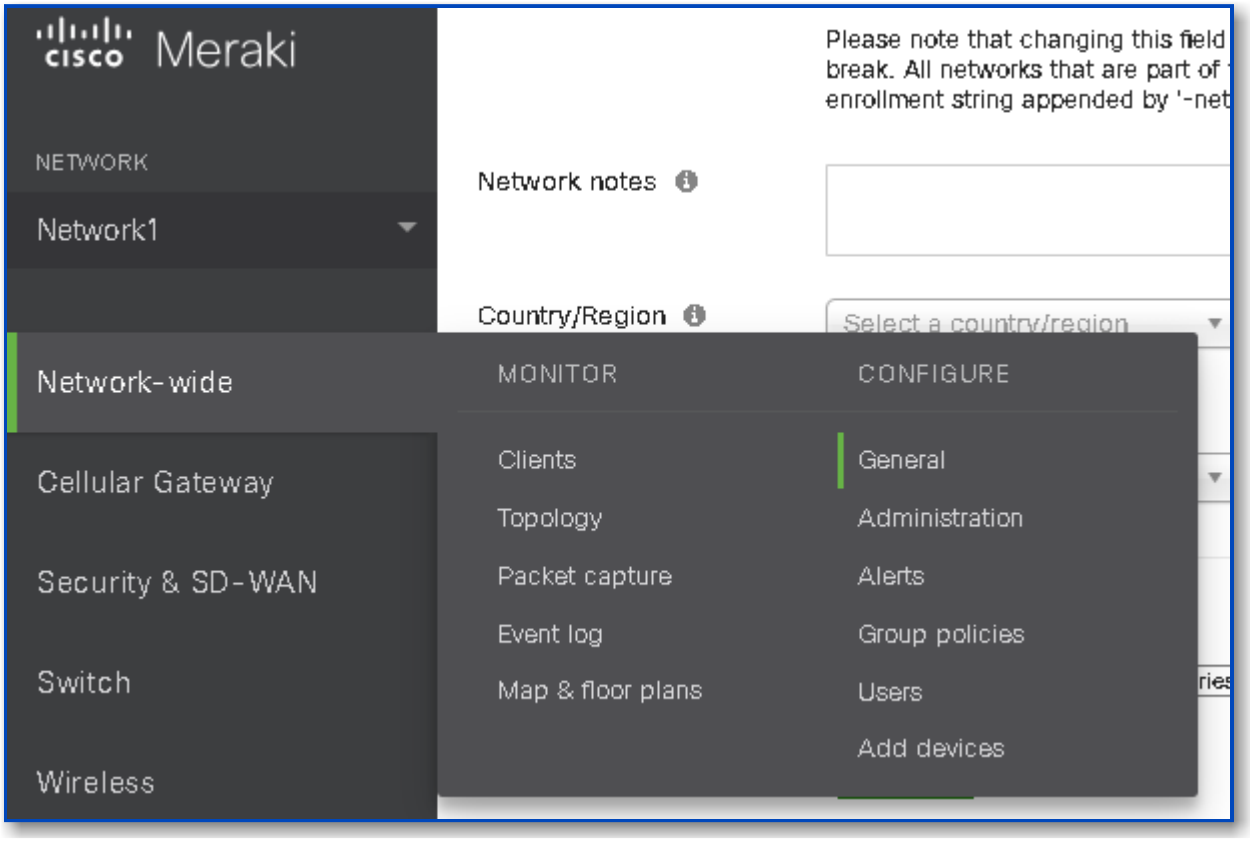
To configure Cisco Meraki devices, configure the Syslog server for each of your networks.

Netwrix recommends assigning a unique identificator to each Cisco Meraki device; otherwise, the product may count them as a single anonymous device.

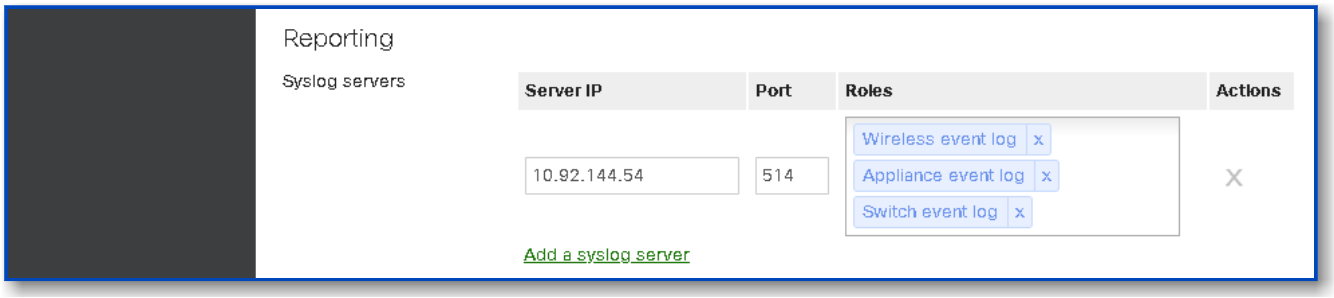
Follow the steps to configure the Syslog server.

Step 1 – Sign in to Cisco Meraki Dashboard.

Step 2 – Navigate to **Network wide** > **Configure** > **General**.



Step 3 – Locate the Reporting section and click Add a syslog server.



Step 4 – In the dialog that opens, complete the following fields:

Option	Description
Server IP	Provide the IP address of the computer that hosts your Netwrix Auditor Server.
Port	Provide the port configured in your monitoring plan for Network Devices (514 by default). See theNetwork Devices topic for additional information.
Roles	Select the following roles: • Appliance event log • Switch event log • Wireless event log

Cisco Meraki Devices Configuration

If you need any additional information about the Cisco Meraki devices configuration, refer to Cisco documentation: Syslog Server Overview and Configuration.

Review a full list of object types Netwrix Auditor can collect on Cisco Meraki network devices.

Object type	Actions	Event ID
Cisco Meraki		
Authentication	• Successful Logon	• 716038 • 113012 • client_vpn_connect • authentication on • type=8021x_auth • type=8021x_eap_success • type=splash_auth • type=wpa_auth
	• **Failed Logon**	• 113020 • 113015 • type=8021x_eap_failure • type=disassociation
Session	• Successful Logon	• 716001 • 713228 • 722033 • 722022

Object type	Actions	Event ID
		• 725001 • 725002 • 725003
	• **Failed Logon**	• 716039 • 722056 • 725006 • 725014
	• **Logoff**	• 716002 • 713259 • 302014 • 302304 • 302016 • 722023 • 725007 • 722030 • 722031 • 113019 • `client_vpn_disconnect` • `type=8021x_deauth`

Object type	Actions	Event ID
		• type=8021x_client_deauth • type=wpa_deauth
Rule	• Activated	• ids-alerts • security_event ids_alerted • security_event security_filtering_file_scanned • security_event security_filtering_disposition_change • type=device_packet_flood • type=rogue_ssid_detected • type=ssid_spoofing_detected
URL	• Read / Failed read	• 716003 • 716004

Configure Fortinet FortiGate Devices

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - The target Fortinet Fortigate device must be configured via Command Line Interface (CLI) as described below.

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

   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. To enable CEF format in some previous FortiOS versions, unselect the Enable CSV checkbox.

4. Click Apply.

Fortinet FortiGate Devices

Review a full list of object types Netwrix Auditor can collect on Fortinet FortiGate devices.

Object type	Actions	LogID
Authentication	• Successful logon	• 0100029002 • 0102043039 • 0102043008 • 0102043029 • 0101037138 / `act=tunnel-up`
	• Failed logon	• 0100029003 • 0101039426 • 0102043009 • 0102043010 • 0101037121 / XAUTH `authentication failed`
Configuration	• Copied	• 0100032211 • 0100032300
	• Modified / Modify (Failed attempt)	• 0100032102 • 0100032104 • 0100032400 • 0100044544 • 0100044545 • 0100044546 • 0100044547 • 0100032565

Object type	Actions	LogID
		• 0100032566 • 0100032567 • 0100032571 • 0100032199 • 0100032202 • 0100032203 • 0100032234 • 0100032235 • 0108035012 • 0100044548
	• Read / Read (Failed attempt)	• 0100032226 • 0100032228 • 0100032229 • 0100032230
Logon	• Successful logon	• 0100032001
	• Failed logon	• 0100032002 • 0100032021
Rule	• Activated	• 0419016384 • 0419016385 • 0419016386 • 0421016399 • 0211008192

Object type	Actions	LogID
		• 0211008194 • 0203008200 • 0212008448 • 0261008450 • 0212008452 • 0212008457 • 0213008704 • 0213008706 • 0263008720 • 0262008960 • 0262008962 • 0262008964 • 0262008966 • 0262008968 • 0262008970 • 0262008972 • 0262008974 • 0211009234 • 0211009236 • 0202009248 • 0954024576 • 0954024579 • 0720018432 • 0720018433

Object type	Actions	LogID
		• 0720018434
Session	• Logoff	• 0100032003 • 0102043040
User	• Add / Remove	• 0100032129 • 0100032131 • 0100032132
	• Modified / Modify (Failed attempt)	• 0100032130

Configure HPE Aruba Devices

To configure your HPE Aruba devices, enable logging to multiple Syslog servers and configure logging levels. Do one of the following:

- To configure HPE Aruba devices via Command Line Interface
- To configure HPE Aruba devices through the Management Console

To configure HPE Aruba devices via Command Line Interface

1. Log in to the Command Line Interface (CLI).
2. Enter the following command to start configuration mode:

   # configure terminal
3. Specify IP address of the computer that hosts your Netwrix Auditor Server to send Syslog messages to:

   # logging <ipaddr> severity information
4. Specify event level for the following categories: security, system, user, wireless, network:

   # logging network level information

logging security level information

logging system level information

logging user level information

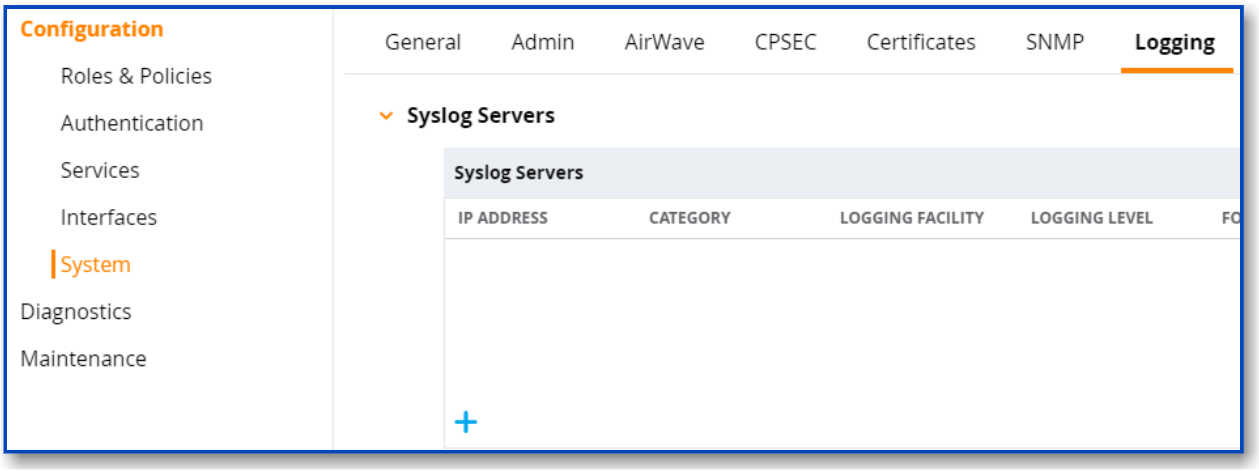
logging wireless level information

5. Apply configuration changes:

   # write memory

To configure HPE Aruba devices through the Management Console

1. Log in to HPE Aruba web interface.
2. Navigate to Mobility Master and select a device or a group of devices you want to monitor with Netwrix Auditor.
3. Navigate to Configuration → System → Logging and click + to add a new Syslog Server.

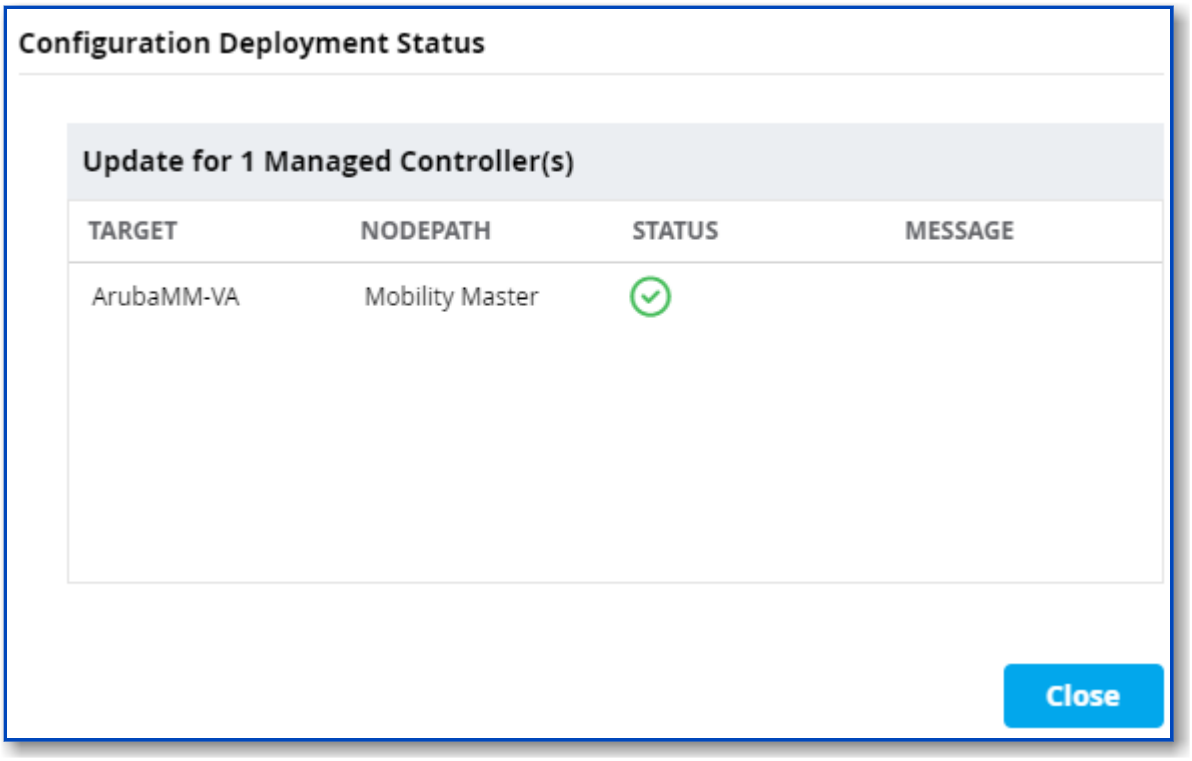


4. In the Add New Syslog Servers dialog, complete the following fields:

Option	Description
IP address	Provide the IP address of the new server.
Category	Select None.
Logging facility	Leave empty.

Option	Description
Logging level	Select Informational.
Format	Select None.

5. Click Submit. The new server is added to the Syslog Servers list.
6. Click Pending Changes on the right.
7. In the Pending Changes for <X> Managed Controller(s) dialog, select the device you want to apply changes to.
8. Click Deploy Changes.
9. If the configuration is correct, you will see the following wizard:



10. Navigate to Configuration → System → Logging and expand the Logging Levels.
11. Select the Informational value for the following parameters:
    - network
    - system
    - wireless
    - security
12. Deploy pending changes for the logging level: repeat steps 6 - 8.

HPE Aruba Devices

Review a full list of object types Netwrix Auditor can collect on HPE Aruba devices.

Object type	Actions	Message ID
Authentication	• Successful logon	• 103047 • 103082 • 103085 • 105004 • 133008 • 133005 • 133098
	• Failed logon	• 522275 • 541003 • 103046 • 103048 • 103067 • 103068 • 103083 • 103084 • 105002 • 105003 • 133009 • 133006 • 133099

Object type	Actions	Message ID
		• 125021 • 125022 • 125031 • 125033 • 125071
Configuration	• Add / Added (Failed attempt) • Removed / Remove (Failed attempt) • Modified / Modify (Failed attempt)	• 125012 • (109012 • 124037 • 124036 • 124010 • 325013 • 325014 • 325015 • 325018 • 325019 • 335000 • 335009 • 335016 • 335015 • 335010 • 335013 • 335001 • 305034 • 335002

Object type	Actions	Message ID
		• 125063 • 125065 • 125067 • 125069 • 125064 • 125066 • 125068 • 125060 • 125061 • 125072 • 133109 • 133022 • 133104 • ECC error detected • Power supply failure
Rule	Activated	• 127054 • 127033 • 127068 • 127034 • 127006 • 127086 • 127064 • 127073 • 127079 • 127082 • 127084

Object type	Actions	Message ID
		• 127080 • 127083 • 127081 • 127085 • 127007 • 127074 • 127036 • 127047 • 127066 • 127043 • 127067 • 127087 • 127078 • 127035 • 127032 • 127072 • 127088 • 127109 • 127071 • 127077 • 127065 • 127075 • 127046 • 127044

Object type	Actions	Message ID
		• 127045 • 127116 • 127117 • 127052 • 127053 • 127069 • 127070 • 127014 • 127015 • 127016 • 127017 • 127029 • 127030 • 127008 • 127009 • 127010 • 127011 • 127028 • 127061 • 127062 • 127063 • 127039 • 127040 • 127041 • 127042
Session	• Logoff	• 103040 • 103042 • 103056 • 103069

Object type	Actions	Message ID
Logon	• Logon succeeded	• 125023 • 125024 • 125032 • 125070
Role	• Add / Added (Failed attempt)	• 125011

Configure Juniper Devices

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - The target Juniper device must be configured via JunOS Command Line Interface (CLI) as described below.

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). Network Devices

set system syslog time-format <current year>

commit

Juniper Devices

Review a full list of object types Netwrix Auditor can collect on Juniper network devices.

Object type	Actions	Event ID
Logon	• Successful logon	• LOGIN_INFORMATION • Accepted keyboard-interactive/pam • WEB_AUTH_SUCCESS • JADE_AUTH_SUCCESS
	• Failed logon	• LOGIN_FAILED • SSHD_LOGIN_FAILED LIBJNX_LOGIN_ACCOUNT_LOCKED

Object type	Actions	Event ID
		• WEB_AUTH_FAIL JADE_AUTH_FAILURE
Authentication	• Successful Logon	• FWAUTH_HTTP_USER_AUTH_ACCEPTED • FWAUTH_WEBAUTH_SUCCESS • FWAUTH_FTP_USER_AUTH_ACCEPTED • FWAUTH_TELNET_USER_AUTH_ACCEPTED • DYNAMIC_VPN_AUTH_OK
	• Failed logon	• FWAUTH_HTTP_USER_AUTH_FAIL • FWAUTH_WEBAUTH_FAIL • FWAUTH_FTP_USER_AUTH_FAIL • FWAUTH_TELNET_USER_AUTH_FAIL • DYNAMIC_VPN_AUTH_FAIL
Configuration	• Modified / Modify (Failed attempt)	• UI_FACTORY_OPERATION

Object type	Actions	Event ID
		• UI_INITIALSETUP_OPERATION • UI_RESCUE_OPERATION • UI_LOAD_EVENT • UI_CFG_AUDIT_OTHER • UI_CFG_AUDIT_SET: • UI_CFG_AUDIT_NEW • UI_CFG_AUDIT_SET_SECRET • UI_COMMIT: • UI_COMMIT_PROGRESS • UI_COMMIT_COMPLETED • UI_COMMIT_AT_COMPLETED • UI_COMMIT_NOT_CONFIRMED • UI_COMMIT_CONFIRMED_REMINDER • UI_COMMIT_AT_ABORT • UI_COMMIT_AT_FAILED • UI_COMMIT_COMPRESS_FAILED • UI_COMMIT_ROLLBACK_FAILED
Rule	• Activated	• RT_SCREEN_ICMP • RT_SCREEN_IP

Object type	Actions	Event ID
		• RT_SCREEN_TCP • RT_SCREEN_TCP_DST_IP • RT_SCREEN_TCP_SRC_IP • RT_SCREEN_UDP • AV_VIRUS_DETECTED_MT • ANTISPAM_SPAM_DETECTED_MT • IDP_APPDDOS_APP_ATTACK_EVENT • IDP_APPDDOS_APP_STATE_EVENT • IDP_ATTACK_LOG_EVENT

Configure PaloAlto Devices

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - Create a Syslog Server profile and syslog forwarding for the target PaloAlto device via Web Interface as described below.

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

Follow the steps to configure a Syslog server profile.

Step 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>).

Step 2 – In the Web Interface, navigate to **Device** > **Server Profiles** > **Syslog**.

Step 3 – Click **Add** and specify profile name, for example, *"SyslogProf1"*.

Step 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.
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.

Follow the steps to configure syslog forwarding.

Step 1 – In the Web Interface, navigate to **Device** > **Log Settings**.

Step 2 – For System, Config, and User ID logs, click Add and enter unique name of your syslog server.

Step 3 – On the syslog panel, click Add and select the syslog profile you created above.

Step 4 – Click **Commit** and review the logs on the syslog server.

NOTE: After configuring the monitoring plan, Netwrix Auditor will listen to the logs forwarded by the Palo Alto device.

PaloAlto Devices

Review a full list of object types Netwrix Auditor can collect on PaloAlto network devices.

Object type	Actions	Event ID
Logon	• Successful logon	• logged in
	• **Failed logon**	• failed authentication for user • authentication failed for user
Authentication	• Successful Logon	• authentication succeeded for user • USERID,login, • globalprotectportal-auth-succ
	• **Failed Logon**	• authentication failed for user • globalprotectportal-auth-fail
Configuration	• Modified / Modify (Failed attempt)	• commit

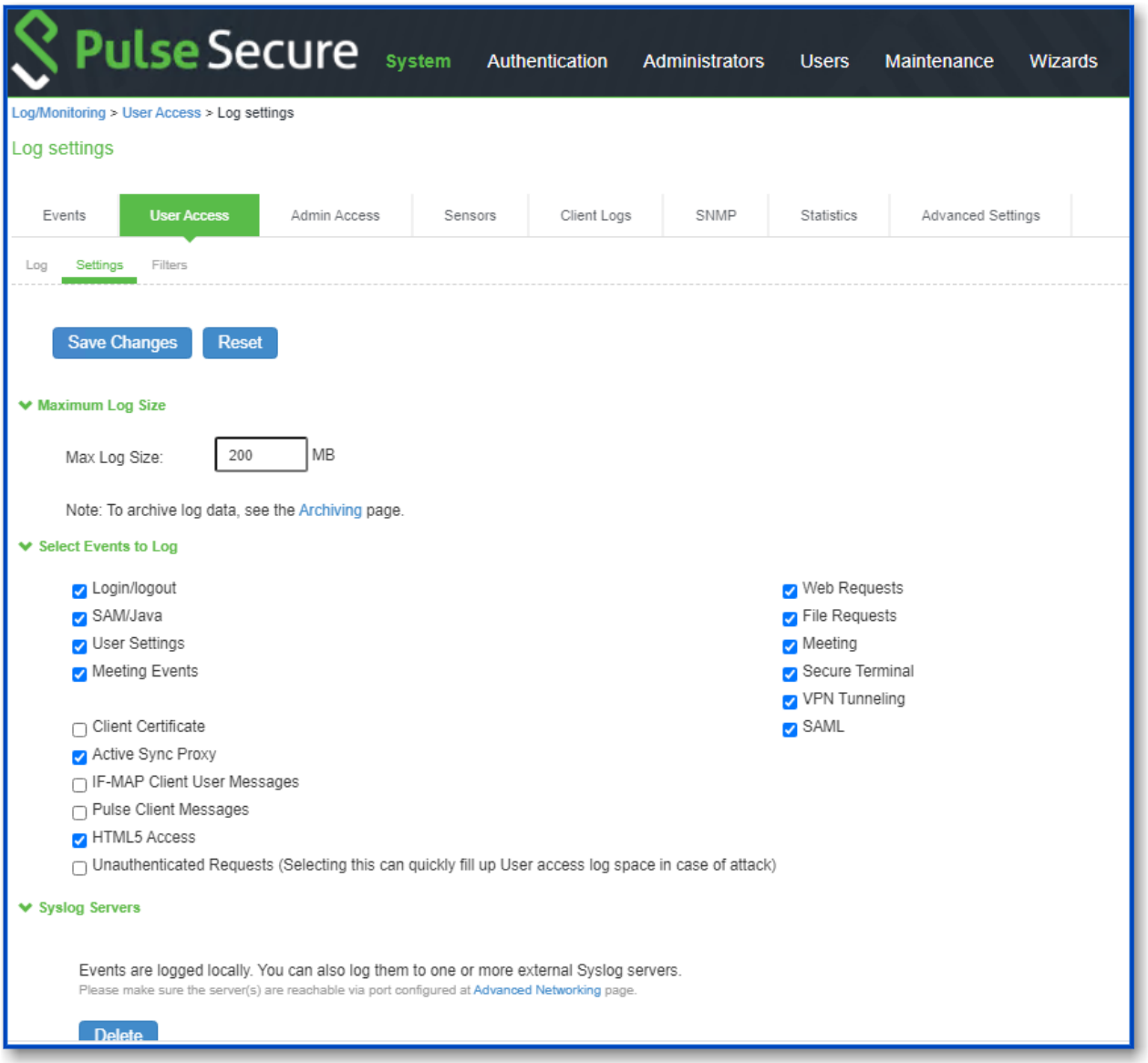
Object type	Actions	Event ID
Environment	• Read / Read (Failed attempt)	• connect-server-monitor-failure
Session	• Logoff	• logged out
User	• Add / Added (Failed attempt)	• config mgt-config users • config shared local-user-database user
	• **Modified / Modify (Failed attempt)**	• config mgt-config users • config shared local-user-database user
	• **Removed / Remove (Failed attempt)**	• config mgt-config users • config shared local-user-database user

Configure Pulse Secure Devices

1. Connect to your Pulse Secure device: launch an Internet browser and enter the IP address or device DNS name in the URL field (https://<IP address / Device DNS name>/admin).
2. In the Web Interface, navigate to System → Log/Monitoring.
3. Under Log/Monitoring, expand the User Access link.
4. Locate the Settings tab.

5. Under the Select Events to Log, select the following (minimal requirement, select other events if needed):

   - Login/Logout
   - VPN Tunneling



6. Under the Syslog Servers, complete the following fields:

Option	Description
Server nameIP	Specify the IP address of the computer where resides.
Facility	Select desired facility.

Option	Description
Type	Select UDP.
Client Certificate	Use default values.
Filter	Select Standard.

7. Save your changes.
8. Switch to the Admin Access tab.
9. Under the Select Events to Log, select the following (minimal requirement, select other events if needed):
   - Administrator logins
   - Administrator changes
10. Repeat the step 6 for Syslog Servers configuration.
11. Save your changes.
12. Navigate to System → Configuration → Advanced Networking.
13. Expand the Select the source port to be used for the following features link.
14. Locate the Syslog parameter and set it to *Internal*.

    Netwrix Auditor must be accessible from the selected network interface
15. Save your changes.
16. Start Netwrix Auditor.
17. Navigate to your monitoring plan for Network Devices. See Monitoring Plans
18. Provide the IP address of the interface you specified on the step 14 as the Computer item for your monitoring plan. See Active Directory

Pulse Secure Devices

Review a full list of object types Netwrix Auditor can collect on Pulse Secure network devices.

Object Type	Actions	
Logon	• Successful logon	• user authenticated successfully • user logged in successfully • administrative login succeeded • SuperAdmin session created using token for administrative logon recovery • Admin logged in successfully through the local console
	• Failed logon	• Login/authentication failed • Login attempt from the local console failed
	• Logoff	• user logged out or session timed out • admin logged out or session timed out • SuperAdmin session finished or timed out • Admin logged off from the local console
Authentication	• Successful logon	• VPN Tunneling Successful Logon
	• Logoff	• VPN connection closed
Configuration	• Modified	• Server shutdown/reboot/ restart requested • Platform administrator account added • Console administrator password is disabled or enabled • IKEv2 settings modified

Object Type	Actions	
		• Global SAML Settings modified • SAML Metadata Provider added • SAML Metadata Provider removed • SAML Metadata Provider updated • authentication server added • authentication server deleted • authentication server modified • Sign-in policy created • Sign-in policy deleted • Sign-in policy modified • Sign-in policy multiple user session limit modified • Sign-in policy multiple user session modified • Sign-in policy multiple user session warning notification modified • Updated the order of the sign-in policies • Sign-in policy user access parameters modified • Sign-in page created • Sign-in page deleted • Sign-in page updated • Sign-in notification created • Sign-in notification deleted • Sign-in notification updated • Sign-in SAML modified
User	• Added	• user account added
	• Modified	• user account password changed • user account disabled or enabled • user account unlocked • user account modified

Object Type	Actions	
		• admin rights granted • admin rights revoked
	• Removed	• user account removed
Role	• Added	• Role is created
	• Modified	• Role is modified
	• Removed	• Role is deleted
	• Copied	• Role is duplicated
Session	• Session start	• VPN Tunneling Session started
	• Session end	• VPN Tunneling Session ended
Realm	• Added	• Realm added
	• Modified	• IP added to allowed IP list in Realm authentication policy • IP removed from allowed IP list • IP setting reordered • Source IP restriction modified • browser restriction set • Browser restriction modified • browser restriction removed • Browser restriction reordered • Client-side certificate requirement modified • Certificate attribute modified • Password restriction modified

Object Type	Actions	
		• Minimum password length modified • Host Checker restriction is updated • User Limit restriction is modified • Guaranteed minimum number of users is modified • Maximum number of sessions is modified • Maximum number of users is modified • Realm is modified
	• Removed	• Realm deleted
	• Copied	• Realm duplicated
	• Renamed	• Realm renamed

Configure SonicWall Devices

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:

    - Configure log settings, depending on your device type.

To configure your SonicWall devices, do the following:

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 • Send to Syslog Server in Audit Log Settings • Send to Syslog Server in Access Log Settings	Select these checkboxes.
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 • Send to Syslog Server in Access Log Settings	Select these checkboxes.
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 NS 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.

SonicWall Devices

Review a full list of object types Netwrix Auditor can collect on SonicWall network devices.

Object type	Actions	Event ID
Logon	• Successful logon	• User login from an internal zone allowed • User login successful • XAUTH Succeeded with VPN • VPN zone remote user login allowed • WAN zone remote user login allowed • PPP: Authentication successful

Object type	Actions	Event ID
		• Local Authentication Success • RADIUS/LDAP Authentication Success • Successful authentication received for Remotely Triggered • IKEv2 Authentication successful • SSL VPN zone remote user login allowed
	• Failed logon	• User login denied • User login failed • XAUTH Failed with VPN • L2TP PPP Authentication Failed • check username / password • RADIUS/LDAP reports Authentication Failure • Local Authentication Failure • User login to Administration Portal denied • User login failure rate exceeded • User Name authentication Failure locally • ISAKMP_AUTH_FAILED • Guest service limit reached • Guest login denied

Object type	Actions	Event ID
		• Incorrect authentication received for Remotely Triggered • Authentication Timeout during Remotely Triggered • Problem occurred during user group membership retrieval • An error has occurred while sending your • IPsec Authentication Failed
	• Logoff	• User logged out • logged out • Guest Session Timeout • Guest Account Timeout • Guest Idle Timeout • Guest traffic quota exceeded
Authentication	• Successful Logon	• Administrator login allowed • CLI administrator login allowed • VPN zone administrator login allowed • WAN zone administrator login allowed • Configuration mode administration session started

Object type	Actions	Event ID
		• Read-only mode GUI administration session started • Non-config mode GUI administration session started • User login successful • Session Start: • EventMessage: Session Start Success
	• Failed Logon	• Administrator login denied • CLI administrator login denied due to bad credentials • User login failed • The account has been disabled for • is not permitted for this Web App • Authentication for user • Authentication failed • maximum authentication attempts exceeded for • EventMessage: Session Start Failed
	• Logoff	• Administrator logged out • CLI administrator logged out • Configuration mode administration session ended

Object type	Actions	Event ID
		• GUI administration session ended • Logged out • Session End: • EventMessage: Session End • Command='Tunnel'
Configuration	• Add / Added (Failed attempt)	• m=1333 • Scheduled settings generated • A new default Self-Signed certificate was generated successfully • Scheduled Tech Support Report generated • Restarted Tech Support Report generated
	• Modified / Modify (Failed attempt)	• Mail attachment disabled • Watch and report possible SYN floods • Watch and proxy WAN connections when under attack • Always proxy WAN connections • SYN Flood blacklisting enabled by user • SYN Flood blacklisting disabled by user • Administrator name changed

Object type	Actions	Event ID
		• VPN disabled by administrator • VPN enabled by administrator • WLAN disabled by administrator • WLAN enabled by administrator • WLAN disabled by schedule • WLAN enabled by schedule • is added into Group • is removed from Group • m=1334 • Update administrator/user lockout params • Settings imported • Critical Operating System Update failed • msg=\"WAF restarted • HTTP(S) Cache settings were updated • database has been updated • Web Server Fingerprint Protection enforced • About to reconfigure service: • Finished applying configuration changes • Started

Object type	Actions	Event ID
		• Start failed • Stopped
	• Read / Read (Failed attempt)	• m=1203 • m=1204 • Problem loading the URL list • Registration Update Needed, Please restore your existing security service subscriptions • Failed to synchronize license information with Licensing Server • Current settings exported • Error sending • settings sent successfully • Automated scheduled settings successful • Scheduled settings downloaded • Tech Support Report • Tech Support Report sent successfully • Loaded WAF signature database successfully • Error sending • logs sent out successfully
	• Remove / Removed (Failed attempt)	• Scheduled settings deleted

Object type	Actions	Event ID
		• Oldest scheduled Tech Support Report deleted • has been deleted • Event Logs cleared • Audit Logs cleared • Access Logs cleared • Deleting log files • Deleting core files • Deleting snapshots older
Device state	• Modified / Modify (Failed attempt)	• Registration Update Needed, Please restore your existing security service subscriptions • Intrusion Prevention (IDP) subscription has expired • Failed to synchronize license information with Licensing Server
Folder	• Add / Added (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=9&Arg1=
	• Read / Read (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=16&Arg1=
	• Remove / Removed (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=13&Arg1=

Object type	Actions	Event ID
File	• Add / Added (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=31&Arg1=
	• Read / Read (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=25&Arg1=
	• Rename / Renamed (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=14&Arg1=
	• Remove / Removed (Failed attempt)	• Request='GET /cgi-bin/sonicfiles?RacNumber=12&Arg1=
Host	• Read / Read (Failed attempt)	• Received AV Alert • The loaded content URL List has expired • CFS Alert • Mail Filter Alert • Mail attachment deleted • Intrusion Prevention (IDP) subscription has expired • Smurf Amplification attack dropped • TCP Xmas Tree dropped • Source routed IP packet dropped • Mail fragment dropped

Object type	Actions	Event ID
		• PASV response spoof attack dropped • PORT bounce attack dropped • PASV response bounce attack dropped • Spank attack multicast packet dropped • IPS Detection Alert • IPS Prevention Alert • Drop WLAN traffic • IDP Detection Alert • IDP Prevention Alert • Ping of death dropped • IP spoof dropped • Possible SYN flood attack detected • Land attack dropped
Rule	• Activated	• will be denied • msg=\"WAF threat detected • Ping of death dropped • IP spoof dropped • Possible SYN flood attack detected • Land attack dropped • Smurf Amplification attack dropped

Object type	Actions	Event ID
		• Possible port scan detected • Probable port scan detected • Probable TCP FIN scan detected • Probable TCP XMAS scan detected • Probable TCP NULL scan detected • Mail attachment deleted • TCP Xmas Tree dropped • Source routed IP packet dropped • Mail fragment dropped • PASV response spoof attack dropped • PORT bounce attack dropped • PASV response bounce attack dropped • Spank attack multicast packet dropped • IPS Detection Alert • IPS Prevention Alert • Drop WLAN traffic • IDP Detection Alert
Session	• Add / Added (Failed attempt)	• msg=\"New HTTP Request to • msg=\"New HTTPS Request to

Object type	Actions	Event ID
		• msg=\"New HTTP Session for • msg=\"New HTTPS Session for
	• Read / Read (Failed attempt)	• msg=\"WAF threat detected: • will be denied • Access to proxy server denied • Website found in blacklist
	• Logoff	• Connection Closed
User	• Add / Added (Failed attempt)	• Guest account
	• Modified / Modify (Failed attempt)	• Administrator name changed • out user logins allowed • Guest account • User login disabled from • User account
	• Remove / Removed (Failed attempt)	• Guest account • m=1335

Permissions for Network Devices Auditing

Before you start creating a monitoring plan to audit your network devices, 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.

For...	Requirement
• **Cisco ASA** • **Cisco IOS** • **Cisco FTD** • **Fortinet** • **HPE Aruba** • **Juniper** • **Palo Alto** • **Pulse Secure** • **SonicWall** • **HPE**	You can use any account (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.
• **Cisco Meraki**	See the Configure Cisco Meraki Dashboard Account section for additional information.

Oracle Database

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - On the Oracle server, configure the required settings described below.

- On the Auditor console computer, verify that Oracle Data Provider for .NET and Oracle Instant Client are installed and properly configured. See the Permissions for Oracle Database Auditing topic of system requirements.

Ensure that you have met all software requirements on the Oracle Database side. See the Software Requirements topic for additional information.

Before you start monitoring your Oracle Database with Netwrix Auditor, you should configure it to provide audit trails. Depending on your current database version and edition, Oracle supports different auditing types:

Auditing type	Oracle version	Details
Unified Auditing	Oracle Database 23c, 21c, 19c, 18c, 12c	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 for Auditing topic for more information.
Fine Grained Auditing	Oracle Database 23c, 21c, 19c, 18c, 12c, 11g Available for **Enterprise Edition** only.	Supports auditing of actions associated with columns in application tables — along with conditions necessary for an audit record to be generated. Helps to focus on security-relevant columns and rows, ignoring areas that are less important. See Configure Fine Grained Auditing topic for more information.
Standard Auditing (trail auditing mode)	Oracle Database 11g	See topic for more information. Use initialization parameters and the `AUDIT` and `NOAUDIT` SQL statements to audit:

Auditing type	Oracle version	Details
		• SQL statements • privileges • schema objects • network and multitier activities See Oracle documentation for more information. Starting with version 10.5, Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode, in particular: Netwrix Auditor client UI does not display any warnings and / or errors related to Standard Auditing mode operation.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

Considerations for Oracle Database 11g

Starting with version 9.95, Netwrix Auditor for Oracle Database is focused on versions 12c and above. It means that Oracle Database 11g users will not be able to benefit from latest features and improvements of the product. Oracle Database 11g users should also consider its support expiration dates set by the vendor. So, when planning your Netwrix Auditor deployment, consider the following:

- Several limitations apply to Oracle 11g support in Netwrix Auditor 9.96:
  - Oracle wallets are not supported
  - Lightweight drivers for Oracle Instant Client are not supported
  - Auditor client UI does not display any warnings and / or errors regarding to trail audit mode operation
- If you are using Oracle Database 11g and have performed seamless upgrade to the latest version of Auditor, the audit data collection will operate properly. However, consider and keep in mind Oracle Database 11g support expiration dates.

If you are using Oracle Database 12c or later, make sure you have Unified auditing mode enabled. Otherwise, Netwrix Auditor may not operate properly. See the Migrate to Unified Audit topic for additional information.

See the Software Requirements topic for additional information.

Configuration

If you are using Oracle Wallet to connect to your database, see the Create and Configure Oracle Wallet topic for configuration details.

Oracle Wallet is not supported for Oracle 11g. If you are unsure of your audit settings, refer to the Verify Your Oracle Database Audit Settings

Follow the steps for proper configuration.

Step 1 – Configure Data Collecting Account, as described in the Permissions for Oracle Database Auditing topic.

Step 2 – Configure required protocols and ports, as described in the Oracle Database Ports topic.

Oracle Database objects

Review a full list of object types Netwrix Auditor can collect on Oracle Database. If you deployed your Oracle Database in a cluster mode (Oracle Real Application Cluster), a host name also will be reported.

Details marked with asterisk (*) are reported for Oracle Database 11g only.

Details marked with asterisk (**) are reported for Oracle Database 12c only.

Oracle Object modification under Privileges and object rename under Rename are reported without Object type (“Not available” is displayed).

Oracle Database startup under System Settings is reported without Workstation (“Not available” is displayed).

Object type	Actions	Details
Directories		

Object type	Actions	Details
• **Directory**	• Added / Add (Failed attempt) • Removed / Remove (Failed attempt)	• Cause (for failed attempts) • Container name** • Database User • Program name / Database session requester** • Privilege for action • Session ID • Object schema
Executable objects		
• **Procedure** • **Function** • **Package** • **Package body** • **Java**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove (Failed attempt)	• Cause (for failed attempts) • Container name** • Database User • Privilege for action • Program name / Database session requester** • Session ID • Unified policy name**
For Oracle 11g database Modified / Modify (Failed attempt) events will not be monitored for the following objects: *Procedure, Function, Package, Package body* since native audit of these events is not supported. See the Database SQL Language Reference for additional information.		
Logons		
• **Logon**	• Successful logon / Failed logon • Logoff	• Cause (for failed attempts) • Client IP (only for logon events) • Container name** • Database User

Object type	Actions	Details
		• Privilege for action • Program name / Database session requester** • Session ID • Object schema • Unified policy name**
Materialized views		
• **Materialized view**	• Added / Failed Add • Removed / Failed Remove	• Cause (for failed attempts) • Container name** • Database user • With option • Program name / Database session requester** • Session ID • Object schema • Unified policy name**
Privileges		
• **Object**	• Modified / Modify (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • With option • Privilege user • Program name / Database session requester** • Session ID • Unified policy name**
• **Role**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user

Object type	Actions	Details
	• Removed / Remove (Failed attempt)	• With option • Program name / Database session requester** • Role name • Session ID • Unified policy name**
• **Database**	• Modified / Modify (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • With option • Program name / Database session requester** • Session ID • Unified policy name**
Profiles		
• **Profile**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • Privilege for action • Program name / Database session requester** • Session ID • Unified policy name**
Rename		
• **Object**	• Renamed / Rename (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • New object name • With option

Object type	Actions	Details
		• Privilege user • Session ID • Unified policy name**
Roles		
• **Role**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • Privilege for action • Program name / Database session requester** • Session ID • Unified policy name**
Data		
• **Data**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Read / Read (Failed attempt) • Removed / Remove (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • FGA policy name • Session ID
System Settings		
• **Audit Policy**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • With option • Program name / Database session requester** • Session ID • Unified policy name**
• **Database**	• Modified / Modify (Failed attempt)	

Object type	Actions	Details
Tables		
• **Table**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • Program name / Database session requester** • Session ID • Object schema • Unified policy name
Triggers		
• **Trigger**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • With option • Program name / Database session requester** • Referenced table • Referenced table schema • Session ID • Object schema • Triggered by* • Unified policy name**
Users		
• **User**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • Privilege for action • Program name / Database session requester** • Session ID

Object type	Actions	Details
		• Unified policy name**
Views		
• **View**	• Added / Add (Failed attempt) • Removed / Remove (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • With option • Program name / Database session requester** • Session ID • Object schema • Unified policy name**
Oracle Datapump		
• **Datapump**	• Read / Read (Failed attempt) • Modified / Modify (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • Datapump boolean parameters • Datapump text parameters • Program name / Database session requester** • Session ID
Oracle Recovery Manager (RMAN)		
• **RMAN**	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Read / Read (Failed attempt) • Removed / Remove (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • Program name / Database session requester** • RMAN operation

Object type	Actions	Details
Oracle SQL*Loader Direct Path Load		
• **Direct Path Load API**	• Modified / Modify (Failed attempt)	• Cause (for failed attempts) Container name** • Database user • Program name / Database session requester** • Session ID

Oracle Database Ports

Review a full list of protocols and ports required for Netwrix Auditor for Oracle Database.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 1521 TCP port. On your Oracle Database Server (target), allow inbound connections to local 1521 TCP port.

Port	Protocol	Source	Target	Purpose
1521	TCP	Netwrix Auditor Server	Oracle Database Server	Allows Oracle client connections to the database via the Oracle's SQL*Net protocol. You can configure it during installation. Port 1521 is the default client connections port, however, you can configure another TCP port via the Oracle

Port	Protocol	Source	Target	Purpose
				configuration and administration tools.
2484	TCP	Netwrix Auditor Server	Oracle Database Server	The default SSL port for secured Oracle client connections to the database via the Oracle's SQL*Net protocol. Open this port if you need secure connection.
53	UDP	Netwrix Auditor Server	DNS Server	DNS Client

Configure Oracle Database for Auditing

This topic explains how to configure Oracle Database for the following versions of the Oracle Database Software:

- Configure Oracle Database 12c, 18c, 19c for Auditing
- Configure Oracle Database 11g for Auditing

Configure Oracle Database 12c, 18c, 19c for Auditing

The following auditing modes are available for Oracle Database 12c, 18c, 19c:

- 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.

After an audit policy has been enabled or disabled, Netwrix Auditor starts collecting data after a successful logon session.

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

- Mixed Mode—Default auditing in a newly installed database. It enables both traditional and the new **Unified Auditing** facilities. Netwrix recommends using **Unified Auditing** mode if you do not have any trail audit facilities in your infrastructure.

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

To configure Oracle Database 12c, 18c, 19c 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. You can set them to audit the following:

   - Configuration changes
   - Successful and failed data access and changes
   - Oracle Data Pump, Oracle Recovery Manager (RMAN) and Oracle SQL*Loader Direct Path Load components

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

To monitor...	Execute the command...
	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; 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,

To monitor...	Execute the command...
	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 Recovery Manager, and Oracle SQL*Loader Direct Path Load	• Create the audit policies (e.g., nwx_sqlloader_dp_pol, etc.): No special configuration required to audit RMAN events. CREATE AUDIT POLICY nwx_datapump_exp_pol ACTIONS 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.

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.

Also, remember to do the following:

- Configure Data Collecting Account as described in Permissions for Oracle Database Auditing topic.
- Configure ports as described in Oracle Database Ports topic.

NOTE: Traditional auditing is deprecated in Oracle Database 21c. Oracle recommends using Unified Auditing, which enables selective and more effective auditing within Oracle Database. See the Oracle website for more information.

Configure Oracle Database 11g for Auditing

This section explains how to configure **Standard Auditing** on your Oracle Database 11g, preparing for monitoring with the product.

Starting with version 10.5, Auditor provides limited support of Oracle Database 11g. See the Considerations for Oracle Database 11g topic for additional information.

Verify that Oracle Data Provider for .NET and Oracle Instant Client are installed and properly configured on the computer where AUDITOR Server is installed. The product does not provide any special notification for that.

Follow the steps to configure **Standard Auditing** on your Oracle Database 11g:

Step 1 – Select the audit trail to store audit records. Oracle Database has the following options:

- **Database audit trail**— Set by default.
- **XML audit trail**— Recommended.
- **OS files**—Not supported by current version of Netwrix Auditor.

Step 2 – Enable auditing of Oracle Database changes, using the corresponding command.

Store Oracle Audit Records

Follow the steps to select Audit Trail to store Oracle Audit Records:

Step 1 – On the computer where your database is deployed, run the sqlplus tool.

Step 2 – Connect to your Oracle Database using Oracle account with the SYSDBA privilege. For example:

```
OracleUser as sysdba
```

Step 3 – Enter your password.

Depending on where you want to store audit records, execute the required command.

Store to...	Execute...

Store audit records to XML audit trail (recommended).
 	
Use this audit trail if you want Netwrix Auditor to report on actions performed by users with SYSDBA and SYSOPER privileges. Otherwise, these actions will not be audited.
	`ALTER SYSTEM SET audit_trail=XML SCOPE=SPFILE;`
	
	If you want to enable auditing of actions performed by SYS user and by users connecting with SYSDBA and SYSOPER privileges, execute:
	
	`ALTER SYSTEM SET audit_sys_operations=TRUE SCOPE=SPFILE;`

Store to...	Execute...
Database audit trail (default setting) **In this case, actions performed by user SYS and users connecting with SYSDBA and SYSOPER privileges will not be audited.**	`ALTER SYSTEM SET audit_trail=DB SCOPE=SPFILE;`

Store audit records to XML or database audit trail and keep full text of SQL-specific query in audit records.
 	
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;`

Step 4 – If you turned auditing on or off, you will need to restart the database. For that, run the following:

```
SHUTDOWN IMMEDIATE

STARTUP
```

If you only changed auditing settings, database restart is not required.

If you are using 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 additional information on restarting your instances.

Enable Auditing of Oracle Database Changes

Follow the steps to enable auditing of Oracle Database changes:

Step 1 – On the computer where your database is deployed, run the sqlplus tool.

Step 2 – Connect to your Oracle Database—use Oracle account with the SYSDBA privilege. For example:

```
OracleUser as sysdba
```

Step 3 – Enter your password.

Step 4 – Depending on your monitoring requirements, enable auditing of the database parameters with the related command.

To monitor for...	Execute...

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;`
	
	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>;` **You can specify several users separated by commas.**

To monitor for...	Execute...
Successful data access and changes	AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME> BY ACCESS WHENEVER SUCCESSFUL;
Failed data access and change	AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME, FLASHBACK ON <TABLE_NAME> BY ACCESS WHENEVER NOT SUCCESSFUL;
Successful and failed data access and changes	AUDIT SELECT,INSERT,DELETE,UPDATE,RENAME,F LASHBACK ON <TABLE_NAME>;

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

- `AUDIT_TRAIL`
- `AUDIT`

After an audit parameter has been enabled or disabled, Auditor will start collecting data after successful logon session.

Also, remember to do the following:

- Configure Data Collecting Account. See the Permissions for Oracle Database Auditing topic for additional information.
- Configure ports. See the Oracle Database Ports topic for additional information about ports and protocols required for auditing.

Migrate to Unified Audit

Starting with 10.5 version, Netwrix Auditor provides limited support of Oracle Database 11g and trail auditing mode accordingly. See Considerations for Oracle Database Auditing for more information.

When planning your migration, consider that you can select the following scenario:

- Migration to pure unified auditing. See the corresponding Oracle documentation article: Migrating to Unified Auditing for Oracle Database.
- Use a mixed-mode audit facility (not recommended).

Perform the following steps according to official Oracle documentation:

1. To migrate to Unified Auditing for Oracle Database
2. Manage Earlier Audit Records After You Migrate to Unified Auditing

To migrate to Unified Auditing for Oracle Database

The procedure contains basic migration steps. Refer to Oracle_Database_Upgrade_Guide for more detailed upgrade scenario.

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:

   sqlplus sys as sysdba

   Enter password: password
3. Check if your Oracle database has already been migrated to unified auditing:

   SQL> SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';

   If the `value` is `true`, unified auditing mode is already enabled in your database.

   In this case, you can ignore further steps and start managing your earlier audit records. Refer to Oracle documentation for more information: Managing Earlier Audit Records After You Migrate to Unified Auditing.

   If the `value` is `false`, proceed with the steps below.
4. Stop the database. Do the following, depending on your environment:

For...	Do...
Single-instance environments	In sqlplus tool, execute the following command: SQL> SHUTDOWN IMMEDIATE SQL> EXIT

For...	Do...
Windows systems	Stop the Oracle service: net stop OracleService%ORACLE_SID%
Oracle RAC installations	Shut down each database instance as follows: srvctl stop database -db db_name

5. Stop the listener. Stopping the listener is not necessary for Oracle RAC and Grid Infrastructure listeners.

   lsnrctl stop listener_name

   To find your listener name, execute the following command:

   lsnrctl status

   The `Alias` parameter shows listener name.

6. Navigate to `$ORACLE_HOME /rdbms/lib` directory.

7. Enable the unified auditing executable. Do the following depending on your infrastructure:

For...	Do...
Windows systems	Rename the `%ORACLE_HOME%/bin/orauniaud12.dll.dbl` file to `%ORACLE_HOME%/bin/orauniaud12.dll`.
UNIX-based systems	Execute the following command: make -f ins_rdbms.mk uniaud_on ioracle ORACLE_HOME=$ORACLE_HOME

8. Restart the listener.

   lsnrctl start listener_name

9. Restart the database. Do the following, depending on your environment:

For...	Do...
Single-instance environments	In sqlplus tool, execute the following command: sqlplus sys as sysoper Enter password: password SQL> STARTUP
Windows systems	Start the Oracle service: net start OracleService%ORACLE_SID%
Oracle RAC installations	Start each database instance as follows: srvctl start database -db db_name

See also:

1. Manage Earlier Audit Records After You Migrate to Unified Auditing
2. Remove the Unified Auditing Functionality

Configure Fine Grained Auditing

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

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.

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');

Refer to Oracle documentation for additional information on Working with Oracle Fine Grained Auditing.

Create and Configure Oracle Wallet

Oracle Wallet is a file that stores database authentication and signing credentials. It allows users to securely access databases without providing credentials to third-party software (for example, Netwrix Auditor), and easily connect to Oracle products, including located in the clouds (e.g. Autonomous Data Warehouse).

A configured Wallet consists of two files, `cwallet.sso` and `ewallet.p12` stored in a secure Wallet directory

Create Oracle Wallet

There are multiple methods to create Oracle Wallet files. For example:

- Using Oracle Wallet Manager. Refer to the following Oracle help article for more information: Creating a New Oracle Wallet.
- Using a console. As an example, refer to the following Oracle help article for WebLogic JDBC: Creating and Managing Oracle Wallet.
- Using other Oracle products. For example, Autonomous Data Warehouse. Refer to the following Oracle help article for more information: Download Client Credentials (Wallets).

Install Oracle Instant Client

To perform clear install of Oracle Instant Client, follow the instructions below. If you have Oracle Client installed, see the Update Existing Oracle Client Installation topic for additional information.

Follow the steps to install Oracle Instant Client

Step 1 – Download the appropriate package from Oracle website: Instant Client Packages. Netwrix recommends installing the latest available version but the product is compatible with version 12 and above.

Step 2 – Download client credentials and store the file in a secure location. See Download Client Credentials (Wallets) for more information.

Step 3 – Unzip your credentials file into a secure location.

Step 4 – Navigate to a folder where you unzipped your credentials and locate the sqlnet.ora file.

Step 5 – Replace the `"?/network/admin"` parameter with the name of the folder containing client credentials. For example:

Windows-based platforms:

WALLET_LOCATION = (SOURCE = (METHOD = file) (METHOD_DATA = (DIRECTORY="D:\\myapp\
\atp_credentials")))

SSL_SERVER_DN_MATCH=yes

Step 6 – Create the `TNS_ADMIN` environment variable and set it to the location of the credentials file.

This variable is used to change the directory path of Oracle Net Services configuration files from the default location of `ORACLE_HOME\network\admin` to the location of the secure folder containing the credentials file you saved in Step 2. Set the `TNS_ADMIN` environment variable to the directory where the unzipped credentials files are, not to the credentials file itself.

Step 7 – Navigate to a folder where you unzipped your credentials and locate the tnsnames.ora file. The file is used to map connection information for each Oracle service to a logical alias.

Step 8 – Review sample tnsnames.ora file where `myOracle` – is a logical alias for the wallet:

myOracle =

(description=

(address=((ADDRESS = (PROTOCOL = TCP)(HOST = server1)(PORT = 1521))

(CONNECT_DATA =

)

)

Keep in mind that the wallet alias in the configuration file must equal to Netwrix Auditor item name.

Configure Oracle Instant Client for HTTP Proxy Connections

If the client is behind a firewall and your network configuration requires an HTTP proxy to connect to the internet, perform the following steps to update the `sqlnet.ora` and `tnsnames.ora` files.

HTTP proxy connections are available starting with Oracle Instant Client 12.2.0.1 or later.

1. Add the following line to the `sqlnet.ora` file to enable connections through an HTTP proxy:

   SQLNET.USE_HTTPS_PROXY=on

2. Open the `tnsnames.ora.` file and add the following HTTP proxy connection definitions:

   - `https_proxy` — specify the proxy server hostname. For example, `proxyhostname`.
   - `https_proxy_port` — specify port used for HTTP proxy connection. For example, `80`.

   Review configuration example:

   ATPC_high =

   (description=

   (address=

   (https_proxy=proxyhostname)(https_proxy_port=80)(protocol=tcps)(port=1522)(host=atpc.example.oraclecloud.com)

)

   (connect_data=(service_name=atpc1_high.atpc.oraclecloud.com)

)

(security=(ssl_server_cert_dn="atpc.example.oraclecloud.com,OU=Oracle BMCS US,O=Oracle Corporation,L=Redwood City,ST=California,C=US")

)

)

Configuring `sqlnet.ora` and `tnsnames.ora` for the HTTP proxy may not be enough depending on your organization's network configuration and security policies. For example, some networks require a username and password for the HTTP proxy. In such cases, contact your network administrator to open outbound connections to hosts in the oraclecloud.com domain using port `1522` without going through an HTTP proxy.

Update Existing Oracle Client Installation

Netwrix assumes that you have `sqlnet.ora` and `tnsnames.ora` files and the `TNS_ADMIN` environment variable.

Do the following:

1. Update your sqlnet.ora file. Example:

   WALLET_LOCATION = (SOURCE = (METHOD = file) (METHOD_DATA = (DIRECTORY="/home/atpc_credentials")))

2. Copy the entries in the `tnsnames.ora` file provided in the Autonomous Transaction Processing wallet to your existing `tnsnames.ora` file.

See also:

-
- Oracle Wallet

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 19c (Unified Auditing)	`select ENTITY_NAME, ENABLED_OPTION, SUCCESS, FAILURE from AUDIT_UNIFIED_ENABLED_POLICIES;`
Oracle Database 12c, 18c, 19c (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;`

Oracle Database 11g(Standard Auditing)
 	
Starting with version 10.5 , NETWRIX AUDITOR provides limited support of Oracle Database 11g and trail auditing mode accordingly.
	`SELECT audit_option, success, failure FROM dba_stmt_audit_opts;`
	
	To review your initialization parameters, execute the following command:
	
	`SHOW PARAMETERS audit%r;`

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.

Permissions for Oracle Database Auditing

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.

Follow the steps to grant CREATE SESSION and SELECT privileges to the account.

Step 1 – On the computer where your database is deployed, run the sqlplus tool.

Step 2 – Connect to your Oracle Database.

NOTE: Use Oracle account with the SYSDBA privilege, for example:

```
OracleUser as sysdba
```

Step 3 – Enter the account password.

Step 4 – 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. To create a new account, use the following command:: `CREATE USER <account_name> IDENTIFIED BY PASSWORD;`

Step 5 – Grant `CREATE SESSION` system privilege to that account. For that, execute: `GRANT CREATE SESSION TO <account_name>;`

Step 6 – Grant `SELECT` privilege on the required object to that account. See the For Oracle Database Auditing topic for the detailed object list. For that, execute: `GRANT SELECT ON <object> TO <account_name>;` For example: `GRANT SELECT ON aud$ TO OracleUser;`

CREATE SESSION and SELECT privileges now granted to the account.

Alternatively, you can grant the default administrator role to that account. For that, execute: `GRANT DBA TO <account_name>;`

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 certain objects must be granted to that account:

Oracle Database 12c, 18c, 19c	Grant `SELECT` privilege on the following objects: • `aud$`

	• gv_$xml_audit_trail • dba_stmt_audit_opts • v_$parameter • dba_obj_audit_opts • dba_audit_policies • dba_audit_mgmt_clean_events • gv_$instance • fga_log$ • gv_$unified_audit_trail • all_unified_audit_actions • audit_unified_policies • audit_unified_enabled_policies • audsys.aud$unified (for Oracle Database 12c Release 2 and higher)
Oracle Database 11g Starting with version 10.5, Netwrix Auditor provides limited support of Oracle Database 11g.	Grant SELECT privilege on the following objects: • aud$ • gv_$xml_audit_trail • dba_stmt_audit_opts • v_$parameter • dba_obj_audit_opts • dba_audit_policies • dba_audit_mgmt_clean_events • gv_$instance • fga_log$

- You can grant the default **Administrator** role to the account.
- If you are going to configure Fine Grained Auditing, make sure that you are using Oracle Database *Enterprise Edition*. Then grant privileges depending on your Oracle Database version.

SharePoint

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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.
    - In this case, 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, Auditor will automatically delete the events older than 1 day from its audit log.
- Manually – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - 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). See the SharePoint Ports topic for additional information.

Configure Audit Log Trimming

Follow the steps to configure Audit Log Trimming on your SharePoint farm.

Step 1 – Log in as an administrator to the audited SharePoint site collection.

Step 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).

Step 3 – Under the Site Collection Administration section, select Site collection audit settings.

Step 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.

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

Configure Events Auditing Settings

Follow the steps to configure event auditing settings.

Step 1 – Log in as an administrator to the audited SharePoint site collection.

Step 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).

Step 3 – Under the Site Collection Administration section, select Site collection audit settings.

Step 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.

Step 5 – Consider that if you are using SharePoint 2019, then to enable this option you will have to adjust audit settings automatically with Auditor (see the Create a New Monitoring Plan topic for additional information), or use some scripting.

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 the Install for SharePoint Core Service topic for additional information.

Follow the steps to enable SharePoint Administration Service.

Step 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 and higher) or** Administrative Tools **(Windows 2012)** > **Services**.

Step 2 – Locate the SharePoint Administration service (SPAdminV4), right-click it and select Properties.

Step 3 – In the General tab, set the Startup type to *"Automatic"* and click Apply.

Step 4 – Click Start to start the service.

SharePoint objects

Review a full list of object types and attributes Netwrix Auditor can collect on SharePoint.

The attributes marked with * are reported without details, only the fact of change is reported.

The changes to object types marked with ** are reported with the "Not applicable" value in the "Who" and "Workstation" columns.

The changes to object types and attributes marked with *** are reported with the "Not applicable" value in the "Workstation" column.

Read access is reported for documents and lists and displays "Not applicable" in the "Workstation" column.

Object type	Attributes
Group* **	• Membership
Permission Level* **	• Permissions
Site	• Site URL • Permissions*** • Permission Inheritance***

Object type	Attributes
List	• Permissions*** • Permission Inheritance***
List Item	• Attachments • Permissions*** • Permission Inheritance*** • List Item Properties*
Document	• Document URL • Permissions*** • Permission Inheritance*** • Document Properties* • Content Modifications*
Farm**	• Configuration Database • Configuration Database Server • Version • Managed Account for "Web Application Pool - {name}" • Managed Account for "Service Application Pool - {name}" • Managed Account for "Windows Service - {name}" • Managed Account for "Farm Account"

Object type	Attributes
	• Managed Accounts
Web Application **	• Web Application URL • Name • Port • User Permissions • Alternate Access Mappings • Content Database • Blocked File Extensions
Site Collection**	• Site Collection URL • Content Database • Content Database Server • Site Storage Maximum Limit • Site Storage Warning Limit • Sandboxed Solutions Resource Maximum Quota • Sandboxed Solutions Resource Warning Quota • Quota Template • Lock Status
Server**	• Name
Service**	• Name

Object type	Attributes
	• Status
Permission Policy Level**	• Name • Grant Permissions • Deny Permissions • Site Collection Permissions
User Policy**	• Display Name • Permissions
Anonymous Policy**	• Zone • Permissions
Farm Solution**	• Name • Status • Last Operation Time
Farm Feature**	• Name • Status

To collect State-in-Time data from a SharePoint farm, the following is required:

- for site collection processing – lock status must differ from *No access* for Netwrix Auditor service account
- for web application processing – the following permissions must be assigned to Netwrix Auditor service account:
  - Open items
  - View items
  - Browse directories

- View pages
- Browse user information
- Open
- Enumerate permissions

Also, state-in-time data collection is supported for SharePoint farm.

Means Granted

The Means granted column in the Account Permissions in SharePoint and SharePoint Object Permissions State-in-Time reports list detailed permissions and permission levels by user account.

Review the following for additional information:

Means granted	Description
Permission level	Default permission levels are predefined sets of permissions that you can assign to individual users, groups of users, or security groups, based on their functional requirements and on security considerations. SharePoint Server permission levels are defined at the site collection level; by default, they are inherited from the parent object. For more information on SharePoint permissions and permission levels read the following Microsoft article: User permissions and permission levels in SharePoint Server.
Zone: Default (policy) **Zone: Intranet (policy)** **Zone: Internet (policy)** **Zone: Custom (policy)** **Zone: Extranet (policy)**	Zone If you want to expose the same content in a web application to different types of users by using additional URLs or authentication methods, you can extend an existing web application into a new zone. When you extend the web application into a new zone, you create a separate Internet Information

Means granted	Description
	Services (IIS) web site to serve the same content, but with a unique URL and authentication type. For more information on SharePoint zones read the following Microsoft article: Extend claims-based web applications in SharePoint . Policies Web application policies represent a concept that allows SharePoint administrators to grant or deny permissions to users and groups for sites under a web application. These granted or denied permissions take preference over the permissions set for the sites in the web application. For more information on SharePoint web application policies read the following Microsoft article: Manage permissions for a web application in SharePoint Server.
Site collection administrator	The *SharePoint site collection administrator* is a permission type that overrides Full Control permission. It cannot be locked out of any subsite, list, library, item, or page on the site. The permissions inheritance for any of these elements can be broken at any time, and permissions can be changed so that even users with Full Control will have lesser permissions or even no permissions at all. In all cases the SharePoint site collection administrator will always have full access to all elements and all data. For more information, read the following Microsoft article: Change site collection administrators in SharePoint Server.
Site Collection lock status	Lock statuses apply to a site collection and are used to control the actions allowed on site collection.

Means granted	Description
	For more information on lock statuses, read the following Microsoft article: Manage the lock status for site collections in SharePoint Server.
Web application user permissions	Sites and site collections have a variety of permissions that can be set, such as adding or editing list items or documents. These permissions are normally given to a user by assigning a particular permission level, such as *Full Control*, *Contribute*, or *View Only*. Each individual permission can be enabled or disabled for entire web application. For more information on web application user permissions, read the following Microsoft article: Manage permissions for a web application in SharePoint Server.
Farm account	Farm account is a service account used to run the Central Administration web site application pool. It has *dbo* access to the configuration database. For more information on SharePoint service accounts, read the following Microsoft articles: • Plan for administrative and service accounts in SharePoint Server • Account permissions and security settings in SharePoint Servers 2016 and 2019 Public Preview
Service account for web application pool	Service account for web application pool is used for internal purposes across a SharePoint farm, except for Central administration. For more information on application pool account, read the following Microsoft article: Application pool account.

SharePoint Ports

Review a full list of protocols and ports required for Netwrix Auditor for SharePoint.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 137 UDP port. On front end server (target), allow inbound connections to local 137 UDP port.

Port	Protocol	Source	Target	Purpose
137 **138** **445**	UDP	Netwrix Auditor Server	Windows Server running FrontEnd Server	Core Service installation
139 **445**	TCP	Netwrix Auditor Server	Windows Server running FrontEnd Server	Core Service installation
Custom port	TCP	Netwrix Auditor Server	Central Administration – FrontEnd Server	HTTP/ HTTPS Used to connect to SharePoint Central Administration

Permissions 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.

Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

For more information on gMSA, refer to Use Group Managed Service Account (gMSA)Microsoft documentation.

These group Managed Service Accounts should meet the related requirements.

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 Installation topic.
2. On the SQL Server hosting SharePoint database: the SharePoint_Shell_Access role. See the Assigning 'SharePoint_Shell_Access' Role topic for additional information.
3. If you plan to collect state-in-time data from a SharePoint farm, the account should also meet the requirements below:
   - For site collection processing — lock status for this account 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

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>
```

Define Log On As a Service Policy

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

Follow the steps to define log on as a service policy:

Step 1 – On the computer where Auditor Server is installed, open the **Local Security Policy** snap-in: navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** and select Local Security Policy.

Step 2 – Navigate to **Security Settings > Local Policies > User Rights Assignment** and locate the **Log on as a service** policy.

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

The Log On is now defined as a policy.

SQL Server

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

The IT Infrastructure for monitoring is configured automatically. Your current audit settings will be checked on each data collection and adjusted if necessary.

Checking for Primary Key

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.

SQL Server Objects

Review a full list of all object and data types Netwrix Auditor can collect on SQL Server.

Monitored Object Types

The table below contains the full list of object types that Netwrix Auditor monitors on SQL Servers. The product reports on adding and removing of object types below (Application Roles, Database, Jobs, etc.) and modifying attributes of these objects (listed in the "*Attributes*" column).

As for logons, the product collects successful and failed logon attempts for Windows and SQL logons:

Logon Type	Action
SQL logon	• Successful logon • Failed logon
Windows logon	• Successful logon • Failed logon

Review the full list of monitored object types and their attributes:

The attributes marked with asterisk (*) are reported only for the SQL Server item, not for availability groups.

Object type	Attributes
SQL Objects	

Object type	Attributes
Application Role	• Date Created • Date Modified • Default Schema • Extended Properties • Id • Name • Owned Schemas
Backup	• Backup name • Description • Device name • logical_device_name • Size • Type
Column	• Allow nulls • ANSI Padding Status • Collation • Computed Text • Default Constraint • Full Text • ID

Object type	Attributes
	• Identity • Identity increment • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale • Primary Key • Rule • Rule Schema • System Type • XML Schema Namespace
Constraints	• Date Created • Date Modified • Definition • ID • Is system named • MS shipped • Name • Published

Object type	Attributes
	• Schema published
Credentials*	• Id • Identity • Date Created • Date Modified • Name
Database	• Compatibility • Database Size • Database Space Available • Date Created • Date Modified • Extended Properties • File Id • File Group • File Name • Growth • Id • Name • Options • Owner • Permissions

Object type	Attributes
	• Size • Usage
Database Role	• Date Created • Date Modified • Extended Properties • Id • Name • Owner • Owned Schemas • Role Members
Functions	• Date Created • Date Modified • Id • Name • Permissions • Type
Jobs*	• Automatically delete job • Category • Date Created

Object type	Attributes
	• Date Modified • Description • Email notification • Email operator • Enabled • ID • Name • Net send notification • Net send operator • Owner • Page notification • Page operator • Schedules • Write to the Windows Application event log
Job Steps*	• ID • Name • On Failure • On Success • Output file • Process exit code of a successful command • Retry attempts • Retry interval (minutes)

Object type	Attributes
	• Step • Type
Jobs Schedules*	• Date Created • Date Modified • Enabled • ID • Name • Owner • Schedule Type • Settings
Indexes	• Allow page locks • Name • Primary key • Ignore duplicate values • Unique constraint • Allow row locks • Type • Disabled • Included Columns • Fill factor • Data Space ID

Object type	Attributes
	• Index Key Columns • Padded • Hypothetical • Unique
Keys	• Name • ID • Date Created • Date Modified • MS shipped • Published • Schema published • Disabled • Not for replication • Not trusted • Delete referential action • Update referential action • Is system named
Login*	• Date Created • Date Modified • Default Database • Default Language

Object type	Attributes
	• Disabled • Enforce Password Expiration • Enforce Password Policy • Id • Name • Password Hash • Server Roles
Restore	• Type
Schema	• Date Created • Date Modified • Extended Properties • Id • Name • Owner • Permissions
Server Instance*	• Ad Hoc Distributed Queries • Affinity I/O Mask • Affinity Mask • Agent XPs

Object type	Attributes
	• Allow Updates • Awe Enabled • Blocked Process Threshold • C2 Audit Mode • Clr Enabled • Collation • Cost Threshold For Parallelism • Cross Db Ownership Chaining • Cursor Threshold • Database Mail XPs • Date Modified • Default Full-text Language • Default Language • Default Trace Enabled • Disallow Results From Triggers • Fill Factor (%) • Ft Crawl Bandwidth (max) • Ft Crawl Bandwidth (min) • Ft Notify Bandwidth (max) • Ft Notify Bandwidth (min) • Id • In-doubt Xact Resolution • Index Create Memory (K)

Object type	Attributes
	• Lightweight Pooling • Locks • Max Degree Of Parallelism • Max Full-text Crawl Range • Max Server Memory (M) • Max Text Repl Size (B) • Max Worker Threads • Media Retention • Min Memory Per Query (K) • Min Server Memory (M) • Name • Nested Triggers • Network Packet Size (B) • Ole Automation Procedures • Open Objects • Permissions • PH Timeout (s) • Precompute Rank • Priority Boost • Query Wait (s) • Query Governor Cost Limit • Recovery Interval (min) • Remote Admin Connections

Object type	Attributes
	• Remote Login Timeout (s) • Remote Proc Trans • Remote Query Timeout (s) • Remote Access • Replication XPs • Scan For Startup Procs • Server Trigger Recursion • Set Working Set Size • Show Advanced Options • SMO And DMO XPs • SQL Mail XPs • Status • Transform Noise Words • Two Digit Year Cutoff • User Connections • User Instances Enabled • User Instance Timeout • User Options • Web Assistant Procedures • Xp_cmdshell
Server Role*	• Date Created • Date Modified

Object type	Attributes
	• Id • Name • Role Members
Stored Procedure	• ANSI NULLs • Date Created • Date Modified • Encrypted • Execute as • FOR replication • Id • Name • Permissions • Quoted Identifier • Recompile • Schema
Table	• ANSI NULLs • Date Created • Date Modified • Filegroup • Id • Name

Object type	Attributes
	• Partition scheme • Permissions • Schema • Table is partitioned • Table is replicated • Text filegroup
Triggers	Only DML table triggers are supported. • Date Created • Date Modified • Disabled • ID • Instead of trigger • MS shipped • Name • Not for replication
User	• Date Created • Date Modified • Default Schema • Extended Properties • Id • Name

Object type	Attributes
	• Owned Schemas • Roles
View	• ANSI NULLs • Date Created • Date Modified • Encrypted • Id • Name • Permissions • Quoted Identifier • Schema • Schema bound
View Column	• Allow nulls • ANSI Padding Status • Collation • Computed Text • Default Constraint • Full Text • ID • Identity • Identity increment

Object type	Attributes
	• Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale • Rule • Rule Schema • System Type • XML Schema Namespace • XML Schema Namespace schema
View Index	• Allow Page Locks • Allow Row Locks • ID • Data Space ID • Disabled • Fill Factor • Hypothetical • Ignore Dup Key • Name • Padindex

Object type	Attributes
	• Primary Key • Schema Name • Type • Unique • Unique Constraint • View Name
View Index Column	• Column ID • ID • Included Column • Index ID • Key Ordinal • Name • Partition Ordinal • Schema Name • Sort Order • View Name

Monitored Data Types

The following list contains the names of all data types monitored by Netwrix Auditor:

bigint bit	hierarchyid int float	smallint smallmoney table

char cursor date datetime2 datetime datetimeoffset decimal	money nchar nvarchar numeric real smalldatetime	time timestamp tinyint uniqueidentifier varchar xml

Next Steps

Also remember to do the following:

- Configure Data Collecting Account as described in Permissions for SQL Server Auditing section.
- Configure ports as described in the SQL Server Ports section.

SQL Server Ports

Review a full list of protocols and ports required for Netwrix Auditor for SQL Server.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 1433 TCP port. On the computer hosting default SQL Server instance (target), allow inbound connections to local 1433 TCP port.

Port	Protocol	Source	Target	Purpose
1433	TCP	Netwrix Auditor Server	Default SQL Server Instance	Connection to the default named instance server. Port 1433 is the default connections port, however, you can configure another TCP port.
1434	UDP	Netwrix Auditor Server	SQL Server Browser Service	Service which helps resolving named instance servers
Dynamic: **1024 -65535**	TCP	Netwrix Auditor Server	Named SQL Server Instance	Connection to the named instance servers

Permissions 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.

You can use group Managed Service Accounts (gMSA) as data collecting accounts.

On the target SQL Server:

1. To access SQL Server, Windows authentication will be used, so data collection account should be a Windows account specified in the *domain\user* format (*domain\user$* for Managed Service Account). SQL Server logins and authentication method are not supported.

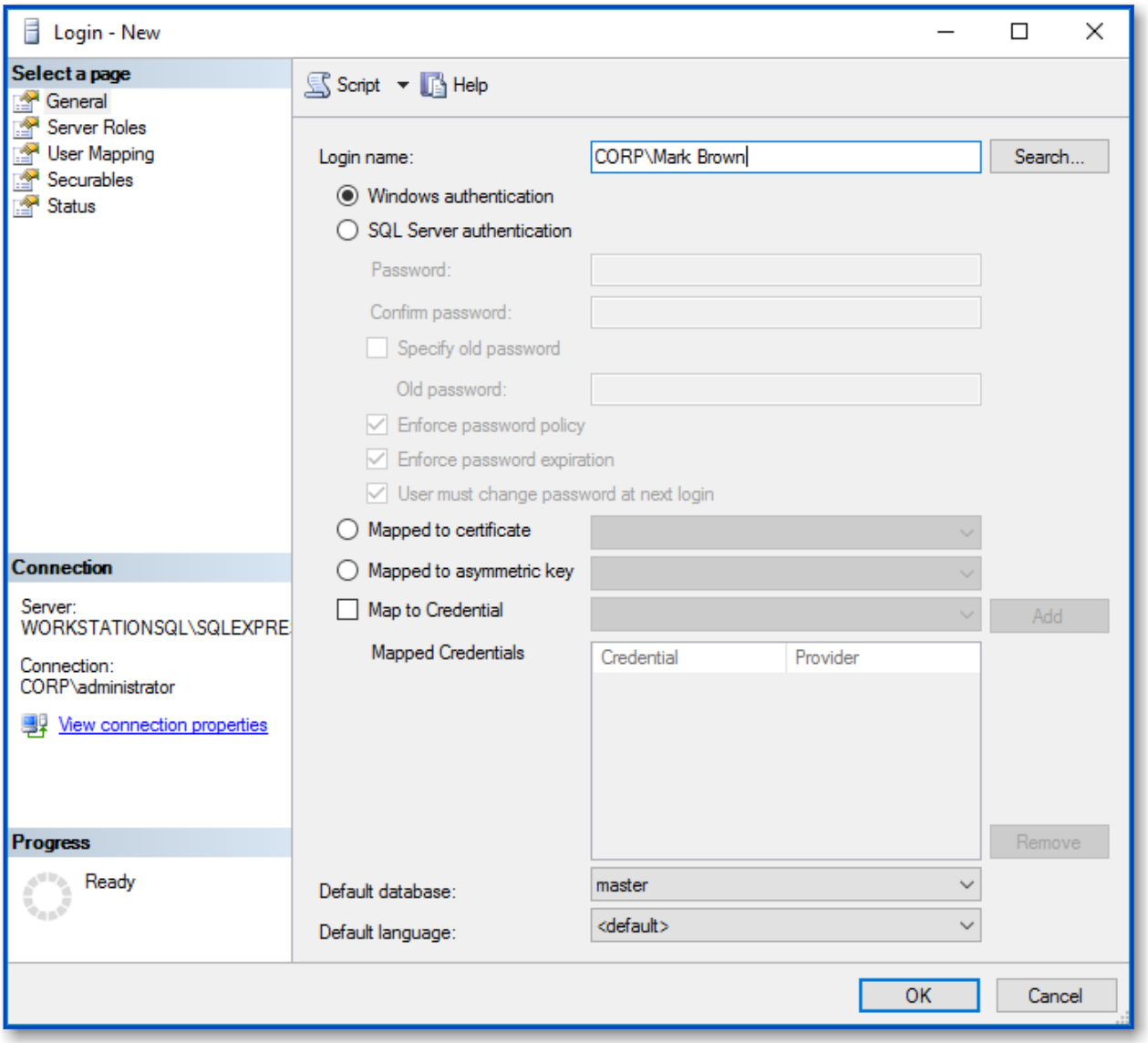
2. The account must be assigned the **System Administrator** server role for this SQL Server. See Assigning 'System Administrator' Role section for more information.
3. For auditing SQL Server availability on groups, the account must have the sysadmin server role granted on each server added to an availability group.

4. If you plan to collect state-in-time data from SQL Server, in addition to requirements above the account will also need:

    - Local **Administrator** rights on the target SQL Server.
    - If SQL Server is included in the Active Directory domain, the account should also be included in that domain.

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.

Configuring Trace Logging

If trace logging is disabled in SQL Server, then changes will be reported in Netwrix Auditor as made by *system*. To detect actual change initiator, Netwrix Auditor needs native trace logs data. During every data collection, Netwrix Auditor will check if the internal SQL audit mechanism is enabled, and enable it if necessary. To read more, refer to this Netwrix Knowledge Base article.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

In some cases, however, you may need to disable trace logging on your SQL Server instance. For that, follow the procedure below.

If you enable monitoring of SQL logons, SQL trace for these logons will be created anyway.

Follow the steps to exclude SQL Server instance from turning trace logging on automatically.

Step 1 – On Netwrix Auditor server, go to the *%Netwrix Auditor installation folder%\SQL Server Auditing* folder.

Step 2 – Locate the *omittracelist.txt* file and open it for editing.

Step 3 – Specify SQL Server instances that you want to exclude from switching trace logging on automatically. Syntax: `server\instance name`

Each entry must be a separate line. Lines that start with the # sign are treated as comments and will be ignored.

With trace logging disabled, the "Who", "Workstation" and "When" values will be not reported correctly by Netwrix Auditor (except for content changes).

By default, SQL Server trace logs will be stored in the predefined location (depending on the SQL Server version). For example, SQL Server 2019 error logs are located at *<drive>:\Program Files\Microsoft SQL Server\MSSQL13.<InstanceName>\MSSQL\Log*.

You can change this default location, using the *pathstotracelogs.txt* file.

Follow the steps to change trace log location.

Step 1 – On Netwrix Auditor server, go to *%Netwrix Auditor installation folder%\SQL Server Auditing* folder.

Step 2 – Locate the *pathstotracelogs.txt* file and open it for editing.

Step 3 – Specify SQL Server instance that you need to audit and enter a UNC path to the folder where you want the trace logs to be stored. Syntax: `SQLServer\Instance|UNC path`

Each entry must be a separate line. Lines that start with the # sign are treated as comments and will be ignored.

Example:

```
SQLSRV01\MSSQL2016|C:\Logs\NA trace logs\
```

If you want to change trace logs location for multiple instances of one SQL server, make sure that specified UNC paths are unique across these instances.

Correct:

```
SQLSRV01\MSSQL2014|C:\Program Files\Microsoft SQL Server\MSSQL\LOG\

SQLSRV01\MSSQL2019|C:\Logs\SQL trace logs\
```

Incorrect:

```
SQLSRV01\MSSQL2014|C:\Logs\SQL trace logs\

SQLSRV01\MSSQL2019|C:\Logs\SQL trace logs\
```

User Activity

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - In the target 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.
        - The User Activity Core Service is installed on the monitored computers. See the Install Netwrix Auditor Agent to Audit User Activity topic for additional information.
        - .NET 4.8 must be installed.
    - On the Auditor console computer:
        - 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.
        - .NET 4.8 must be installed.

See the following topics for additional information:

- Configure Data Collection Settings
- Configure Video Recordings Playback Settings

User Sessions

Review a full list of all session actions when auditing user sessions with Netwrix Auditor.

Object type	Action	What	Description
User session	Session start	Monitoring start	• Logon (session creation)

Object type	Action	What	Description
			• Start of monitoring (after service install or deploy)
	Session start	Local session start	—
	Session end	Sign-out	• User initiated sign-out / logoff
	Session end	Shutdown	• Computer shutdown • Service stop / crash (appears after one starts service again)
	Session start / Session end	Screensaver off / Screensaver on	—
	Session start / Session end	Unlock / Lock	—
	Session start	Console connection	• Connect locally to existing session
	Session end	Console disconnection	• Switch user • Remote connect to existing session
	Session start	Remote connection	• Connect through RDP

Object type	Action	What	Description
	Session end	Remote disconnection	• Disconnect in RDP or just close RDP session

Run As Monitoring

Netwrix Auditor for User Activity can monitor programs executed under different user accounts. Review the table below to discover how different *"run as"* scenarios are reflected in the product.

Object type	Details	Description
Window	None	User runs application.
Window	Application Run As: <account_name>	Standard user runs an application under credentials of another standard user.
Elevated Window	Application Run As: <account_name>	User runs program through Run As Administrator or Accepts UAC (User Account Control) elevation prompts.
Elevated Window	None	Administrator runs the program set to always Run as Administrator. For example, Server Manager.

Install Netwrix Auditor Agent to Audit User Activity

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

Before installing Netwrix Auditor agent to audit user activity, make sure that:

- The audit settings are configured properly.
- The Data Processing Account has access to the administrative shares.

Follow the steps to install Netwrix Auditor agent to audit user activity.

Step 1 – Navigate to *%Netwrix Auditor Installation Folder%\User Activity Video Recording* and copy the UACoreSvcSetup.msi file to the audited computer.

NOTE: This is the default location. However, it may be changed because users can move this folder.

Step 2 – Run the installation package.

Step 3 – Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

Step 4 – On the Agent Settings page, specify the host server (i.e., the name of the computer where Netwrix Auditor is installed) and the server TCP port.

User Activity Ports

Review a full list of protocols and ports required for monitoring User Activity.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on any monitored computer (source), allow outbound connections to remote 9004 TCP port. On the computer where Netwrix Auditor Server resides (target), allow inbound connections to local 9004 TCP port.

Port	Protocol	Source	Target	Purpose
9004	TCP	Monitored computer	Netwrix Auditor Server	Core Service communications
9003	TCP	Netwrix Auditor Server	Monitored computer	Core Service communications
139 **445**	TCP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol (RPC) Remote registry
Dynamic: **1024 -65535**	TCP	Netwrix Auditor Server	Monitored computer	Windows Management Instrumentation
135	TCP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol (RPC) Core Service installation
137 through 139	UDP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol (RPC) Core Service installation
445	TCP	Netwrix Auditor Server	Monitored computer	SMB 2.0/3.0

Port	Protocol	Source	Target	Purpose
				Video files copy
–	ICMP	Netwrix Auditor Server	Monitored computer	Core Service communications

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 the Check the Windows Services Status topic for additional information.
- The **File and Printer Sharing** and the **Windows Management Instrumentation** features are allowed to communicate through Windows Firewall. See the Windows Features Communication topic for additional 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. See the Open Local TCP Port 9004 topic for additional information.
- Local TCP Port 9003 is opened for inbound connections on the audited computers. See the Open Local TCP Port 9003 topic for additional information.
- Remote TCP Port 9004 is opened for outbound connections on the audited computers. See the Open Remote TCP Port 9004 topic for additional information.

Check the Windows Services Status

Follow the steps to check the status and startup type of Windows services.

Step 1 – Navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Services**.

Step 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.

Step 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.

Step 4 – Perform the steps above for the **Windows Management Instrumentation** service.

Windows Features Communication

Follow the steps to allow Windows features to communicate through Firewall.

Step 1 – Navigate to **Start** → **Control Panel** and select **Windows Firewall.**

Step 2 – In the **Help Protect your computer with Windows Firewall** page, click **Allow a program or feature through Windows Firewall** on the left.

Step 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.

Step 4 – Repeat step 3 for the **Windows Management Instrumentation (WMI)** feature.

Open Local TCP Port 9004

Follow the steps to open Local TCP Port 9004 for inbound connections.

Step 1 – On the computer where Netwrix Auditor is installed, navigate to **Start** → **Control Panel** and select **Windows Firewall.**

Step 2 – In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select Inbound Rules on the left.

Step 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.

Step 5 – Double-click the newly created rule and open the Protocols and Ports tab.

Step 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"*.

Open Local TCP Port 9003

Follow the steps to open Local TCP Port 9003 for inbound connections.

Step 1 – On a target computer navigate to **Start** → **Control Panel** and select **Windows Firewall.**

Step 2 – In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select Inbound Rules on the left.

Step 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

Option	Setting
Name	Rule name, for example UA Core Service inbound rule.

Step 5 – Double-click the newly created rule and open the Protocols and Ports tab.

Step 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"*.

Open Remote TCP Port 9004

Follow the steps to open Remote TCP Port 9004 for outbound connections.

Step 1 – On a target computer, navigate to **Start** → **Control Panel** and select **Windows Firewall.**

Step 2 – In the **Help Protect your computer with Windows Firewall** page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select Outbound Rules on the left.

Step 4 – Click New Rule. In the New Outbound 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*.

Option	Setting
Action	Allow the connection
Profile	Applies to Domain
Name	Rule name, for example UA Core Service outbound rule.

Step 5 – Double-click the newly created rule and open the Protocols and Ports tab.

Step 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"*.

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 via console, the following settings must be configured:

- 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 the To Add an Account to Netwrix Auditor Client Users Group topic for additional 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 the To Enable Windows Features topic for additional information.

To be able to watch video files captured by Netwrix Auditor via direct links, 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 the To Configure Internet Explorer Security Settings topic for additional information.
- JavaScript must be enabled. See the To Enable JavaScript topic for additional information.
- Internet Explorer Enhanced Security Configuration (IE ESC) must be disabled. See the To Disable Internet Explorer Enhanced Security Configuration (IE ESC) topic for additional information.

All Internet Explorer-related settings are relevant only for those who watch videos not in Netwrix Auditor console.

NOTE: Microsoft is in the process of deprecating Internet Explorer. However, if you are trying to access the video recordings from browser via direct links (reports on SSRS portal, subscriptions, activity summaries, search export results), IE engine should be present on the client machine. IE might be disabled with GPO, but it should not be removed completely. Recommended option is to use Edge with "IE mode" option enabled.

To Configure Internet Explorer Security Settings

Follow the steps to configure Internet Explorer security settings.

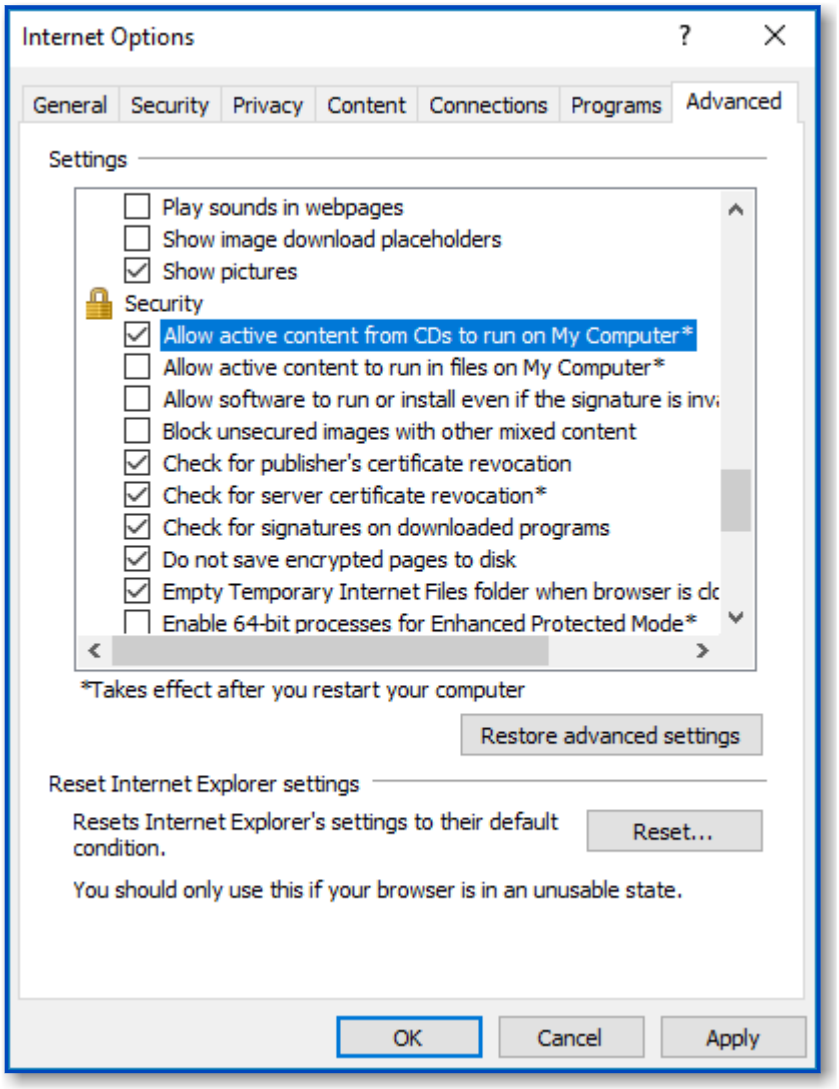
Step 1 – In Internet Explorer, navigate to **Tools** > **Internet Options**.

Step 2 – Switch to the Security tab and select **Local Intranet**. Click **Custom Level**.

Step 3 – In the Security Settings - Local Intranet Zone dialog, scroll down to **Downloads** and verify that **File download** is set to **Enable**.

Step 4 – In the Internet Options dialog, switch to the **Advanced** tab.

Step 5 – Local Security and select the **Allow active content to run in files on My Computer** checkbox.



To Enable JavaScript

Follow the steps to enable JavaScript.

Step 1 – In Internet Explorer, navigate to **Tools** > **Internet Options**.

Step 2 – Switch to the Security tab and select **Internet**. Click **Custom Level**.

Step 3 – In the Security Settings - Internet Zone dialog, scroll down to **Scripting** and verify that **Active scripting** is set to **Enable**.

To Disable Internet Explorer Enhanced Security Configuration (IE ESC)

Follow the steps to disable Internet Explorer enhanced security configuration.

Step 1 – Navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Server Manager**.

Step 2 – In the Security Information section, click Configure IE ESC link on the right to disable it.

To Add an Account to Netwrix Auditor Client Users Group

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.

Follow the steps to add an account to the Netwrix Auditor Client Users group.

Step 1 – On the computer where Netwrix Auditor Server is installed, start the Local Users and Computers snap-in.

Step 2 – Navigate to the Groups node and locate the Netwrix Auditor Client Users group.

Step 3 – In the Netwrix Auditor Client Users Properties dialog, click **Add**.

Step 4 – Specify the users you want to be included in this group.

To Enable Windows Features

Follow the steps if Netwrix Auditor Server is installed on the Windows Server 2012 and later.

Step 1 – Navigate to **Start** > **Server Manager**.

Step 2 – In the Server Manager window, click **Add roles and features**.

Step 3 – On the Select Features step, select one of the following Windows features and the follow the installation prompts:

- Ink and Handwriting Services
- Media Foundation
- User Interface and Infrastructure > Desktop Experience

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.

Step 4 – Restart your computer to complete features installation.

VMware

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring automatically through a monitoring plan. No manual configurations are required.

Review a full list of object types and attributes Netwrix Auditor can collect on VMware server (standalone host or vCenter server).

Object type	Attributes
Virtual Machine	• Annotation • Check and upgrade Tools • Connect at power on • Connected • Current Snapshot • Disable Acceleration • Enable Logging • Force BIOS Setup • Guest OS

Object type	Attributes
	• Guest OS Version • Guest Power Management • Guest State • Hardware Page Table Virtualization • Hyper-threaded Core Sharing • Memory Size (M) • Notes • Number of virtual processors • Operation mode of guest OS • Power Off Type • Power On • Power State • Power-on Boot Delay • Record Debugging Information • Reset Type • Resource Pool • Run VMware Tools Scripts After Powering On • Run VMware Tools Scripts After Resuming • Run VMware Tools Scripts Before Powering Off • Run VMware Tools Scripts Before Suspending • Snapshot Description • Snapshot Name • Suspend Type • Synchronize guest time with host • Swap file Location • Template • Virtual Machine Name • VirtualCdrom Device Type • VirtualCdrom Mode • VirtualDisk Capacity(K) • VirtualDisk Datastore • VirtualDisk Disk Mode • VirtualDisk Share Level • VirtualDisk Unit Number • VirtualFloppy Device Type • VirtualParallelPort Connection • VirtualPCNet32 MAC Address Type • VirtualPCNet32 MAC Address • VirtualPCNet32 Wake on LAN • VirtualSerialPort Connection • VirtualSerialPort Far End • VirtualSerialPort Near End • VirtualSerialPort Yield CPU on poll • VirtualSCSIController Controller Type

Object type	Attributes
	• VirtualSCSIController Bus Sharing • VirtualSCSIController Bus Number
Authorization Manager	• Authorization Manager Name • Privilege
Cluster Resource	• Available CPU • Available Hosts • Available Memory • Name • Swap Policy for Virtual Machines • VMware DRS • VMware DRS Automation Level • VMware DRS Migration threshold • VMware DRS Power Management • VMware DRS 'Keep Virtual Machines Together' Rule Name • VMware DRS 'Keep Virtual Machines Together' Rule Enabled • VMware DRS 'Keep Virtual Machines Together' Rule Status • VMware DRS 'Keep Virtual Machines Together' Rule Virtual Machine • VMware DRS 'Separate Virtual Machines' Rule Name • VMware DRS 'Separate Virtual Machines' Rule Enabled • VMware DRS 'Separate Virtual Machines' Rule Status • VMware DRS 'Separate Virtual Machines' Rule Virtual Machine • VMware DRS Virtual Machine Automation Mode • VMware HA • VMware HA Admission Control • VMware HA Isolation Response • VMware HA Restart Priority • VMware HA Number of host failures allowed • VMware HA Advanced Option • VMware HA Isolation Response

Object type	Attributes
	• VMware HA Restart Priority
Computer Resource	• Name
Datacenter	• Name
Data Store	• Accessible • Name
Distributed Port Group	• Name • Distributed Virtual Switch • Ports Number • Uplink
Distributed Switch	• Name • Port Group • Uplink Port
Folder	• Folder Name
Host System	• Configuration Status • CPU Expandable Reservation • CPU Limit • CPU Reservation • CPU Shares Level • CPU Shares • Datastore accessible to Host • Memory Expandable Reservation • Memory Limit • Memory Reservation

Object type	Attributes
	• Memory Shares Level • Memory Shares • NTP required • NTP uninstallable • NTP running • NTP policy • NTP Servers • Overall Status • Port Group Allow Promiscuous • Port Group MAC Address Changes • Port Group Forged Transmits • Port Group VLAN ID • Port Group Attached uplink adapter • Service Console IP Address of port • Virtual Switch Allow Promiscuous • Virtual Switch MAC Address Changes • Virtual Switch Forged Transmits • Virtual Switch Number of Ports • Virtual Switch Attached uplink adapter • VMkernel IP Address of port
Resource Pool	• Name
VirtualApp	• Name • Child • Parent Folder

Users and groups

Starting with the version 10.5, Netwrix Auditor for VMware collects data on VMware users and groups.

To audit users and groups, vCenter 6.5 and above required.

The following objects are monitored:

- vCenter Single Sign-On (SSO) Users. The product collects data from vCenter.

- Localos users. For these users, the product collects data from ESXi and vCenter.

  the Who value is reported as *"Not Applicable"* for the localos users if the data was collected from the entire vCenter.

- VMware groups. The product collects data from vCenter.

Object type	Actions	Attributes
SSO User	• Added • Modified • Removed	• Description • Email • FullName • Disabled
Localos user	• Added • Modified • Removed	• Disabled • FullName • Locked • Member Of • Name
Group	• Added • Modified • Removed	• Member • Description

Netwrix Auditor may report on several changes with *who* reported as *system* due to the native VMware audit peculiarities

Considerations and Limitations

The following considerations refer to VMware infrastructure monitoring with Netwrix Auditor:

- A VM that was moved from one resource pool to another (within the same VMware host) will be reported as *Modified*.

- If an ESXi host was specified as a monitored item in the corresponding monitoring plan, but a virtual machine was created using the vCenter Server (not this ESXi host) management facilities, information about this VM creation will not be collected. To work around, specify the vCenter Server as a monitored item in the monitoring plan.
- For ESXi host permission changes, the "What" field in the Activity Records (and, therefore, reports and search results) will report *\root*.
- Netwrix Auditor will not collect data on *Failed Logon* event in case of incorrect logon attempt through VMware vCenter Single Sign-On.
- Also, data on the logon attempts performed using SSH will not be collected.
- For custom role creation event, initiator will be reported as *System*.

VMware Ports

Review a full list of protocols and ports required for Netwrix Auditor for VMware.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 443 TCP port. On the VMware server (target), allow inbound connections to local 443 TCP port.

Port	Protocol	Source	Target	Purpose
443	TCP	Netwrix Auditor Server	VMware	HTTPS Connection to VMware VSphere via SDK

Permissions 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. Contact your virtual infrastructure administrator if necessary.

On the target VMware hosts:

- To collect state-in-time data, and auditing SSO users, local users, and groups, the account must be included in the **Administrators** group for the vCenter SSO domain. (If you have assigned the **Read-only** role to that account, it should be removed.)
- To collect activity data, the account must have at least Read-only role on the audited hosts.

See the following VMware article for additional information: Add Members to a vCenter Single Sign-On Group.

Then you will provide this account in the monitoring plan wizard — it will be used as default account to process all items (VMware servers) included in the monitoring plan. However, if you want to use specific settings for each of your VMware servers, you can provide custom account when configuring a corresponding monitored item.

See also:

- Create a New Monitoring Plan step of the monitoring plan wizard

Windows Server

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:

    - The Remote Registry and the Windows Management Instrumentation (WMI) service must be started. See the Enable Remote Registry and Windows Management Instrumentation Services topic and the Configure Windows Registry Audit Settings topic for additional information.

- 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 Changeadvanced audit policies must be set to *"Success"*.
  - See the Configure Local Audit Policies topic and the Configure Advanced Audit Policies topic for additional information.
- 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. This policy should be configured manually since Auditor does not enable it automatically. See the Configure Enable Persistent Time Stamp Policy topic for additional information.
- 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"*. See the Adjusting Event Log Size and Retention Settings topic for additional information.
- 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"*. See the Adjust DHCP Server Operational Log Settings topic for additional information.
- 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)
    - If the audited servers are behind the Firewall, review the list of protocols and ports required for Netwrix Auditor and make sure that these ports are opened. See the Windows Server Ports topic for additional information.
    - For auditing removable storage media, two Event Trace Session objects must be created. See the Configure Removable Storage Media for Monitoring topic for additional information.
    - If you want to use Network traffic compression, make sure that the Auditor console computer is accessible by its FQDN name.
    - For auditing IIS:
        - 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"*.

Whatever method you choose to configure Windows Server for auditing (manual or automated), also remember to do the following:

1. Configure Data Collecting Account, as described in the Data Collecting Account topic.
2. Configure required protocols and ports, as described in the Windows Server Ports topic.

Exclude Monitored Objects

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Windows Server monitoring scope.

Follow the steps to exclude data from the Windows Server monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Windows Server Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- Wildcards (* and ?) are supported. A backslash (\) must be put in front of (*), (?), (,), and (\) if they are a part of an entry value.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitcollectlist.txt	Contains a list of objects and their properties to be excluded from being monitored.
	
	If you want to restart monitoring these objects, remove them from the omitcollectlist.txt and run data collection at least twice.
		`monitoring plan name,server name,class name,property name,property value`
		
		`class name` is a mandatory parameter, it cannot be replaced with a wildcard. `property name` and `property value` are optional, but cannot be replaced with wildcards either.
		
		For example:
		
		`**,server,MicrosoftDNS_Server`
		`**,*,StdServerRegProv`

omiterrors.txt	Contains a list of errors/warnings to be omitted from logging to the Netwrix Auditor System Health event log.	`monitoring plan name,server name,error text`

File	Description	Syntax
		For example: `*,productionserver1.corp.local,*Access is denied*`

omitreportlist.txt	Contains a list of objects to be excluded from reports and Activity Summary emails. In this case audit data is still being collected.	`monitoring plan name,who,where,object type,what,property name`
		
		For example:
		
		`*,CORP\\jsmith,*,*,*,*`

omitsitcollectlist.txt	Contains a list of objects to be excluded from State-in-time reports.	`monitoring planname,server name,class name,property name,property value`
		
		`class name` is a mandatory parameter, it cannot be replaced with a wildcard. `property name` and `property value` are optional, but cannot be replaced with wildcards either.
		
		For example:
		
		`*,server,MicrosoftDNS_Server`
		
		`*,*,StdServerRegProv`

omitstorelist.txt	Contains a list of objects to be excluded from being stored to the Audit Archive and showing up in reports. In this case audit data is still being collected.	`monitoring plan name,who,where,object type,what,property name` For example:

File	Description	Syntax
		,,*,Scheduled task,Scheduled Tasks\\User_Feed_Synchronization*,*

Monitored Objects

This section lists Windows Server components and settings whose changes Netwrix Auditor can monitor.

When monitoring a Windows Server, Netwrix Auditor needs to audit some registry settings. See the Windows Server Registry Keys section for additional information. If you want Netwrix Auditor to audit custom registry keys, see the Monitoring Custom Registry KeysMonitoring Custom Registry Keystopic for additional information.

In the table below, double asterisks (**) indicates the components and settings for which the Who value is reported as *"Not Applicable"*.

Object type	Attributes
General Computer Settings	
Computer	• System state changed to Started • System state changed to Stopped. Reason: Reason type • System state changed to Stopped. Reason: unexpected shutdown or system failure
Computer Name	• Computer Description • Name • Domain
Environment Variables	• Type

Object type	Attributes
	• Value
Event Log	• Event Log Cleared
General	• Caption • Organization • Registered User • Serial Number • Service Pack** • Version**
Remote	• Enable Remote Desktop on this computer
Startup and Recovery	• Automatically Restart • Dump File • Dump Type • Overwrite any existing file • Send Alert • System Startup Delay • Write an Event
System Time	• System time changed from ... to ... • Time zone changed Not supported on Windows Server 2008 SP2 and Windows Server 2008 R2.
Add / Remove Programs	
Add or Remove Programs	• Installed For** • Version

Object type	Attributes
Services	
System Service	• Action in case of failed service startup • Action in case of service stopping • Allow service to interact with desktop • Caption • Created • Deleted • Description • Name • Path to executable • Service Account • Service Type • Start Mode • Error Control
Audit Policies	
Local Audit Policy	• Added Audit settings Only for the Global Object Access Auditing advanced policies. • Successful audit enabled/disabled • Failure audit enabled/disabled
Per-User Local Audit Policy	• Success audit include added • Success audit include removed • Failure audit include added • Failure audit include removed • Success audit exclude added • Success audit exclude removed • Failure audit exclude added • Failure audit exclude remove
Hardware	
Base Board**	• Hosting Board

Object type	Attributes
	• Status • Manufacturer • Product • Version • Serial Number
BIOS**	• Manufacturer • Version
Bus**	• Bus Type • Status
Cache Memory**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Purpose • Status
CD-ROM Drive**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Media Type • Name • SCSI Bus • SCSI Logical Unit • SCSI Port • SCSI Target ID • Status
Disk Partition**	• Primary Partition • Size (bytes) • Starting offset (bytes)

Object type	Attributes
Display Adapter**	• Adapter RAM (bytes) • Adapter Type • Bits/Pixel • Configuration Manager Error Code • Driver Version • Installed Drivers • Last Error Description • Last Error Code • Refresh Rate • Resolution • Status
DMA**	• Status
Floppy Drive**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Hard Drive**	• Bytes/Sector • Configuration Manager Error Code • Interface Type • Last Error Description • Last Error Code • Media Loaded • Media Type • Model • Partitions • SCSI Bus • SCSI Logical Unit • SCSI Port • SCSI Target ID • Sectors/Track • Size (bytes) • Status • Total Cylinders • Total Heads • Total Sectors

Object type	Attributes
	• Total Tracks • Tracks/Cylinder
IDE**	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Status
Infrared**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Keyboard**	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Layout • Name • Status
Logical Disk**	• Description • File System • Size (bytes) • Status
Monitor**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Monitor Type • Status

Object type	Attributes
Network Adapter	• Adapter Type * • Configuration Manager Error Code • Default IP Gateway * • DHCP Enabled* • DHCP Server • DNS Server Search Order • IP Address * • Last Error Description • Last Error Code • MAC Address • Network Connection Name • Network Connection Status • Service Name • Status * — indicates the properties whose changes may not be reported correctly, displaying "*Who*" (i.e. initiator's account) as *System*.
Network Protocol**	• Description • Status
Parallel Ports**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
PCMCIA Controller**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Physical Memory**	• Capacity (bytes) • Status • Manufacturer • Memory Type

Object type	Attributes
	• Speed • Part Number • Serial Number
Pointing Device**	• Configuration Manager Error Code • Double Click Threshold • Handedness • Hardware Type • Last Error Description • Last Error Code • Number of buttons • Status
Printing	• Comment** • Hidden** • Local** • Location** • Name** • Network** • Port Name** • Printer error information • Published** • Shared** • Share Name** • Status
Processor**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Max Clock Speed (MHz) • Name • Status
SCSI**	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code

Object type	Attributes
	• Status
Serial Ports**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Maximum Bits/Second • Name • Status
Sound Device**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
System Slot**	• Slot Designation • Status
USB Controller**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Name • Status
USB Hub**	• Configuration Manager Error Code • Last Error Description • Last Error Code • Name • Status
DHCP configuration	

Object type	Attributes
If the DHCP server runs on Windows Server 2008 (or below), then the Who value for DHCP server configuration events is reported as *"Not Applicable"*.	
Server role	• Added • Removed
Server settings	• Type: ◦ IPv4 ◦ IPv4 Filters ◦ IPv6 • Action: ◦ Modified
DHCP scope	• Type: ◦ IPv4 ◦ Multicast IPv4 ◦ Superscope for IPv4 ◦ IPv6 • Action: ◦ Added ◦ Removed ◦ Modified ◦ Moved
DHCP Reservation	• Type: ◦ IPv4 ◦ IPv6 • Action: ◦ Added ◦ Removed ◦ Modified
DHCP Policy	• Type: ◦ IPv4

Object type	Attributes
	◦ IPv4 server-wide • Action: ◦ Added ◦ Removed ◦ Modified ◦ Renamed
Removable media	
Removable Storage Media**	Netwrix Auditor does not report on floppy/optical disk and memory card storage medias. For removable storages, the When value reports actual time when a change was made and/or a target server was started. • Device class: ◦ CD and DVD ◦ Floppy Drives ◦ Removable Disk ◦ Tape Drives ◦ Windows Portable Devices When the Audit Object Access local audit policy and/or the Audit Central Access Policy Staging \ Audit Removable Storage advanced audit policies are enabled on the target server, the `gpupdate /force` command execution issues removable storage restart. These actions are disclosed in Netwrix Auditor reports, search, and activity summaries. Note that these actions are system, not user-effected.
Scheduled Tasks	
Scheduled Task	• Account Name • Application

Object type	Attributes
	• Comment • Creator • Enabled • Parameters • Triggers
Local Users and Groups	
Local Group	• Description • Name • Members
Local User	• Description • Disabled/Enabled • Full Name • Name • User cannot change password • Password Never Expires • User must change password at next logon
DNS Configuration	
The Who value will be reported for DNS configuration settings only if the DNS server runs on Windows Server 2012 R2. See the following Microsoft article for additional information: Update adds query logging and change auditing to Windows DNS servers.	
DNS Server	• Address Answer Limit • Allow Update • Auto Cache Update • Auto Config File Zones • Bind Secondaries • Boot Method • Default Aging State • Default No Refresh Interval • Default Refresh Interval • Disable Auto Reverse Zones • Disjoint Nets

Object type	Attributes
	• Ds Available • Ds Polling Interval • Ds Tombstone Interval • EDns Cache Timeout • Enable Directory Partitions • Enable Dns Sec • Enable EDns Probes • CD-ROM D Enable Netmask Ordering • Event Log Level • Fail On Load If Bad Zone Data • Forward Delegations • Forwarders • Forwarding Timeout • Is Slave • Listen Addresses • Log File Max Size • Log File Path • Log Level • Loose Wildcarding • Max Cache TTL • Max Negative Cache TTL • Name Check Flag • No Recursion • Recursion Retry • Recursion Timeout • Round Robin • Rpc Protocol • Scavenging Interval • Secure Cache Against Pollution • Send Port • Server Addresses
DNS Zone	• Aging State • Allow update • Auto created • Data file name • Ds integrated

Object type	Attributes
	• Expires after • Forwarder slave • Forwarder timeout • Master servers • Minimum TTL • No refresh interval • Notify • Notify servers • Owner name • Paused • Primary server • Refresh interval • Responsible person • Retry interval • Reverse • Scavenge servers • Secondary servers • Secure secondaries • Shutdown • TTL • User NB stat • Use WINS • Zone type
DNS Resource Records	
The Who value will be reported for DNS Resource Records only if the DNS server runs Windows Server 2012 R2. See the following Microsoft article for additional information: Update adds query logging and change auditing to Windows DNS servers.	
DNS AAAA	• Container name • IPv6 Address • Owner name • Record class • TTL • Zone type
DNS AFSDB	• Container name • Owner name

Object type	Attributes
	• Server name • Server subtype • Record class • TTL • Zone type
DNS ATM A	• ATM Address • Container name • Format • Owner name • Record class • TTL • Value • Zone type
DNS A	• Container name • IP Address • Owner name • Record class • TTL • Zone type
DNS CNAME	• Container name • FQDN for target host • Owner name • Record class • TTL • Zone type
DNS DHCID	• Container name • DHCID (base 64) • Owner name • Record class • TTL

Object type	Attributes
	• Zone type
DNS DNAME	• Container name • FQDN for target domain • Owner name • Record class • TTL • Zone type
DNS DNSKEY	• Algorithm • Container name • Key type • Key (base 64) • Name type • Owner name • Protocol • Record class • Signatory field • TTL • Zone type
DNS DS	• Algorithm • Container name • Data • DigestType • Key tag • Owner name • Record class • TTL • Zone type

Object type	Attributes
DNS HINFO	• Container name • CPU type • Operating system • Owner name • Record class • TTL • Zone type
DNS ISDN	• Container name • ISDN phone number and DDI • ISDN subaddress • Owner name • Record class • TTL • Zone type
DNS KEY	• Algorithm • Container name • Key type • Key (base 64) • Name type • Owner name • Protocol • Record class • Signatory field • TTL • Zone type
DNS MB* **	• Container name • Mailbox host • Owner name • Record class • TTL • Zone type

Object type	Attributes
DNS MD	• Container name • MD host • Owner name • Record class • TTL • Zone type
DNS MF	• Container name • MF host • Owner name • Record class • TTL • Zone type
DNS MG	• Container name • Member mailbox • Owner name • Record class • TTL • Zone type
DNS MINFO	• Container name • Error mailbox • Owner name • Responsible mailbox • Record class • TTL • Zone type
DNS MR	• Container name • Owner name

Object type	Attributes
	• Replacement mailbox • Record class • TTL • Zone type
DNS MX	• Container name • FQDN of mail server • Mail server priority • Owner name • Record class • TTL • Zone type
DNS NAPTR	• Container name • Flag string • Order • Owner name • Preference • Record class • Regular expression string • Replacement domain • Service string • TTL • Zone type
DNS NS	• Container name • Name servers • Owner name • TTL
DNS NXT	• Container name • Next domain name • Owner name • Record class • Record types

Object type	Attributes
	• TTL • Zone type
DNS PTR	• Container name • Owner name • PTR domain name • Record class • TTL • Zone type
DNS RP	• Container name • Mailbox of responsible person • Optional associated text (TXT) record • Owner name • Record class • TTL • Zone type
DNS RRSIG	• Algorithm • Container name • Key tag • Labels • Original TTL • Owner name • Record class • Signature expiration (GMT) • Signature inception (GMT) • Signature (base 64) • Signer's name • TTL • Type covered • Zone type
DNS RT	• Container name • Intermediate host • Owner name

Object type	Attributes
	• Preference • Record class • TTL • Zone type
DNS SIG	• Algorithm • Container name • Key tag • Labels • Original TTL • Owner name • Record class • Signature expiration (GMT) • Signature inception (GMT) • Signature (base 64) • Signer's name • TTL • Type covered • Zone type
DNS SRV	• Container name • Host offering this service • Owner name • Port number • Priority • Record class • TTL • Weight • Zone type
DNS TEXT	• Container name • Owner name • Record class • Text • TTL • Zone type

Object type	Attributes
DNS WINS	• Cache time-out • Container name • Do not replicate this record • Lookup time-out • Owner name • Record class • Wins servers • Zone type
DNS WKS	• Container name • IP address • Owner name • Protocol • Record class • Services • TTL • Zone type
DNS X25	• Container name • Owner name • Record • Record class • TTL • X.121 PSDN address • Zone type
File Shares	
Share	• Access-based enumeration • Caching • Description • Enable BranchCache • Encrypt data access • Folder path • Share permissions • User limit

Windows Server Registry Keys

If you want to monitor changes to system components on a Windows Server, make sure that Windows Registry audit settings are configured on that Windows server.

This refers to the following keys:

- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_USERS\.DEFAULT

For these keys and subkeys, the following advanced permissions must be audited ("*Successful*" audit type required):

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

The below is the full list of keys (and subkeys) involved in Windows Server auditing.

Hardware	• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces(|\.*) • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}(|\.*) • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}(|\.*) • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services(|\.*)

General	• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl(|\.*) • HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CrashControl(|\.*) • HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Control\CrashControl(|\.*) • HKEY_LOCAL_MACHINE\Software\WOW6432NODE\Microsoft\Windows NT\CurrentVersion(|\.*) • HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion(|\.*)
Software	• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL(|\.*) • HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL(|\.*)
Services	• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services(|\.*) • HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services(|\.*)

	• HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services(|\.*)
RemovableMedia	• SYSTEM\CurrentControlSet\Enum

Consider that audit data for the registry keys themselves will not appear in Netwrix Auditor reports, alerts or search results, as it is only used as one of the sources for the Activity Records formation.

- You can configure these settings automatically using Netwrix Auditor, as described in the Settings for Data Collection topic. Corresponding audit settings will be also applied automatically after you select a checkbox under **Monitor changes to system components** on the **General** tab in the Windows Server data source properties.

Audit settings will be automatically adjusted only for the keys/subkeys involved in the monitoring of selected components (granular adjustment). For example, if you selected **Services**, the program will adjust the audit settings for the following subkeys:

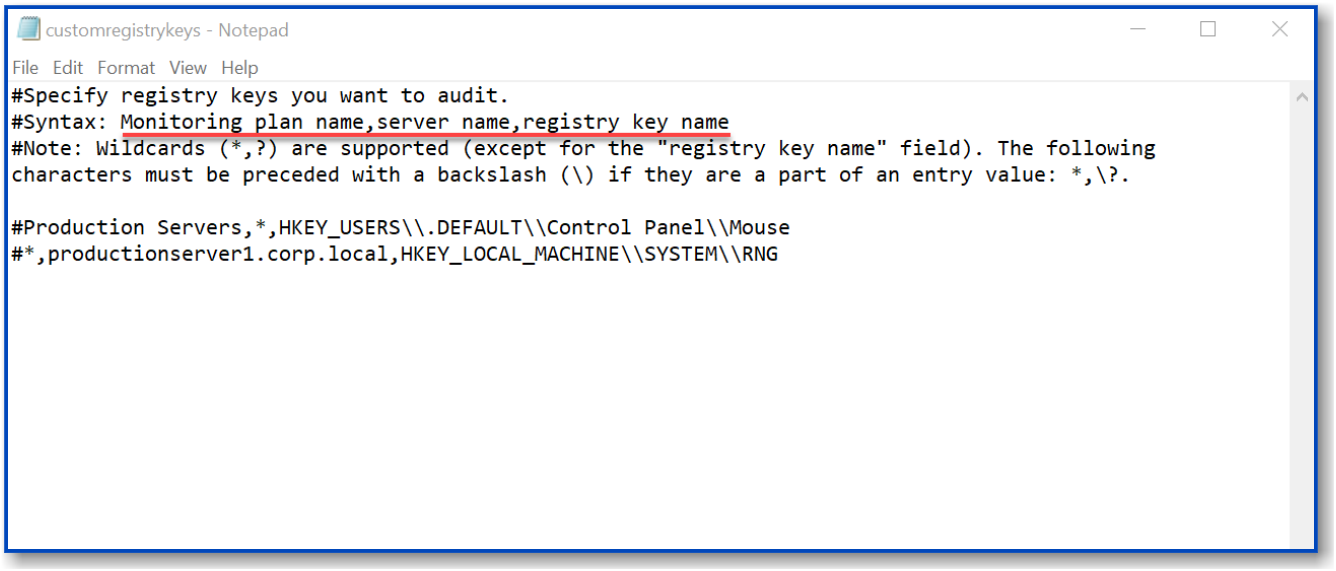
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services(|\\.*)
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services(|\\.*)
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services(|\\.*)

- To configure the audit settings manually, refer to the Configure Windows Registry Audit Settings topic for additional information.

Monitoring Custom Registry Keys

Follow the steps to monitor custom registry keys.

Step 1 – On the computer where Auditor Server resides, navigate to *%Netwrix Auditor installation folder%\Windows Server Auditing.*



Step 2 – Edit the following parameters of the customregistrykeys.txt file:

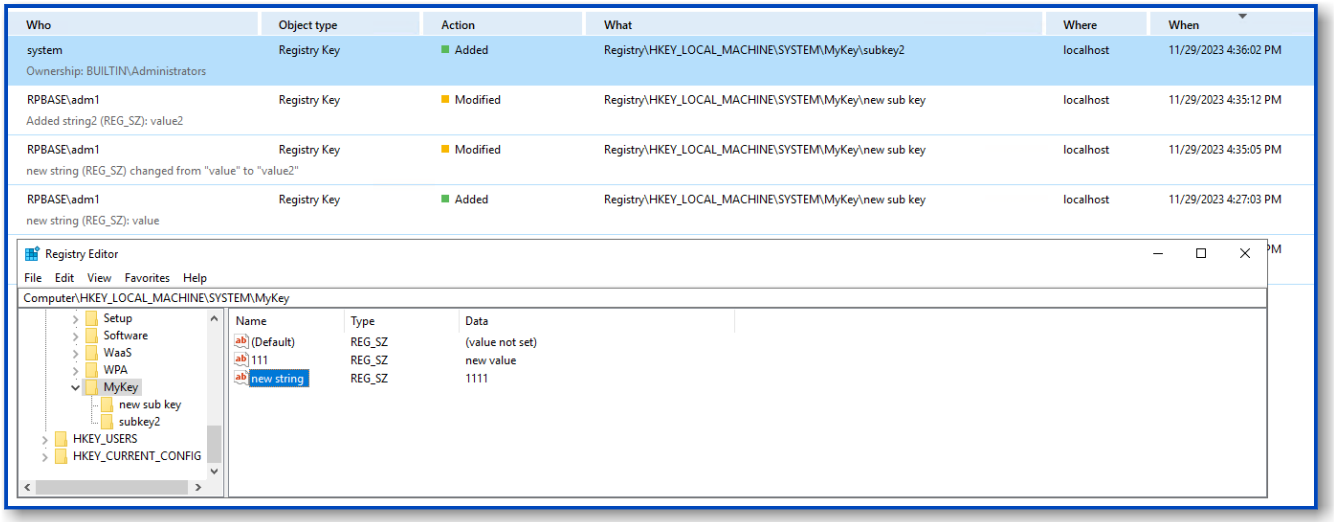
`monitoring plan name,server name,registry key name`

For example:

`#*,productionserver1.corp.local,HKEY_LOCAL_MACHINE\\sYsTEM\\RNG`

Step 3 – Consider the following:

- Each entry must be a separate line.
- Wildcards (* and ?) are supported (except for the `registry key name` field). A backslash (\) must be put in front of (*), (?), (,), and (\) if they are a part of an entry value.
- Lines that start with the # sign are treated as comments and are ignored.



NOTE: In some cases, **Who** will be the system and **When** will be collection time, because there is no necessary event in the Security log with this path.

VM Template Cloning

While VM cloning is supported by Netwrix Auditor, an additional setup process should be taken into consideration before the deployment process.

Every monitored VM instance gets a unique ID assigned for monitoring and data collection purposes. To ensure proper operation, the VM template must be excluded from the monitoring scope beforehand. Omitting the VM template will allow Netwrix Auditor to assign unique IDs correctly and collect data as intended.

Follow the steps to add the template server to exclusions.

Step 1 – In main Netwrix Auditor menu, select **Monitoring plans**.

Step 2 – Select your Windows Server monitoring plan and click **Edit**.

Step 3 – Choose the AD Container containing the template VM and click **Edit data source** in the right pane.

Step 4 – In the left pane, select **Containers and Computers**.

Step 5 – Check the **Exclude these objects** checkbox and add the template VM by clicking **Add Computer**.

VM template server is added to exclusions and ready to use.

Windows Server Ports

Review a full list of protocols and ports required for Netwrix Auditor for Windows Server.

- Allow outbound connections from the dynamic (1024 - 65535) local port on the computer where Netwrix Auditor Server resides.
- Allow outbound connections to remote ports on the source and inbound connections to local ports on the target.

Tip for reading the table: For example, on the computer where Netwrix Auditor Server resides (source), allow outbound connections to remote 139 TCP port. On monitored computers (target), allow inbound connections to local 139 TCP port.

Port	Protocol	Source	Target	Purpose
139 **445**	TCP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol (RPC) Remote registry
135 **+ Dynamic:** **1024 -65535**	TCP	Netwrix Auditor Server	Monitored computer	Windows Management Instrumentation Collect objects
135 **+ Dynamic:** **1024 -65535**	TCP	Netwrix Auditor Server	Monitored computer	Collect removable storage insertions. Allow the following process to use the port: %systemroot%\system32\plasrv.exe
135	TCP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol (RPC) Core Service installation
137 through 139	UDP	Netwrix Auditor Server	Monitored computer	Service Control Manager Remote Protocol (RPC) Core Service installation

Port	Protocol	Source	Target	Purpose
445	TCP	Netwrix Auditor Server	Monitored computer	SMB 2.0/3.0
9011	TCP	Computers where Netwrix Auditor for Windows Server Compression Services reside	Netwrix Auditor Server	Network traffic compression and interaction with services

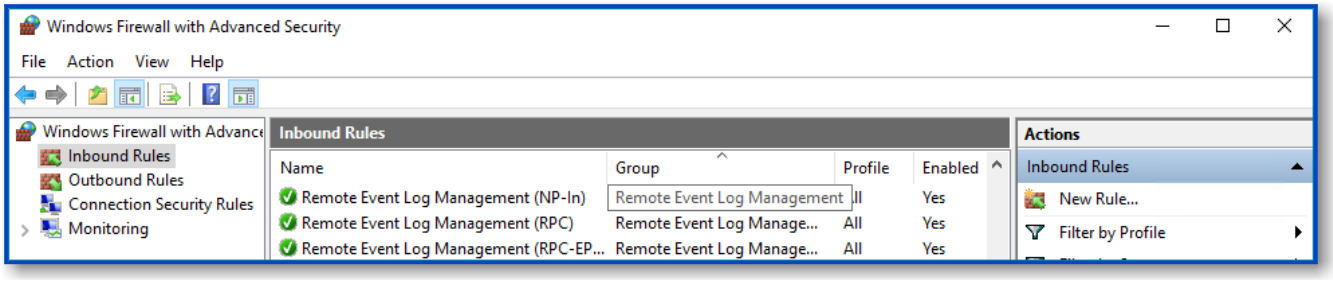
Configure Windows Firewall Inbound Connection Rules

You can also 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.

Step 1 – On each audited server, navigate to **Start** > **Control Panel** and select **Windows Firewall**.

Step 2 – In the Help Protect your computer with Windows Firewall page, click **Advanced settings** on the left.

Step 3 – In the Windows Firewall with Advanced Security dialog, select **Inbound Rules** on the left.



Step 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)
- Remote Service Management (NP-In)
- Remote Service Management (RPC)
- Remote Service Management (RPC)
- Performance Logs and Alerts (DCOM-In)
- Performance Logs and Alerts (Tcp-In)

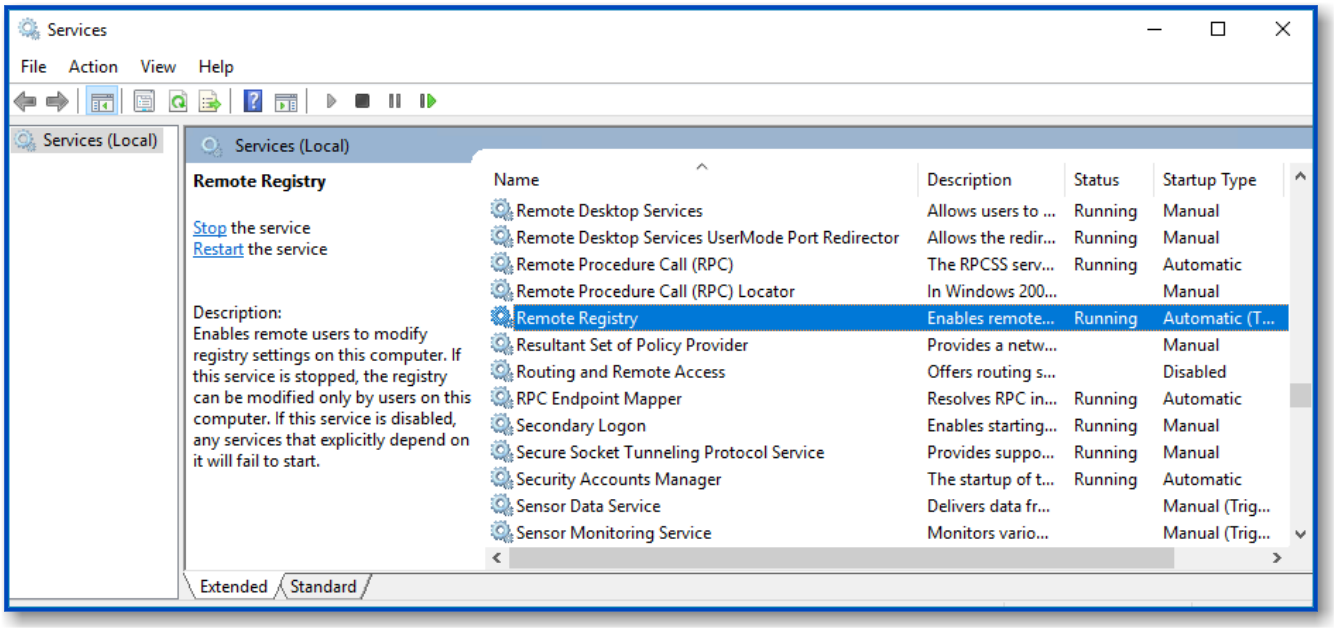
If you plan to audit Windows Server 2019 or Windows 10 Update 1803 without network compression service, make sure the following inbound connection rules are enabled:

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

Enable Remote Registry and Windows Management Instrumentation Services

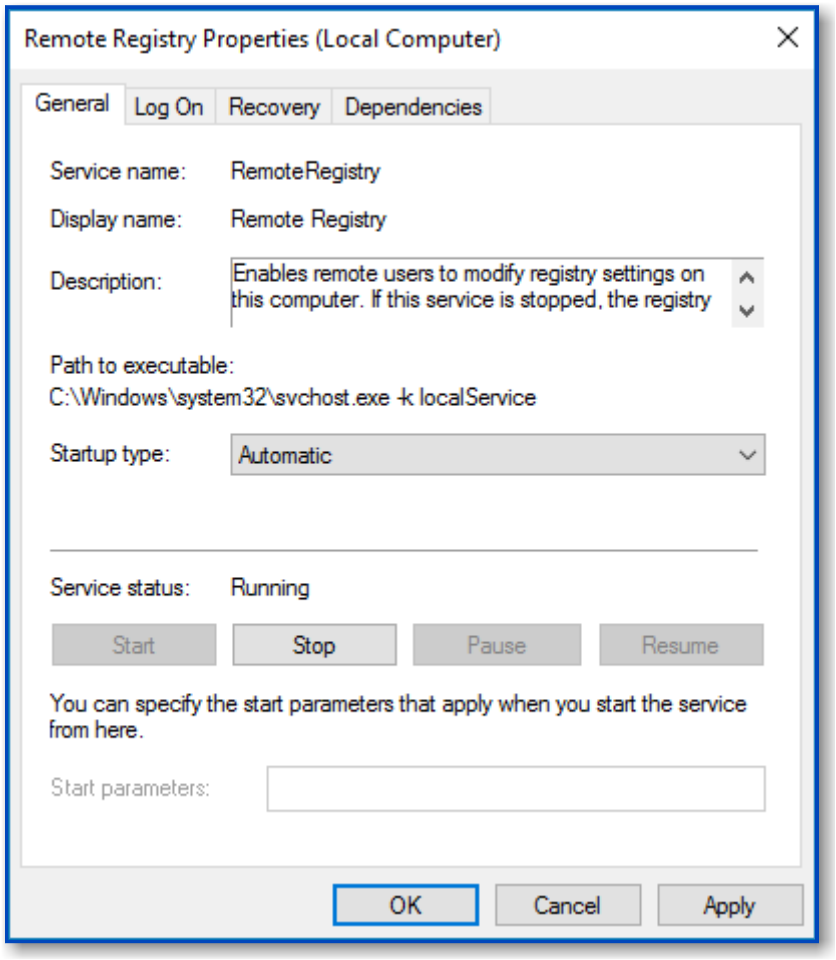
Follow the steps to enable the Remote Registry service.

Step 1 – Navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Services**.



Step 2 – In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.

Step 3 – In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



Step 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.

NOTE: The Remote Registry should be enabled on the target server.

5. Locate the Windows Management Instrumentation service and repeat these steps.

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` and `HKEY_LOCAL_MACHINE\SYSTEM` keys:

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

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

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

Configuring Windows registry audit settings on pre-Windows Server 2012 versions

Step 1 – On your target server, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.

Step 2 – In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.

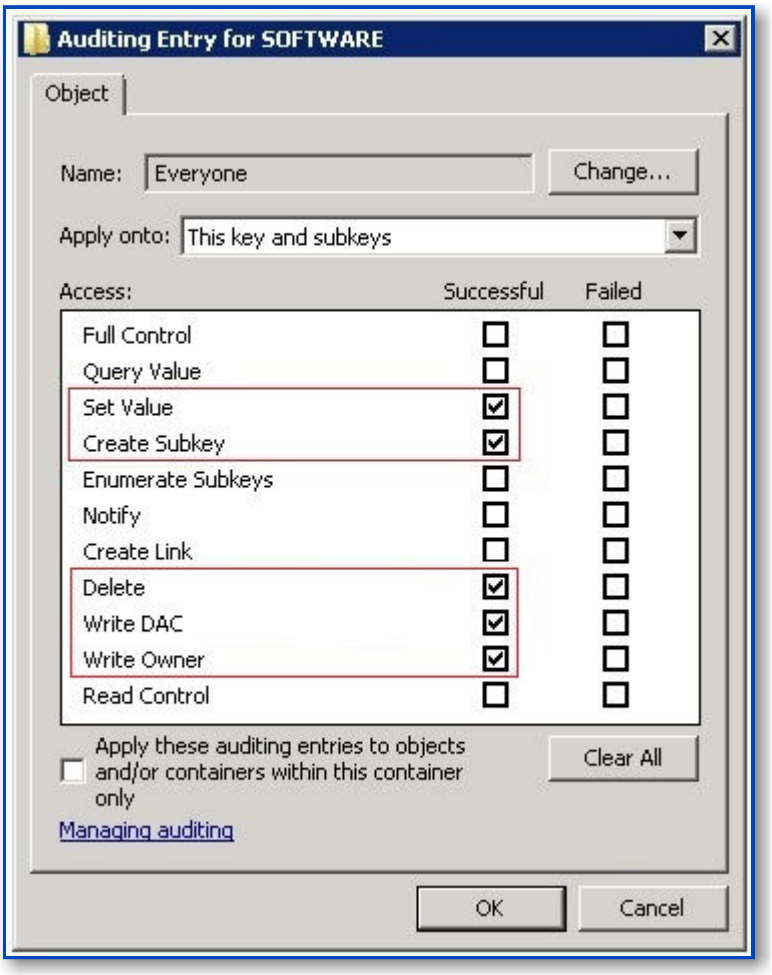
Step 3 – In the **Permissions for SOFTWARE** dialog, click **Advanced**.

Step 4 – In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.

Step 5 – Select the **Everyone** group.

Step 6 – In the **Auditing Entry for SOFTWARE** dialog, select *"Successful"* for the following access types:

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



Repeat the same steps for the HKEY_LOCAL_MACHINE\sYsTEM key.

Configuring Windows registry audit settings on Windows Server 2012 and above

Step 1 – On your target server, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.

Step 2 – In the registry tree, expand the **HKEY_LOCAL_MACHINE** key, right-click **SOFTWARE** and select **Permissions** from the pop-up menu.

Step 3 – In the **Permissions for SOFTWARE** dialog, click **Advanced**.

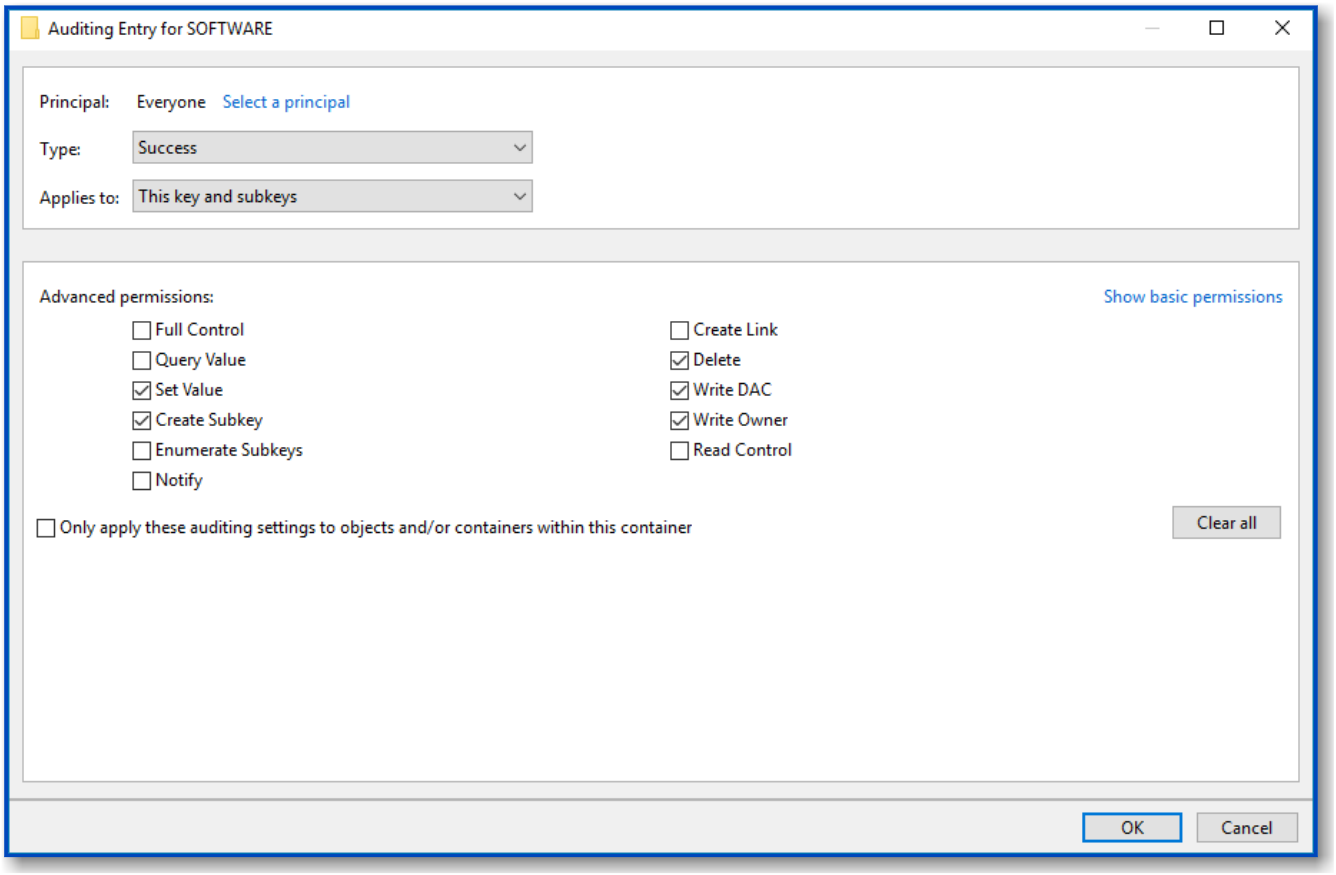
Step 4 – In the **Advanced Security Settings for SOFTWARE** dialog, select the **Auditing** tab and click **Add**.

Step 5 – Click **Select a principal link** and specify the **Everyone** group in the **Enter the object name to select** field.

Step 6 – Set **Type** to *"Success"* and **Applies to** to *"This key and subkeys*.

Step 7 – Click **Show advanced permissions** and select the following access types:

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



Repeat the same steps for the `HKEY_LOCAL_MACHINE\SYSTEM` key.

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

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 the Configure Advanced Audit Policies topic for more information.

Manual Configuration

While there are several methods to configure local audit policies, this topic 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.

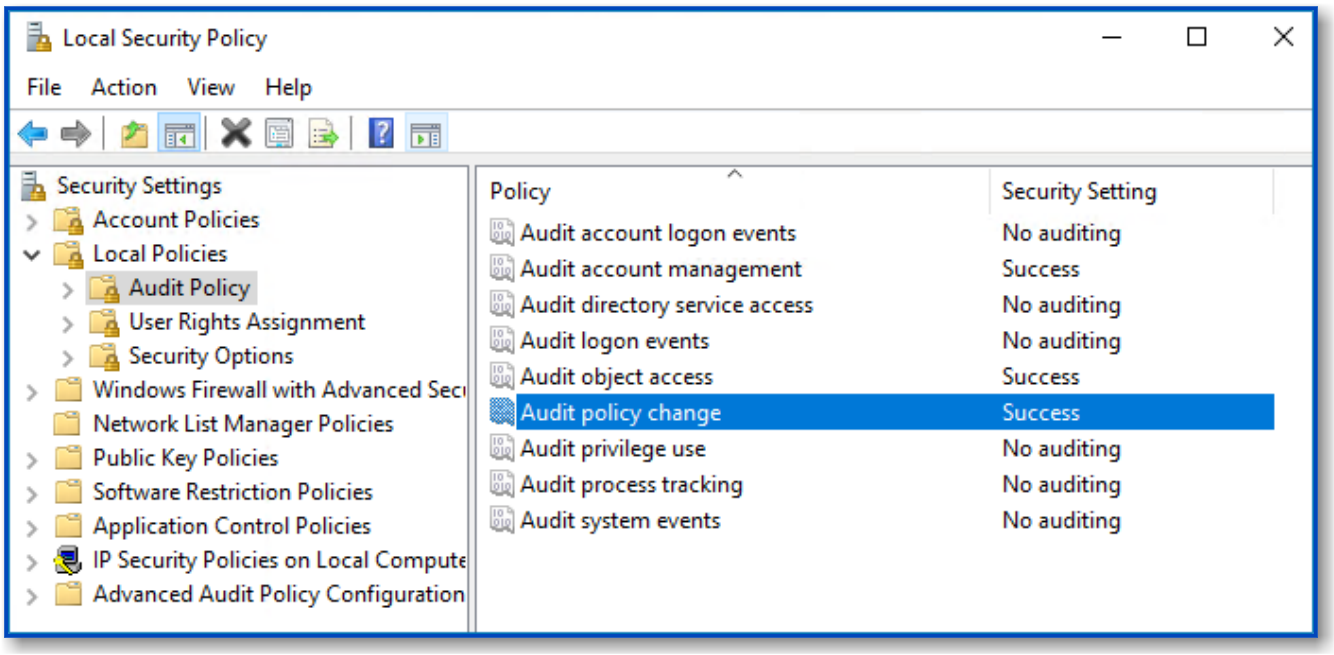
Follow the steps to configure local audit policies.

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

Step 2 – Navigate to **Security Settings > Local Policies >** Audit Policy.

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

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



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

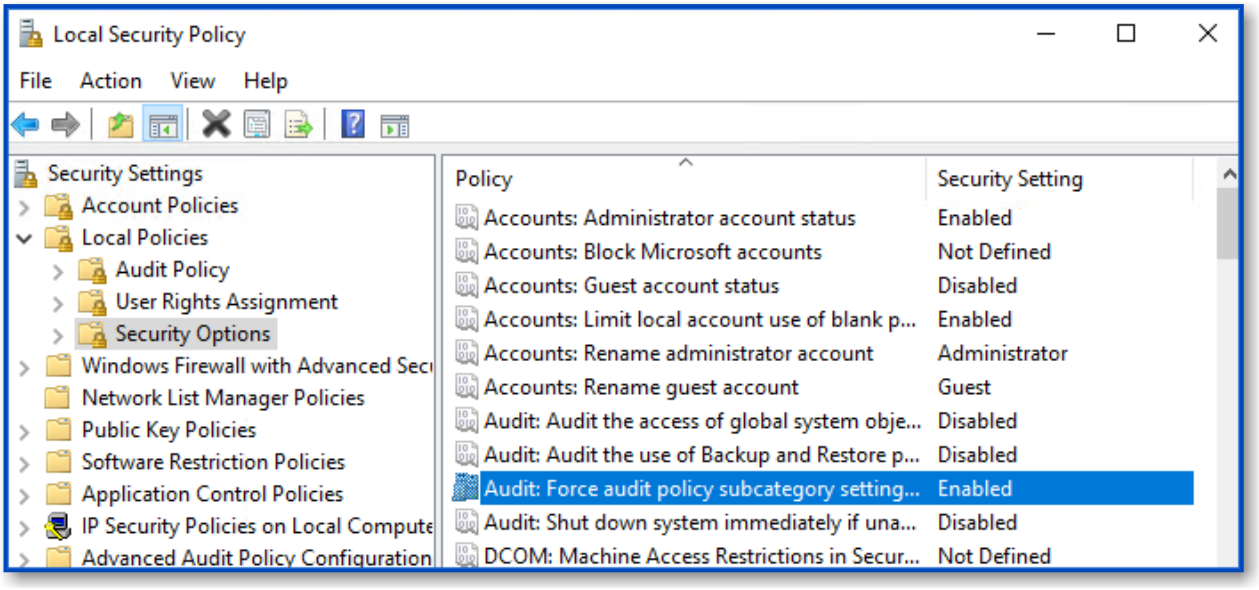
To configure security options

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 and higher) or** Administrative Tools **(Windows 2012)** → 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.

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`

Audit subcategory	Command
File Share	`auditpol /set /subcategory:"File Share" /success:enable /failure:disable`
Audit Policy Change	`auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:disable`

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"`.

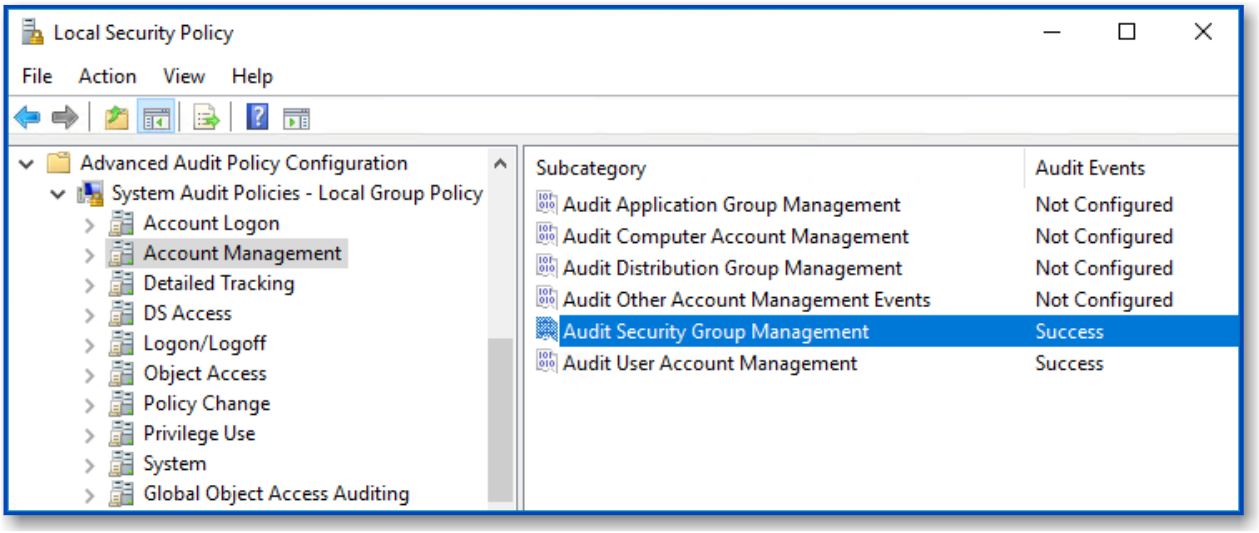
To configure advanced audit policies on Windows Server 2008 R2 / Windows 7 and above

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 and higher) or** Administrative Tools **(Windows 2012)** → 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 Subnode	Policy Name	Audit Events
Policy Change	• Audit Audit Policy Change	*"Success"*



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
- Setup
- System
- Applications and Services logs >Microsoft>Windows>TaskScheduler>Operational
- Applications and Services logs>Microsoft>Windows>DNS-Server>Audit (only for DCs running Windows Server 2012 R2 and above)

- Applications and Services logs > AD FS >Admin log (for AD FS servers)

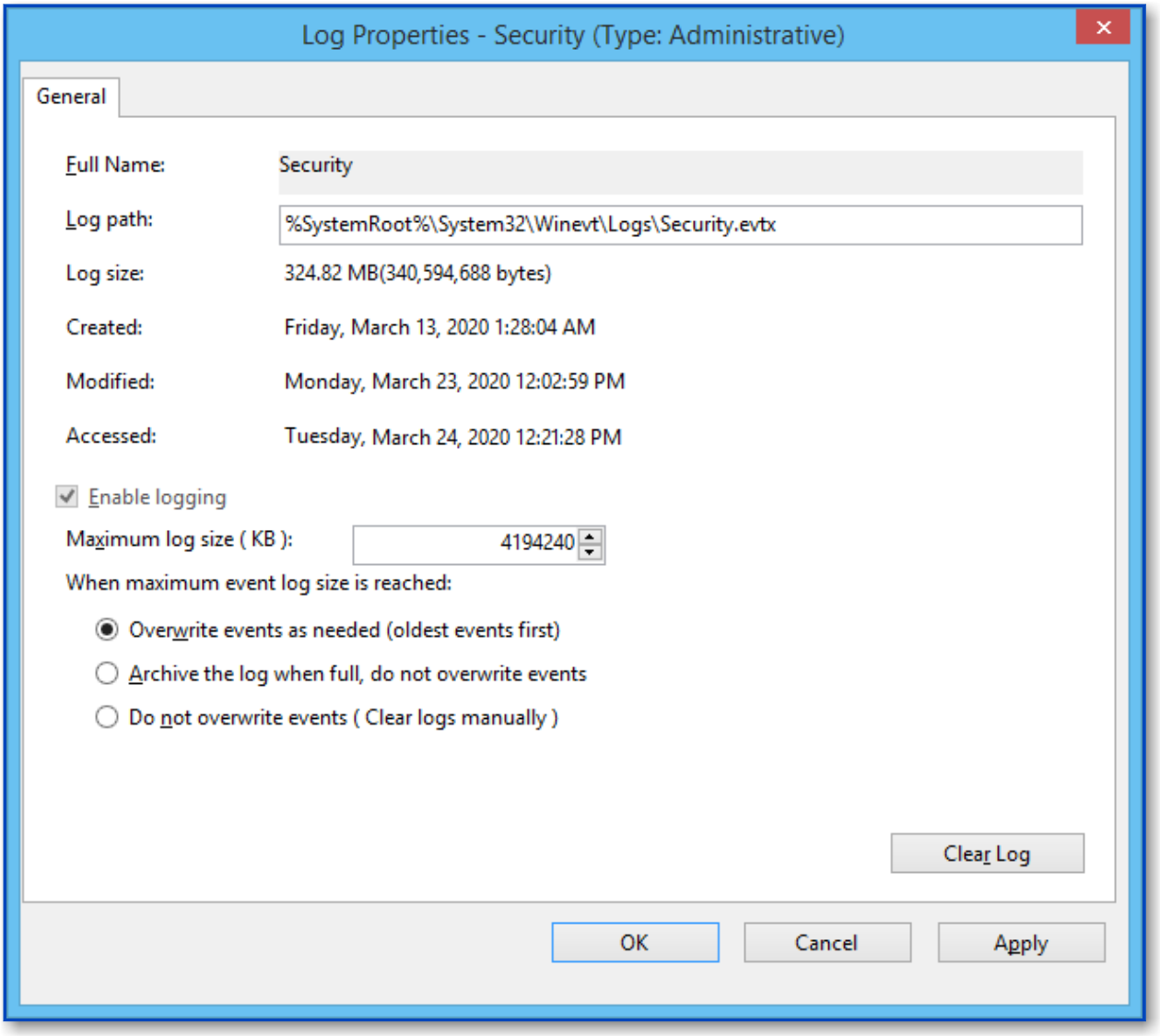
To read about event log settings recommended by Microsoft, refer to this article.

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

Manually

To configure the event log size and retention method

1. On a target server, navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** → **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 you need.

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)**.

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**

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

     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.
   - **Applications and Services Logs** → **AD FS** →**Admin**

     Applies to AD FS servers.

Using Group Policy

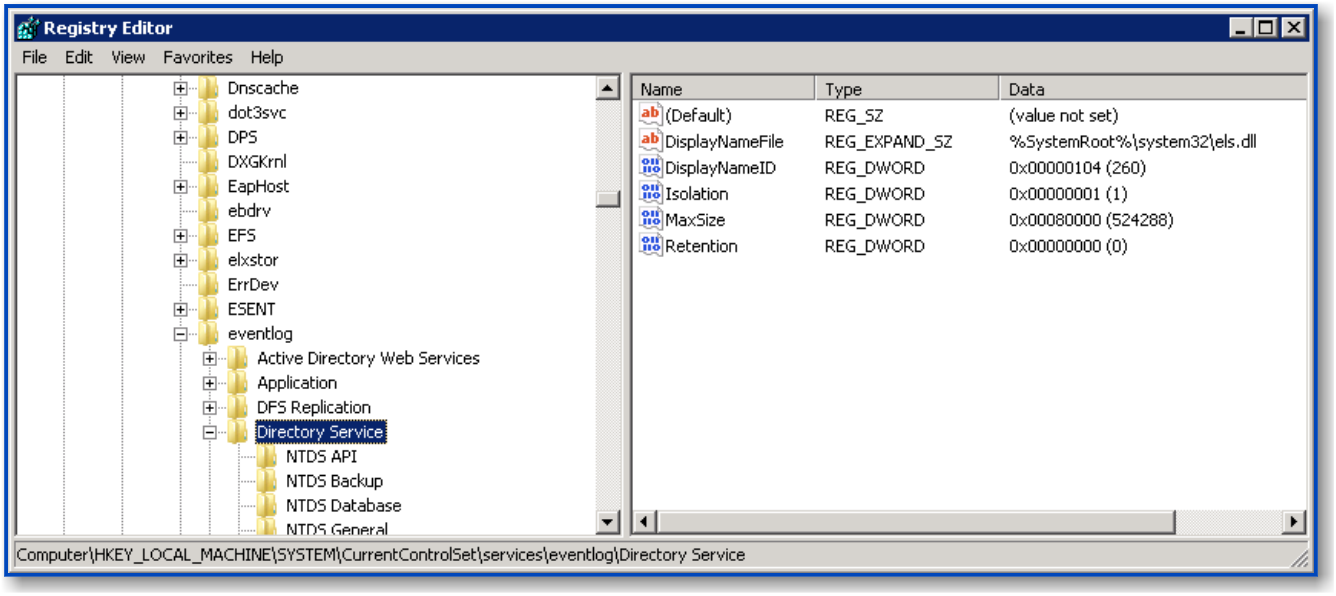
Personnel with administrative rights can use Group Policy Objects to apply configuration settings to multiple servers in bulk.

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

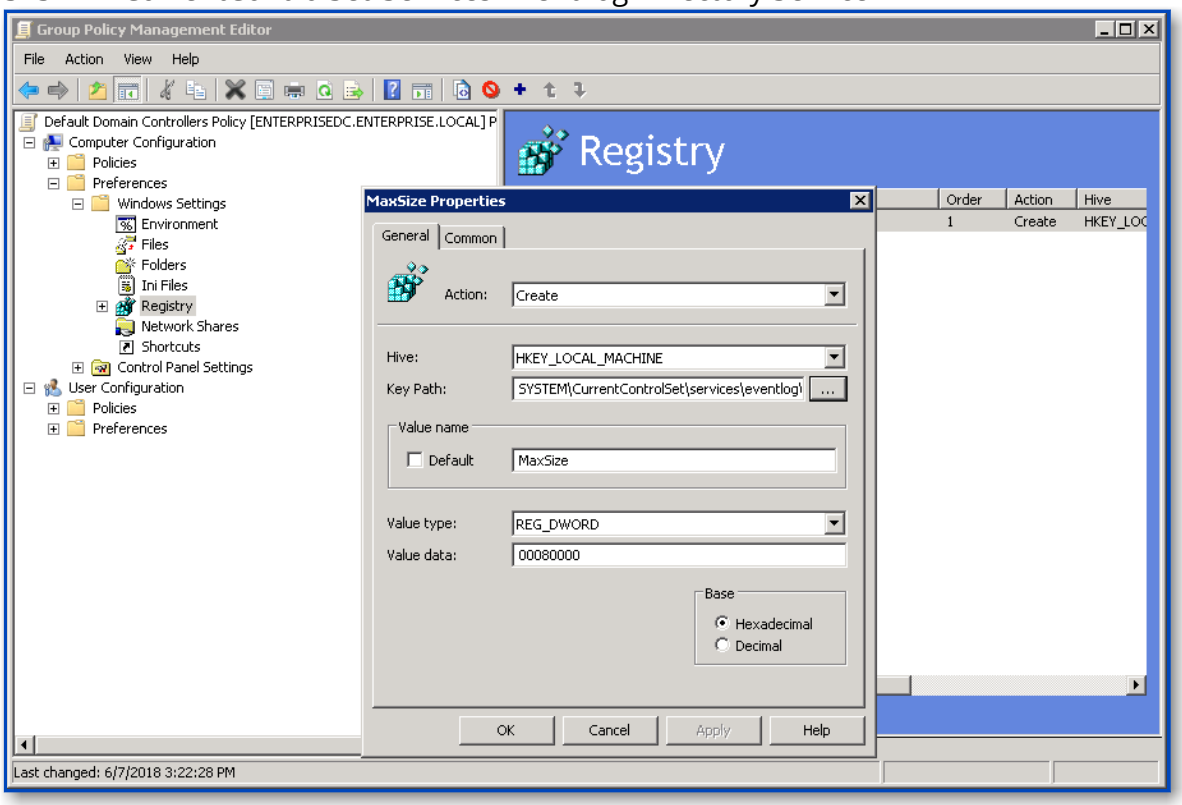
1. Open the registry editor and go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\<log_name>. For example: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Directory Service
2. Set the MaxSize to the required decimal value (in bytes).



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.

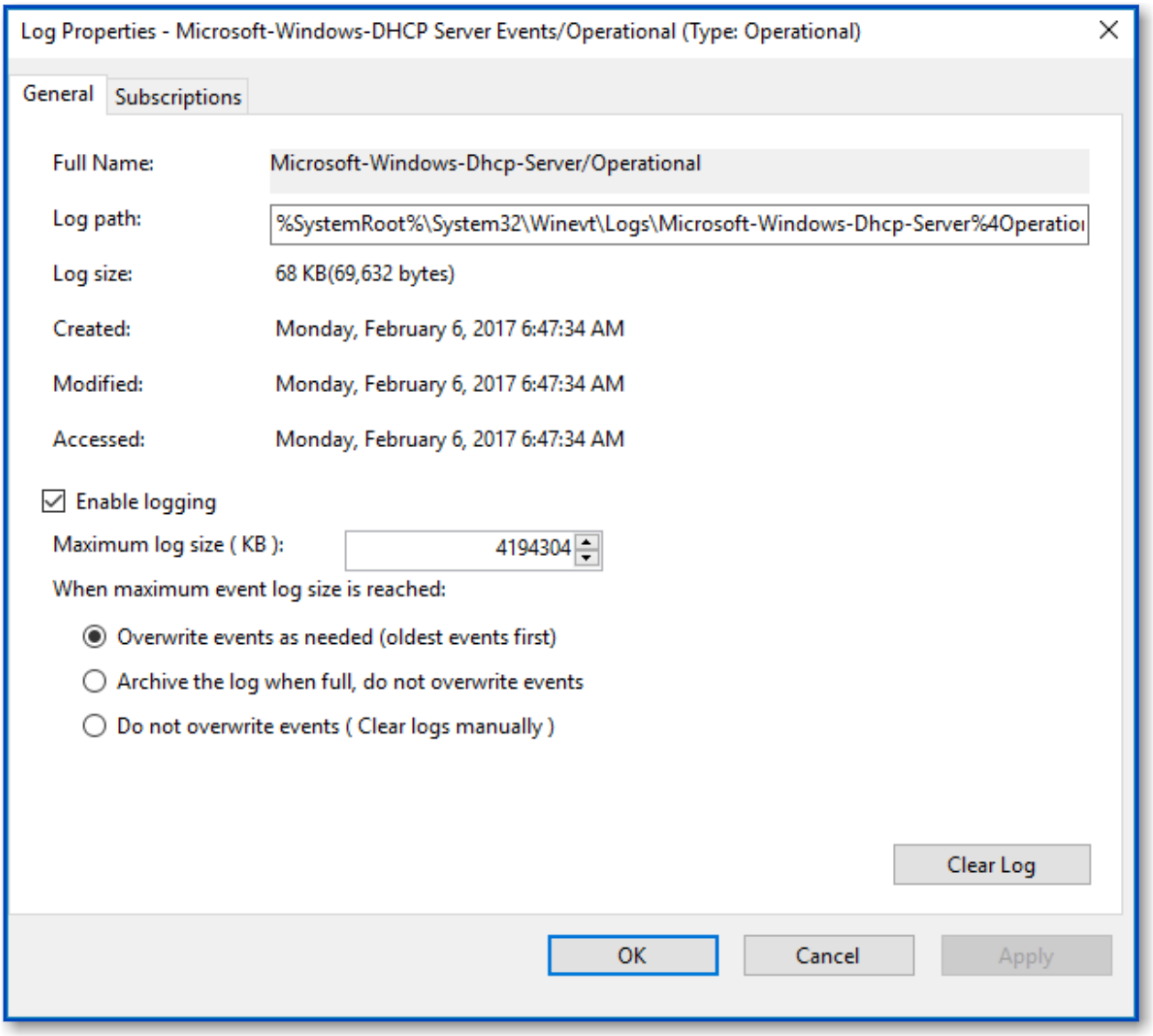
Adjust DHCP Server Operational Log Settings

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.

Configure Removable Storage Media for Monitoring

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

Review the following:

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. To review Event Trace Session objects' configurationhow to modify the root directory.

   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

   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. To review Event Trace Session objects' configurationhow to modify the root directory.

   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*

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

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

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

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

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

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

Configure Enable Persistent Time Stamp Policy

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

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"*

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

Internet Information Services (IIS)

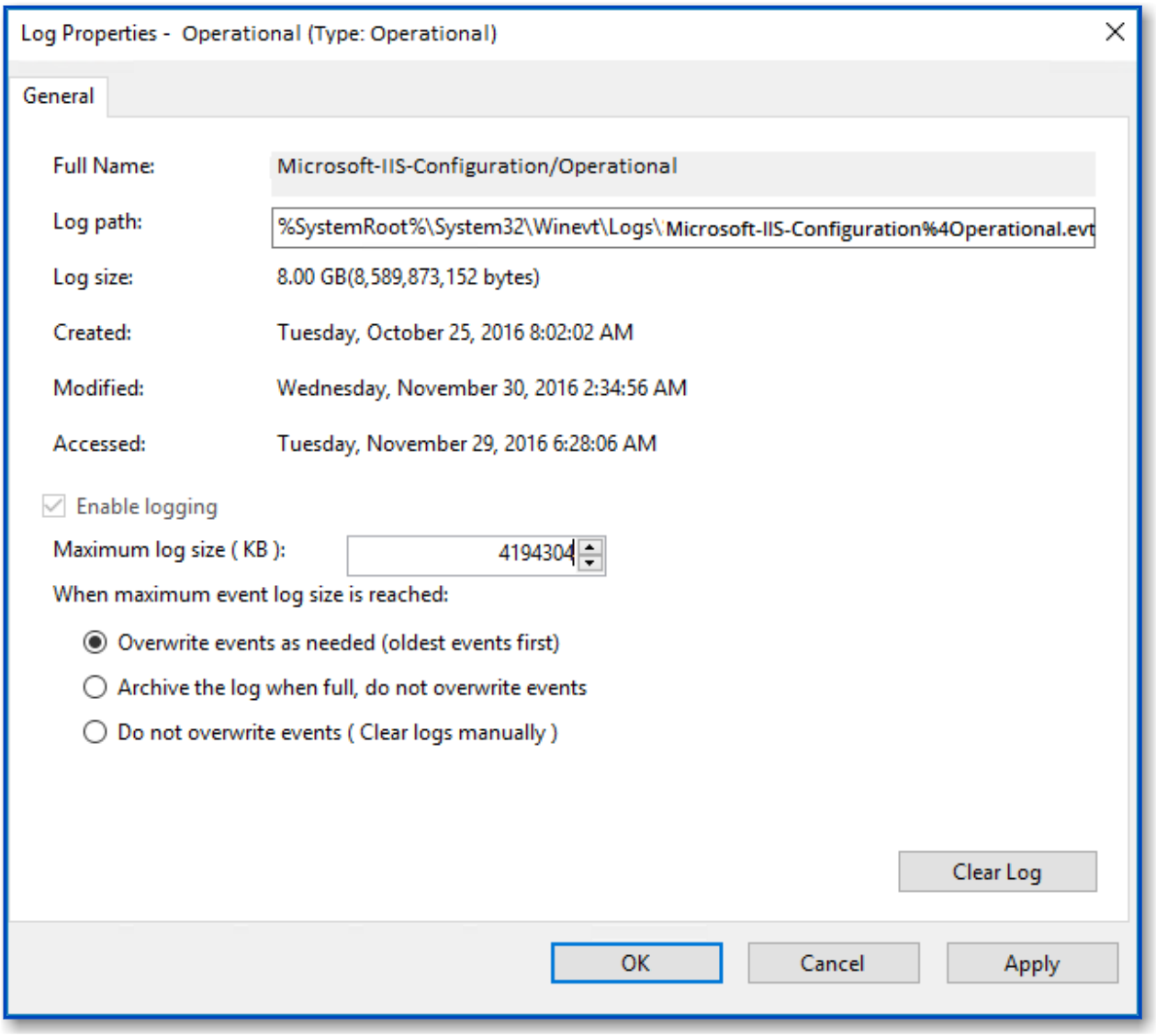
To be able to process Internet Information Services (IIS) events, you must enable the Remote Registry service on the target computers. Windows Server

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 and higher) or** Administrative Tools **(Windows 2012)** → 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)**.

Windows Server Registry Keys

Review the basic registry keys that you may need to configure for monitoring Windows Server with Netwrix Auditor. Navigate to Start → Run and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Windows Server Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the CleanAutoBackupLogs key.

Event Log

Review the basic registry keys that you may need to configure for monitoring event logs with Netwrix Auditor. Navigate to Start → Run and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager\<monitoring plan name>\Database Settings	

Registry key (REG_DWORD type)	Description / Value
ConnectionTimeout	Defines SQL database connection timeout (in seconds).
BatchTimeOut	Defines batch writing timeout (in seconds).
DeadLockErrorCount	Defines the number of write attempts to a SQL database.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the CleanAutoBackupLogs key.
WriteAgentsToApplicationLog	Defines whether to write the events produced by the Netwrix Auditor Event Log Compression Service to the Application Log of a monitored machine: • 0—Disabled • 1—Enabled

Registry key (REG_DWORD type)	Description / Value
WriteToApplicationLog	Defines whether to write events produced by Netwrix Auditor to the Application Log of the machine where the product is installed: • 0—No • 1—Yes

Permissions 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 (or in the monitored item settings).

The account used for data collection must meet the following requirements on the target servers:

- The "Manage auditing and security log" policy must be defined for this account. See the Permissions for Active Directory Auditing topic for additional information.
- This account must be a member of the local Administrators group.

Assign Permission To Read the Registry Key

NOTE: This permission is required 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, it is recommended to assign permissions through Group Policy.

To assign permissions manually, use the Registry Editor snap-in or the Group Policy Management console.

Assign Permission via the Registry Editor Snap-in

Follow the steps to assign permission via the Registry Editor snap-in:

Step 1 – On your target server, open Registry Editor: navigate to **Start > Run** and type *"regedit"*.

Step 2 – In the left pane, navigate to *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\EventLog\Security*.

Step 3 – Right-click the **Security** node and select **Permissions** from the pop-up menu.

Step 4 – Click **Add** and enter the name of the user that you want to grant permissions to.

Step 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.

Assign Permission using the Group Policy Management Console

Follow the steps to assign permission using the Group Policy Management console;

Step 1 – Open the Group Policy Management console on any domain controller in the target domain: navigate to Start > Windows Administrative Tools (Windows Server 2016/2019) or Administrative Tools (Windows 2012 R2 and below) > Group Policy Management.

Step 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.

Step 3 – In the Group Policy Management Editor dialog, expand the Computer Configuration node on the left and navigate to Policies > Windows Settings > Security Settings > Registry.

Step 4 – Right-click in the pane and select Add Key.

Step 5 – Navigate to `HKEY_LOCAL_MACHINE\SECURITY\Policy\PolAdtEv` and click OK.

Step 6 – Click Add and enter the name of the user that you want to grant permissions to and press Enter.

Step 7 – Check Allow next to the *"Read"* permission and click OK.

In the pop-up window, select Propagate inheritable permissions to all subkeys and click OK.

Repeat the steps 4-7 for keys below:

- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlSet\Control\SecurePipeServers\winreg`;
- `HKEY_LOCAL_MACHINE\sYsTEM\CurrentControlSet\services\EventLog\Security`.

Step 8 – Close Group Policy Management console.

Step 9 – Open command prompt and input the `gpupdate /force` command and press Enter. The group policy will be updated.

Step 10 – Type `repadmin /syncall` command and press Enter for replicate GPO changes to other domain controllers.

Step 11 – Ensure that new GPO settings were applied to the domain controllers.

Installation

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

- Install Netwrix Auditor
- Installing Core Services

It also includes advanced scenarios such as:

- Install Client via Group Policy
- Install in Silent Mode

Install Netwrix Auditor

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

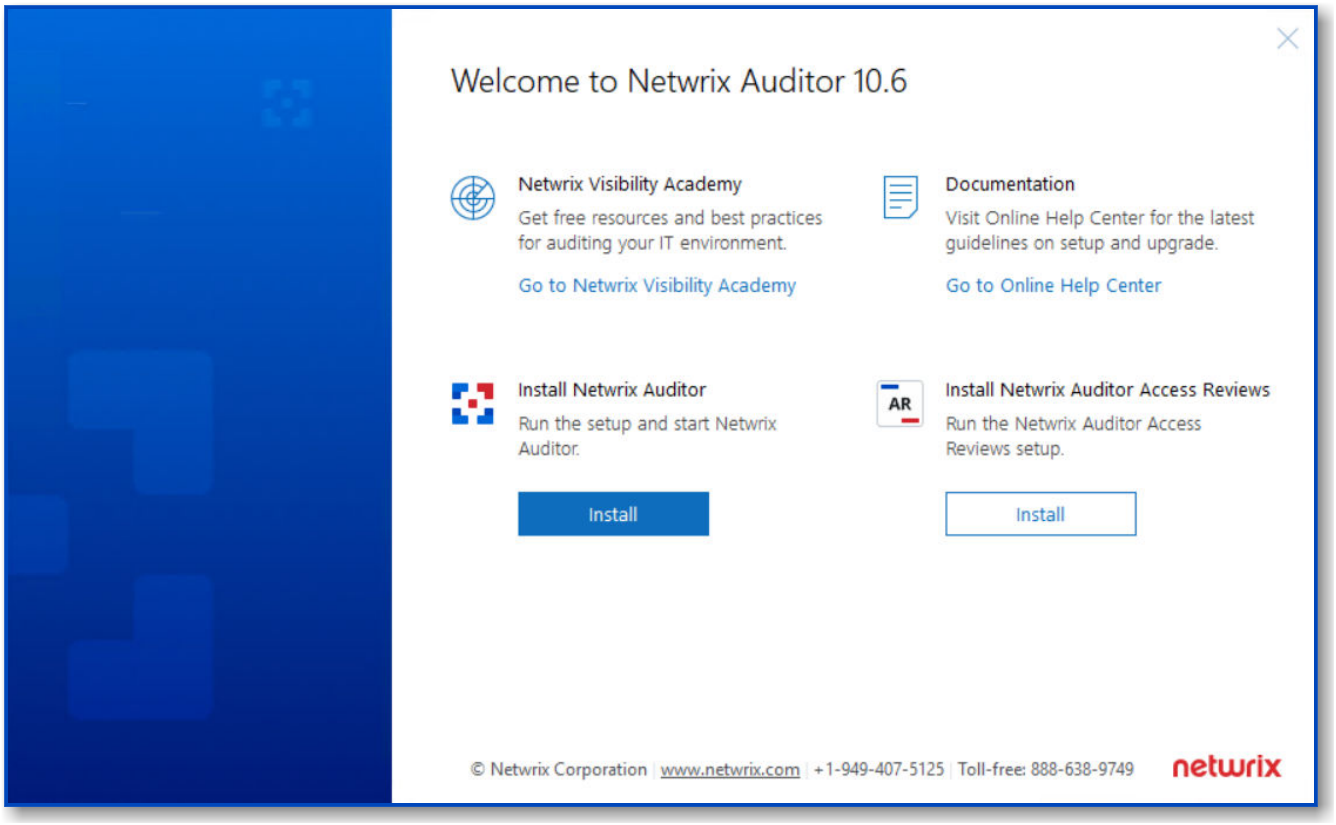
CAUTION: To keep your systems safe, NETWRIX AUDITOR should not be exposed to inbound access from the internet.

Follow these steps to install Netwrix Auditor

Step 1 – Download Netwrix Auditor 10.7 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. Also, you must be a member of the local Administrators group to run the Netwrix Auditor installation.

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



Step 3 – Follow the instructions of the setup wizard. When prompted, accept the license agreement.

Step 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 Auditor Server and the Auditor Client will be installed.
- Client installation—Select if you want to install a UI client to provide access to configuration and audit data.

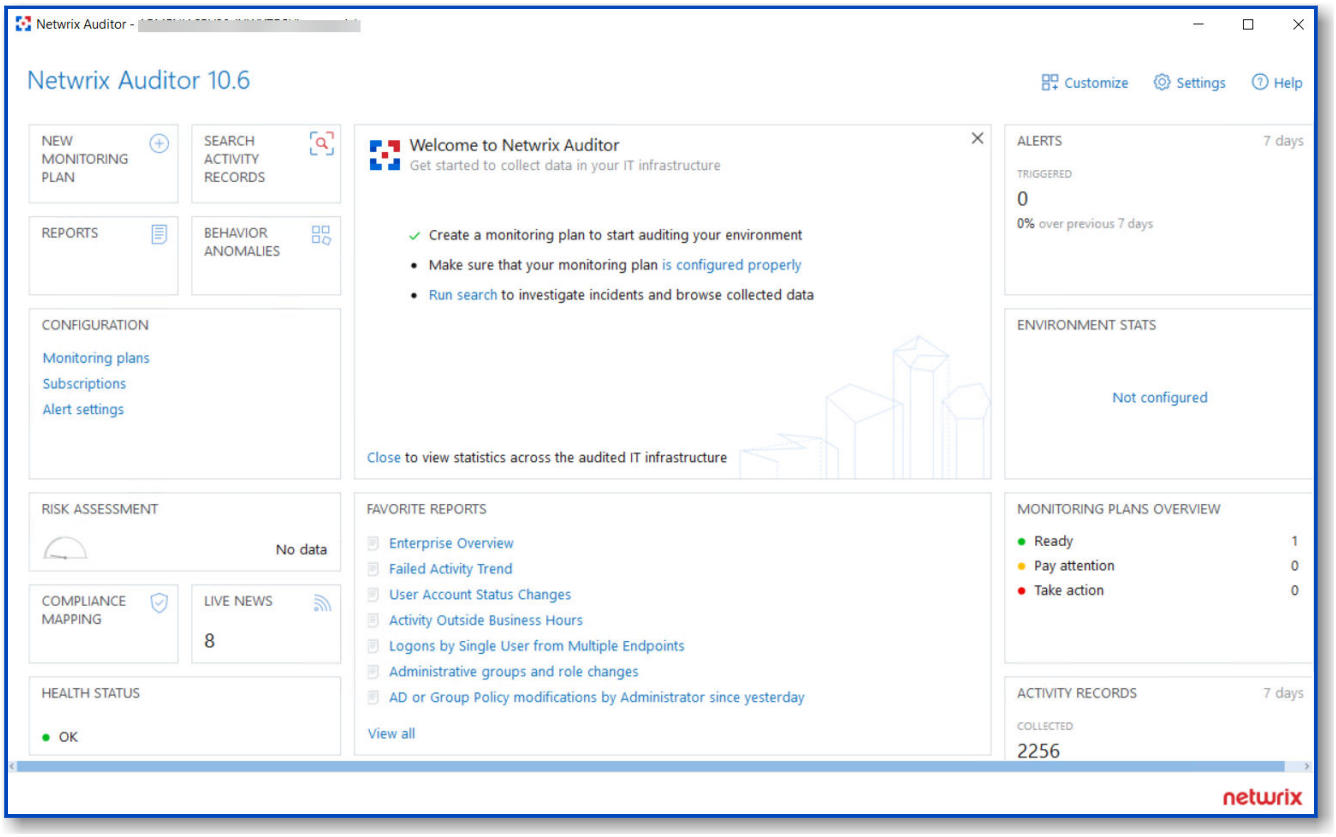
Step 5 – On the Destination Folder step, specify the installation folder.

Step 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.

You can always opt-out of the Netwrix Customer Experience Program later. See the About Netwrix Auditor topic for additional information.

Step 7 – Click Install.

After a successful installation, Auditor shortcut will be added to the **Start** menu and screen and the product will start. See the First Launch topic for additional information on the product navigation.



Netwrix looks beyond the traditional on-premises installation and provides Auditor for cloud and virtual environments. For example, you can deploy 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.

Installing Core Services

To audit SharePoint farms and user activity, Netwrix Auditor provides Core Services that must be installed in the audited environment to collect audit data. Both Core Services can be installed either automatically when setting up auditing in Netwrix Auditor, or manually.

Refer to the following sections below for manual installation instructions:

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

Install 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.

If installing via Group Policy, make sure to deploy Netwrix Auditor client and Netwrix Auditor server on different machines. If both components are installed on the same machine, you may experience issues with future upgrades.

To run the Netwrix Auditor installation, you must be a member of the local Administrators group.

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.

Create and Distribute Installation Package

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

   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.

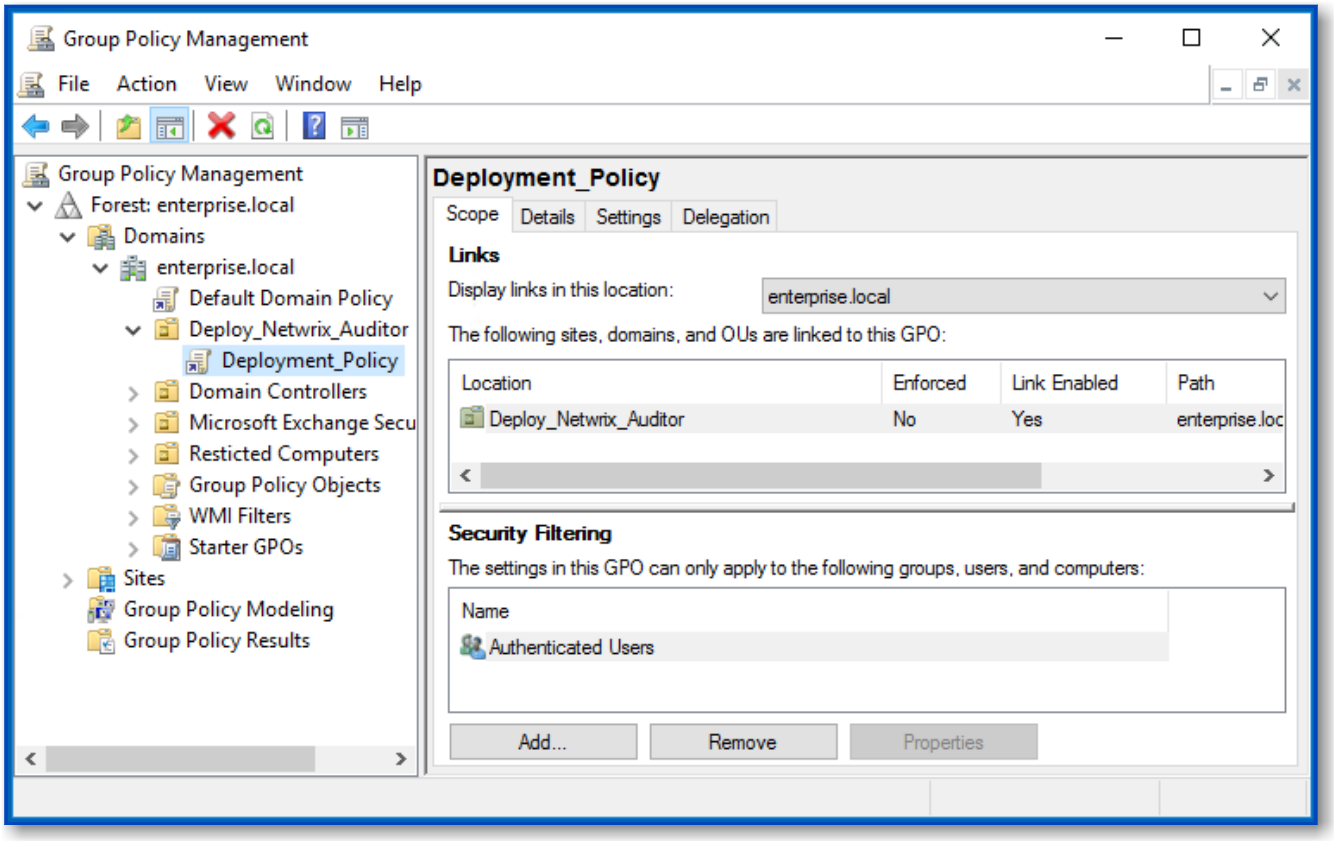
Create a Group Policy to Deploy Netwrix Auditor

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.

Follow the steps to create a Group Policy

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

Step 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**.



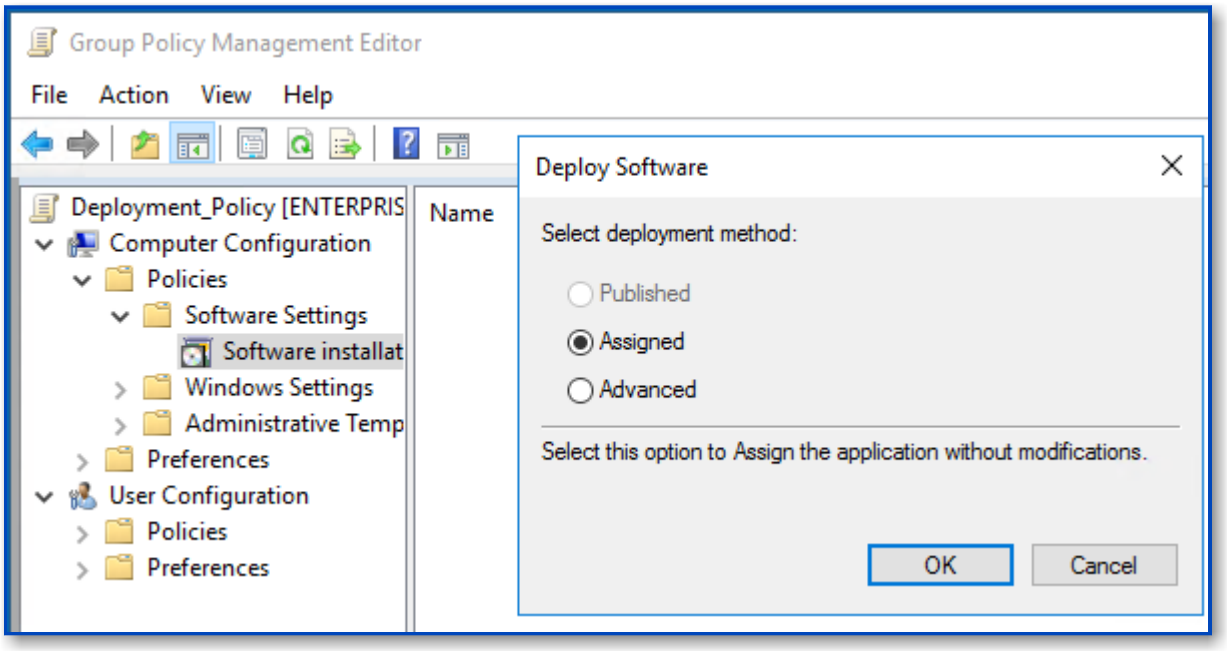
Step 3 – Right-click the newly created GPO and select **Edit** from the pop-up menu.

Step 4 – In the Group Policy Management Editor dialog, expand the **Computer Configuration** node on the left and navigate to **Policies → Software Settings → Software installation.**

Step 5 – In the right page, right-click and select New → Package.

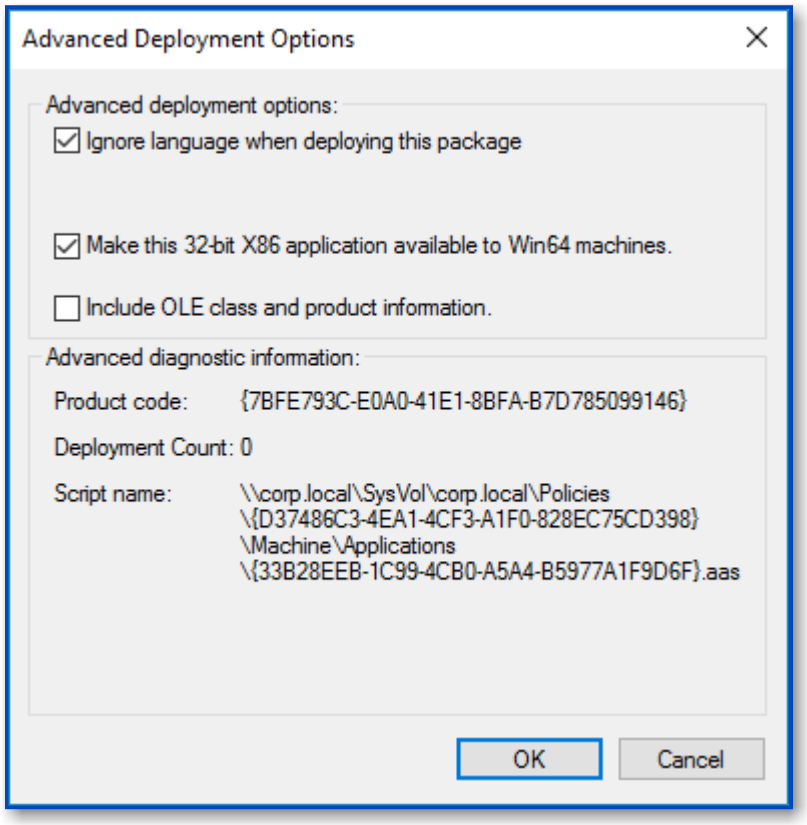
Step 6 – In the dialog that opens, locate Netwrix_Auditor_client.msi and click Open.

Step 7 – In the Deploy Software dialog, select Advanced.



Step 8 – In the Netwrix Auditor Properties dialog, select the Deployment tab and click Advanced.

Step 9 – In the Advanced Deployment Options dialog, select the Ignore language when deploying this package checkbox.



Step 10 – Close the Netwrix Auditor Properties dialog.

Step 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.

Install in Silent Mode

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

Follow the steps to install Auditor in a silent mode.

Step 1 – Download the product installation package.

Step 2 – Open the command prompt: navigate to Start > Run and type "*cmd*".

Step 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.

Step 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

First Launch

To start using Netwrix Auditor

1. Navigate to Start → Netwrix Auditor.
2. Log into the product.

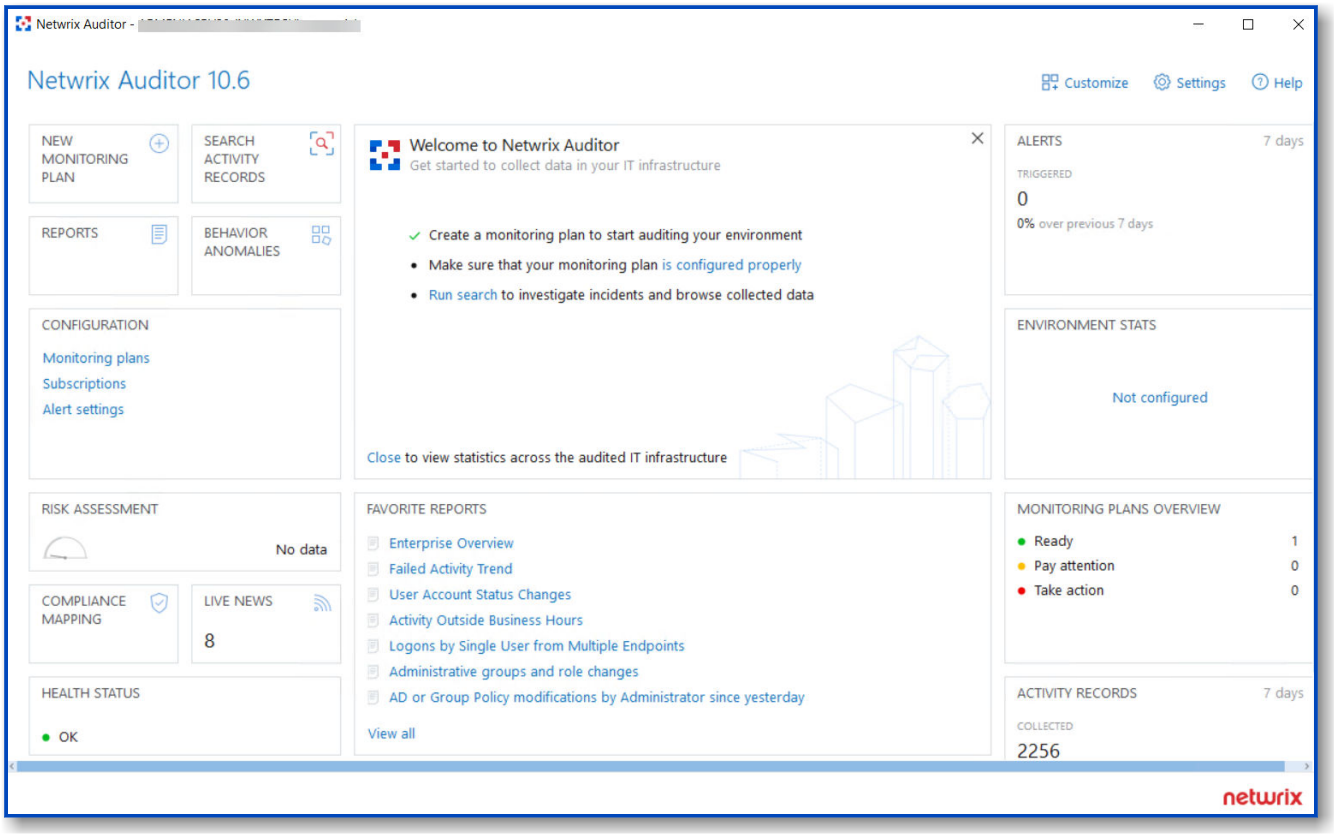
   This step is required if Netwrix Auditor is installed remotely (not on computer that hosts Netwrix Auditor Server).

   You can configure a single Netwrix Auditor client to work with several Netwrix Auditor Servers. To switch to another server, reopen the Netwrix Auditor client and provide another host name (e.g., *rootdc2*, *WKSWin12r2.enterprise.local*).

   For your convenience, the Host field is prepopulated with your computer name. By default, you can log in with your Windows credentials by simply clicking Connect. Select Use specified credentials if you want to log in as another user.

   Make sure you have sufficient permissions to access the product. If you cannot log into Netwrix Auditor with your Windows credentials, contact your Netwrix Auditor administrator.

After logging into Netwrix Auditor, you will see the following window:



Take a closer look at the Home page. It contains everything you need to enable complete visibility in your environment.

See next:

- Navigation

Automate Sign-in to the Client

When you launch Netwrix Auditor client installed on the same machine as Netwrix Auditor server, connection to that server is established automatically using your current account. However, if you want to connect to Netwrix Auditor Server installed on another computer, you will be prompted to specify connection parameters: server name and user credentials.

To automate the sign-in process, users who need to frequently connect to different Netwrix Auditor Servers (for example, Managed Service Providers) may configure the product shortcut: when you click the shortcut, Netwrix Auditor client will display the sign-in window with pre-populated server name and user name. You will only have to enter password.

To create a shortcut for automated sign-in:

1. Navigate to the Netwrix Auditor client installation directory and locate the AuditIntelligence.exe file (default location is *C:\Program Files (x86)\Netwrix Auditor\Audit Intelligence\AuditIntelligence.exe).*
2. Create a shortcut for this executable file.
3. Right-click the created shortcut and select Properties.
4. In the Target field, a path to the executable file will be shown. Add the following parameters to the end:

   ```
   /s:server_name /u:user_name /specify_creds
   ```

   where:

   - `server_name`—your Netwrix Auditor Server name or IP address.
   - `user_name`— Netwrix Auditor user who will log in.

   Example:

   ```
   "C:\Program Files (x86)\Netwrix Auditor\Audit Intelligence\Audit Intelligence.exe" /s:host.corp.local /u:corp\analyst /specify_creds
   ```

5. Click Apply.

You can create as many shortcuts with different parameters as needed.

Install for SharePoint Core Service

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

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 SharePoint 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 Permissions for SharePoint Auditing topic for more information.

Follow the steps to install Netwrix Auditor for SharePoint Core Service manually.

Step 1 – On the computer where 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.

Step 2 – Run the installation package.

Step 3 – Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

Install for 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.

Follow the steps to install Netwrix Auditor User Activity Core Service.

Step 1 – On the computer where Auditor Server resides, navigate to *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Video Recording* and copy the UACoreSvcSetup.msi file to the audited computer.

Step 2 – Run the installation package.

Step 3 – Follow the instructions of the setup wizard. When prompted, accept the license agreement and specify the installation folder.

Step 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.

Install User Activity Core Service with the Command Prompt

Follow the steps to perform a silent installation of the User Activity Core Service with the command prompt.

Step 1 – On the computer where Auditor Server resides,, navigate to *%ProgramFiles% (x86)\Netwrix Auditor\User Activity Video Recording* and copy the **UACoreSvcSetup.msi** file to the audited computer or to a file share the target server(s) can access.

Step 2 – Run the following commands on target servers:

- `CD %PathToInstaller%`
- `msiexec.exe /i "UACoreSvcSetup.msi" ALLUSERS=1 /qn /norestart /log output.log UAVR_SERVERNAME=%NAServer% UAVR_SERVERPORT=9004`

Step 3 – Replace *%PathToInstaller%* with the path to the folder you copied the **UACoreSvcSetup.msi** file.

Step 4 – Replace *%NAServer%* with the name of your Netwrix Auditor server.

Virtual Deployment Overview

In addition to on-premises deployment, Netwrix Auditor offers the deployment option that can speed time-to-value by getting you up and running in less than 15 minutes.

Virtual appliance—If you run a Microsoft Hyper-V or VMware vSphere, you can deploy Auditor as a virtual appliance. Virtual appliance is a VM image file with installed Netwrix Auditor. The image is also configured to use Microsoft Edge as a default web browser.

Navigate to the Netwrix website at Netwrix Auditor Virtual Appliance and start the **Virtual Appliance Download Manager**.

Review the following for additional information:

- Virtual Deployment
- Available Configurations

Virtual Deployment

This section explains how to import a virtual machine with installed Auditor to your virtual environment.

Review the following for additional information:

- Requirements to Deploy Virtual Appliance
- Import Virtual Machine from Image to VMware
- Import Virtual Machine from Image to Hyper-V

Available Configurations

The following virtual appliance configurations are available:

Guest OS	SQL Server
Generalized Windows Server 2022 **(180-day evaluation version)**	Microsoft SQL Server 2019 Express Edition, with native Reporting Services installed
Generalized Windows Server 2019 **(180-day evaluation version)**	Microsoft SQL Server 2019 Express Edition, with native Reporting Services installed

The virtual appliance also contains Access Information Center for Auditor version installed.

Considerations and Limitations

- Consider Microsoft limits for evaluation versions of Windows Server. If your deployment is offline, you have 10 days to complete online activation, otherwise your Windows evaluation license expires, and Auditor virtual appliance will shut down every hour. If the OS has Internet access, it is granted 180 days trial.

  Provide a valid license key for Windows Server, or go to Microsoft Licensing Activation Center to register your license online. Depending on the selected virtual appliance configuration, refer to one of the Microsoft articles for additional information:

    - Windows Server 2022
    - Windows Server 2019

  Also, you can register you license by phone. See the following Microsoft article: Microsoft Licensing Activation Centers worldwide telephone numbers for additional information.

- Microsoft SQL Server Express Edition is only recommended for evaluation, PoC or small deployments. For production deployment planning in bigger environments, refer to requirements and recommendations listed in the Requirements for SQL Server to Store Audit Data section.

Requirements to Deploy Virtual Appliance

This section lists supported virtualization platforms and default hardware configuration required for the virtual machine where Auditor virtual appliance will be deployed.

The requirements below are sufficient for evaluation purposes only. See the Requirements topic for additional information.

Supported Platforms

The table below lists supported virtualization platforms for the virtual appliance deployment:

Virtual Infrastructure	Supported Version
VMware vSphere	• VMware server: ESXi 7.0, 6.7, 6.5, 6.0 • VMware workstation: 11 and 12 You can also add the Virtual Appliance to the Content Library of your VMware Cloud on AWS SDDC and then deploy this Virtual Appliance to the cloud-based ESXi host.
Microsoft Hyper-V	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016

Virtual Infrastructure	Supported Version
	• Microsoft Windows Server 2012 R2

Virtual Machine Hardware Requirements

When deploying Auditor virtual appliance, a pre-configured virtual machine will be created from the template. Below is the default hardware configuration for the VM where you plan to deploy the virtual appliance:

Parameter	Value
General	
Processor	4 cores
RAM	16 GB
HDD	• Local Disk (C:) 100 GB • Data (D:) 300 GB
VMware only	
Total Video Memory	16 MB
Network adapter	vmxnet3
Other	Check and upgrade VMware Tools during power cycle.

Cloud Deployment

Try playing around with Netwrix Auditor to see how it helps you enable complete visibility with enhanced cloud deployment options:

- Amazon Marketplace—Discover Netwrix Auditor if you have an active AWS account.

Consider that this section describes evaluation steps to investigate the Netwrix Auditor functionality and it does not contain detailed instructions on how to use and configure Amazon services and instances. Refer to AWS Documentation for more information.

- Microsoft Azure Marketplace—Discover Netwrix Auditor if you have an active Microsoft account.

You can also add Netwrix Auditor Virtual Appliance to the Content Library of your VMware Cloud on AWS SDDC and then deploy this Virtual Appliance to the cloud-based ESXi host, following the steps described in this guide. In this deployment scenario, Netwrix Auditor will be able to work with other VMs running on that ESXi host.

Import Virtual Machine from Image to VMware

Perform the following steps to import a virtual machine:

Step 1 – Connect to your vSphere infrastructure using vSphere Web client, right-click the object you need (datacenter, ESXi host, VM folder or resource pool) and select Deploy OVF Template.

Step 2 – If you are running VMware 6.0, connect to vSphere using the on-premises vSphere client and select File → Deploy OVF Template.

Follow the instructions in the table below:

Step	Description
Source	Browse for the folder that contains the Auditor virtual appliance template.
OVF Template Details	Review information on this template.
Name and Location	Select a name for the new virtual machine (optional; default name is *"Netwrix Auditor"*). The name must be unique within the Inventory folder; it may contain up to 80 characters including spaces.

Step	Description
Resource Pool	Select a resource pool to deploy the virtual appliance.
Storage	Select the destination storage.
Disk Format	To optimize the disk space, it is recommended to select Thin Provision.
Network Mapping	If you have multiple networks on your ESXi Server, select the Destination network for a new virtual machine.
Ready to Complete	Review your virtual machine settings. Click Finish to complete the wizard.

Select the newly created virtual machine and click Power On.

Deploy Virtual Appliance to VMware Cloud on AWS

Perform the following steps to deploy virtual appliance:

Step 3 – Import the NetwrixAuditor.ova file to a Content Library of VMware vSphere, as described in this VMware article: Import Items to a Content Library.

Step 4 – Start the New Virtual Machine... wizard.

Step 5 – On the Select a creation type step, select Deploy from template.

Step 6 – On the Select a template step, select NetwrixAuditor from your ContentLibrary.

Step 7 – Proceed with the wizard: select name and folder, resources and storage for the VM.

Import Virtual Machine from Image to Hyper-V

Perform the following steps to import a virtual machine:

Step 1 – On your Hyper-V server, unzip the virtual appliance package to the specified location.

Step 2 – Navigate to **Start** → **All Apps** → **Hyper-V Manager**.

Step 3 – In the Hyper-V Manager, navigate to **Actions** → **Import virtual machine** and follow the instructions of the wizard. Review the table below for more information.

Step	Description
Locate Folder	Browse for the folder that contains extracted virtual appliance.
Select Virtual Machine	Select Netwrix Auditor.
Choose Import Type	Choose the import type that best suits your needs.
Choose Network Type	Select a virtual switch.
Summary	Review your virtual machine settings. Click Finish to exit the wizard.

The newly created virtual machine named Netwrix Auditor will appear in the list of virtual machines. Right-click and select Start.

Configure Virtual Appliance

Perform the following steps to configure your virtual appliance:

Step 1 – For **Windows Server**, the EULA will be displayed in the License terms page; read and accept the agreement.

Step 2 – Next, specify a password for the built-in administrator account. Then re-enter your password. Click Finish.

Step 3 – Log in to the virtual machine.

Step 4 – The Windows PowerShell opens and automatically runs the script. Press any key to read the license agreement and then press Y to accept it.

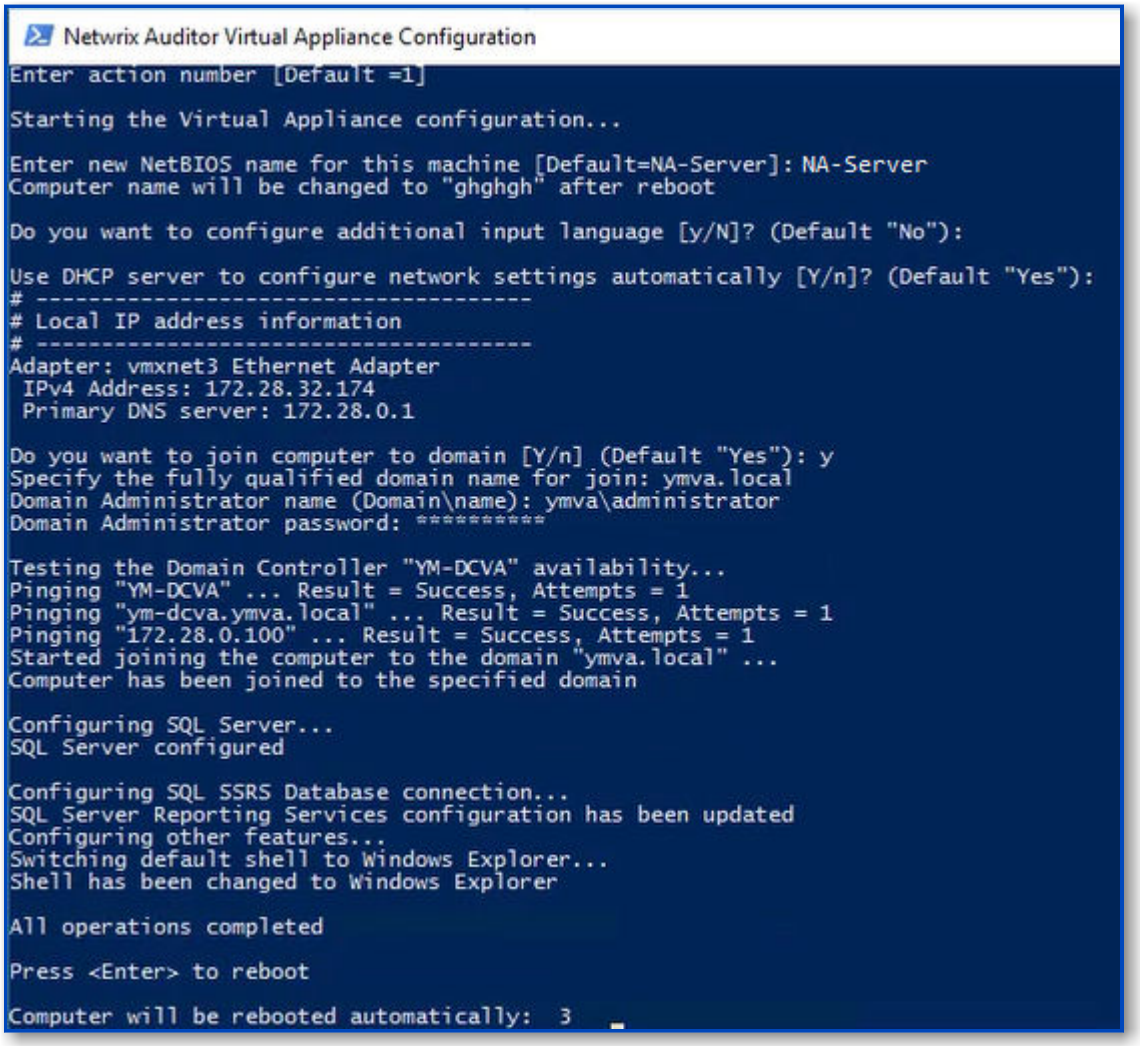
Step 5 – Then you will be prompted to configure the virtual machine. Press Enter to start.

Step	Description
Rename virtual machine	Specify a new name for the virtual machine (e.g., `NA-Server`). The computer name must be properly formatted. It may contain letters (a-z, A-Z), numbers (0-9), and hyphens (-), but no spaces and periods (.). The name may not consist entirely of digits and may not be longer than 15 characters.
Add additional input languages	Select Y if you want to specify additional input languages. Select N to proceed with English.
Configure network	• Select Y to use DHCP server to configure network settings automatically. • Select N to configure required parameters manually. In this case, you will be prompted to set up IP settings manually.
Join computer to the domain or workgroup	**To join a domain**

Step	Description
	Select Y. Specify the fully qualified domain name to join (e.g., `corp.local`). Then specify domain administrator name and password. For your convenience, the account specified will be added to the local Administrators group and set as account for collecting data from the target systems. Domain Users group will be removed from the local Users group after the machine with the appliance joins the domain. The script is starting to test your domain controller: by NETBIOS name first, then by DNS name and finally, using an IP address. If at least one of the tests is successful, the computer will be added to a domain. In case of failure, you will be prompted to do one of the following: • Re-try to joint to the selected domain. In this case, the script uses the DNS name of your domain controller. The name must be resolved. • Continue with Workgroup. See the procedure below on how to join the computer to a workgroup. • Cancel and **Return to Main Menu**. Select if you want to cancel the domain join and re-configure the machine. Press Enter and repeat menu section. You will return to step 5. **To join a workgroup** Select N. Specify the local administrator name and credentials. For your convenience, the account specified will be set as account for collecting data from the target systems. NETWRIX AUDITOR is unable to work in a workgroup. Please confirm if you want to proceed. Otherwise, you will not be able to run reviews on data collected by

Step	Description
	AUDITOR . See the Access Reviews topic for additional information about integration with ACCESS REVIEWS .
Configure SQL Server	The shell script automatically configures SQL Server instance. The sysadmin server role on SQL Server instance is granted automatically to the BUILTIN\Administrators group.

In the example below, review how the shell script configures the new VM:



Step 6 – When the script execution completes, you will be prompted to reboot the virtual machine for the changes to take effect.

Step 7 – After reboot, log in to the virtual machine using the domain administrator credentials (for appliances joined to domain) or local administrator credentials (for appliances joined to workgroup).

For the first time, Auditor Client starts automatically. Later, you can always run it from the Start menu or launch it by double-clicking the Auditor shortcut on the desktop.

Do not close the Virtual Appliance Configuration window until the product configuration completes.

What Is Next

Now you can evaluate Auditor functionality. Review the table below for more information.

To...	Run...	Get more info
• **See a list of audit settings** • **See a list of rights and permissions required for data collecting account**	—	• Supported Data Sources • Data Collecting Account
• **Create a monitoring plan** • **Review data collection status** • **Configure the Long-Term Archive and the Audit Database settings** • **Assign roles and delegate control**	Auditor Client	• Monitoring Plans • Netwrix Auditor Settings • Role-Based Access and Delegation
• **Browse data with interactive search** • **Review diagrams** • **Generate reports** • **Configure report subscriptions** • **Create alerts**	Auditor Client	• Reports • Subscriptions • Alerts

To...	Run...	Get more info
See the data collected by Auditor	Auditor Client	• Access Reviews

NOTE: If any errors occur, please contact Netwrix technical support.

Upgrade to the Latest Version

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

Seamless upgrade to Netwrix Auditor 10.7 is supported for versions 10.6 and 10.5.

If you use an earlier version of Netwrix Auditor, then you need to upgrade sequentially right to version 10.7. Review the following Netwrix knowledge base article for more information: Upgrade Increments for Netwrix Auditor.

Before Starting the Upgrade

Before you start the upgrade, it is strongly recommended taking the following preparatory steps:

Step 1 – Upgrade Netwrix Auditor Server OS to the supported version before upgrading Netwrix Auditor itself.

Step 2 – Check that the account under which you plan to run Netwrix Auditor setup has the local Administrator rights.

Step 3 – Back up Netwrix databases – these are all Audit databases, Integration API database, and others (their default names start with *Netwrix*). To do so:

1. Start Microsoft SQL Server Management Studio and connect to SQL Server instance hosting these databases.
2. In Object Explorer, right-click each Netwrix database and select **Tasks > Back Up**.
3. Wait for the process to complete.

Step 4 – Back up the Long-Term Archive folder, by default located at *C:\ProgramData\Netwrix Auditor\Data*. You can copy and archive this folder manually, or use your preferred backup routine.

Step 5 – If you can capture a snapshot of the server where Netwrix Auditor Server resides, Netwrix recommends doing so.

Step 6 – Finally, close the Netwrix Auditor console.

General Considerations and Known Issues

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 apply to upgrade from 9.96 and 10.

- 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.
- Microsoft Exchange Server 2010 is no longer supported. Please upgrade your Exchange Server to a new version.
- For Netwrix Auditor for SharePoint Online, the following data will be available within 24 hours after upgrade:
  - Current values for SharePoint Online risk metrics (Office 365)
  - Data in the Objects Shared with External or Anonymous Users state-in-time report
  - Numbers of shared objects and drill downs to reports in the SharePoint Online Site Collections External Sharing state-in-time report.
- For auditing cloud-based applications (Microsoft Entra ID, Exhange Online, SharePoint Online, and MS Teams) with Netwrix Auditor using basic authentication: before an upgrade from version 10.0 and earlier, make sure that the account under which the upgrade will be performed has sufficient rights and permissions to perform initial data collection and upgrade. Review the following for more information about required rights and permissions:
  - Permissions for Microsoft Entra ID Auditing
  - Permissions for Exchange Online Auditing
  - Permissions for SharePoint Online Auditing
  - Permissions for Teams Auditing

- For auditing cloud-based applications (Microsoft Entra ID, Exchange Online, SharePoint Online, and MS Teams) with Netwrix Auditor using modern authentication: additional configuration of the Azure AD app permissions is required. Review the following for more information about required rights and permissions:
  - Permissions for Microsoft Entra ID Auditing
  - Permissions for Exchange Online Auditing
  - Permissions for SharePoint Online Auditing
  - Permissions for Teams Auditing
- Netwrix Auditor for Oracle Database. If you use the following combination of the audit settings: Mixed Mode + Fine Grained Auditing, please check your configuration. You may need to re-configure your audit since the Oracle Database data collection mechanism was changed. See the Supported Data Sources and Verify Your Oracle Database Audit Settings topics for additional information.
- During the initial data collection, the product automatically upgrades services responsible for Windows Server and SharePoint network traffic compression. Consider the following:
  - During the Netwrix Auditor for SharePoint Core Service upgrade, your SharePoint sites will be temporarily unavailable. The duration of the upgrade depends on your SharePoint Farms size and usually it takes a few minutes. For bigger SharePoint farms, consider up to 10 minutes for a successful service upgrade and the same for the rollback in case of an upgrade failure.
  - During the Netwrix Auditor for Windows Server Compression Service upgrade you may see the following errors: *"The Compression Service has encountered an internal error: Unable to update the Compression Service on the following server: <server name>"*. Ignore these errors and wait up to one hour for the upgrade completes.
- For the User Password Changes report to function properly after the upgrade, you need to comment out or delete the "*.*PasswordChanged*" line in the omitproplist.txt file again.
- For Exchange Online, the "*Who*" field in search, reports, Activity Summary emails, etc., shows User Principal Name (UPN) instead of Display Name.

Upgrade Procedure

You can upgrade Netwrix Auditor to 10.7 by running the installation package.

Customers who are logged in to the Netwrix Customer Portal can download the latest version of their software products from the My Products page: https://www.netwrix.com/my_products.html. See the Customer Portal Access topic for information on how to register for a Customer Portal account.

Follow the steps to perform the upgrade.

Step 1 – Make sure you have completed the preparatory steps above.

Step 2 – Run the setup on the computer where the Auditor Server resides. See the Installation topic for additional information.

Step 3 – If you have a client-server deployment, then after upgrading the server run the setup on all remote machines where the Auditor Client resides.

Netwrix recommends reviewing your current port configuration after every re-installation or upgrade.

If you were auditing Windows Server 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. During the Netwrix Auditor for SharePoint Core Service upgrade, your SharePoint sites will be temporarily unavailable.

Uninstall Netwrix Auditor

This topic provides instructions to 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 the Uninstall Compression and Core Services topic for additional information.

Follow the steps to uninstall Auditor.

Step 1 – On the computer where Auditor is installed, navigate to **Start > Control Panel > Programs and Features**.

Step 2 – Select Netwrix Auditor and click **Uninstall**.

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

Uninstall Compression and Core Services

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 Auditor Compression services are stopped but not removed when the product is uninstalled. You need to delete them manually prior to uninstalling Auditor.

Delete Netwrix Auditor for Active Directory Compression Service

Follow the steps to uninstall the service.

Step 1 – Navigate to the Active Directory monitoring plan you are using. In the command prompt, execute the following command:

Step 2 – Select your Active Directory data source.

Step 3 – Click **Edit data source** on the right.

Step 4 – Uncheck the **Enable network traffic compression** checkbox.

Step 5 – Remove the network traffic compression service on the domain controller by executing the following command:

```
sc delete adcrsvc
```

Delete Netwrix Auditor for SharePoint Core Service

Follow the steps to delete the Netwrix Auditor for the SharePoint Core Service.

Step 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.

Step 2 – Navigate to **Start > Control Panel > Programs and Features**.

Step 3 – Select the Netwrix Auditor **for SharePoint Core Service** and click Uninstall.

CAUTION: Once you click UNINSTALL you cannot cancel the uninstallation. The NETWRIX AUDITOR **for SharePoint Core Service** will be uninstalled even if you click CANCEL .

Delete Netwrix Auditor for Windows Server Compression Service

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

Follow the steps to delete the Netwrix Auditor for Windows Server Compression Service.

Step 1 – On the target servers, navigate to **Start > Control Panel > Programs and Features**.

Step 2 – Select **Netwrix Auditor for Windows Server Compression Service** and click **Uninstall**.

Delete Netwrix Auditor Mailbox Access Core Service

Follow the steps to delete a Netwrix Auditor Mailbox Access Core Service.

Step 1 – In the command prompt, execute the following command:

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

Step 2 – Remove the following folder: *%SYSTEMROOT%\Netwrix Auditor\Netwrix Auditor Mailbox Access Core Service*

If any argument contains spaces, use double quotes.

Delete Netwrix Auditor User Activity Core Service

Follow the steps to remove the Core Service via Auditor client on the computer where the Auditor Server resides:

Step 1 – In Auditor client, navigate to All **monitoring plans** and specify the plan.

Step 2 – In the right pane, select the **Items** tab.

Step 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.

Step 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.

Step 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:

Step 1 – Navigate to **Start > Control Panel > Programs and Features**.

Step 2 – Select the **Netwrix Auditor User Activity Core Service** and click **Uninstall**.

Delete the Netwrix Auditor Application Deployment Service

The Netwrix Auditor **Application Deployment Service** allows collecting file events and data. The service runs on the target servers.

NOTE: Perform this procedure only if you enabled the Network traffic compression option for Windows File Servers data collection.

Follow the steps to delete the Netwrix Auditor Application Deployment Service.

Step 1 – On the target server, navigate to **Start > Registry Editor > Programs and Features**.

Step 2 – Delete the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NwxExecSvc** registry key.

Step 3 – Restart your machine and the service will be removed.

Delete Netwrix Auditor for File Servers Compression Service

The Netwrix Auditor for File Servers Compression Service runs on the Auditor Server host as designed.

NOTE: This is applicable for NetApp and Dell Data Storage sources. Delete the service irrespective of the Network traffic compression option for Dell Isilon source.

Follow the steps to delete the Netwrix Auditor for File Servers Compression Service.

Step 1 – On the computer where AuditorServer resides, navigate to **Start > Control Panel > Programs and Features**.

Step 2 – Select Netwrix Auditor**for File Servers Compression Service** and click **Uninstall**.

NOTE: This is applicable to NetApp and Dell Data Storage only if the service was installed on the Auditor Server. For a Windows File Server, the service is the Netwrix Auditor Application Deployment Service and runs on the File Server directly.

Delete the Netwrix Auditor Event Log Compression Service

Follow the steps to delete the Netwrix Auditor Event Log Compression Service.

Step 1 – Navigate to **Start > Control Panel > Programs and Features**.

Step 2 – Select **Netwrix Auditor Event Log Compression** > **Service** and click **Uninstall**.

Administration

This section contains information on how to use collected data with Netwrix Auditor:

- First launch of the product
- Navigation
- Search collected data
- Use reports
- Get alerts
- Assess risks
- View behavior anomalies
- Create subscriptions to search and reports
- Detailed information about Netwrix Auditor reports

Collect Data with Netwrix Auditor Administrator Console

This section contains the following information on how to use Netwrix Auditor:

- Integration with Netwrix Access Information Center Overview
- Role-based access and delegation
- Monitored Object Types, Actions, and Attributes
- Monitoring Plans
- Description of the main product features
- Netwrix standalone tools
- Network traffic compression

Navigation

Starting with version 10, the home screen in Netwrix Auditor is customizable so you can instantly get access to the information that is most relevant to you. This section covers the tiles are available and how you can use them to create the home screen that works best for you. It also illustrates the customization process with several common scenarios.

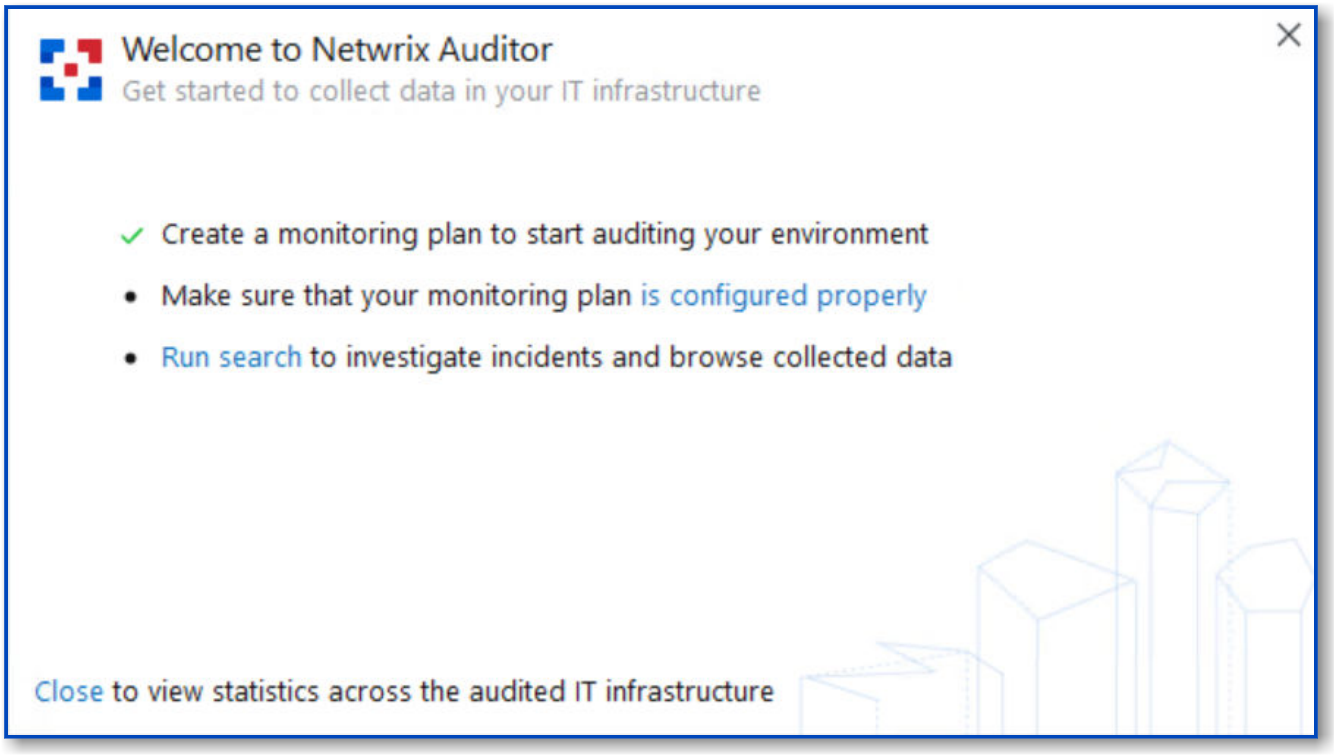
Home Screen Tiles

Home Screen Tiles in the Netwrix Auditor provide an interface that allows users to access main information. The following tiles are displayed on the initially configured Home Screen:

- Welcome to Netwrix Auditor Tile
- Audit Intelligence Tiles
- Configuration Tile

Welcome to Netwrix Auditor Tile

The Welcome to Netwrix Auditor Tile tile provides a checklist you can use to get started collecting and viewing data about your IT ecosystem.

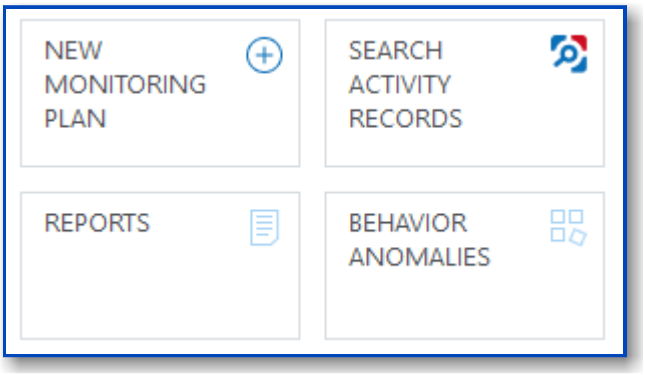


- The "Create a monitoring plan" link prompts you to create a monitoring plan for at least one data source (such as Active Directory, Exchange Online or network devices). For detailed instructions on how to create a monitoring plan, see the Monitoring Plans topic for additional information. Wait until the initial data collection completes.
- Clicking the second link opens a dashboard that lists all the monitoring plans you've created, along with the status and last activity time for each. Review this list and address any errors or warnings. See the Monitoring Overview topic for additional information.
- Once have created a monitoring plan and verified that it is properly configured, run one or more searches to get insights into your IT infrastructure. See the View and Search Collected Data topic for additional information.

When you have completed these three steps, you can close this tile by clicking the "Close" link at the bottom. The checklist will be replaced by statistics across your audited systems. See the Customize Home Screen topic for additional information.

Audit Intelligence Tiles

This section contains four tiles for getting security intelligence about your IT infrastructure:



Tile	Description
NEW MONITORING PLAN	Create a new monitoring plan for a particular data source. See the Create a New Monitoring Plan topic for additional information.
SEARCH ACTIVITY RECORDS	Investigate incidents by running interactive searches using data collected across the entire IT infrastructure. See the View and Search Collected Data topic for additional information.
REPORTS	Access the predefined reports for each data source and create custom reports. See the Reports topic for additional information.
BEHAVIOR ANOMALIES	Detect and investigate unusual behavior in your IT environment. See the Behavior Anomalies topic for additional information.

Configuration Tile

This tile helps you set up and fine-tune auditing of your IT infrastructure. It includes the following links:

Option	Description
Monitoring plans	Opens the Monitoring plans wizard, where you can add, edit and delete monitoring plans, as well as

Option	Description
	group them into folders. See the Monitoring Plans topic for additional information.
Subscriptions	Opens the Subscriptions wizard, which enables you to subscribe to Auditor reports and searches, so you can easily stay informed about what is going on in your infrastructure. See the Subscriptions topic for additional information.
Alert settings	Opens the All Alerts wizard, where you can create, edit, and enable or disable alerts on critical events in your environment. See the Alertstopic for additional information.

Risk Assessment, Compliance Mapping, Live News, and Health Tiles

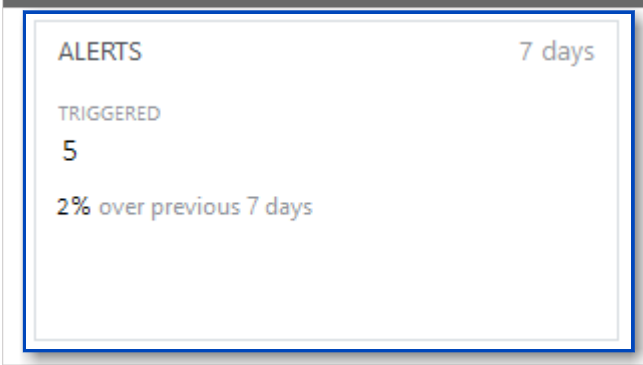
Tile	Description
RISK ASSESSMENT	Opens the Risk Assessment Overview dashboard, which identifies possible configuration issues in your environment that could impact security. See the IT Risk Assessment Overview topic for additional information.
COMPLIANCE MAPPING	Enables you to review how Auditor can help you comply common standards and regulations. See the Compliance Mappings topic for additional information.
LIVE NEWS	Shows the latest Netwrix news, including product updates.
HEALTH STATUS	Opens the Health Status dashboard, which provides at-a-glance insight into product health, data

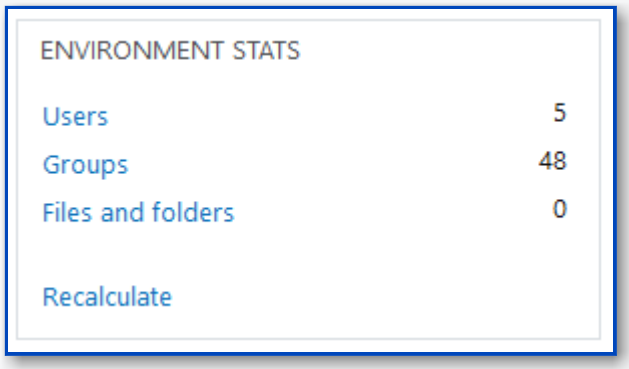
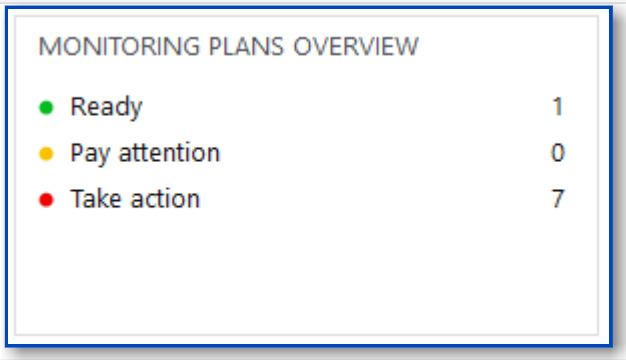
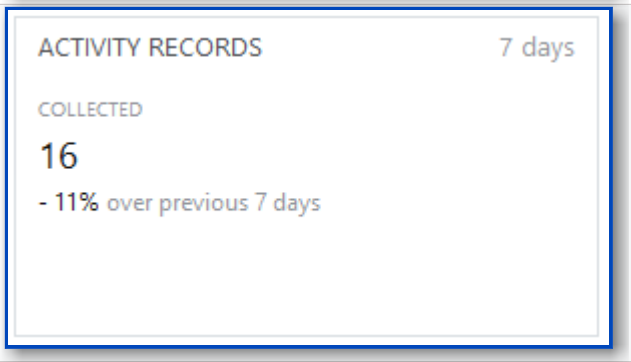
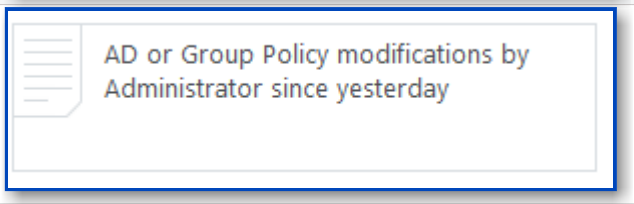
Tile	Description
	collection, storage and more. See the Health Status Dashboard topic for additional information.
ALERTS HISTORY	Clicking this tile opens the Alerts History dashboard, which provides detailed information about the latest alerts triggered in your IT infrastructure, enriched with actionable charts and timelines. See the Alerts Overview Dashboard topic for additional information.

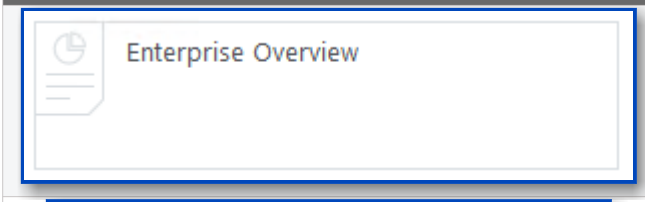
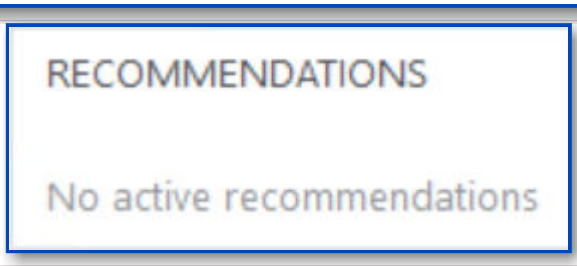
Favorite Reports

Initially, the Favorite Reports tile lists the reports that our customers use most frequently. You can add and remove reports to reflect your needs and interests. If you have more favorite reports than can fit in the tile, simply click **View all** to see the complete list. See the Customizing Favorite Reports topic for additional information.

Other

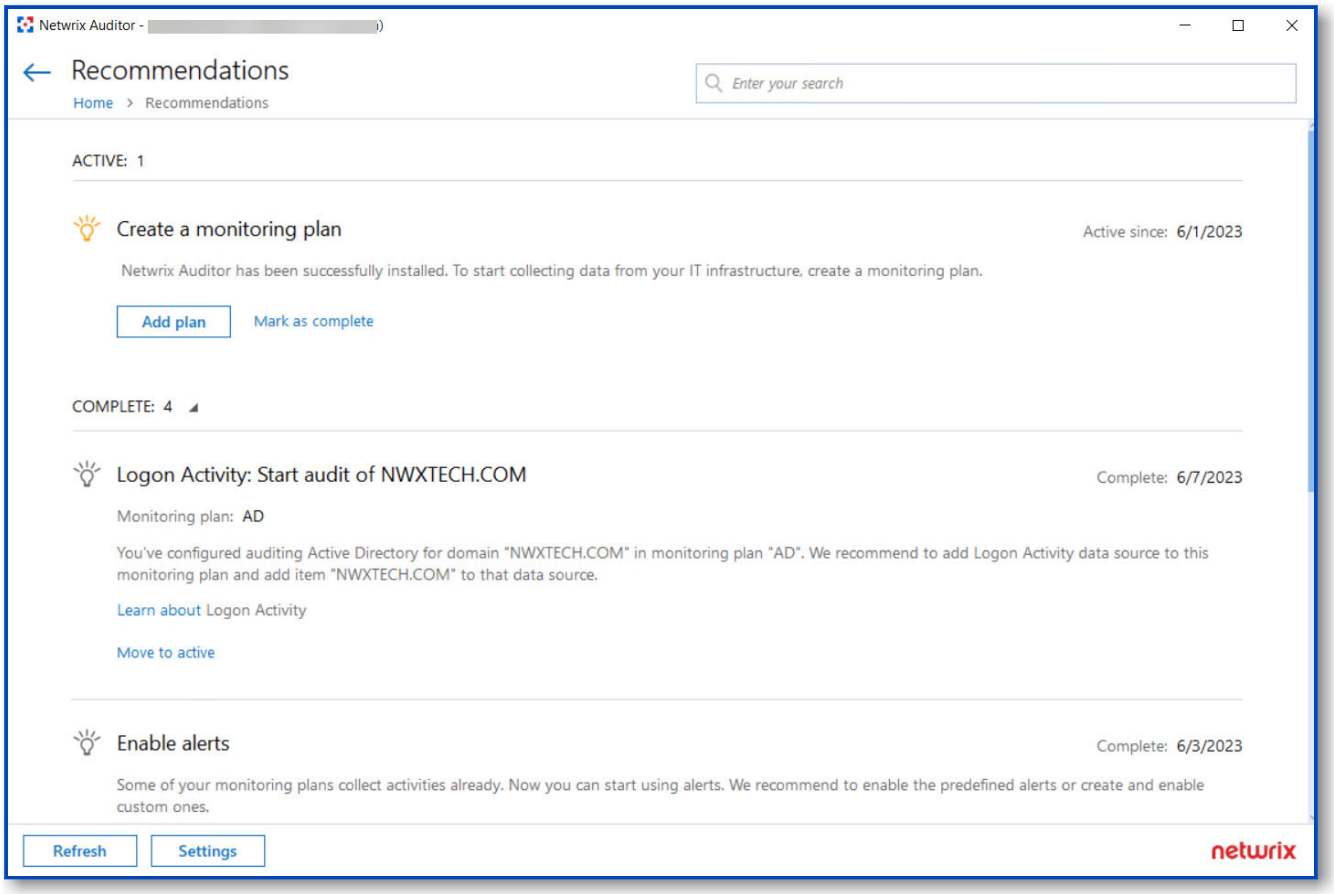
	Opens the Alerts Overview dashboard, which lists the latest alerts triggered in your IT infrastructure, enriched with actionable charts and timelines. See the Alerts Overview Dashboard topic for additional information.

	This tile shows the current number of users, groups, and files and folders in your IT infrastructure in one place. Clicking the link opens the corresponding report: • Users — User Accounts state-in-time report for Active Directory • Groups — Groups state-in-time report for Active Directory • Files and Folders — Folder Tree View state-in-time report for File Servers Click Recalculate to update values.
	Clicking the tile opens the Monitoring Overview dashboard, which shows the current status of each of your monitoring plans. See the Monitoring Overview topic for additional information.
	Clicking the tile opens the Activity Record Statistics dashboard which shows the number of activity records that were collected from your data sources during the last 7 days. See the Activity Records Statistics topic for additional information.
	Opens the listed Auditor report. See the Custom Search-Based Reports topic for additional information.

	Opens the listed Auditor report. See the Predefined Reports topic for additional information.
	Opens the list of the configuration recommendations provided by Netwrix industry experts to take advantage of the Auditor functionality. See the Recommendations topic for additional information.

Recommendations

This section covers the Recommendations interface that contains detailed guidance on the Auditor usage patterns. Once you installed the product, configured your IT infrastructure, and prepared Netwrix Service Accounts, you can start collecting data and review it with Netwrix Auditor. The recommendations are based on your current product configuration and help you to experience the Auditor capabilities in earnest.



Follow the steps to review the recommendations provided by Netwrix industry experts.

Step 1 – On the Auditor home page, click the **Recommendations** tile.

Step 2 – Review the recommendations applicable to your current Auditor configuration and take required steps.

Once the required steps are done, the recommendation goes to the '**Complete**' list. You can move it back to the active state any time you want by clicking the **Move to active** link.

Available Recommendations

Review the list of the recommendations available in Auditor.

Create Your First Monitoring Plan

To start collecting data with Netwrix Auditor, you need to create a monitoring plan that defines data collection, notification, and storage settings and add a source-specific item. This recommendation will appear if you don't have any monitoring plans configured. Clicking the **Add plan** button opens the New Monitoring Plan wizard. See the Create a New Plan topic for additional information about plans configuration. Once completed, you will be prompted to add an item to your plan, otherwise the configuration will be incomplete and the product will not be able to collect data. Auditor automatically suggests item types associated with your data source.

Start Abandoned Data Source Auditing

If you have a license for several applications, Netwrix suggests enabling each undeployed data source for each purchased application if they were never deployed before. Clicking the **Add plan** button opens the New Monitoring Plan wizard. Select the data source you want to monitor with Netwrix Auditor and see the Create a New Plan topic for additional information about further configuration.

Enable State-in-Time Data Collection

If you want to review the state of your system configuration at a specific moment in time, for example, account permissions or group membership, you need to enable the State-in-Time data collection for your data source. See the State–in–Time Reports topic for additional information about the available reports. Clicking the **Go to data source** button opens the settings page of the data source to which this recommendation applies to. See the Manage Data Sources topic for additional information.

NOTE: This recommendation will not be shown for to the File Servers data sources (Windows-based file shares, NetApp Filers, Dell Data Storage, etc.). Navigate to your file server data source and check the state-in-time data collection settings manually.

Subscribe to the Health Summary Email

The Health Summary email includes all statistics on the product operations and health for the last 24 hours; it also notifies you about license status. If you have configured monitoring plans with data sources and items, Netwrix recommends subscribing to Health Summary emails to be notified on the problems that need your attention. See the Health Summary Email topic for additional information.

Clicking the **Go to Notifications** button opens the Netwrix Auditor notifications settings page. See the Notifications topic for additional information.

Logon Activity: Start Auditing Item

If you have the monitoring plans with configured Active Directory data source and domain item, Netwrix recommends creating a new monitoring plan for the Logon Activity data source to review details around interactive and non-interactive logons, including failed logon attempts, and users logon and logoff activity on domain controllers in the audited domain. Clicking the **Add plan** button opens the New Monitoring Plan wizard with the Logon Activity as a selected data source. See the Create a New Plan topic for additional information about further configuration.

Enable Alerts

For the configured monitoring plans, Netwrix recommends enabling alerts to be immediately notified on the suspicious activity. You can enable predefined alerts or create your custom ones.

Clicking the **Open** settings button opens the All Alerts wizard. See the Manage Alerts topic for additional information.

Manage Recommendations

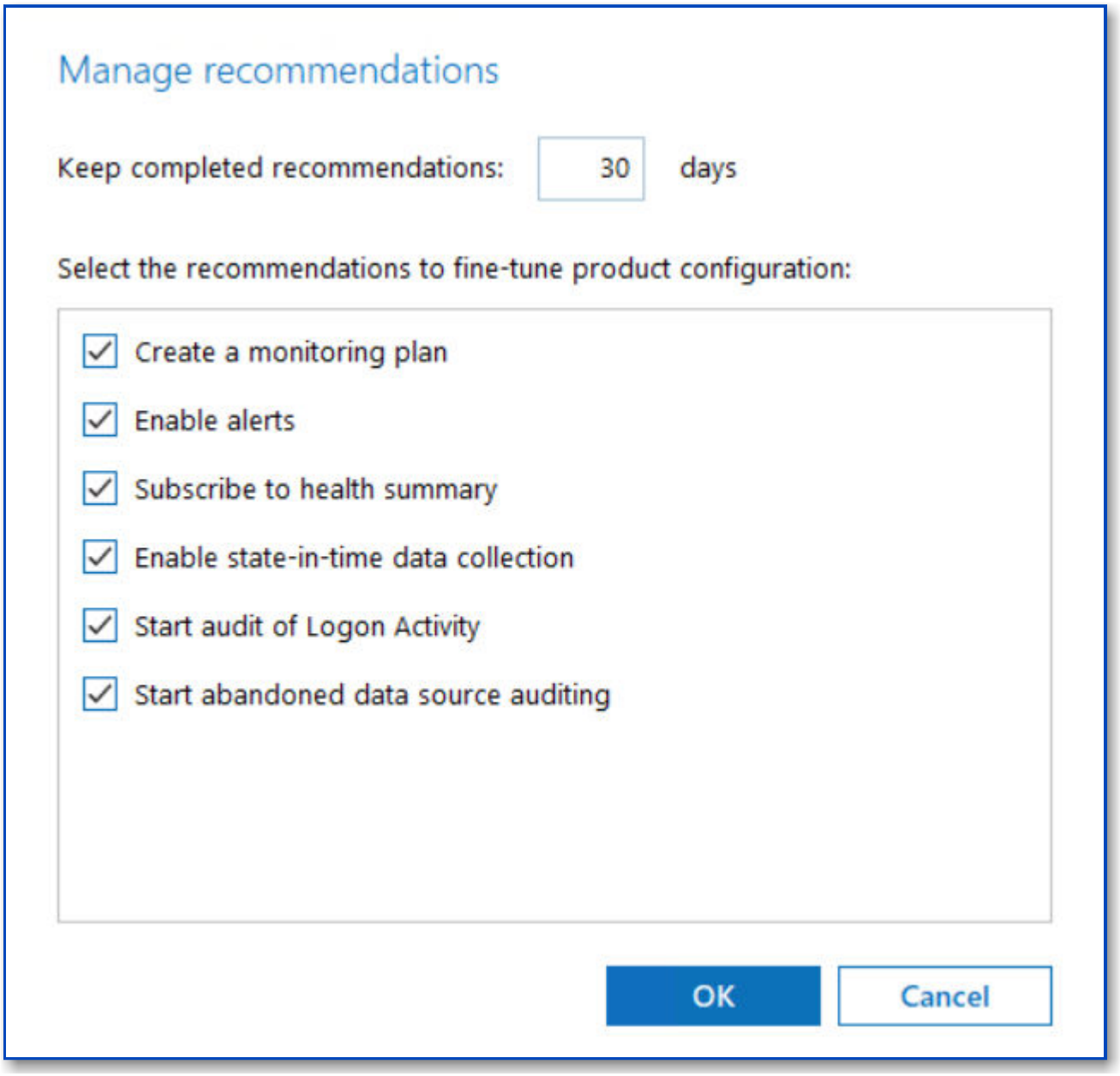
For active recommendations, you can follow the prompts or move them to the completed state by clicking the '**Mark as complete**' link.

For completed recommendations, you can configure the retention period to keep them visible and select their categories for further displaying on the tile. If you want to proceed with a completed recommendation, click the '**Move to active**' link below the recommendation.

Follow the steps to manage recommendations:

Step 1 – On the Auditor home page, click the **Recommendations** tile.

Step 2 – Click **Settings** at the bottom.



Step 3 – In the Manage recommendations dialog, do the following:

- Keep completed recommendations: <30> days – Specify time period in days to keep the completed recommendations visible. The default period is set to 30 days.
- Select the recommendations to fine-tune product configuration – Select recommendations types you want to be displayed. When checked, the recommendations of the selected type appear once your Auditor configuration meets the recommendation conditions.

For example, if you selected the 'Enable State-in-Time data collection', this recommendation appears for each new monitoring plan with disabled state-in-time option.

Step 4 – Click **OK** to save your edits.

To refresh the recommendations list, click the **Refresh** button in the left bottom corner.

Customize Home Screen

Starting with version 10, you can personalize theHome Screen of Netwrix Auditor to display the tiles that best meet your needs. Be sure to plan your screen space, considering which tiles you want to pin and their dimensions. You can modify the size of any tile; horizontal scrolling is also supported. Rest assured that your configurations and data will not be affected by any changes you make to the home screen.

Add a Tile to the Home Screen

Follow the steps to add tile on the Home Screen.

Step 1 – Click Customize in the upper right corner of the home screen.

Step 2 – Select Add tile.

Either search for the tile you want by name, or select it from the list of tiles. Note that tiles are grouped into menus; to view all tiles within a menu, check Show all menu tiles.

Step 3 – Click Add and the selected tile appears on the home screen.

Step 4 – Drag and drop it to the desired location.

Step 5 – Click Apply.

Remove a Tile from the Home Screen

Follow the steps to remove a tile from the Home Screen.

Step 1 – Click Customize in the upper right corner of the home screen.

Step 2 – Select the tile you want to remove.

Step 3 – Click **close (x)**:

Step 4 – Click Apply.

Resize a Tile on the Home Screen

You can change the size of the tile to plan your screen placement and view detailed information on what you are interested in. There are several types of size: small, medium, wide, large, extra large, extra tall. However, not every tile supports all types of sizes. Tiles with graphic information have medium, large and extra large sizes. These sizes provide more screen space, resulting in a better visual representation of data. Additionally, tiles with less information have small and wide sizes. They are designed to open separate windows, providing easy access to features such as search, reports, and live news updates.

Follow the steps to resizea tile.

Step 1 – Click Customize in the upper right corner of the home screen.

Step 2 – Select the tile you want to resize.

Step 3 – Click the **resize** button:

Step 4 – Select the preferred size from the drop-down list.

Restore the Default View

Follow the steps to restore the default Home Screen view.

Step 1 – Click Customize in the upper right corner of the Home Screen.

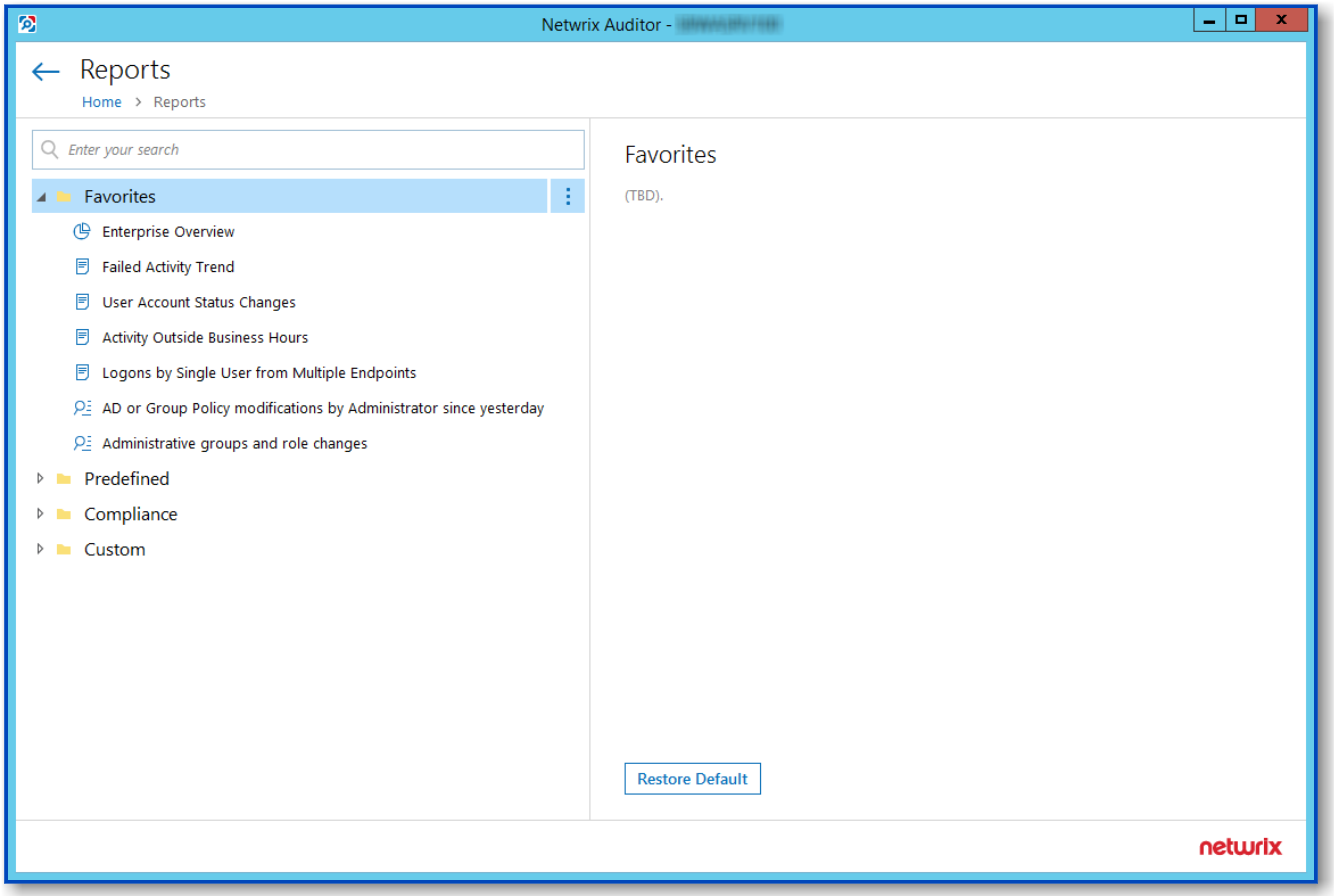
Step 2 – Click Restore default.

Your configuration and data will be preserved during this operation.

Customizing Favorite Reports

The Favorite reports tile displays a shortened list of your favorite reports. To view, edit or update the full list, click View all.

The Home > Reports page opens. This page includes several folders: Favorites, Predefined, Compliance and Custom. Favorite reports are located in the Favorites folder.

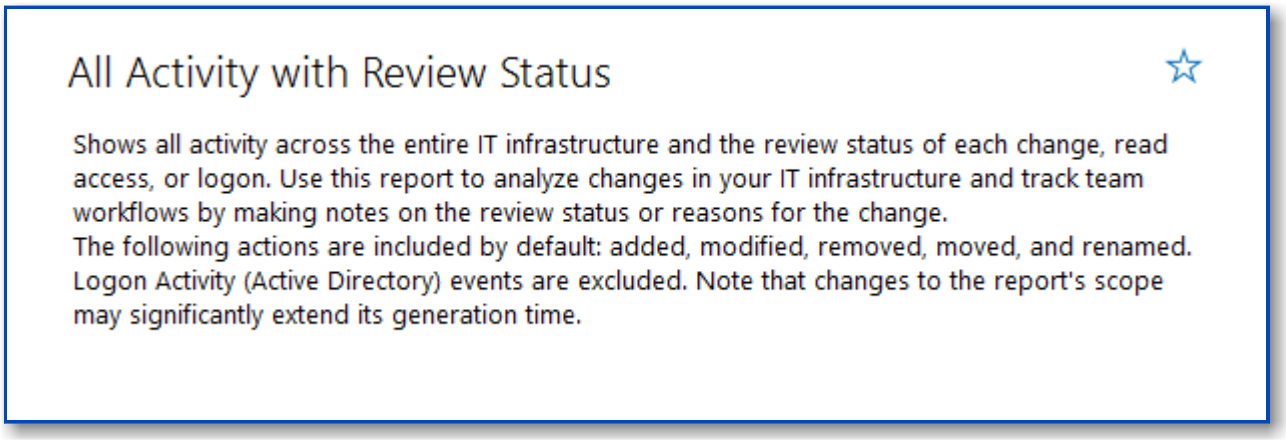


Follow the steps to add or remove a Favorite report

Step 1 – Locate the desired report in one of the other folders.

Step 2 – Click the name of the report to view its description.

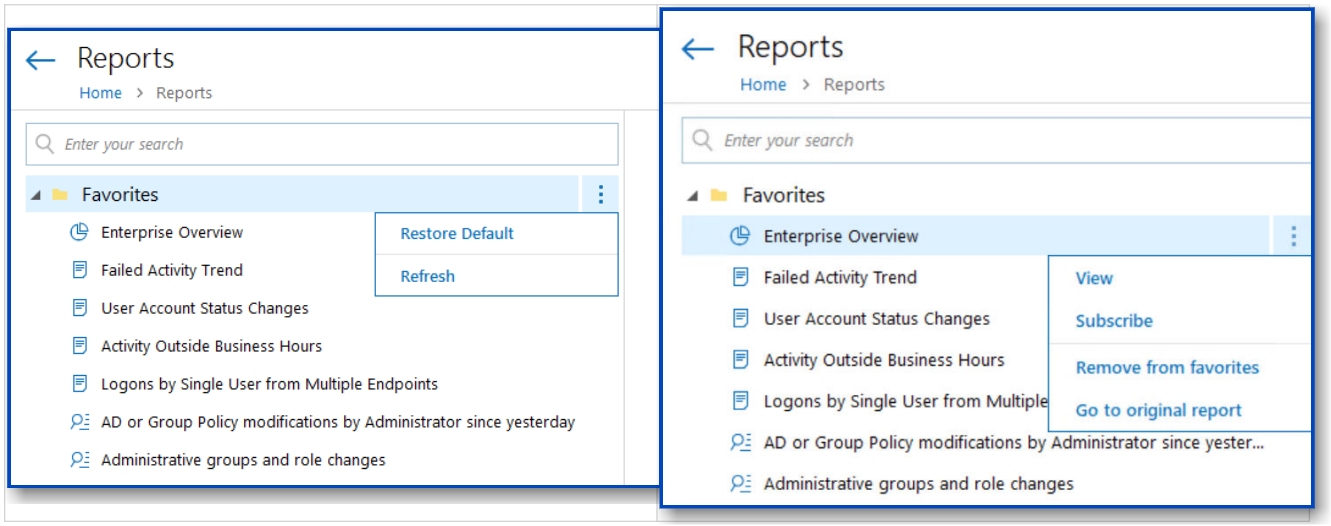
Step 3 – To change whether the report is a favorite, click the star icon in the upper right-hand corner of the report description.



Report Summary with Star icon unchecked

Other Actions for Favorite Reports

The options on the Reports page for Favorite reports are show below:



Favorites Sub-Folder Options	*Favorites > [Report] Options*

Option Name	Description
Restore Default	Repopulates the Favorites sub-folder with all reports that have been marked Favorite. When using Role-Based Access in Netwrix Auditor, if several users mark the same report as **Favorite**, then that report will be removed from the Favorites list if a user removes the report from the Favorites list. Using the **Restore Default** option will re-add the report to the Favorites list for all users that have not removed the Favorite mark.
Refresh	Runs the reports in the Favorites folder to display the most recent information.
View	Opens the Preview Report page. There, you can modify report options (such as the timeframe) if desired, and then click View Report to see the resulting report. See the View Reports topic for additional information.
Subscribe	Opens the Add Subscription to Report page. See the Create Subscriptions topic for additional information.
Add to Favorites	This option is greyed out when viewing the Favorites list, since all the reports shown have already been added to Favorites.
Remove from Favorites	Removes a report from the Favorites list. This option provides the same function as removing a report as a favorite using the **Star** icon.

Option Name	Description
Go to Original	Expands the sub-folder in which the report is originally located. For example, clicking **Go to Original** for the Enterprise Overview report will expand the **Predefined > Organization Level Reports** sub-folder.

Customization Examples

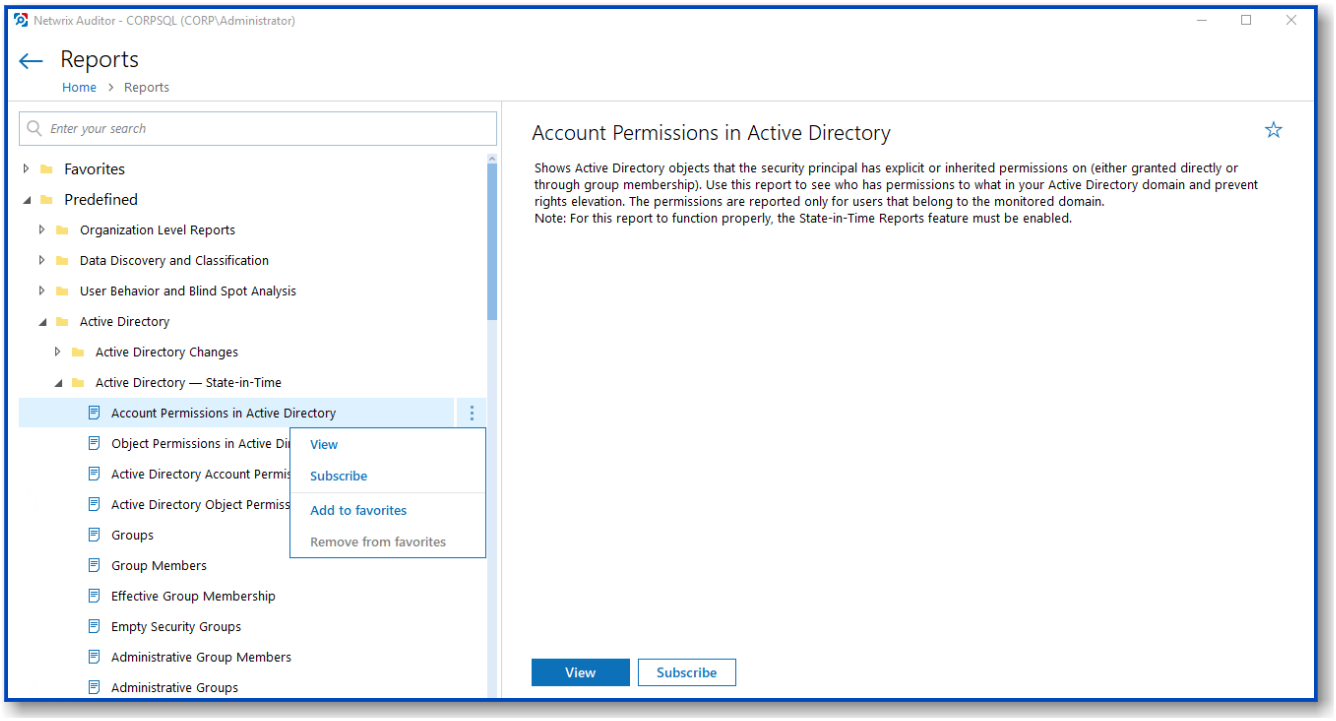
Here are several examples of why and how you might customize the Netwrix Auditor main page.

View Report and Add to Favorites

Follow the steps to view a report and add it to the list of Favorites.

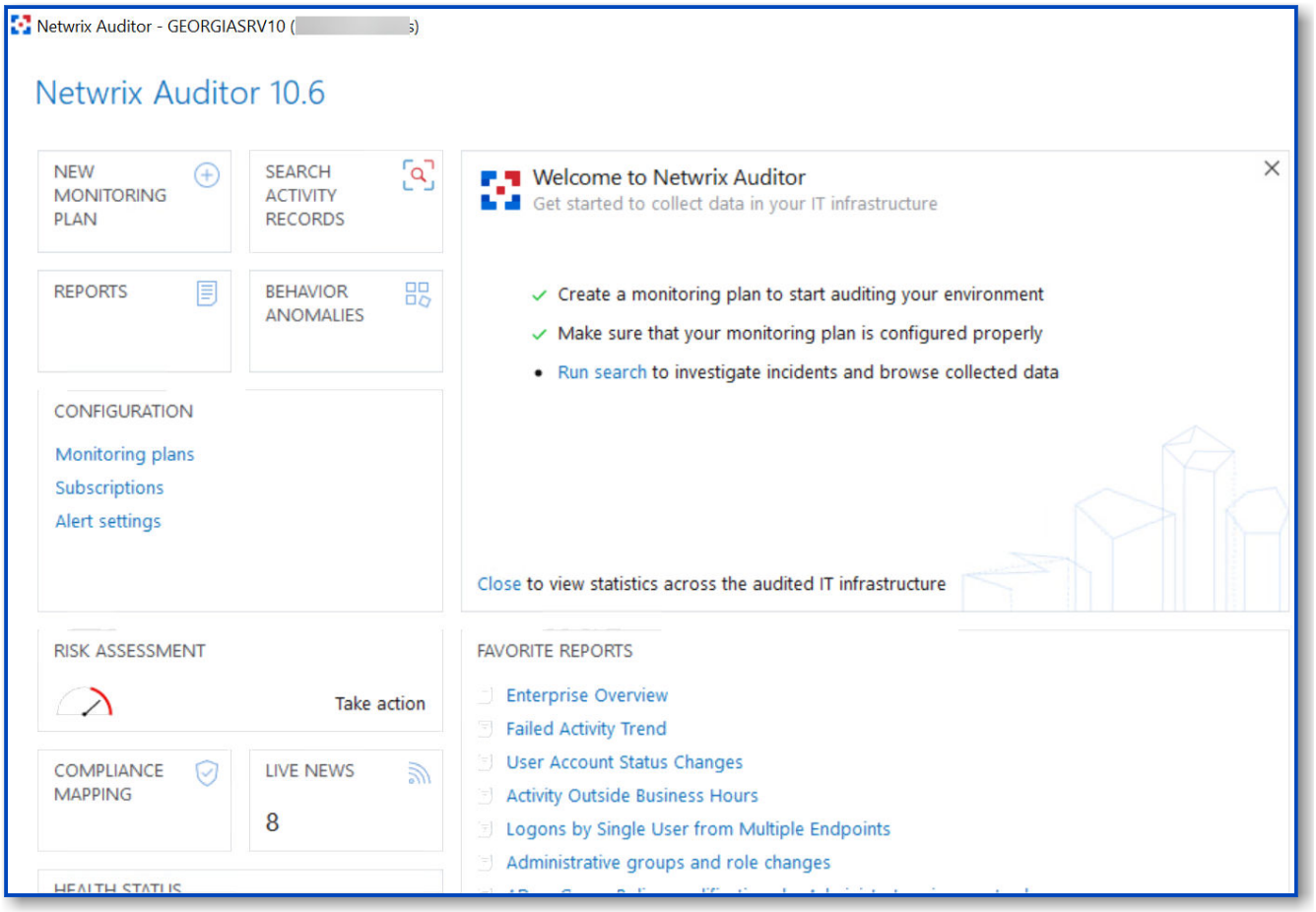
Step 1 – On the main Auditor page, click the Reports tile in the upper left corner.

Step 2 – Open a report you are interested in; for example, Account Permissions in Active Directory:



Step 3 – Click the report menu (three dots) to the right and select Add to favorites. (Alternatively, click the star icon in the upper right corner of the report description.)

The report is added to the Favorite reports section on the home page and you can run it instantly.



Run Search and Create Alert

Follow the steps to run search and create the alert based on the search filters.

Step 1 – On the main Auditor page, click the Search Activity Records tile.

Step 2 – Specify search filters to narrow your search results. See the Use Filters in Simple Mode topic for additional information.

Step 3 – Click Search.

Step 4 – Review your search results.

Step 5 – Navigate to Tools and click Create alert to get instant email or SMS notifications on suspicious activity that matches your current search criteria.

Step 6 – Specify a name for the new alert. See the Create Alertstopic for additional information.

Now, whenever there is activity that matches your search criteria, the appropriate people will receive a notification. You can also review the list of triggered alerts by clicking the Alerts tile on the home page, which opens the Alerts overview dashboard.

Review and Pin Risks

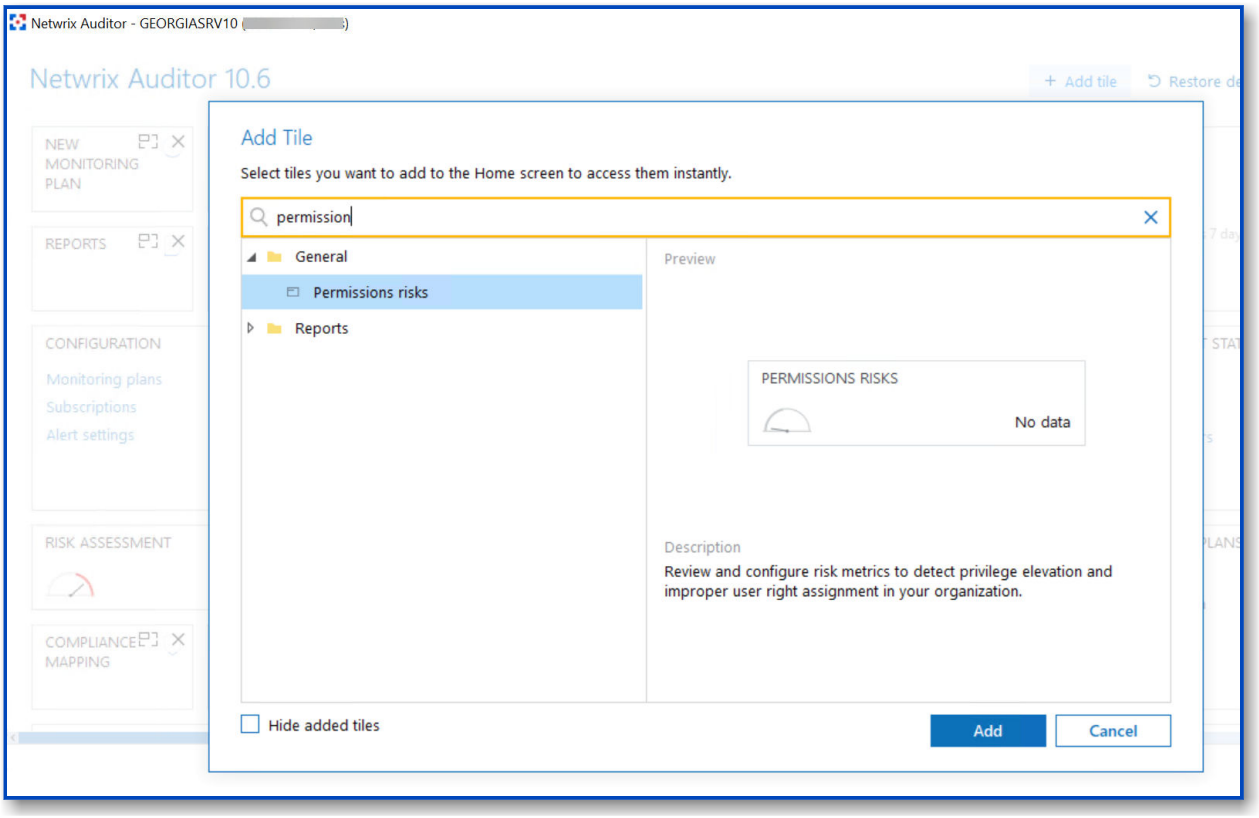
Follow the steps to review risks and pin important ones to the Home Screen.

Step 1 – On the main Auditor page, click the Risk Assessment tile.

Step 2 – Review the Risk Assessment Overview dashbord and select the risk you are interested in, such as "*User Accounts with administrative permissions*". See the IT Risk Assessment Overview topic for additional information.

Step 3 – To access this risk quickly, pin it to the home page, as follows:

1. On the main product page, click Customize.
2. Click Add tile.
3. Search the group of risks you want to pin to the home page (in this case, the "*Permissions*" risks group):



Step 4 – Click Add.

The selected risks group is added to the home screen.

What is Next?

Personalize the home page of the product depending on your business needs. Review the customization settings and collect only required tiles for quick access on the Auditor home page. See the Customize Home Screen topic for additional information.

Netwrix Auditor Settings

In the Settings section, you can configure product settings, such as default SQL Server instance for Audit Database, the Long-Term Archive location and retention period, etc. You can also review information about the product version and your licenses. See the following sections:

- General
- Audit Database

- Long-Term Archive
- Investigations
- Notifications
- Integrations
- Licenses
- About Netwrix Auditor

To modify Netwrix Auditor settings, you must be assigned the *Global administrator* role. See Role-Based Access and Delegation for more information.

General

On the General tab you can configure global Netwrix Auditor settings, e.g., self-audit, tags, accounts and passwords.

Review the following for additional information:

Option	Description
Self-audit	Select to enable data collection for product self-auditing. Self-audit allows tracking every change to monitoring plan, data source, and audit scope and details about it (before-after values) so that you know that scope of data to be audited is complete and changed only in line with workflows adopted by our organization. Review the following for additional information: • Netwrix Auditor Operations and Health
Netwrix Auditor usage statistics	It is optional on your part to help Netwrix improve the quality, reliability, and performance of Netwrix products and services. If selected, Netwrix collects statistical information on how the Licensee uses the product in accordance with applicable law. Visit Netwrix Corporation Software License Agreement for additional information about the program.

Option	Description
	You can review a sample piece of data if you are interested in data acquired by Netwrix.
Tags	Netwrix Auditor allows you to apply tags when creating an alert. With alerts, you can distinguish one alert from another, create groups of similar alerts, etc. The Tags page contains a complete list of alerts that were ever created in the product. See the Alerts topic for additional information. Currently, you cannot assign or create tags on this page. To apply tags to an alert, navigate to alert settings and locate the Apply tags section on the General tab. See the Create Alerts topic for additional information.
Account and passwords	Netwrix Auditor allows you to assign different accounts for monitoring plans. Click **Manage** to review the full list of accounts and associated auditing scope. You can also change accounts' password if necessary.
Access Reviews	Netwrix Auditor supports integration with Netwrix Auditor Access Reviews, which enables business owners to conduct resource and group reviews and recommend changes. See the Access Reviews topic for additional information.

Audit Database

If you want to generate reports and run interactive search queries, you should configure Auditor to store collected data to the SQL Server database (Audit Database). By default, each

monitoring plan will use a dedicated database to store data. So, there are two types of database settings:

- Global settings that apply to all Audit Databases:
  - Default SQL Server instance hosting all databases
  - SQL Server Reporting Services (SSRS) settings
  - Retention settings

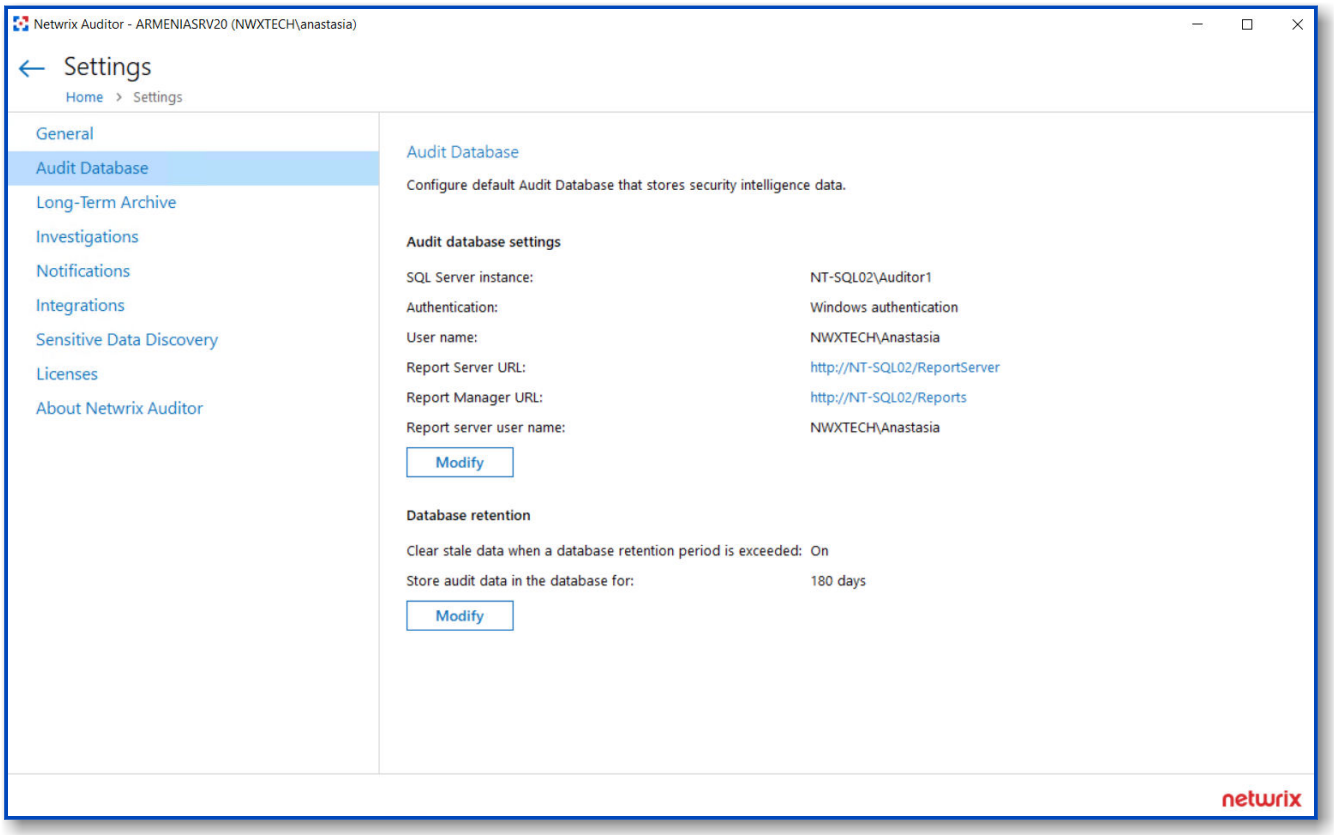
  Usually, initial global settings are configured when you create a first monitoring plan. They become the defaults and appear on the **Settings** > **Audit Database** tab. If you have not specified the default settings before, click Configure.

- Specific settings for each dedicated database. You can configure specific database storage settings for each monitoring plan individually. For that, use the **Monitoring Plan** wizard or navigate to the settings. (Global settings appear as default values there, and you can modify them if needed.) See the Fine-Tune Your Plan and Edit Settings topic for additional information.

Follow the steps to review and update global Audit Database settings:

Step 1 – Navigate to **Settings** > **Audit Database**.

Step 2 – Click **Modify** to edit the settings.



Step 3 – Specify the following database storage settings:

Option	Description
Default SQL Server settings	Specify SQL Server instance name and connection settings.
Database retention	Configure retention if you want audit data to be deleted automatically from your Audit Database after a certain period of time. These settings cannot be modified for a certain plan.
SQL Server Reporting Services settings	Define the Report Server URL and account used to upload data to Report Server. These settings cannot be modified for a certain plan.

Configure Default SQL Server Settings

On the **Settings** > **Audit Database** tab, review settings and click Modify under the Default SQL Server settings section.

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data. If you have more than one Auditor Server running in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Auditor Servers.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication

Option	Description
	• SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. This account must be granted the **database owner (db_owner)** role and the dbcreator server role.
Password	Enter a password.

NOTE: If you want to use Group Managed Service Account (gMSA) to access the SQL Server instance hosting the database, consider that in this case Netwrix Auditor will not be able to generate SSRS-based reports (due to the following Microsoft article: Configure the Unattended Execution Account (Report Server Configuration Manager).

Configure Database Retention

On the **Settings** > **Audit Database** tab, review settings and click Modify under the Database retention section.

These settings are global, that is, they will be applied to all audit databases.

Option	Description
Clear stale data when a database retention period is exceeded	Use this option if you want audit data to be deleted automatically from the corresponding database after a certain period of time.
Store audit data in database for	Specify the retention period for storing audit data in the database. Default retention period is **180 days**.

Option	Description
	When the retention period is over, data will be deleted automatically.

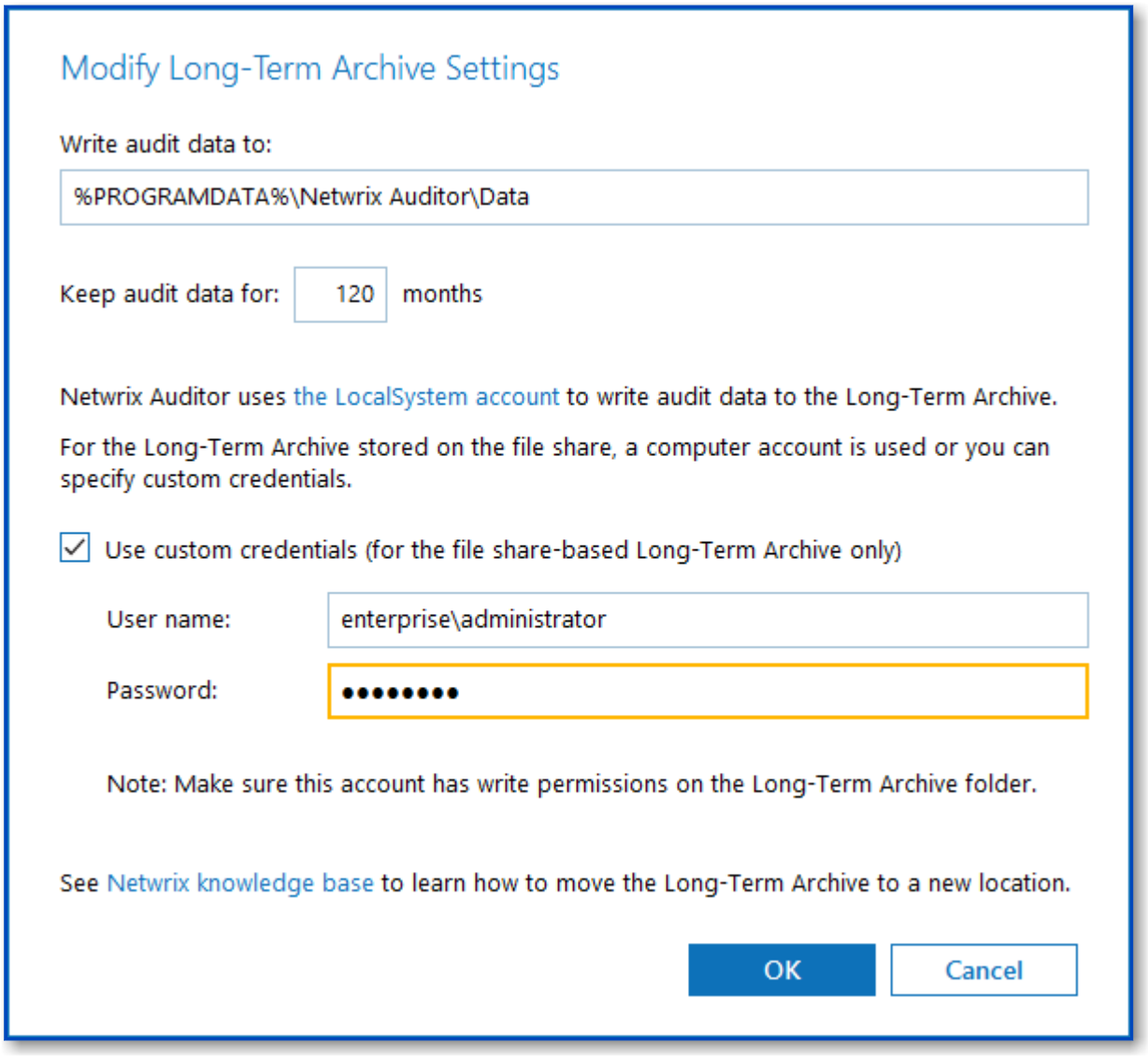
Configure SSRS Settings

On the Settings > Audit Database tab, review settings and click Modify under the SQL Server Reporting Services settings section.

Option	Description
Report Server URL	Specify the Report Server URL. Make sure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Make sure that the resource is reachable.
User name	Specify the account to connect to SSRS. Use the following format: *domain**username* or *hostname**username* Workgroup format (.*username*) is not supported. Use *hostname**username* instead. Make sure this account is granted the Content Manager role on the Report Server. See the SQL Server Reporting Services topic for additional information.
Password	Enter a password.

Long-Term Archive

The Long-Term Archive is configured by default, irrespective of your subscription plan and settings you specified when configuring a monitoring plan. To review and update your Long-Term Archive settings, navigate to **Settings** > **Long-Term Archive** and click Modify.



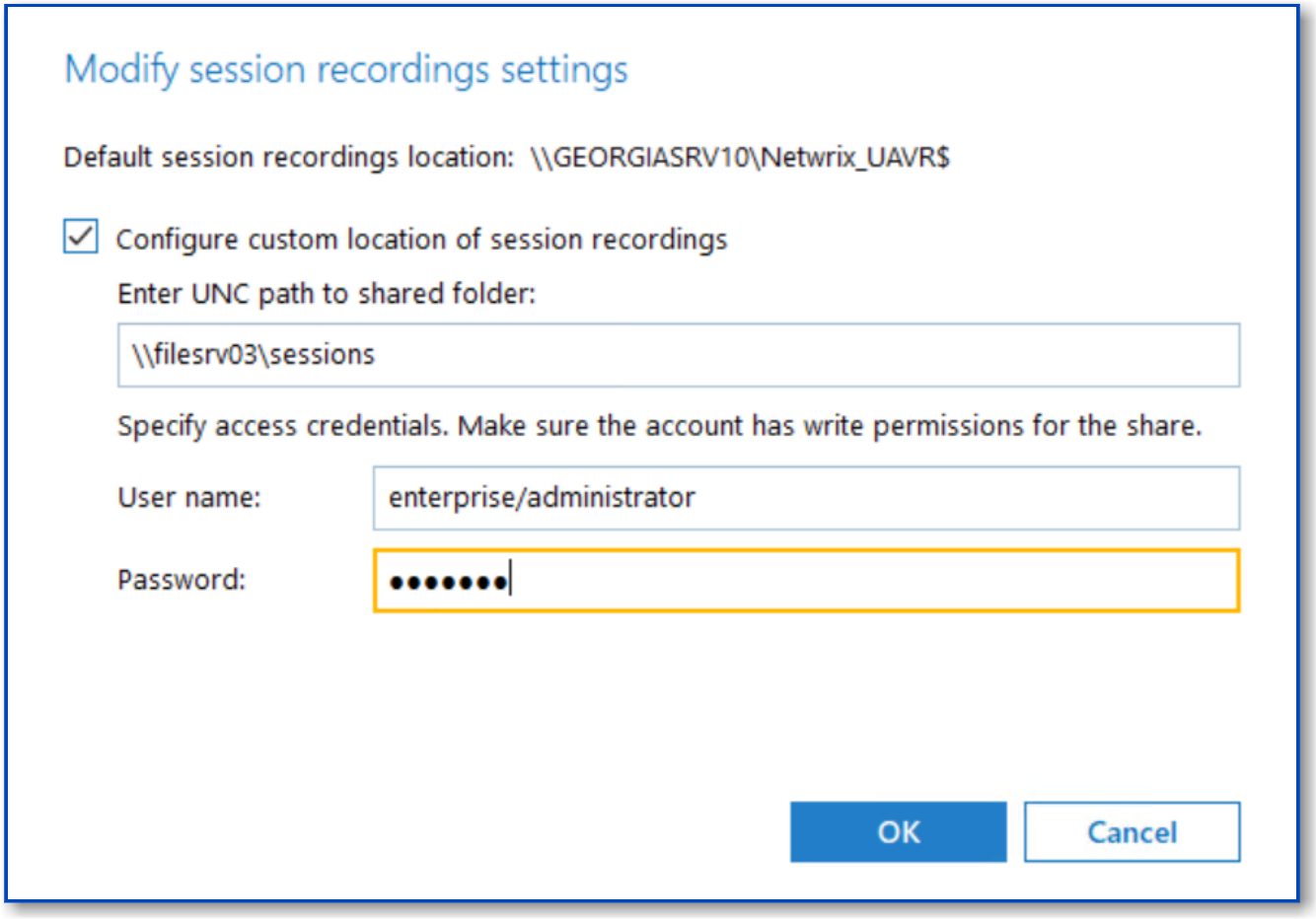
Review the following for additional information:

Option	Description
Long-Term Archive settings	

Option	Description
Write audit data to	Specify the path to a local or shared folder where your audit data will be stored. By default, it is set to *"C:\ProgramData\Netwrix Auditor\Data"*. By default, the LocalSystem account is used to write data to the local-based Long-Term Archive and computer account is used for the file share-based storage. Subscriptions created in the Auditor client are uploaded to file servers under the Long-Term Archive service account as well. It is not recommended to store your Long-Term Archive on a system disk. If you want to move the Long-Term Archive to another location, refer to the following Netwrix Knowledge base article: How to move Long-Term Archive to a new location.
Keep audit data for (in months)	Specify how long data will be stored. By default, it is set to 120 months.
Use custom credentials (for the file share-based Long-Term Archive only)	Select the checkbox and provide user name and password for the Long-Term Archive service account. You can specify a custom account only for the Long-Term Archive stored on a file share. The custom Long-Term Archive service account can 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

Option	Description
	• On the file shares where report subscriptions are saved: ◦ Change share permission ◦ Create files / write data folder permission Subscriptions created in the Auditor client are uploaded to file servers under the Long-Term Archive service account as well. See the Subscriptions topic for additional information.

Setting Recording Settings



Configure custom location of session recordings	Default location for storing session recordings is set to "*<NetwrixAuditorServerName>*\Netwrix_UAVR$". However, storing extra files on the Auditor Server may produce additional load on it, so consider using

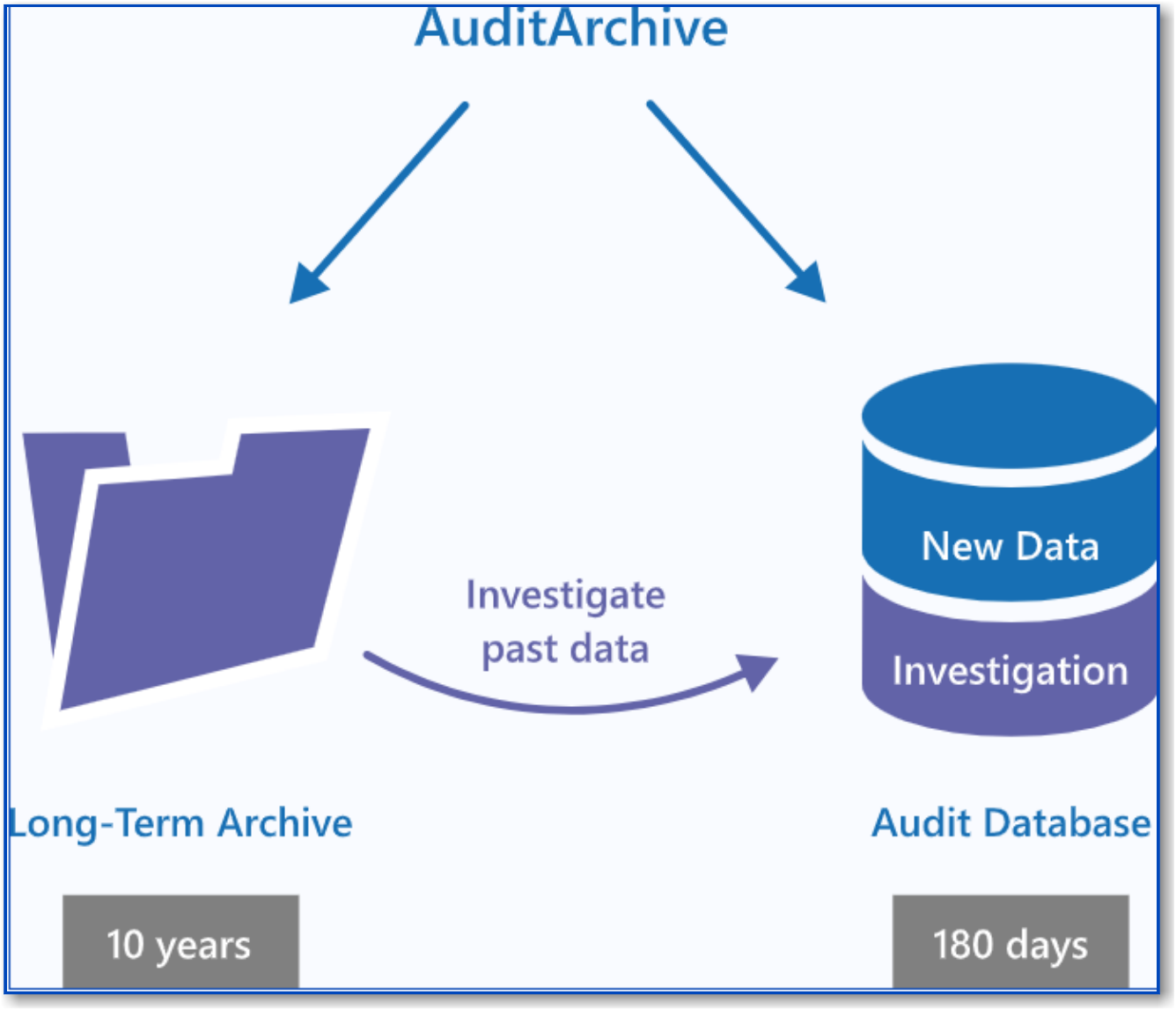
	this option to specify another location where session recordings will be stored.
Enter UNC path to shared folder:	Specify UNC path to the shared folder where user session video recordings will be stored. You can use server name or IP address, for example: *\\172.28.6.33\NA_UserSessions* Using a local folder for that purpose is not recommended, as storing extra files on the Auditor Server will produce additional load on it. Make sure the specified shared folder has enough capacity to store the video files. Retention period for the video files can be adjusted in the related monitoring plan settings (targeted at User Activity data source); default retention is 7 days. See the User Activity topic for additional information. After you specify and save settings for session recordings, it is recommended that you leave them unchanged. Otherwise — if you change the storage location while using Netwrix Auditor for User Activity — please be aware of possible data loss, as Auditor will not automatically move session recordings to a new location.
User name / Password	Provide user name and password for the account that will be used to store session recordings to the specified shared folder. Make sure the account has at least the Write permission for that folder.

Auditor informs you if you are running out of space on a system disk where the Long-Term Archive is stored by default. You will see events in the Netwrix Auditor **System Health** log once the free disk space starts approaching minimum level. When the free disk space is less than 3 GB, the Netwrix services responsible for audit data collection will be stopped.

Investigations

By default, the Audit Database stores data up to 180 days. Once the retention period is over, the data is deleted from the Audit Database and becomes unavailable for reporting and search.

Depending on your company requirements you may need to investigate past incidents and browse old data stored in the Long-Term Archive. Netwrix Auditor allows importing data from the Long-Term Archive to a special "investigation" database. Having imported data there, you can run searches and generate reports with your past data.



To import audit data with the Archive Data Investigation wizard

NOTE: You must be assigned the Global administrator role to import investigation data. To view investigation data, you must be assigned the Global administrator or Global reviewer role. See Assign Roles topic for more information.

1. Navigate to Settings → Investigations.
2. Complete your SQL Server settings.

Option	Description
SQL Server Instance	Specify the name of the SQL Server instance to import your audit data to. If you want to run searches and generate reports, select the same SQL Server instance as the one specified on Settings → Audit Database page. See Audit Database topic for more information.
Database	Select import database name. By default, data is imported to a specially created the Netwrix_ImportDB database but you can select any other. Do not select databases that already contain data. Selecting such databases leads to data overwrites and loss.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. This account must be granted the **database owner (db_owner)** role and the dbcreator server role.
Password	Enter a password.
Clear imported data	Select to delete all previously imported data.

Option	Description
	To prevent SQL Server from overfilling, it is recommended to clear imported data once it is longer needed.

3. Review your New investigation configuration. Click Configure to specify the import scope.

Option	Description
From... To...	Specify the time range for which you want to import past audit data.
Data sources	Select data sources whose audit data you want to import to the Audit Database.
Monitoring plans	Select monitoring plans whose audit data you want to import to the Audit Database. Netwrix Auditor lists monitoring plans that are currently available in the product configuration. Select All to import audit data for all monitoring plans, including those that were removed from the product (or removed and then recreated with the same name—Netwrix Auditor treats them as different monitoring plans). For example, you had a monitoring plan corp.local used for auditing Active Directory. You removed this monitoring plan, but its audit data was preserved in the Long-Term Archive. Then, you created a new monitoring plan for auditing Exchange and named it corp.local again. Its data is also stored in the Long-Term Archive. Netwrix Auditor treats both corp.local monitoring plans—the removed and the current—as different. If you select corp.local in the monitoring plans list, only Exchange data will be imported to Audit Database (as it corresponds to the current monitoring plan configuration). To import Active Directory data from the removed monitoring plan, select All monitoring plans.

4. Click Run.

Notifications

Notification settings are configured when you create the first monitoring plan in the New monitoring plan wizard.

You can update notification settings at any time in the **Settings > Notifications**. To disable notifications, go to **Settings > Notifications > Modify** and select **No notifications** options.

Review the following for additional information:

- Enable Notifications via Exchange Online
- Enable Notifications via SMTP
- Summary Emails and Notifications about Critical Events

Enable Notifications via Exchange Online

To enable Netwrix Auditor to send email notifications via Exchange Online using modern authentication, configure an application. To do this, follow the steps below.

Step 1 – Register a new application in the Microsoft Entra admin center.

Step 1 – Under Identity go to **Applications > App registrations** and choose **New registration**.

Step 2 – Enter the name for your application, choose "Accounts in this organizational directory only". Redirect URL is optional.

Step 3 – Save Client ID and Tenant ID.

Step 4 – Create a new client secret and save it.

Step 5 – Under Microsoft Graph API, go to **Manage > API permissions**, and add the following application permissions to the application:

- Mail.Send
- Mail.ReadWrite

Step 6 – Grant admin consent for these permissions.

Step 7 – In Netwrix Auditor, go to Notification Settings, click Modify, and under Exchange Online enter Tenant name, Application ID and Application secret.

After the application configuration, you can restrict permission so only the specified accounts could use the application to send email. To do this, the following actions required:

- Create a Group
- Add Email to a Group
- Apply Restriction Using PowerShell Commands

Create a Group

Follow the steps to create a group.

Step 1 – Log in to the Exchange admin center with your administrator account.

Step 2 – Under Groupsclick on the **Mail-enabled security** tab.

Step 3 – Click **Add a group**.

Step 4 – Select **Mail-enabled security** and click **Next**.

Step 5 – Set a name and click **Next**.

Step 6 – Set group name and select **Approval**. Its needed to require owner approval to join the group.

Step 7 – Click **Next**.

Step 8 – Click **Create**.

Add Email to a Group

Follow the steps to add emails to group.

Step 1 – In the Exchange admin cente go to Groupsand click on the [Mail-enabled security] tab.

Step 2 – Click on the group you have created and add emails you want to allow APIs to access.

Apply Restriction Using PowerShell Commands

Follow the steps to run following commands using PowerShell.

Step 1 – Open PowerShell

Step 2 – Run the following commands in order:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSignedRun: Install-Module Pow
erShellGet -ForceInstall-Module -Name ExchangeOnlineManagement -ForceGet
-Module ExchangeOnlineManagementConnect-ExchangeOnline -UserPrincipalNam
e {ADMIN_EMAIL_ADDRESS_HERE}
```

Step 3 – Sign in as Admin in the pop-up window.

Step 4 – Run the following command:

```
New-ApplicationAccessPolicy -AppId {APPLICATION_ID_HERE} -PolicyScopeGro
upId {GROUP_EMAIL_ADDRESS_HERE} -AccessRight RestrictAccess -Description
 "YOUR DESCRIPTION HERE."
```

Enable Notifications via SMTP

To enable notifications via SMTP, first select **SMTP** in the **Method** column, then navigate to Default SMTP settings below to review settings used to deliver email notifications, reports, etc., and click Modify to adjust them if necessary.

Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the From field.

Option	Description
	RECOMMENDED: click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
Sender email (from)	Enter the address that will appear in the "*From*" field in email notifications. This option does not affect notifications sent to users' managers and administrators. Before configuring the "*From*" field for user email notifications, make sure that your Exchange supports this option.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL/ TLS)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL anthentification	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission. The option is

Option	Description
	not available for auditing User Activity as well Netwrix Auditor tools.

You can configure Activity Summary frequency, format and delivery time for each monitoring plan individually. See the Fine-Tune Your Plan and Edit Settings topic for more information.

After that, you can specify the recipient who will receive product activity and health summary emails.

Summary Emails and Notifications about Critical Events

Follow the steps to send summary emails and notifications about critical events.

Step 1 – Navigate to the Summary email recipient and click Modify.

Step 2 – Specify recipient address:

- To send to a single recipient, enter personal mailbox address.
- To send to multiple recipients, make sure they are added to a distribution group, and enter the group address. Entering multiple individual addresses is not supported.

To learn more about product health, you can also navigate to the Health status tile in the main window. It will take you to the Health Status dashboard that contains information on the product activity and system health state. See the Health Status Dashboard topic for additional information.

Integrations

Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

The Netwrix Auditor Integration API provides access to audit data collected by Netwrix Auditor through REST API endpoints. According to the RESTful model, each operation is associated with a URL. Integration API provides the following capabilities:

- Data in: Solidify security and meet regulatory compliance standards by enabling visibility into what is going on in any third-party application.

- Data out: Further automate your business processes, IT security and operations workflows by enriching third-party solutions with actionable audit data.

Netwrix Auditor Integration API is enabled by default and communicates through port 9699. Navigate to Settings → Integrations to adjust port settings and review information about possible integrations.

Netwrix recommends adding a special data source to your monitoring plan—Netwrix API.

In Netwrix Auditor 9.0, Netwrix has updated API schemas. See the Compatibility Notice topic for additional information.

To learn more about Integration API capabilities, refer to the Integration API.

Netwrix Privilege Secure

Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure.

The integration can be configured for the following Auditor data sources:

- Active Directory.

  See the Use Netwrix Privilege Secure as a Data Collecting Account topic for additional information.

- Group Policy.

  See the Use Netwrix Privilege Secure as a Data Collecting Account topic for additional information.

- Logon Activity.

  See the Use Netwrix Privilege Secure as a Data Collecting Account topic for additional information.

- Microsoft Entra ID.

  See the How to Add Microsoft Entra ID Monitoring Plan Using Netwrix Privilege Secure topic for additional information.

- Windows File Server.

  See the Use Netwrix Privilege Secure as a Data Collecting Account topic for additional information.

- Windows Server.

  See the Use Netwrix Privilege Secure as a Data Collecting Account topic for additional information.

Software Requirements

Component	Version
Netwrix Auditor	10.7+
Netwrix Privilege Secure	4.2+

Enable and Configure Netwrix Privilege Secure Integration

Follow the steps to enable and configure Netwrix Privilege Secure integration.

Step 1 – In Netwrix Auditor, navigate to Settings in the upper right corner.

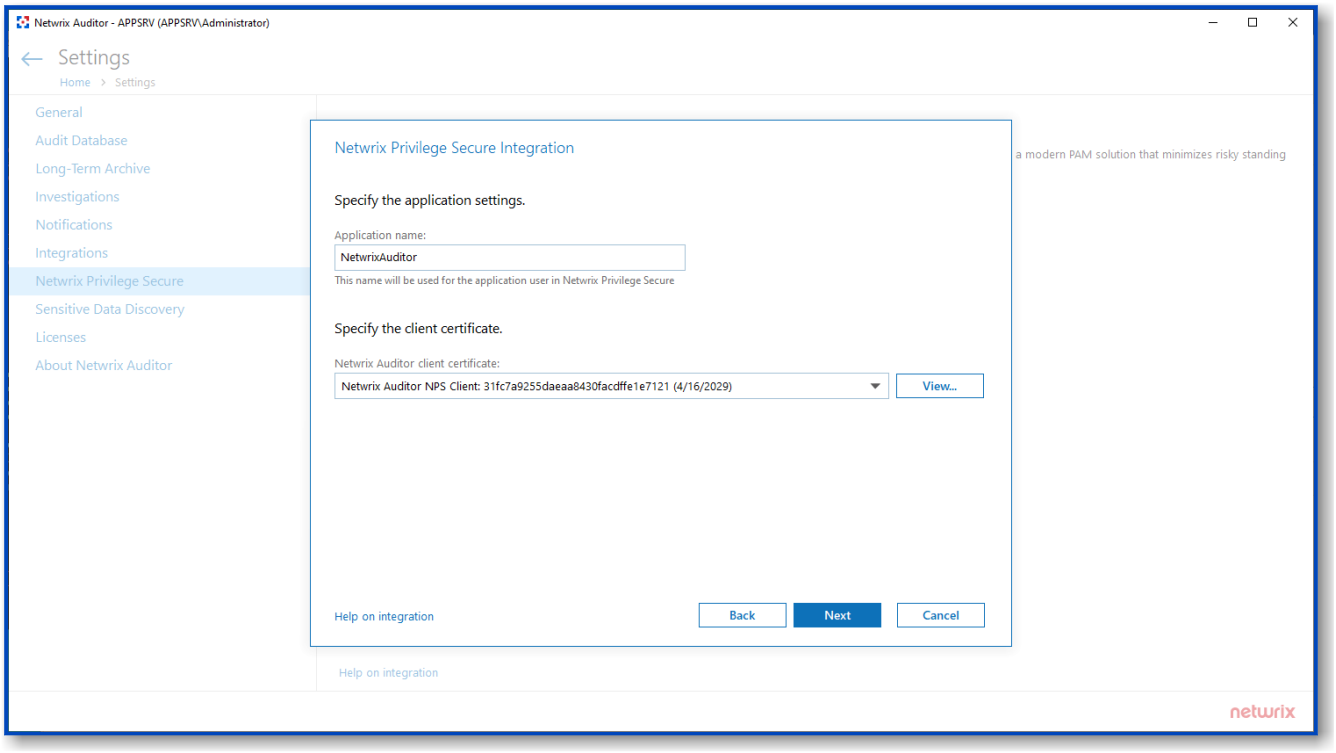
Step 2 – Select Netwrix Privilege Secure.

Step 3 – Click **Set up Integration**.

Step 4 – Specify the Privilege Secure URL.

Step 5 – Specify the application name and Netwrix Auditor client certificate. The following two options are available:

- New/Generate certificate – Create a new certificate.
- Select an existing certificate – Select an available certificate from the drop-down list.



Step 6 – Click **Next**.

Step 7 – You need to manually export the Netwrix Auditor server certificate. To do so, follow the steps below:

1. On the machine where Netwrix Auditor is installed, press the Windows key + R to open the Run dialog box. Type "*mmc*" in the box and click **OK**. This will open MMC (Microsoft Management Console).

2. **Click File > Add/Remove Snap-in...** and locate Certificates icon.

3. In the pop-up window, select the **Computer account** and click **Next**.

4. Make sure that the **Local Computer** option is selected in the next window, then click **Finish**. The Certificates menu will appear.

5. Go to **Certificates (Local Computer) > Personal > Certificates > {Certificate Name}** and click **Export**.

6. After successful export, copy the certificate to the machine where Netwrix Privilege Secure is installed.

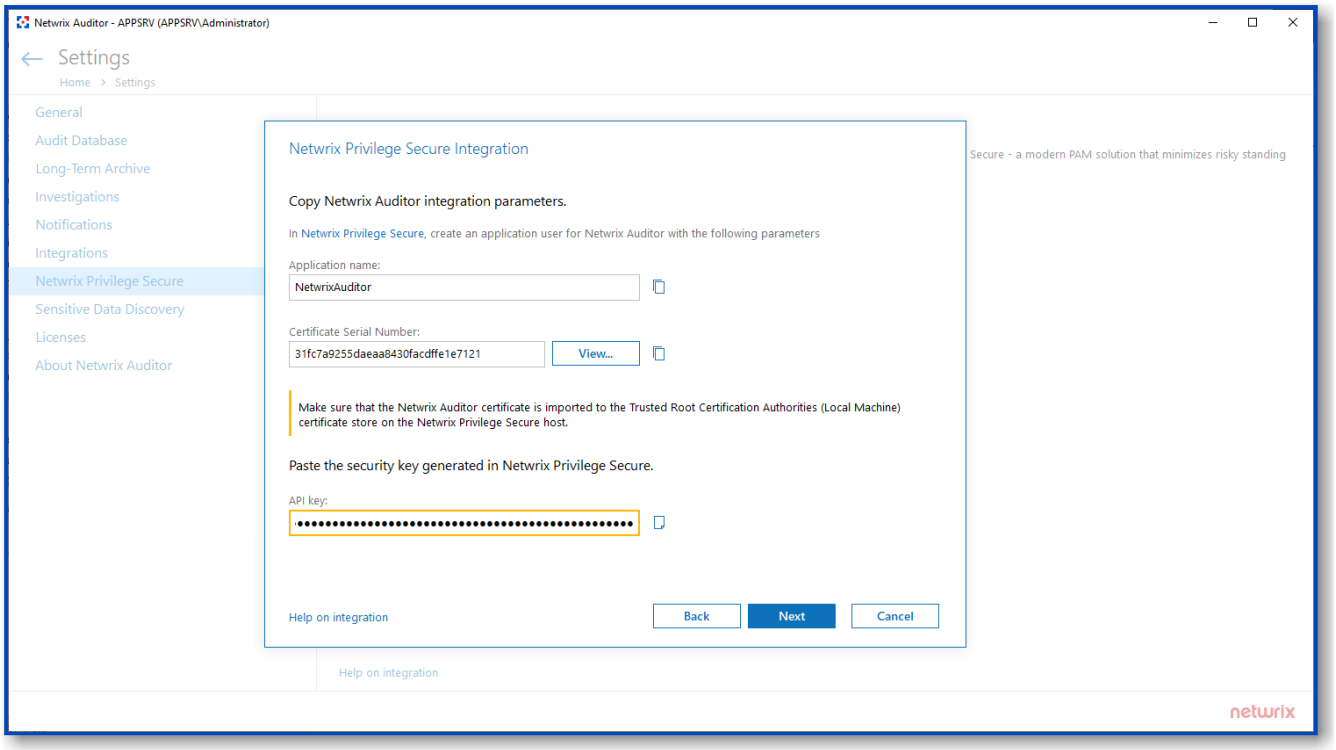
Step 8 – Install the certificate on the machine where Netwrix Privilege Secure is installed. To do so, follow the steps below:

1. Right-click the imported certificate and select **Install Certificate** option.

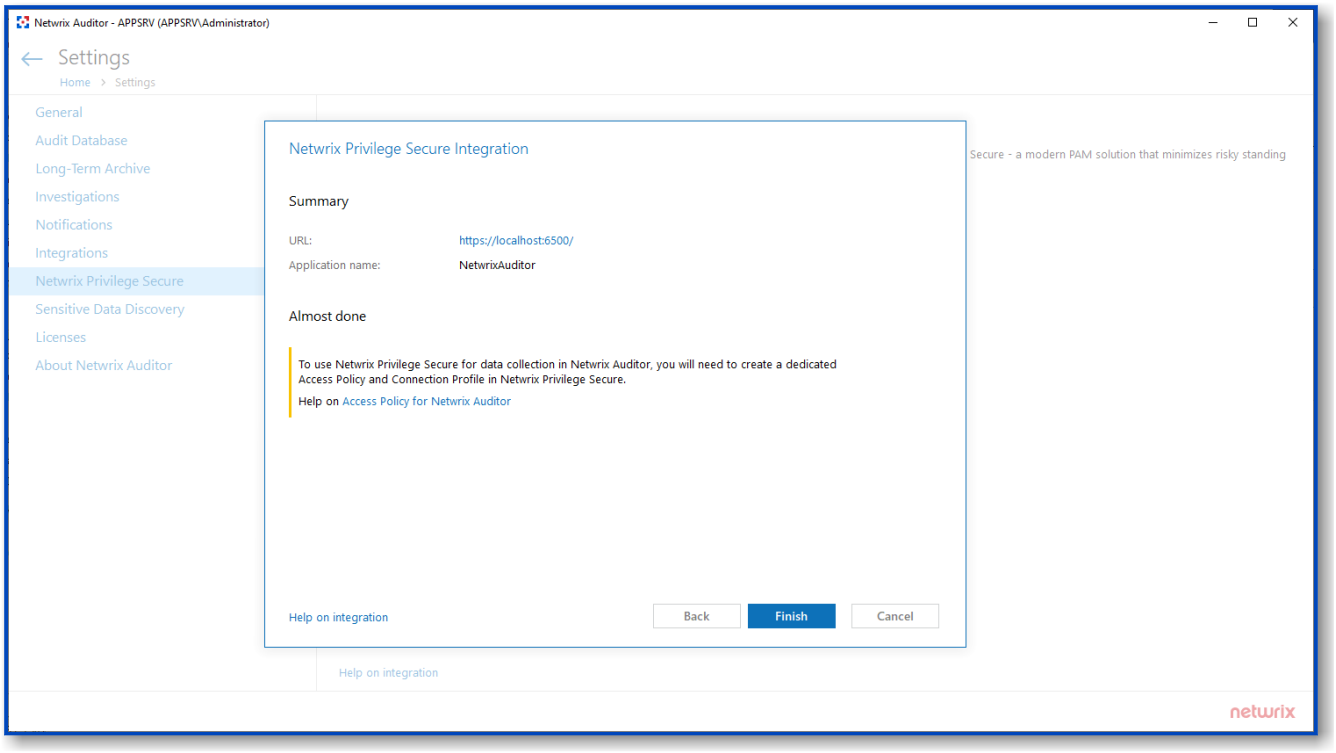
2. In the Certificate Import Wizard, select **Local Machine** as a Store Location and click **Next**.
3. In the next menu, select **Paste all certificates in the following store** option, click **Browse** and select **Trusted Root Certification Authorities** folder in the pop-up menu.
4. Click **Finish**.

Step 9 – Launch Netwrix Privilege Secure to create an application user for Netwrix Auditor with the Application name and Certificate Serial Number that you received. Refer to the Netwrix Privilege Secure documentation for additional instructions.

Step 10 – Provide the security key you got in Netwrix Privilege Secure.



Step 11 – Click **Next**.



Step 12 – After the validation, click **Finish**.

Integration between Netwrix Auditor and Netwrix Privilege Secure is established. Before using the Netwrix Privilege Secure for data collection in Netwrix Auditor, make sure that you created a dedicated Access Policy and Connection Profile in Netwrix Privilege Secure. Refer to the Netwrix Privilege Secure documentation for additional information.

Sensitive Data Discovery

Sensitive Data Discovery is an integration module between Auditor and Netwrix Data Classification. It allows Auditor users to generate reports and configure alerts and search for the sensitive data collected and classified with Netwrix Data Classification (NDC). Refer to the following documentation to learn more about NDC:

- Netwrix Data Classification Documentation

The integration can be configured for the following Auditor data sources:

SharePoint

- SharePoint
- SharePoint Online

File Storage Systems

- Windows File Servers
- EMC
- Netapp
- Nutanix Files
- Qumulo
- Synology

Databases

- SQL Server

The following integration options are available:

- NDC SQL Database Provider – This integration allows users to generate State-in-Time reports showing data categories for the sensitive data classified with Netwrix Data Classification. Available for File storage systems, SharePoint, and SharePoint Online.
- NDC Endpoint Provider – This integration allows users to receive alerts triggered by specific events related to the sensitive data classified with Netwrix Data Classification. When enabled, Netwrix users can also browse sensitive data with the search. Available for File storage systems (including Windows file server, EMC, NetApp, Nutanix File server, Synology, and Qumulo), SharePoint Online, and SQL Server.

This section lists all requirements for monitoring plans configuration and required versions of Netwrix Auditor and Netwrix Data Classification. Also, it lists requirements for the accounts used by Sensitive Data Discovery .

Permissions for Integration with Netwrix Data Classification

The account must be granted the following rights and permissions:

- The Database datareader server role must be assigned to the account on the SQL Server instance where the NDC SQL database resides.

Netwrix recommends using different accounts to connect to the SQL Server instances where NDC SQL database and Categories database reside.

NOTE: Netwrix Data Classification and Netwrix Auditor integration (NDC Provider) currently does not support Single Sign-On. Single Sign-on needs to be disabled in Netwrix Data Classification in order for the account used by the NDC Provider to authenticate.

The account you are using for integration should have Rest API access in the Netwrix Data Classification. You can add it in **NDC console > Settings > Users**. Refer to the Netwrix Data Classification documentation for additional information.

Requirements for Monitoring Plans in Netwrix Auditor

For File Storage Systems:

- Monitoring plan for File Servers data source with activity audit enabled in Netwrix Auditor;
- Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match)

For SharePoint:

- Monitoring plan for SharePoint data source with activity audit enabled in Netwrix Auditor
- Netwrix Data Classification instance configured to crawl from the same source;

For SharePoint Online:

- Monitoring plan for SharePoint Online data source with activity audit enabled in Netwrix Auditor
- Netwrix Data Classification instance configured to crawl from the same source

For SQL Server:

- Monitoring plan for SQL Server data source with activity audit enabled in Netwrix Auditor
- Netwrix Data Classification instance configured to crawl from the same source;

Software Requirements

Component	Version
Netwrix Auditor	10.0+
Netwrix Data Classification	5.6.1+

Enable and configure Sensitive Data Discovery

This section contains instructions on how to enable and configure Sensitive Data Discovery to include sensitive data in Netwrix Auditor reports, search, and alerts.

Ensure that your account meets the requirements and has all server roles assigned. Follow these steps to enable and configure Sensitive Data Discovery:

Step 1 – In Netwrix Auditor, navigate to Setting in the upper right corner.

Step 2 – Select **Sensitive Data Discovery**.

Step 3 – Configure the following settings:

- Enable NDC SQL Database Provider – Select Enable in the Connect to NDC SQL database field and then click Configure to specify NDC SQL database connection settings.
- SQL Server instance – Specify the name of the SQL Server instance where the NDC SQL database resides
- Database – Specify the name of the database (NDC SQL database by default)
- Authentication – Select the authentication type you want to use to connect to the SQL Server instance:
    - Windows authentication
    - SQL Server authentication

- User name – Specify the account to be used to connect to the SQL Server instance. For example, *WORKSTATIONNDC/integrator*.
- Password – Provide a password for that account
- Enable NDC Endpoint Provider – Select Enable in the Connect to NDC via API field and then click Configure to specify NDC endpoint connection settings.
    - NDC Web Console address – Provide the URL of your Netwrix Data Classification web console. For example: *http://workstationndc/conceptQS*.
    - User name – Provide the name of account that will be used to connect to NDC web console. For example, *WORKSTATIONNDC/integrator*. A user must be granted both: the 'REST API User' and 'Superuser' permissions in NDC. See the User Management topic in the Netwrix Data Classification Documentation for additional information.
    - Password – Provide a password for that account

What is Next

Follow the steps to run a data collection and review sensitive data.

Step 1 – Navigate to your File storage system, SharePoint, SharePoint Online, or SQL Server monitoring plan.

Step 2 – Run data collection.

Step 3 – Consider that data collection for SharePoint Online may take a while.

Step 4 – Perform some changes and run data collection again.

Step 5 – Review sensitive data.

Netwrix suggests the following integration scenarios:

For NDC SQL Database Provider:

Review your sensitive data in Data Discovery and Classification reports. Refer to the following Netwrix Auditor help center article for more information about these reports: Data Discovery and Classification Reports.

ForNDC Endpoint Provider:

- Browse your data with Netwrix search.

- **NOTE:** Shortly after the data collection, changes related to sensitive content are reported without data categories. For example, if a user adds some sensitive data to the SharePoint Online document that initially does not contain sensitive data; this will be reported as document modification with empty "*data categories*" field. Another example: a user creates a new document containing sensitive data on a file server; this will be reported as a file add with empty "data categories" field. In this case, you have to wait until Netwrix Auditor processes information collected by NDC. It takes a while depending on a number of processed objects in your infrastructure and reindexing settings configured in Netwrix Data Classification. See the Manage Sources and Control Data Processing topic in the Netwrix Data Classification Documentation for additional information.

- Click the **Select** column in the Tools menu and review data categories (taxonomies) of your sensitive documents.

- Use filtering capabilities to narrow your search results. See the Use Filters in Advanced Mode topic for additional information.

- Create an alert triggered by specific actions with your sensitive data.

RECOMMENDED: Netwrix recommends enable threshold to trigger the new alert. In this case, a single alert will be sent instead of many alerts. This can be helpful when Netwrix Auditor detects many activity records matching the filters you specified. See the Alerts topic for additional information.

Licenses

The Licenses tab allows you to review the status of your current licenses, update them and add new licenses. To learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs.

Follow the steps to update or add a license.

Step 1 – Click **Update**.

Step 2 – In the dialog that opens, do one of the following:

- Select Load from file, click Browse and point to a license file received from your sales representative.
- Select Enter manually and type in your company name, license count and license codes.

Notes for Managed Service Providers

Being a Managed Service Provider (MSP) you are supplied with a special MSP license that allows you to deploy Netwrix Auditor on several servers with the same license key. In this case the license count is based on total number of users across all managed client environments.

MSP billing is calculated based on the arithmetic average of the number of licenses used in that month. This is determined by the following formula:

```
(LicensesUsedOnDay1 + LicensesUsedOnDay2 … LicensesUsedOnDay29 +
LicensesUsedOnDay30) / 30
```

To ensure that licenses are calculated correctly (per heartbeat) by Netwrix, perform the following steps.

Step 1 – Create organizational units within audited domains and add there service accounts you want to exclude from license count.

Step 2 – On the computer where Auditor Server resides, navigate to *Netwrix Auditor installation folder\Netwrix Auditor\Administrative Console* and locate MSP.xml.

Step 3 – In MSP.xml, provide the following:

- CustomInstanceIdentificator – It is used to identify a server where Netwrix Auditor Server is installed. It can be any custom name, for example a server name, code name or any other name you use to distinguish one server from another (e.g., ABCServer).

  NOTE: Netwrix recommends you to assign a unique identifier for each client. This information is stored in the Netwrix Partner Portal and helps you identify each instance when you invoice customers for Netwrix services.

  Netwrix gathers the following information about MSP licenses: identifier, license key and license count.

- ServiceAccount Path – It is a path to OU that contains service accounts. You can add several OUs to MSP.xml, one per line.

For example:

```
<?xml version="1.0" encoding="utf-8" ?>
<MSPSettings>
    <CustomInstanceIdentificator>CompanyABCServer</CustomInstanceIdentificator>
    <ServiceAccounts>
        <ServiceAccount Path="domain.com/Users/Service Accounts" />
        <ServiceAccount Path="domain2.com/Users/Service Accounts" />
    </ServiceAccounts>
</MSPSettings>
```

NOTE: MSP.xml file must be formatted in accordance with XML standard. If company name (used as identifier) or service account path includes & (ampersand), " (double quotes) or ' (single quotes), < (less than), > (greater than) symbols, they must be replaced with corresponding HTML entities.

RECOMMENDED: Netwrix recommends avoiding special characters since some web browsers (e.g., Internet Explorer 8) have troubles processing them.

Symbol	XML entity
& **e.g., Ally & Sons**	& e.g., Ally & Sons
" **e.g., Domain1\Users\"Stars"**	" e.g., Domain1\Users\"Stars"
' **e.g., Domain1\Users\O'Hara**	' e.g., Domain1\Users\O'Hara
< **e.g., Company<1**	< e.g., Company<1
> **e.g., ID>500**	> e.g., ID>500

Step 4 – Navigate to *Netwrix Auditor installation folder\Netwrix Auditor\Administrative Console* and start **Netwrix.CallHome.MSPTool.exe**. The tool transfers information on service accounts to Netwrix Auditor. Netwrix Auditor uses this information to exclude service accounts from license count so that only heartbeat users will be calculated.

NOTE: You must run Netwrix.CallHome.MSPTool.exe every time you update MSP.xml.

The appearance of the license will be reflected in the MSP portal.

About Netwrix Auditor

The About Netwrix Auditor tab contains complete information on the product:

Option	Description
Netwrix Auditor	Review current version of Netwrix Auditor.
Check for updates	Select to check for available updates now.
Check for updates automatically and show notifications about new product versions	Netwrix Auditor periodically checks for updates so you don't have to. When an update is available, a user is immediately noticed.
Getting Help	Click the link to visit Netwrix Auditor Help Center and access configuration guidelines and step-by-step instructions online.

Customize Branding

Netwrix Auditor allows customizing look and feel of your reports, search subscriptions and exported search results—you can skip Netwrix logo, add your company logo and title. However, users are not empowered to customize layout or color scheme.

Review the following for additional information:

- Customize Branding in AuditIntelligence Outputs
- Customize Branding in Reports

Customize Branding in AuditIntelligence Outputs

You can customize branding for the following AuditIntelligence outputs:

- Search results delivered as pdf file in the search subscription email;

- Search results exported to pdf file;

- Risk Assessment dashboard exported to pdf file;
- Risk Assessment dashboard delivered in the subscription email;
- Overview dashboard exported to pdf file;
- Overview dashboard delivered in the subscription email.

Please note the following rebranding limitations and requirements to the logo file:

1. Make sure you have full Netwrix Auditor installation: Netwrix Auditor Server and Client to enable rebranding.
2. Since Netwrix applies company's logo as is, keep in mind reasonable limitations of your logo dimensions. You can find examples of appropriate logo files in the rebranding archive (file Logo.png). Re-size your logo and verify that subscriptions emails and pdf files look fine after rebranding.
3. Only PNG images can be used as logo files.

4. Endure that image file is located in the default directory or custom folder. Consider the following:

    - For subscription emails, just put the logo file to *%ALLUSERSPROFILE%\Netwrix Auditor\Branding* and run the script to update email look and feel.
    - For exported pdf files, make sure that the logo file is located in the default directory for each user that is going to work with exported search results, Risk Assessment and Overview dashboards. Otherwise, specify custom path to logo file. Default path to logo for exported files is *%LOCALAPPDATA%\Netwrix Auditor\Audit Intelligence\Resources*.

Follow the steps t o customize branding

Step 1 – On the computer where the Netwrix Auditor Server is installed, navigate to *%ALLUSERSPROFILE%\Netwrix Auditor* and locate the Rebranding.zip package.

Step 2 – Unzip the package to any folder on the computer where Netwrix Auditor Server is installed.

Step 3 – Run SearchRebranding.ps1 considering the following:

- Use default paths to logo files—Run the script and type your company name as the `report_title`.

- Use custom paths to logo files—run the script as follows:

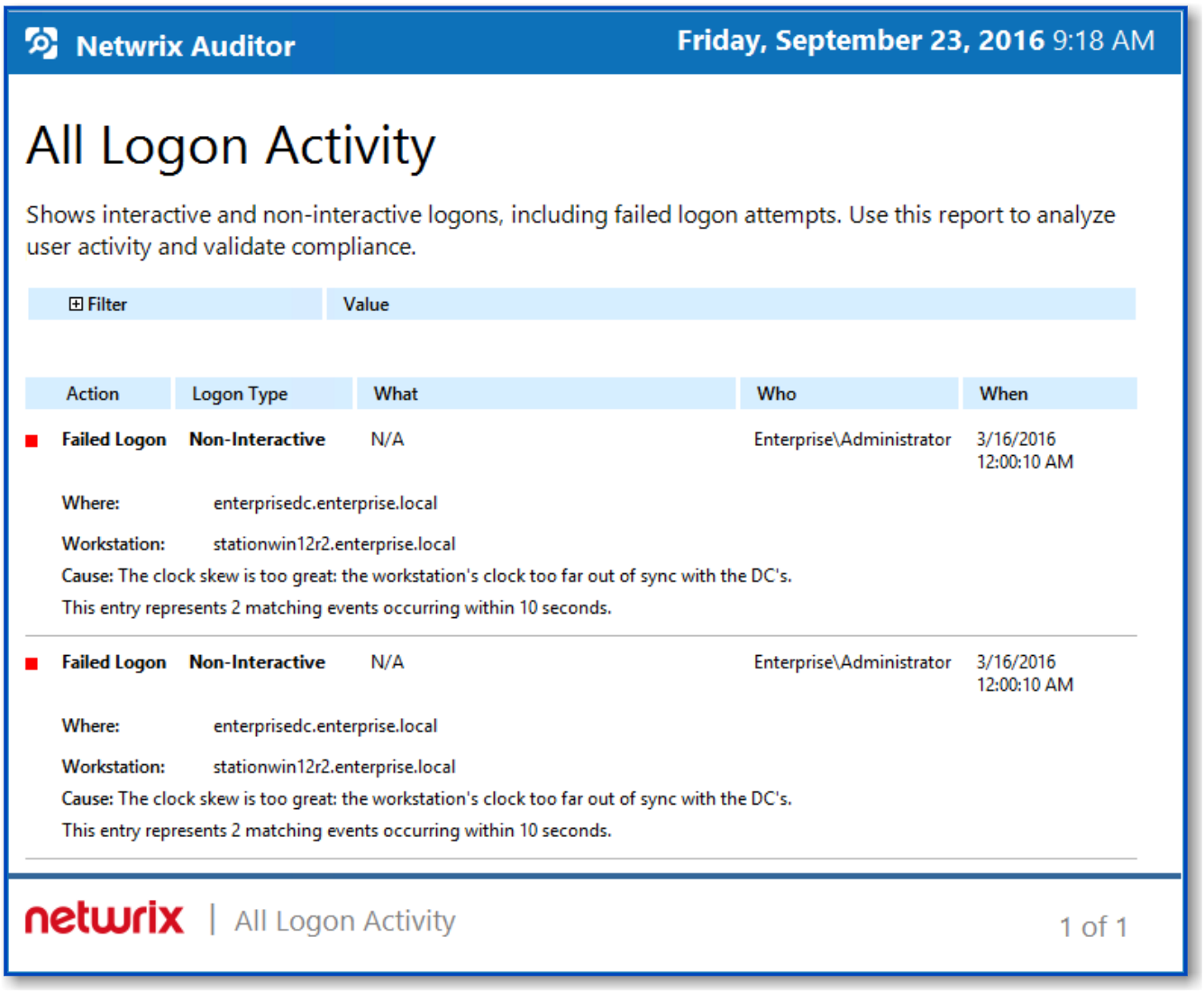
```
SearchRebranding.ps1 -subscriptions_logo_path <custom_path>
-export_logo_path <custom_path>
```

Step 4 – Generate any test subscription email or export a dashboard to pdf file to verify that rebranding applied.

To restore original look and feel, run the script and replace"*True*" with "*False*" in the "*enabled*" section.

Customize Branding in Reports

By default, Netwrix Auditor reports look as follows:



Report branding is customized on Netwrix Auditor Server side that means that all clients connected to this server will have the same look and feel for reports.

Follow the steps to customize branding.

Step 1 – On the computer where Auditor Server resides, navigate to *C:\Program Data\Netwrix Auditor\Rebranding*.

Step 2 – Right-click the Rebranding.ps1 script and select Edit. Windows PowerShell ISE will start.

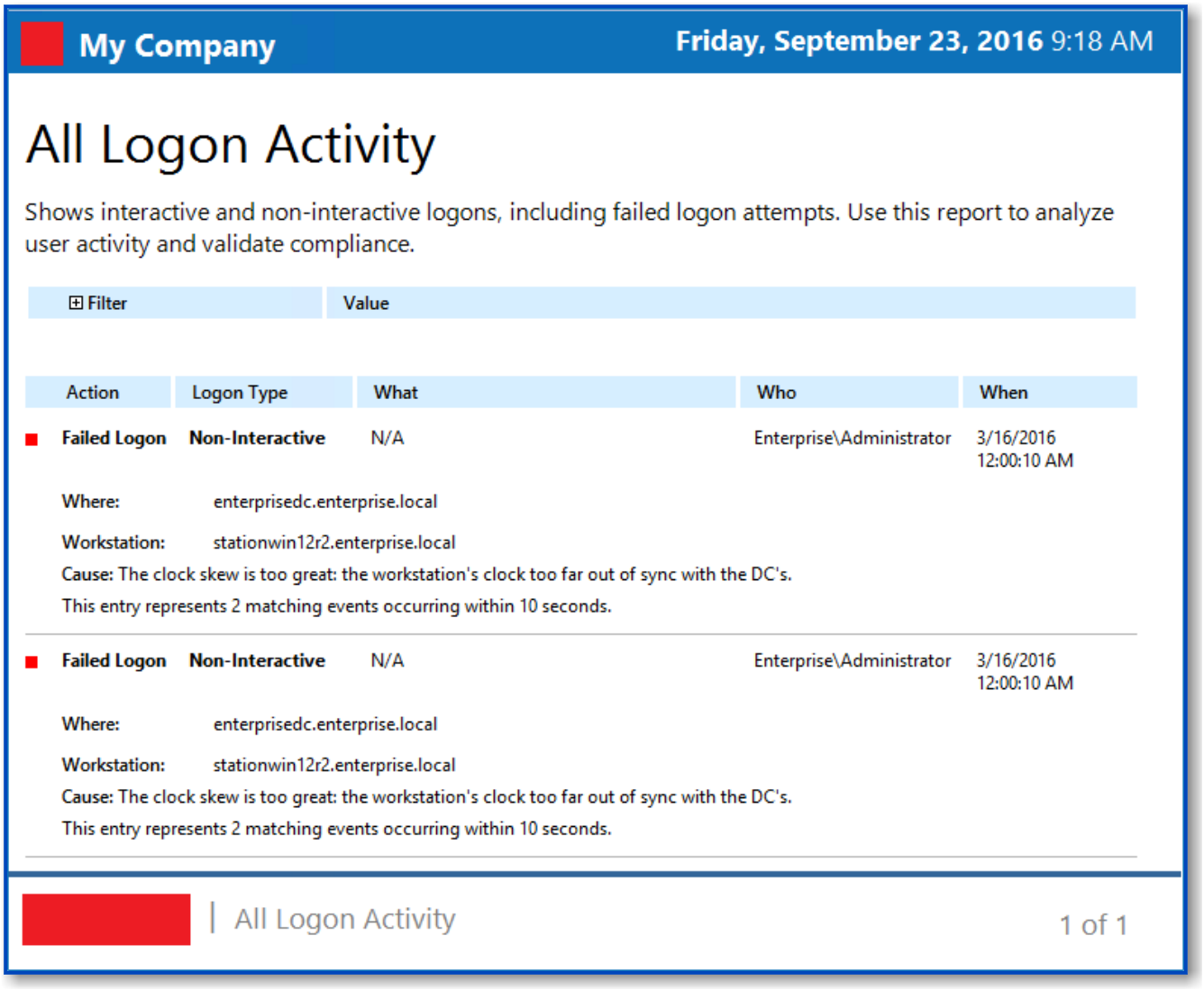
Step 3 – Review the script and provide parameters.

Parameter	Description
UseIntegratedSecurity	Defines whether to use Windows Authentication when connecting to SQL Server instance. Enabled by default.
UserName	Defines a username used to connect to SQL Server instance in case of SQL Server Authentication. Leave blank if you use Windows Authentication.
Password	Defines a password used to connect to SQL Server instance in case of SQL Server Authentication. Leave blank if you use Windows Authentication.
SQLServerInstance	Defines a SQL Server instance where your Audit Database resides. By default, local unnamed instance is selected.
DBName	By default, the database responsible for Netwrix Auditor look and feel is Netwrix_CommonDB. If you renamed this database, provide a new name.

Parameter	Description
HeaderImageFullPath	Defines a full path to the png image with the new report header (product logo). Supported size: 21x21px (WxH).
FooterImageFullPath	Defines a full path to the png image with the new report footer (logo). Supported size: 105x22px (WxH).
HeaderText	Defines text in the report header. Max length: 21 characters.
FooterURL	Defines URL that opens on clicking the report logo in the footer.

Step 4 – Click the arrow button to run the script. The user who runs the script is granted the db_owner role on the Netwrix_CommonDB database.

After running the script, start the Netwrix Auditor client and generate a report. The branding will be updated.



Follow the steps to restore original look.

Step 1 – On the computer where Auditor Server resides, navigate to the script location.

Step 2 – Right-click a script and select Edit. Windows PowerShell ISE will start.

Step 3 – Run the script as it is. The user who runs the script must be granted the db_owner role on the Common_DB database in a local unnamed SQL Server configured as default for Netwrix Auditor.

Monitoring Plans

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Supported Data Sources – Configure data source as required to be monitored

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan.

A monitoring plan defines data collection, notification, and storage settings.

To start collecting data, and add items to its scope.

Follow the steps to collect data from your environment.

Step 1 – Create a monitoring plan with the wizard. Select the data source when you start the monitoring plan wizard, and its initial settings are configured at the wizard steps. See the Create a New Monitoring Plan topic for additional information.

Step 2 – Fine-tune data source settings, if necessary: use the data source properties to modify data collection settings, customize the monitoring scope, and more.

Step 3 – Add items to be monitored. An item is a specific object you want to audit, e.g., a VMware server or a SharePoint farm. As soon as the item is added, to the monitoring plan, Auditor starts collecting data from it. See the Add Items for Monitoring topic for additional information.

Step 4 – To view and modify your plans, in the main Auditor window click the Monitoring Plans tile, then expand the All Monitoring Plans tree.

To..	Do..
See how data collection goes on	Click on a plan name. You will see all data sources included in the plan and data collection status for each data source.

To..	Do..
Start data collection manually	1. Select a plan and click Edit. 2. In the monitoring plan window, click Update in the right pane. Data collection will be started (status for the data sources will be displayed as *Working*). Do the same if you need to generate Activity Summary with the latest changes.
View collected data	1. Select a plan and click Edit. 2. In the right pane, go to the Intelligence section (in the bottom) and click Search. The search page will appear, displaying the collected data filtered out accordingly (i.e. provided by this monitoring plan).
Modify plan settings, add or delete data sources, add or delete items	Select a plan and click Edit. On the page that opens, review your plan settings. Then follow the instructions described in these sections: • Add Items for Monitoring • Fine-Tune Your Plan and Edit Settings
Assign roles	Click Delegate to review current delegations and assign roles. You can delegate control over a monitoring plan to another administrator, or grant read access—Reviewer role—to the data collected by this plan. To simplify delegation, you can further organize the monitoring plans into folders. See the Role-Based Access and Delegation topic for additional information.

Using historical data

For many data sources, you can instruct Netwrix Auditor to collect state-in-time data along with event data. For that, Netwrix Auditor uses state-in-time snapshots of the relevant system (for example, see VMware).

To keep users up-to-date on actual system state, Auditor updates the latest snapshot on the regular basis. Thus, only the latest snapshot is available for ongoing reporting in the product.

However, you may need to generate reports based on the historical data. For that, you must import the historical snapshots to the database.

To import snapshots, you must be assigned the *Global administrator* or the *Global reviewer* role.

Follow the steps to import historical snapshots.

Step 1 – Select the monitoring plan you need.

Step 2 – Select the required data source and click **Edit data source** on the right to open its properties.

Step 3 – Click **General** on the left.

Step 4 – In the **Manage historical snapshots** section, click **Manage**.

Step 5 – In the **Manage Snapshots** window, select the snapshots that you want to import — use the arrows to move the selected snapshots to the **Snapshots available for reporting** list. When finished, click **OK**.

See the Role-Based Access and Delegation topic for additional information.

Create a New Monitoring Plan

To create monitoring plans, user account must be assigned the *Global administrator* in Auditor. Users with the *Configurator* role can create plans only within a delegated folder. See the Role-Based Access and Delegation topic for additional information.

To start creating a plan, do any of the following:

- On the main Auditor page, in the Quick Start section, click the tile with a data source of your choice, e.g., Active Directory. If you need a data source that is not listed on the main page, click All data sources.
- On the main Auditor page, in the Configuration section, click the Monitoring Plans tile. On the Monitoring Plans page, select Add Plan.

Then follow the steps in the Monitoring Plan Wizard.

Step 1 – Choose a data source for monitoring.

Step 2 – Specify an account for collecting data.

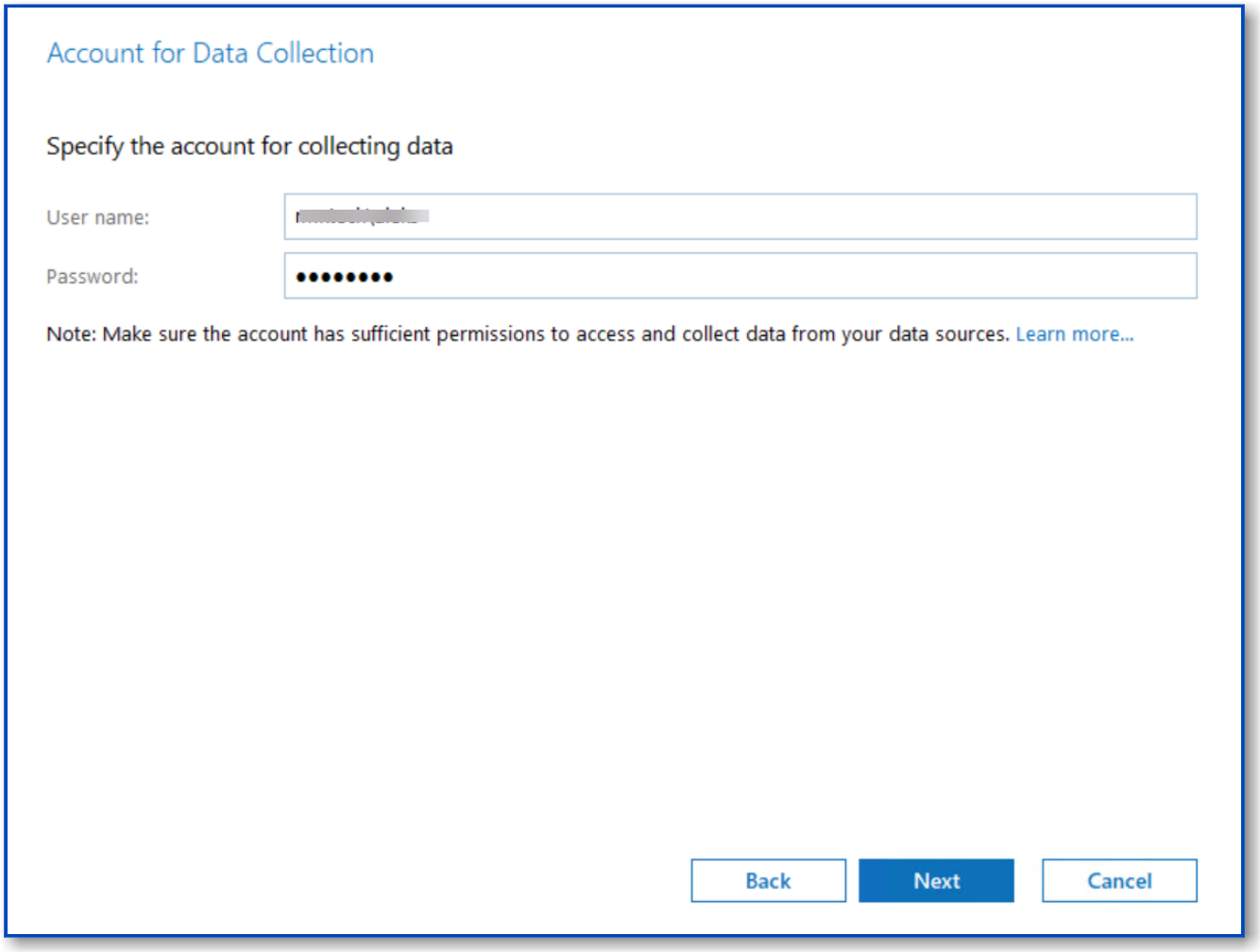
Step 3 – Specify default SQL Server instance and configure the Audit Database to store your data.

Step 4 – Configure notification settings.

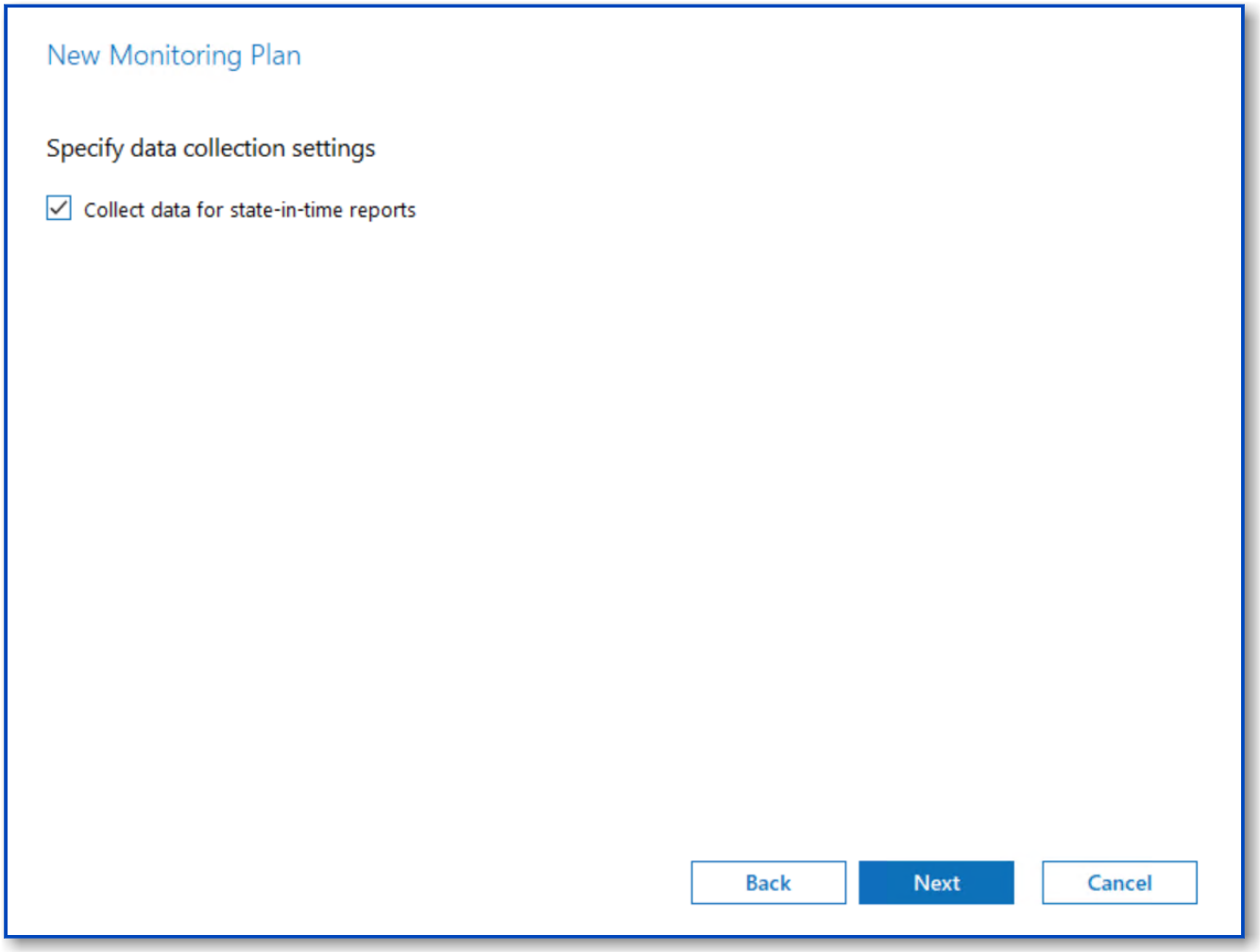
Step 5 – Specify the recipients who will receive daily activity summaries.

Step 6 – Specify a plan name.

Settings for Data Collection



At this step of the wizard, specify the account that Auditor will use to access the data source, and general settings for data collection.



Option	Description
Specify the account for collecting data	If applicable, you can create a data collecting account in the following ways: • Not specified – Select this option if you want to choose the Netwrix Privilege Secure as the data collecting account for the Monitoring Plan. See the Netwrix Privilege Secure topic for additional information. • User/password – Provide a username and password for the account that Auditor will use

Option	Description
	to collect data. By default, the user name is prepopulated with your account name. • gMSA – Use the group Managed Service Account (gMSA) as data collecting account. For more details about gMSA usage, see the Use Group Managed Service Account (gMSA) topic. **NOTE:** If you want to audit network devices or Microsoft Entra ID (formerly Azure AD)/Office 365 infrastructure, you need to use *not specified* account. Make sure the account has sufficient permissions to collect data. For a full list of the rights and permissions, and instructions on how to configure them, refer to theData Collecting Account. Netwrix recommends creating a special service account with extended permissions. When you configure a monitoring plan for the first time, the account you specify for data collection will be set as default.
Enable network traffic compression	If selected, this option instructs Auditor to deploy a special utility that will run on the audited computers and do the following: • Collect and pre-filter audit data • Compress data and forward it to Auditor Server. This approach helps to optimize load balance and reduce network traffic. So, using this option can be recommended especially for distributed networks with remote locations that have limited bandwidth. See the Network Traffic Compression topic for additional information.
Adjust audit settings automatically	Auditor can configure audit settings in your environment automatically. Select Adjust audit settings automatically. In this case, Auditor will continually check and enforce the relevant audit

Option	Description
	policies. For some data sources (currently, Active Directory and Logon Activity) you will be offered to launch a special utility that will detect current audit settings, check them against requirements and then adjust them automatically. See the Audit Configuration Assistant topic for additional information. You may also want to apply audit settings via GPO (for example, for Windows Servers). Auditor has certain limitations when configuring audit settings for NetApp and Dell Data Storage. See the File Servers topic for additional information. If any conflicts are detected with your current settings, automatic audit configuration will not be performed. Select this option if you want to audit file shares on NetApp Data ONTAP 7 and 8 in 7-mode. For NetApp Clustered Data ONTAP 8 and ONTAP 9, only audit settings for file shares can be configured automatically, other settings must be applied manually. If you plan to monitor EMC Isilon, clear the checkbox. Currently, Auditor cannot configure audit on Dell Isilon appliances automatically. If you want to audit Dell VNX/VNXe, select Adjust audit settings automatically, but only audit settings for file shares will configured, the rest of settings must be configured manually. For a full list of audit settings and instructions on how to configure them manually, see the Supported Data Sources for additional information.
Launch Audit Configuration Assistant	Click to launch a specially intended utility that will assess your environment readiness for monitoring and adjust audit settings, if necessary. The tool will be launched in a new window. See the Audit Configuration Assistant topic for additional information.

Option	Description
Collect data for state-in-time reports	State-in-time reports are based on the daily configuration snapshots of your audited systems; they help you to analyze particular aspects of the environment. State-in-time configuration snapshots are also used for IT risks assessment metrics and reports. This data collection option is available if you are creating a monitoring plan for any of the following data sources: • Active Directory • File Servers • Windows Server • Group Policy • SharePoint • SharePoint Online • Exchange Online • SQL Server • VMware See the State–In–Time Reports and IT Risk Assessment Overview topics for additional information.

Default SQL Server Instance

To provide searching, alerting and reporting capabilities, Auditor needs an SQL Server where audit data will be stored in the databases. To store data from the data sources included in the monitoring plan, the wizard creates an Audit Database for each plan. At this step, you should specify the default SQL Server instance that will host Auditor databases. See the Requirements for SQL Server to Store Audit Data topic for additional information.

Alternatively, you can instruct Auditor not to store data to the databases but only to the repository (Long-Term Archive) – in this scenario, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided.

Auditor skips this step if you have already configured Audit Database settings for other monitoring plans.

Select one of the following options:

- Disable security intelligence and make data available only in activity summaries — select this option if you do not want audit data to be written to the Audit Database. In this case, data will be available only in Activity Summary emails. Alerts, reports and search capabilities will not be supported.

  If you later clear this option to start saving data to the database, consider that already collected audit data will not be imported in that database.

- Install a new instance of Microsoft SQL Server Express automatically — this option is available at the first run of the wizard. It allows you to deploy SQL Server 2016 SP2 Express with Advanced Services on the local machine. This SQL Server will be used as default host for Auditor databases.

  It is strongly recommended that you plan for your databases first, as described in Requirements for SQL Server to Store Audit Data section. Remember that database size in SQL Server Express edition may be insufficient for your audited infrastructure.

- Use an existing SQL Server instance — select this option to use an existing SQL Server instance.

  Local SQL Server instance is detected automatically, and input fields are pre-populated with its settings.

  Complete the following fields:

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data. If you have more than one Auditor Server running in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Auditor Servers.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: ◦ Windows authentication ◦ SQL Server authentication

Option	Description
User name	Specify the account to be used to connect to the SQL Server instance. This account must be granted the **database owner (db_owner)** role and the dbcreator server role.
Password	Enter a password.

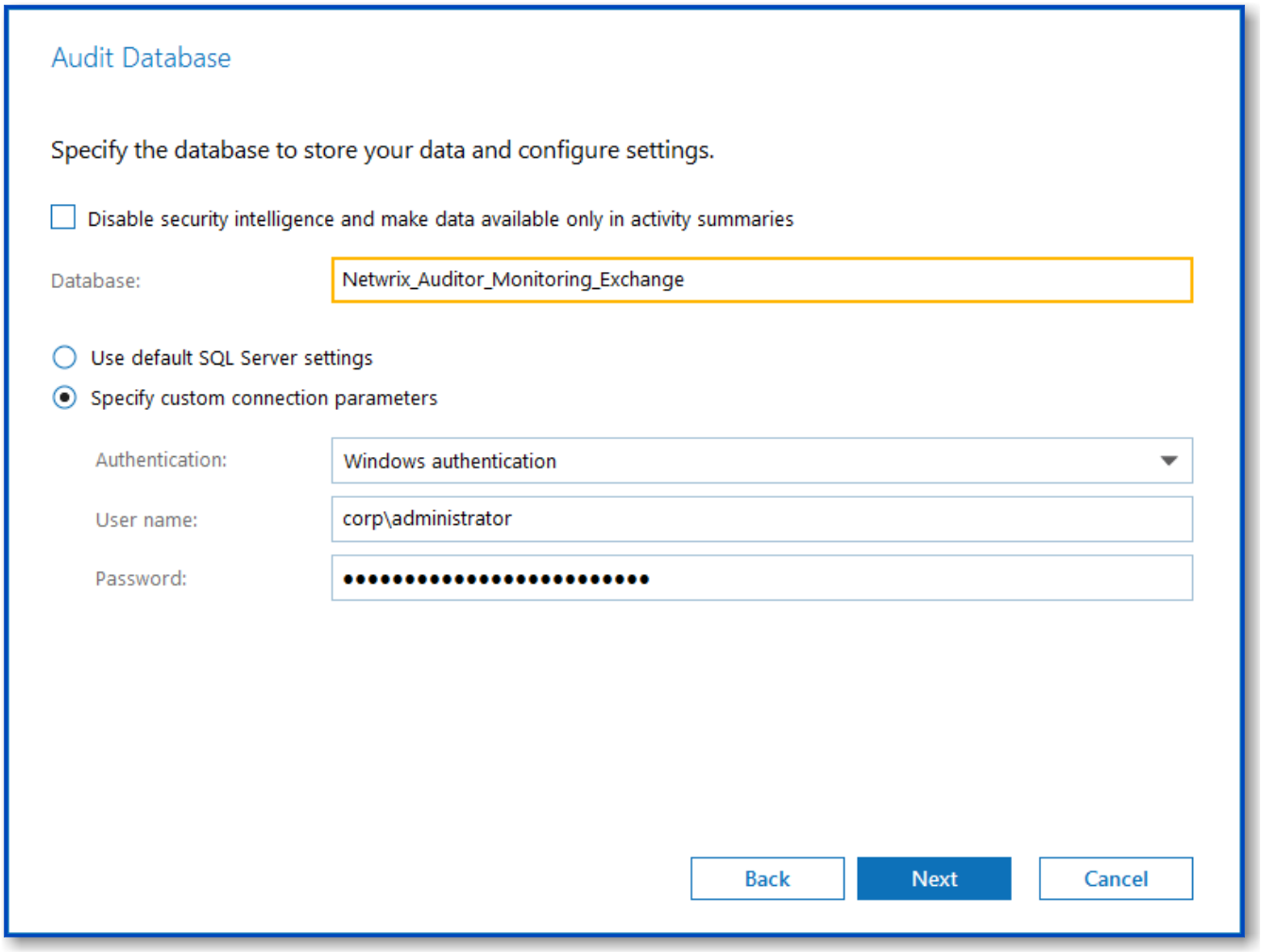
NOTE: If you want to use Group Managed Service Account (gMSA) to access the SQL Server instance hosting the database, consider that in this case Netwrix Auditor will not be able to generate SSRS-based reports (due to the following Microsoft article: Configure the Unattended Execution Account (Report Server Configuration Manager).

Database Settings

At this step, you need to specify a database where Netwrix Auditor will store data collected from the data sources included in this monitoring plan.

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

You can use default settings for your SQL Server instance or modify them (e.g., use a different authentication method or user). You can also change these settings later. See the Audit Database topic for additional information.



Configure the following:

Setting	Description
Disable security intelligence ...	Only select this option if you do not want your data to be stored in the database. In this case, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided. To store data to the database, leave this check box cleared.

Setting	Description
Database	Default database name is *Netwrix_Auditor_<monitoring_plan_name>*. It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g. *Exchange_Audit_Data* or *OracleSrv02_Audit_Data*), or so. If you decided to use the existing SQL Server instance instead of dedicated, you may want to use *Netwrix_Auditor* prefix to distinguish Netwrix Auditor databases from others.
Use default SQL Server settings	Select this option if you want Auditor to connect to the SQL Server instance using the default settings you specified at the Default SQL Server Instance step.
Specify custom connection parameters	Select this option to use custom credentials when connecting to SQL Server. Specify authentication method and the account that Auditor will use. Make sure this account has sufficient rights to connect to SQL Server and work with the databases.

Auditor will connect to the default SQL Server instance and create a database with the specified name on it.

Global settings that apply to all databases with audit data (including retention period and SSRS server used for reporting) are available on the Audit Database page of Auditor settings. See the Audit Database topic for additional information.

SMTP Server Settings

When you create the first monitoring plan, you are prompted to specify the email settings that will be used for activity and health summaries, reports and alerts delivery. For the monitoring plans that follow, Netwrix Auditor will automatically detect SMTP settings; however, for your

first plan you should provide them manually. See the Notifications topic for additional information.

You can skip this step if you do not want to receive email notifications, or configure SMTP settings later, as described in the related section.

Email Notification Recipients

Specify who will receive daily emails: Activity Summary Email on changes in the monitored infrastructure, and Health Summary Email on Auditor operations and health.

Click Add Recipient and provide email address.

RECOMMENDED: click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

Monitoring Plan Summary

At this step of the wizard, to provide a meaningful name and optional description for your monitoring plan.

To start collecting data, you should specify the objects (items) that belong to the target data source and should be processed according to the settings of this monitoring plan. For example, for Exchange data source the item will be your Exchange server, for Windows Server data source - computer, IP range or AD container, and so on. To add items right after finishing the monitoring plan wizard, select the Add item now checkbox. See the Add Items for Monitoring topic for additional information.

A monitoring plan cannot collect data until at least one item is specified.

Some data sources require additional system components and updates to be installed on your computer. In this case, Auditor will inform you and prompt you to check data source prerequisites instead of adding an item.

Once you complete the wizard, you can:

- Add items to your plan
- Add more data sources
- Customize data source's scope and settings (e.g., enable read access auditing)
- Fine-tune or modify plan settings
- Delegate control of the plan configuration or collected data to other users.

Manage Data Sources

You can fine-tune data collection for each data source. Settings that you configure for the data source will be applied to all items belonging to that data source. Using data source settings, you can, for example:

- Enable state-in-time data collection (currently supported for several data sources)
- Depending on the data source, customize the monitoring scope (e.g., enable read access auditing, monitoring of failed attempts)

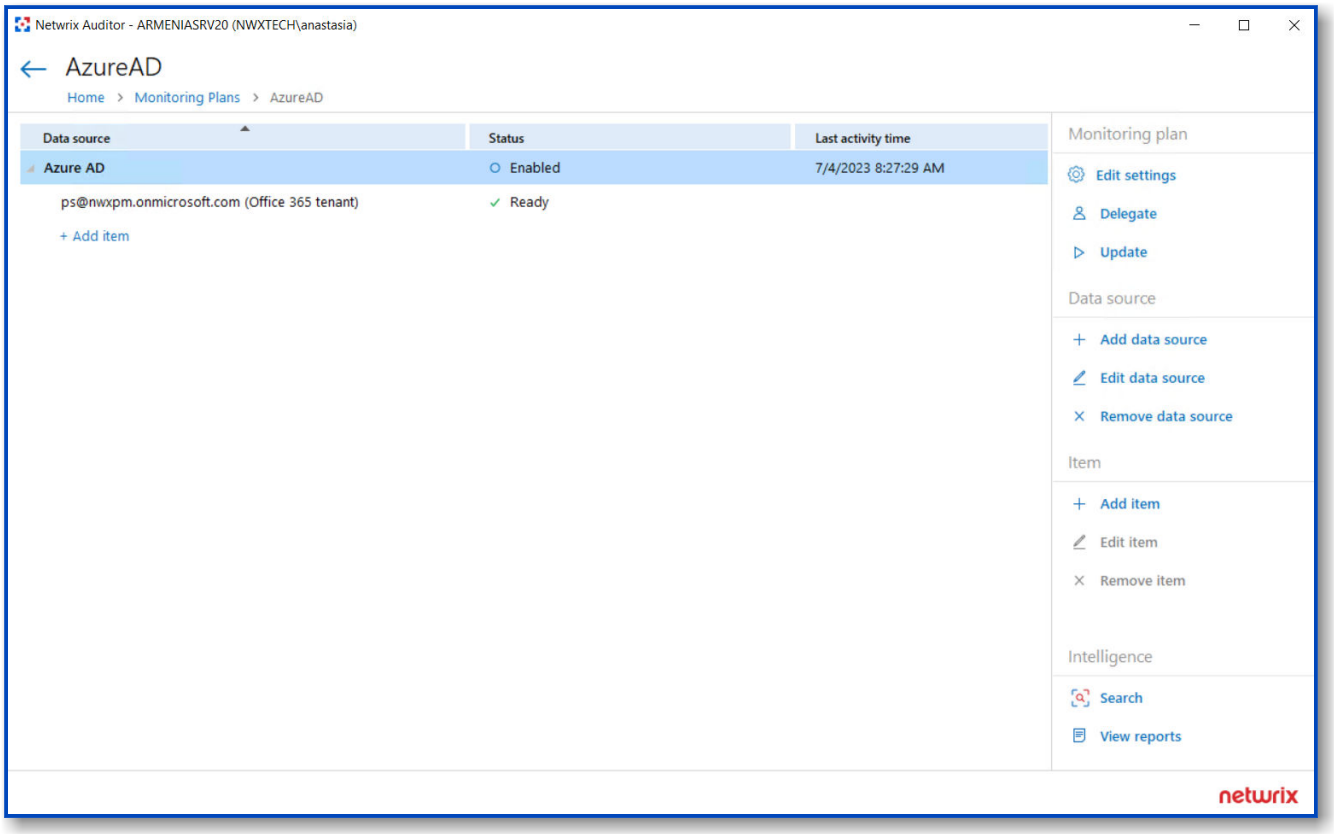
To add, modify and remove data sources, enable or disable monitoring, you must be assigned the Global administrator role in the product or the Configurator role on the plan. See the Role-Based Access and Delegation topic for additional information.

Modify Data Source Settings

Follow the steps to modify data source settings.

Step 1 – Select the monitoring plan you need and click **Edit**.

Step 2 – Within the monitoring plan window, highlight the data source (the first one is the row right under the blue table header) and click Edit data source on the right:



Step 3 – Modify data source settings as you need.

Step 4 – When finished, click **Save**.

Review the following for additional information:

- Active Directory
- Active Directory Federation Services
- Microsoft Entra ID
- Exchange
- Exchange Online
- File Servers
- Group Policy
- Logon Activity
- MS Teams

- Network Devices
- Oracle Database
- SharePoint
- SharePoint Online
- SQL Server
- User Activity
- VMware
- Windows File Share

Also, you can add a data source to the monitoring plan, or remove a data source that is no longer needed.

Add a Data Source to an Existing Plan

Follow the steps to add a data source to existing plan.

Step 1 – Select the monitoring plan you need and click Edit.

Step 2 – In the right pane, select Add data source.

Step 3 – Specify a data source.

Step 4 – Configure settings specific to your data source.

Step 5 – When finished, click the **Add** button to save the settings.

Add Items for Monitoring

Once you completed monitoring plan wizard and specified data sources, add items for monitoring. You can add as many items for a data source as you want. In this case, all items will share settings you specified for this data source.

Each data source has a dedicated item type. Netwrix Auditor automatically suggests item types associated with your data source.

Data Source	Item
Active Directory **Group Policy** **Exchange** **Logon Activity**	Domain
Active Directory Federation Services	Federation Server
Microsoft Entra ID **Exchange Online** **SharePoint Online** **Microsoft Teams**	Microsoft Entra ID
File Servers **(including Windows file server, Dell, NetApp, Nutanix File server, Synology, and Qumulo)**	AD Container File Servers Dell Isilon Dell VNX VNXe File Servers NetApp Windows File Share Nutanix SMB Shares Qumulo Synology By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-

Data Source	Item
	defined hidden shares, select the related option in the monitored item settings. Remember that administrative hidden shares like default system root or Windows directory (ADMIN$), default drive shares (D$, E$), etc. will not be monitored. See the topics on the monitored items for details.
Network Devices	Syslog Device Cisco Meraki Dashboard
Oracle Database	Oracle Database Instance
SharePoint	SharePoint Farm
SQL Server	SQL Server Instance SQL Server Availability Group
VMware	VMware ESX/ESXi/vCenter
Windows Server **User Activity**	File Servers AD Container File Servers
Netwrix API	Integration API

To add, modify and remove items, you must be assigned the Global administrator role in the product or the **Configurator** role on the plan. See the Role-Based Access and Delegationtopic for additional information.

Follow the steps to add a new item to a data source:

Step 6 – Navigate to your plan settings.

Step 7 – Click Add item under the data source.

Step 8 – Provide the object name and configure item settings.

You can fine-tune data collection for each item individually. To do it, select an item within your monitoring plan and click Edit item. For each item, you can:

- Specify a custom account for data collection
- Customize settings specific your item (e.g., specify SharePoint site collections)

Configure Monitoring Scope

In some environments, it may not be necessary to monitor the entire IT infrastructure. Netwrix monitoring scope can be configured on the Data Source and/or Item levels. the section below contains examples on how to use omit functionality in Auditor.

In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Use case	Related documentation
Active Directory	
I want to omit all activity by a specific service account or service accounts with specific naming pattern.	Active Directory
If Netwrix user is responsible just for a limited scope within corporate AD, s/he needs to omit everything else.	Active Directory

Use case	Related documentation
	• Always both activity and state in time data are omitted. • In group/Not in group filters don't not process groups from omitted OUs.
Logon Activity	
I want to omit domain logons by a specific service account or service accounts with specific naming pattern.	Logon Activity
File Servers **(including Windows file server, Dell, NetApp, Nutanix File server)**	
I have a server named *StationWin16* where I can't install .Net 4.5 in OU where I keep all member servers. I want to suppress errors from this server by excluding it from the Netwrix auditing scope.	AD Container
A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Then, s/he does not want the product to monitor this folder at all.	File Servers Dell Isilon Dell VNX VNXe NetApp Windows File Share Nutanix SMB Shares
A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this	File Servers

Use case	Related documentation
share. Then, s/he does not want the product to monitor this folder at all.	Dell Isilon Dell VNX VNXe NetApp Windows File Share Nutanix SMB Shares
A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Netwrix Auditor to collect State-in-Time data for this folder.	File Servers Dell Isilon Dell VNX VNXe NetApp Windows File Share Nutanix SMB Shares
I want to exclude specific computers within an IP range from the Netwrix auditing scope.	File Servers
SQL Server	
I want to know if *corp\administrator* user is messing with SQL data.	SQL Server Instance
As a Auditor administrator I want to exclude the *domain\nwxserviceaccount* service account activity from SQL server audit so that I get reports without changes made by automatic systems.	SQL Server Instance

Use case	Related documentation
As a Auditor administrator I want to exclude all changes performed by *MyCustomTool*.	SQL Server Instance
SharePoint	
I want to exclude the *domain\nwxserviceaccount* account from data collection as it produces standard activity that doesn't require monitoring.	SharePoint Farm
As a Auditor Administrator I want to exclude shared *PublicList* from read audit.	SharePoint Farm
I have a server named StationWin16 where I can't install .Net 4.5 in OU where I keep all member servers. I want to suppress errors from this server by excluding it from the Netwrix auditing scope.	**AD Container**
I want to exclude specific computers within an IP range from the Netwrix auditing scope.	**File Servers**
I have a virtual machine named "testvm" I use for testing purposes, so I want to exclude it from being monitored.	**VMware ESX/ESXi/vCenter**

Data Collecting Account

This is a service account that Auditor uses to collect audit data from the monitored items, such asdomains, OUs and servers. Netwrix recommends the creation of a dedicated service account for that purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements in the table below.

Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available:

- User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
- Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information.
- Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.
- Application and secret for Microsoft 365 with modern authentication.

Each data collecting accounts should meet the requirements from the table below, depending on the data source.

Data source	Required rights and permissions:
Active Directory	Permissions for Active Directory Auditing
Active Directory Federation Services	Permissions for AD FS Auditing
Microsoft Entra ID (formerly Azure AD), Exchange Online, SharePoint Online, MS Teams	Permissions for Microsoft Entra ID Auditing Permissions for Exchange Online Auditing Permissions for SharePoint Online Auditing Permissions for Teams Auditing
Exchange	Permissions for Exchange Auditing

Data source	Required rights and permissions:
Windows File Servers	Permissions for Windows File Server Auditing
Dell Isilon	Permissions for Dell Isilon/PowerScale Auditing
Dell VNX/VNXe/Unity	Permissions for Dell Data Storage Auditing
NetApp	Permissions for NetApp Auditing
Nutanix Files	Permissions for Nutanix Files Auditing
Qumulo	Permissions for Qumulo Auditing
Synology	Permissions for Synology Auditing
Network Devices	Permissions for Network Devices Auditing
Oracle Database	Permissions for Oracle Database Auditing
SharePoint	Permissions for SharePoint Auditing
SQL Server	Permissions for SQL Server Auditing
VMware	Permissions for VMware Server Auditing

Data source	Required rights and permissions:
Windows Server (including DNS and DHCP)	Permissions for Windows Server Auditing
Event Log (including IIS)—collected with Event Log Manager	Permissions for Windows Server Auditing
Group Policy	Permissions for Group Policy Auditing
Logon Activity	Permissions for Logon Activity Auditing
Inactive Users in Active Directory—collected with Inactive User Tracker	In the target domain • A member of the Domain Admins group
Password Expiration in Active Directory—collected with Password Expiration Notifier	In the target domain • A member of the Domain Users group
User Activity	On the target server • A member of the local Administrators group
Sensitive Data Discovery	Sensitive Data Discovery

Update Credentials for Account

Once a Data Collecting Account has been configured, you can always update the password for this account in Netwrix Auditor.

Follow the steps to update credentials for the accounts used by Auditor:

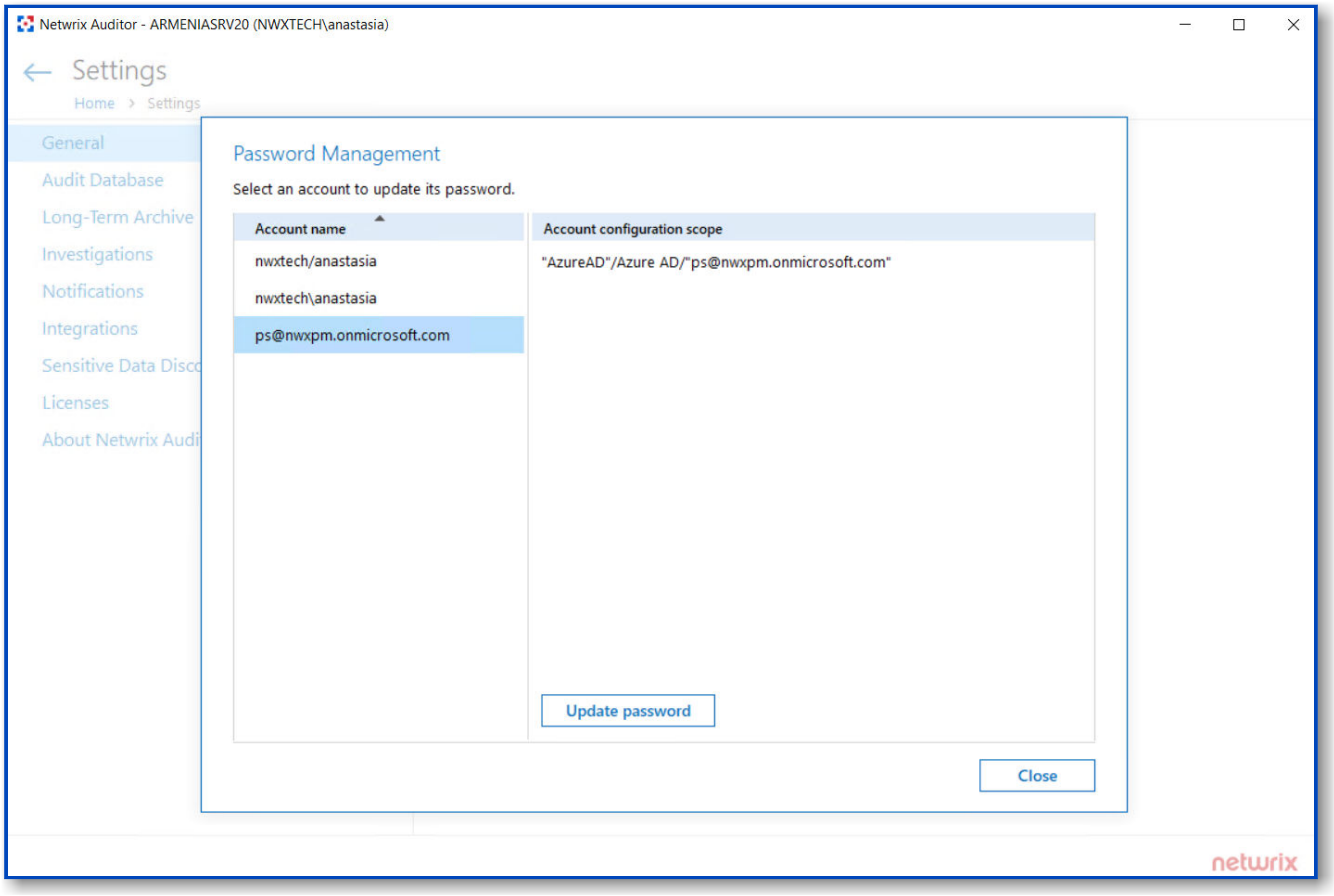
Step 1 – On the Auditor home page, navigate to **Settings**.

Step 2 – Locate the General tab.

Step 3 – Click the **Manage** button under **Accounts and Passwords**.

Step 4 – Select an account you want to update the password for.

Step 5 – Review the account configuration scope and click **Update password** next to this account.



Step 6 – Save your edits.

See the General topic for additional information.

Active Directory

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Active Directory – Configure data source as required to be monitored

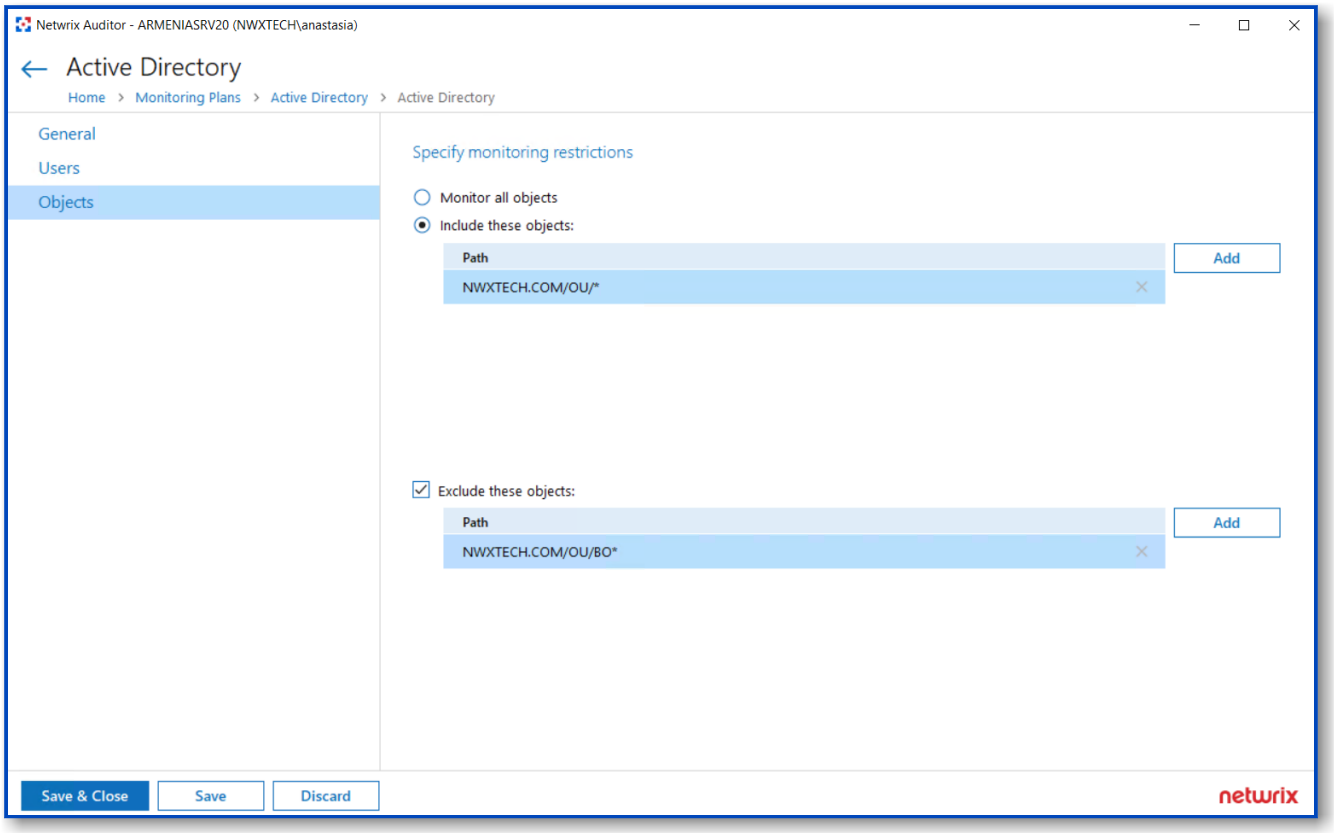
Complete the following fields:

Option	Description
General	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Monitor Active Directory partitions	Select which of your Active Directory environment partitions you want to audit. By default, Auditor only tracks changes to the Domain partition and the Configuration partition of the audited domain. If you also want to audit changes to the Schema partition, or to disable auditing of changes to the Configuration partition, select one of the following: • Domain—Stores users, computers, groups and other objects. Updates to this partition are replicated only to domain controllers within the domain. • Configuration—Stores configuration objects for the entire forest. Updates to this partition are replicated to all domain controllers in the forest. Configuration objects store the information on sites, services, directory partitions, etc. • Schema—Stores class and attribute definitions for all existing and possible Active Directory

Option	Description
	objects. Updates to this partition are replicated to all domain controllers in the forest. You cannot disable auditing the Domain partition for changes.
Detect additional details	Specify additional information to include in reports and activity summaries. Select Group membershipif you want to include Group membership of the account under which the change was made.
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the Active Directory configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them.
Collect data for state-in-time reports	Configure Auditor to store daily snapshots of your Active Directory domain configuration required for

Option	Description
	further state-in-time reports generation. See the State–In–Time Reports topic for additional information. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database. For that, in the Manage historical snapshots section, click **Manage** and select the snapshots that you want to import. To import snapshots, you must be assigned the Global administrator or the Global reviewer role . Move the selected snapshots to the Snapshots available for reporting list using the arrow button. When finished, click **OK**.
Users	
Specify monitoring restrictions	Specify user accounts to exclude from data collection (and, therefore, search results, reports and Activity Summaries). To add a user to the exclusion list, click Add, then provide the user name in the *domain**user* format. Consider the following: • Use NetBIOS format for domain name: *mydomain* • Some audit data (events) may contain *System* as the user (initiator) account name. To exclude such data, specify "*System*" when adding a user name here. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular

Option	Description
	audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.
Objects	
Specify monitoring restrictions	Specify restrictions for the objects to monitor in your Active Directory. Use them to create the lists of specific objects to include and / or exclude from the monitoring scope (and, therefore, search results, reports and Activity Summaries). The following options are available: • Monitor all objects • **Include these objects** • **Exclude these objects** To create a list of inclusions / exclusions, click Add and enter object path using one of the following formats: • Canonical name, for example: *mydomain.local/Computers/filesrv01* OR • Object path as shown in the "*What*" column of reports and search results, for example: *\local\mydomain\Computers\filesrv01* You can use a wildcard (*) to replace any number of characters in the path. See the examples below for more information.



Examples

The following examples explain how the exclusion rules work. Same logic applies to the inclusion rules.

- *dc11.local/OU* will exclude the OU itself. However, objects within this OU will not be excluded.
- *dc11.local/OU/** will exclude objects within the OU. However, the OU itself will not be excluded.
- *dc11.local/OU** will exclude the OU itself, all objects within it, and also all objects whose path begins with *dc11.local/OU* (like *dc11.local/OU_HQ*).

So, with the settings as in the screenshot above, the program will monitor all objects within the *OU*, except for the objects whose path begins with *enterprise.local/OU/BO*. The OU itself, however, will not be monitored, meaning that, for example, its renaming will not be reported.

In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Enable Auditing of Active Directory Partitions

This topic applies to auditing Active Directory only.

Active Directory environment consists of the following directory partitions:

- Domain partition — Stores users, computers, groups and other objects. Updates to this partition are replicated only to domain controllers within the domain.
- Configuration partition — Stores configuration objects for the entire forest. Updates to this partition are replicated to all domain controllers in the forest. Configuration objects store the information on sites, services, directory partitions, etc.
- Schema partition — Stores class and attribute definitions for all existing and possible Active Directory objects. Updates to this partition are replicated to all domain controllers in the forest.

By default, Netwrix Auditor only tracks changes to the Domain partition and the Configuration partition of the audited domain. If you also want to audit changes to the Schema partition, or to disable auditing of changes to the Configuration partition do the following:

You cannot disable auditing the Domain partition for changes.

To enable auditing of the Configuration and Schema partitions

- Navigate to All monitoring plans > your monitoring plan > Active Directory.
- In the right pane, click **Configure**, next to Advanced Options.
- In the Advanced Options dialog, select **Configuration** and **Schema**.

Information on changes to the selected partitions will be available in reports and will be saved in snapshots.

AD Container

Complete the following fields:

Option	Description
General	

Option	Description
Specify AD container	Specify a whole AD domain, OU or container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be audited within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Click **Exclude** to specify AD domains, OUs, and containers you do not want to audit. In the Exclude Containers dialog, click Add and specify an object. The list of containers does not include child domains of trusted domains. Use other options **(Computer, IP range** to specify the target computers.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. If using a group Managed Service Account (gMSA), you can specify only the account name in the *domain\account$* format. Password field can be empty. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information. Refer to the Permissions for Active Directory Auditing topic for more information on using Netwrix Privilege Secure as an account for data collection. A custom account must be granted the same permissions and access rights as the default account

Option	Description
	used for data collection. See theData Collecting Account topic for additional information.
Containers and Computers	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Depending on the type of the object you want to exclude, select one of the following: • Add AD Container – Browse for a container to be excluded from being audited. You can select a whole AD domain, OU or container. • Add Computer – Provide the name of the computer you want to exclude as shown in the "*Where*" column of reports and Activity Summaries. For example, *backupsrv01.mydomain.local*. Wildcards (*) are not supported. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion

Option	Description
	settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Domain

Complete the following fields:

Option	Description
Specify Active Directory domain	Specify the audited domain name in the FQDN format. For example, "*company.local*".
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available: • User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information. • Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information. • Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.

Refer to the Permissions for Active Directory Auditing topic for more information on using Netwrix Privilege Secure as an account for data collection.

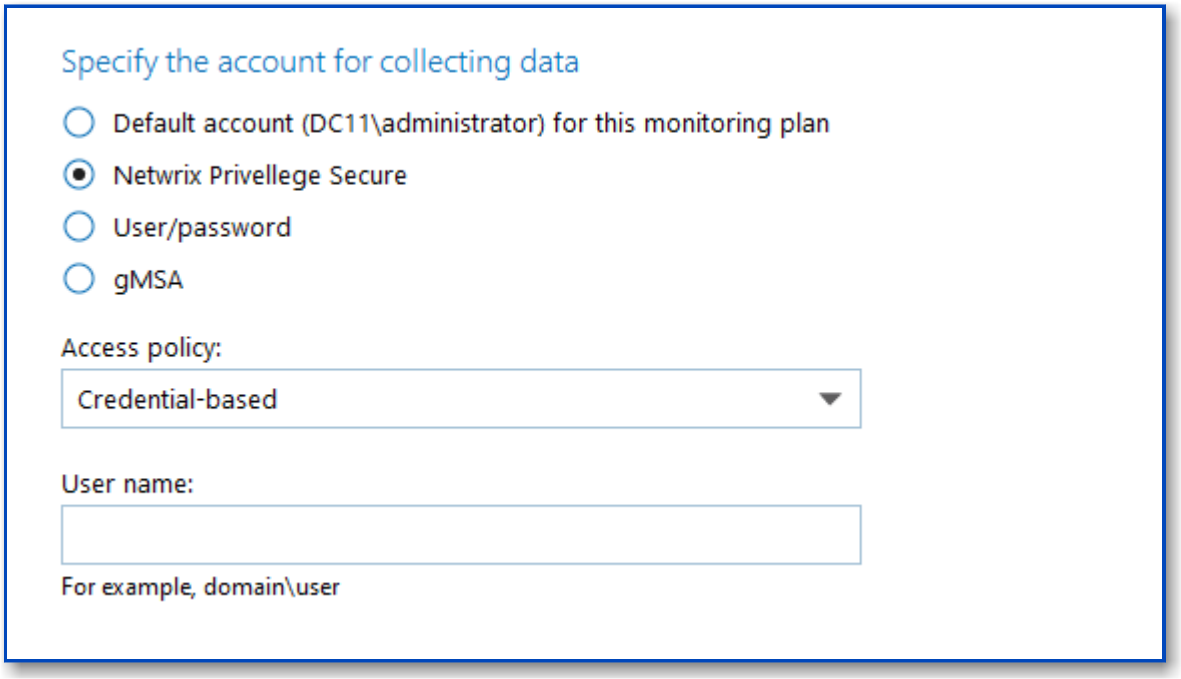
Use Netwrix Privilege Secure as a Data Collecting Account

Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

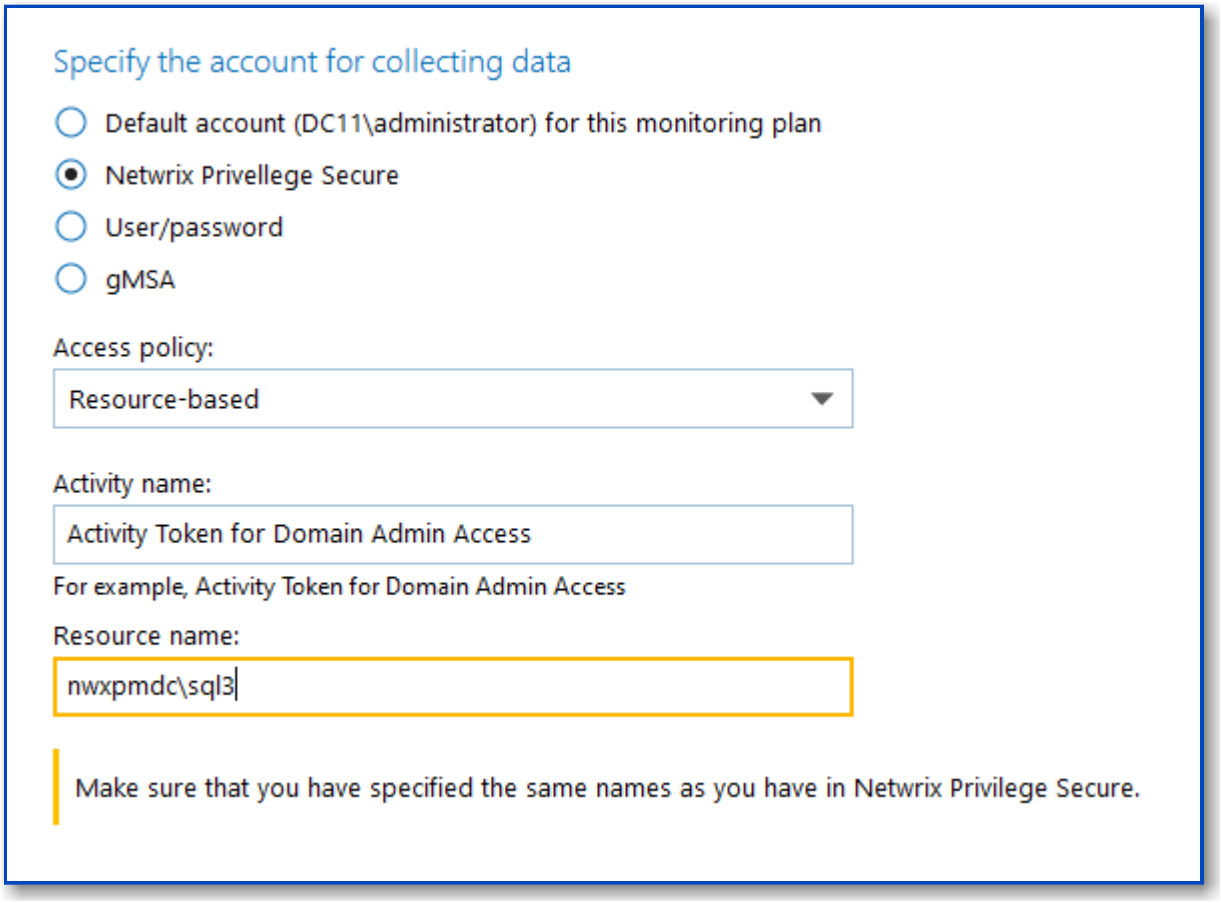
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

Active Directory Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Active Directory monitoring scope. You can apply restrictions to monitoring scope via the UI. See the Objects topic for additional information.

RECOMMENDED: Configure monitoring scope restrictions on the Active Directory monitoring plan page. See the Active Directory topic for additional information.

Follow the steps to exclude data from the Active Directory monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

addprops.txt	Contains a list of properties that should be included for newly created AD objects.
	
	When a new object is added, Auditor does not show any data in the Details column in the Activity Summary emails. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.
		`Object type:property:`
		
		For example, to show a group description on this group's creation, add the following line:
		`group:description:`

allowedpathlist.txt	Contains a list of AD paths to be included in Activity Summaries, reports, and search results.	`Path` The path must be provided in the same format as it is displayed in the What column. For example, if you only want to monitor specific OU(s)

File	Description	Syntax
		in the AD domain, but not the entire domain. You can put a wildcard (*) in the omitpathlist.txt file to exclude all paths, and then specify the OU(s) you want to monitor in the allowedpathlist.txt file. Adding the widlcard (*) to omitpathlist.txt will not allow Netwrix Auditor to run AD state-in-time data collection.
omitallowedpathlist.txt	Contains a list of AD paths to be excluded from Activity Summaries, reports, and search results. This file can be used if you want to exclude certain paths inside those specified in the allowedpathlist.txt file.	`Path` The path must be provided in the same format as it is displayed in the What column. For example, you can put a wildcard (*) in the omitpathlist.txt file to exclude all paths, then specify the OU(s) you want to monitor in the allowedpathlist.txt file, and then specify the paths you want to exclude from within them in the omitallowedpathlist.txt file. Adding the widlcard (*) to omitpathlist.txt will not allow Netwrix Auditor to run AD state-in-time data collection.
omitexchangeserverlist.txt	Specify the Microsoft Exchange 2010 servers to be excluded from data collection.	`FQDN_server_name` **NOTE:** You can use the wildcard (*) when specifying servers for exclusion.

File	Description	Syntax
omitobjlist.txt	Contains a list of object types to be excluded from Activity Summaries, reports, and search results.	`Object type` For example, to omit changes to the printQueue object, add the following line: `printQueue`.
omitpathlist.txt	Contains a list of AD paths to be excluded from Activity Summaries, reports, and search results.	`Path` The path must be provided in the same format as it is displayed in the What column. For example, to exclude changes to the Service Desk OU, add the following line: `*\Service Desk\*`.
omitproplist.txt	Contains a list of object types and properties to be excluded from Activity Summaries, reports, and search results.	`object_type.property_name` If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example to exclude the adminCount property from reports, add the following line: `*.adminCount`.
omitreporterrors.txt	Contains a list of errors to be excluded from Netwrix Health Log. Thus, these errors will not appear in the Activity Summary emails.	`Error message text` For example, if you have advanced audit settings applied to your domain controllers policy, the following error will be returned in the Activity Summary emails:

File	Description	Syntax
		`Auditing of Directory Service Access is not enabled for this DC. Adjust the audit policy settings using the Active Directory Audit Configuration Wizard or see the product documentation for more information.` Add the text of this error message to this file to stop getting it in the Activity Summary emails.
omitsnapshotpathlist.txt	Contains a list of AD paths to be excluded from AD snapshots.	`Path` The path must be provided in the same format as it is displayed in the What column. For example, to exclude data on the Disabled Accounts OU from the Snapshot report, add the following line: `*\Disabled Accounts*`.
omitstorelist.txt	Contains a list of object types and properties to be excluded from AD snapshots.	`object_type.property_name` If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example to exclude data on the AD adminDescription property, add the following line: `*.adminDescription`.

File	Description	Syntax
omituserlist.txt	Contains a list of users you want to exclude from search results, reports and Activity Summaries.	`domain\username` For example, `*\administrator`.
processaddedprops.txt	Contains a list of properties that should be included for newly created AD objects. When a new object is created, Auditor does not show any data in the Details column in reports. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.	`object type:property:` For example, if you want a user's Description property to be displayed in the reports when a user is added, add the following line: `User:Description:`
processdeletedprops.txt	Contains a list of properties that should be included for deleted AD objects. When an object is deleted, Auditor does not show any data in the Details column in reports. If you want to see the information on certain attributes of a deleted object, specify these attributes in this file.	`object type:property:` For example, if you want a user's Description property to be displayed in the reports when a user is deleted, add the following line: `User:Description:`
propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in Activity Summaries, reports, and search results.	`classname.attrname=intelligiblename` For example, if you want the adminDescription property to be displayed in the reports as Admin Screen Description, add the following line: `*.adminDesciption=Admin Screen Description`

Example

To exclude the "*corp/Administrator*" user from being audited, use the following syntax in the **omitusers.txt** file:

```
# Specify users whose activity you want to exclude from Active Directory
 search results, reports and Activity Summaries.# Syntax: Domain\Usernam
e# Note: Wildcard * is supported and can replace any number of character
s.# Example:# Corp\Administrator
```

Active Directory Federation Services

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- AD FS – Configure data source as required to be monitored

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Schedule AD FS logons collection	Specify period for AD FS logons collection.
Specify data collection method	You can enable network traffic compression. If enabled, a Compression Service will be automatically launched on the audited computer, collecting and pre-filtering data. This significantly improves data transfer

Option	Description
	and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. Do not select the checkbox if you want to configure audit settings manually. For a full list of audit settings required to collect comprehensive audit data and instructions on how to configure them, refer to AD FS.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Federation Server

If you are going to audit an entire AD FS farm, consider adding all AD FS server one by one as items to your monitoring plan. Otherwise, your audit scope may contain warnings, errors or incomplete data.

Complete the following fields:

Option	Description
Specify AD FS federation server	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network.

Option	Description
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

Microsoft Entra ID

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Microsoft Entra ID – Configure data source as required to be monitored

You can use the following data collecting account options:

- Username and password.
- Integration with the Netwrix Privilege Secure. See the Netwrix Privilege Secure and How to Add Microsoft Entra ID Monitoring Plan Using Netwrix Privilege Secure topics for additional information.
- Application and secret for Microsoft 365 with modern authentication.

To add a new monitoring plan for Entra ID, you need to launch the New Monitoring Plan wizard, either from the Home screen, or from the Monitoring plans menu under the All Monitoring Plans section.

Configure Data Source Settings

Default data source settings will be configured during the completion of the New Monitoring Plan wizard. To customize the settings, you need to open your monitoring plan, and click **Edit data source** on the right side of the screen.

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Monitor Microsoft Entra ID logon activity	Specify what types of logon events you want to monitor: successful or failed, performed through Windows and SQL authentication. • Failed logons • Successful logons
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

This instruction shows how to collect audit data from the Microsoft 365 tenant.

If you plan to use modern authentication, see the Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID topic for additional information on how to prepare Microsoft Entra ID app with required permissions. Make sure you have the following at hand:

- Tenant name
- For modern authentication: Application (client) ID
- Application secret

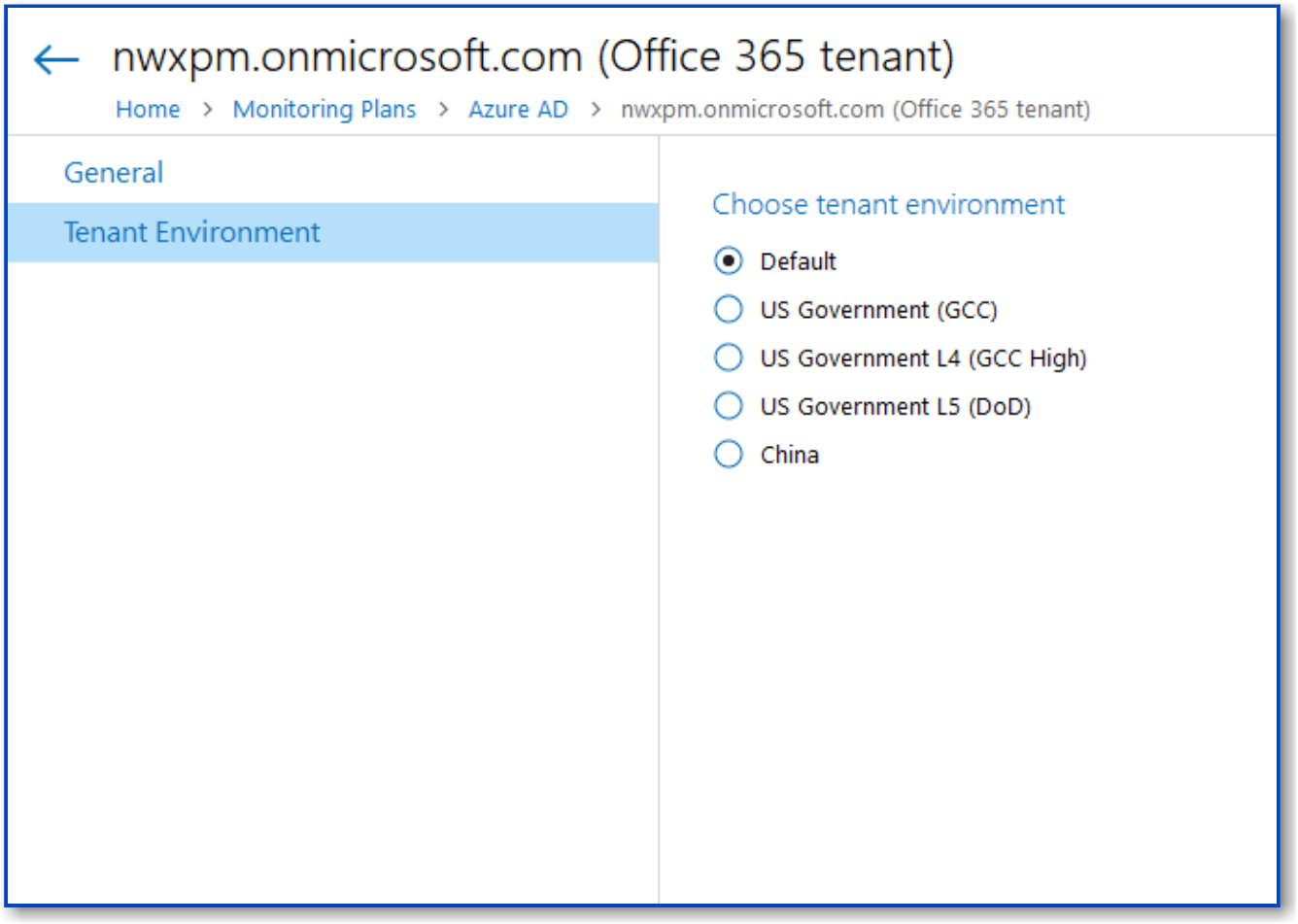
- For basic authentication: User name and password

Types of data that can be collected by Netwrix Auditor from the Microsoft 365 tenant depend on the authentication option you choose.

Follow the steps to configure Office 365 tenant as a monitored item.

Step 1 – On the **General** page of the item properties, specify **Tenant name**:

- If you are going to use **Basic authentication**, you can proceed to the next step – **Tenant name** will be filled in automatically after it.
    - **NOTE:** Basic authentication is no longer possible for Exchange Online. For the already existing tenants it is still possible to use basic authentication for SharePoint Online and Microsoft Entra ID monitoring.
- If you are going to use **Modern authentication**, paste the obtained name. See the Using Modern Authentication with Microsoft Entra ID topic for additional information.

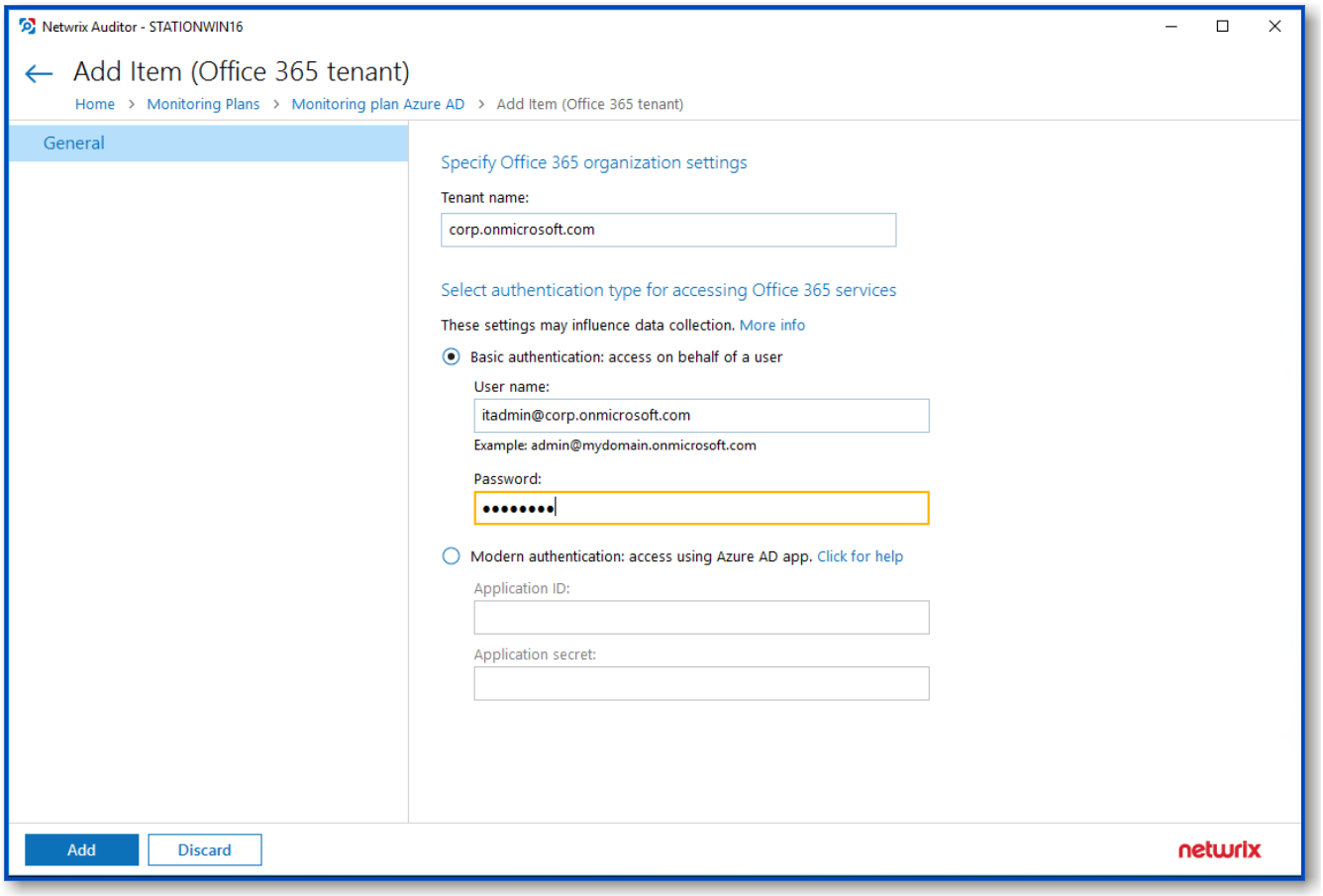


If you are using a government tenant, please click the **Tenant Environment** tab and select the desired tenant environment.

Step 2 – Select authentication method that will be used when accessing Office 365 services:

- Basic authentication:
  - Selected, Office 365 organization will be accessed on behalf of the user you specify.
  - Enter **User name** and **password**; use any of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*.
  - The **Tenant name** field then will be filled in automatically.
  - Make sure this user account has sufficient access rights. See Using Basic Authentication with Microsoft Entra ID topic for additional information.
- Modern authentication:
  - Selected, Office 365 organization will be accessed using the Microsoft Entra ID (formerly Azure AD) app you prepared. Enter:
    - **Application ID**;
      - **Application secret**.
  - See the Using Modern Authentication with Microsoft Entra ID for additional information.

Step 3 – Click the **Add** button.



You can use a single account to collect audit data for different Office 365 services (Microsoft Entra ID, Exchange Online, SharePoint Online); however, Netwrix recommends that you specify individual credentials for each of them.

How to Add Microsoft Entra ID Monitoring Plan Using Netwrix Privilege Secure

NOTE: Netwrix Privilege Secure resource-based integration works only with basic authentication. Ephemeral accounts will be created or elevated to be used as data collecting accounts. If you want to use modern authentication and the Netwrix Privilege Secure integration, you need to choose a credential-based access policy, save your application and secret in Netwrix Privilege Secure, and provide the Application ID instead of the user name.

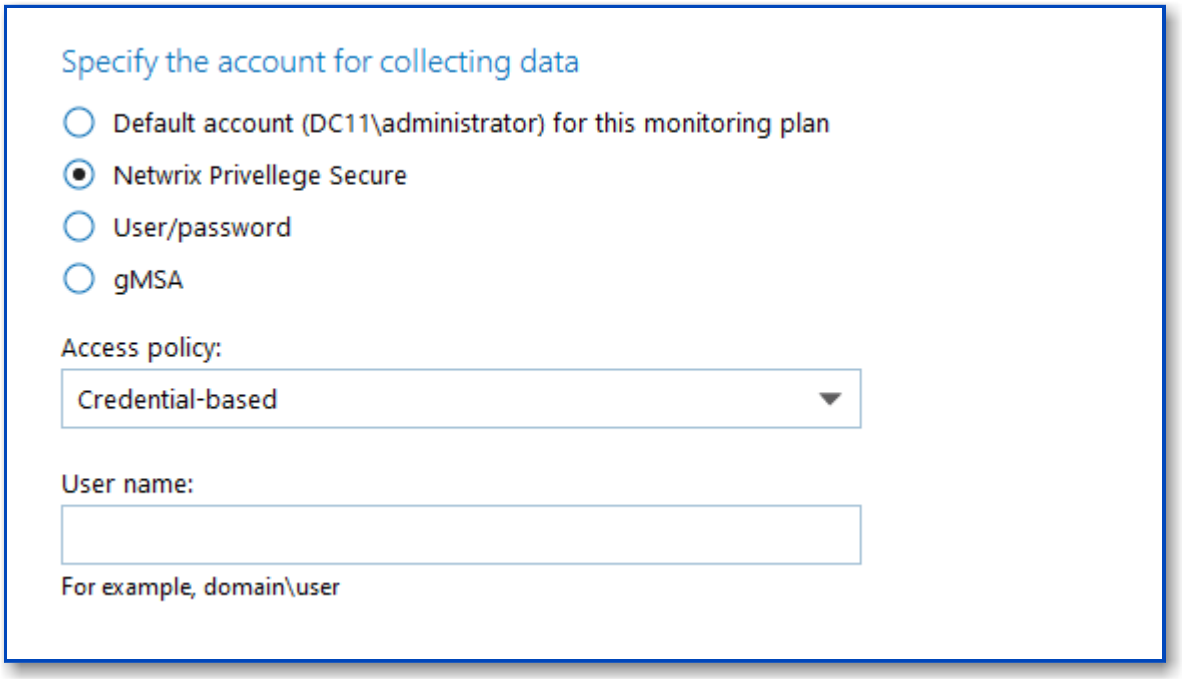
Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix

Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

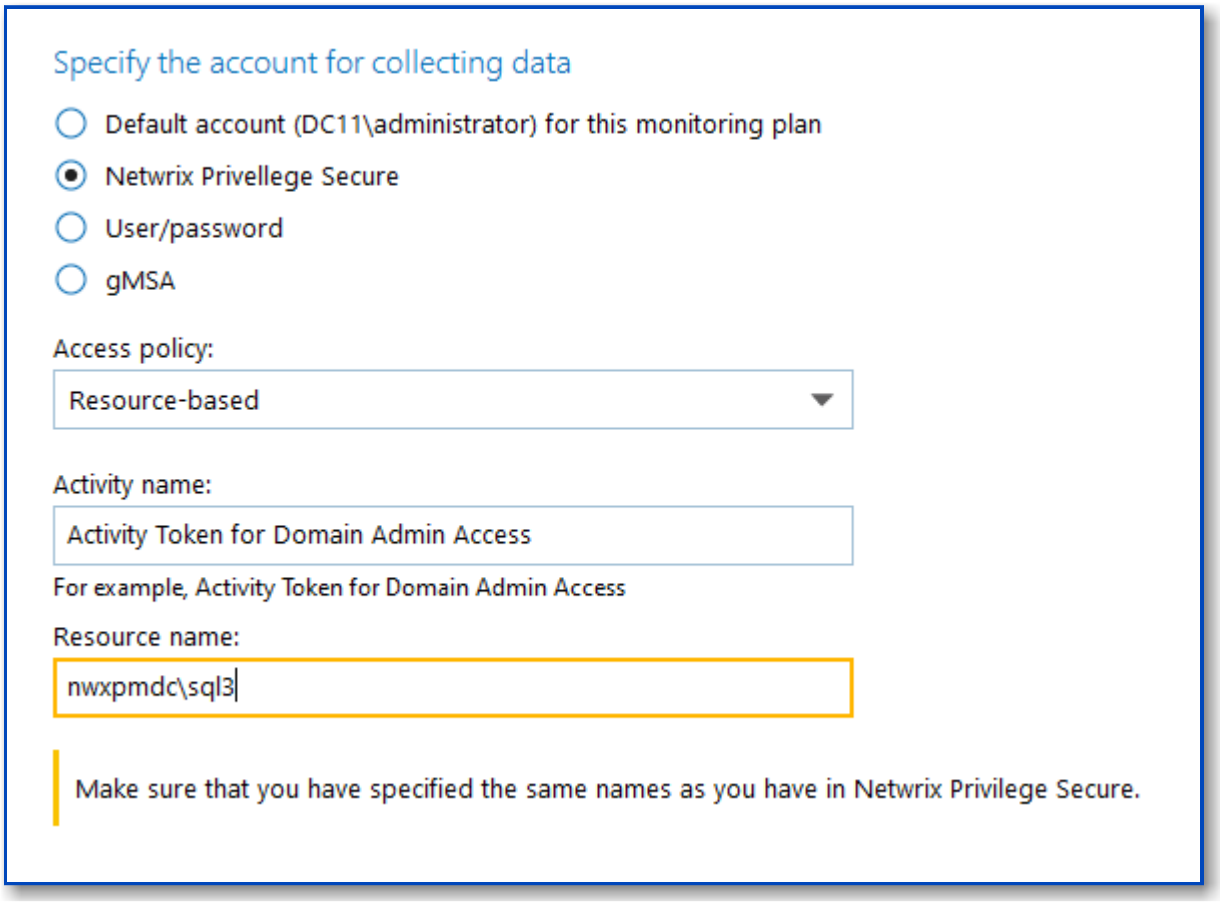
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

Microsoft Entra ID Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Microsoft Entra ID (formerly Azure AD) monitoring scope or modify the way it will be displayed.

NOTE: Omitting user accounts does not decrease the license consumption count for Microsoft Entra ID.

Follow the steps to exclude data from the Microsoft Entra ID monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Azure AD Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omituserlist.txt	Contains a list of users you want to exclude from Microsoft Entra ID search results, Azure AD Changesreports and Activity Summaries.	user@tenant.com
adomiteventuserlist.txt	Contains a list of users whose user names you want to exclude from Microsoft Entra ID search results, reports and Activity Summaries. The rest of change details (action, object type, etc.) will be reported, but the Who value will be "system".	user@tenant.com
exomiteventuserlist.txt	Contains a list of Exchange whose user names you want to exclude from Microsoft Entra ID search results, reports and Activity Summaries. The rest of change details (action, object type, etc.) will be reported, but the Who value will be "system". This list omits changes made by users through Exchange admin center.	user@tenant.com
maapioperationtypes.txt	Contains an overall list of object types that will be displayed in search results, reports, and Activity	operation = object type For example:

File	Description	Syntax
	Summaries for each particular operation. By default, the list contains mapping for the most frequent operations (e.g., add user, update policy, remove member). The rest will be reported with Microsoft Entra ID object object type.	add owner to group = Group
omitproplist.txt	Contains a list of object classes and attributes to be excluded from Microsoft Entra ID search results, reports and Activity Summaries.	classname.attrname If there is no full stop, the entire line is considered a class name.
propnames.txt	Contains a list of human-readable names for object types and attributes to be displayed in search results, reports, and Activity Summaries.	object=friendlyname object.property=friendlyname For example: *.PasswordChanged = Password Changed
proptypes.txt	Defines how values will be displayed in the Details columns in Microsoft Entra ID search results, reports, and Activity Summaries.	For example: *.Role.DisplayName = MultiValued

Exchange

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections

- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Exchange – Configure data source as required to be monitored

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Detect additional details	Specify additional information to include in reports and activity summaries. Select Group membershipif you want to include Group membership of the account under which the change was made.
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the Exchange configuration topic for additional information about audit settings required to collect

Option	Description
	comprehensive audit data and the instructions on how to configure them.
Collect data on non-owner access to mailboxes	Enable monitoring of unauthorized access to mailboxes within your Exchange Online organization. Configure the following: • Notify users if someone gained access to their mailboxes—Select this checkbox if you want to notify users on non-owner access to their mailboxes. • Notify only specific users—Select this checkbox and click Add Recipient to specify the list of users who will receive notifications on non-owner access to their mailboxes. Users not included in this list will not be notified. • Enable automatic audit configuration— If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. See the Exchange and Exchange Online topics for additional information about the audit settings required for Auditor to collect comprehensive audit data and instructions on how to configure them. 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.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Domain

Complete the following fields:

Option	Description
Specify Active Directory domain	Specify the audited domain name in the FQDN format. For example, "*company.local*".
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available: • User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information. • Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information. • Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.

See the Permissions for Exchange Auditing topic for additional information.

Exchange Monitoring Scope

You can fine-tune Auditor by specifying data that you want to exclude from the Exchange monitoring scope. In addition, you can exclude data from non-owner access auditing.

- Exchange Monitoring Scope
- To exclude users or mailboxes from the Mailbox Access monitoring scope

Follow the steps to exclude data from the Exchange monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

aal_omitlist.txt	For Exchange 2010 and above, the file contains a list of changes performed by cmdlets. To exclude a change from reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`cmdlet.attrname`
		For example:
		`Set-User`
		`Set-ContactSet-Group`
		`#Update-AddressList`
		`Add-ADPermissionRemove-ADPermission`
		`#RBAC:`
		`*-MailboxAuditLogSearch`
		`*-AdminAuditLogSearch`

aal_propnames.txt	For Exchange 2010 and above, the file contains a list of human-readable names of changed attributes to be displayed in change reports. To exclude a change from the reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`classname.attrname=intelligiblename`
		For example:
		`*-OutlookAnywhere.SSLOffloading = Allow secure channel (SSL) offloading`

omitobjlist_ecr.txt	Contains a list of human-readable names of object classes to be excluded from change reports.	`Classname` For example:

File	Description	Syntax
		exchangeAdminService msExchMessageDeliveryConfig Exchange_DSAccessDC
omitpathlist_ecr.txt	Contains a list of AD paths to be excluded from change reports.	Path For example: *\Microsoft Exchange System Objects\SystemMailbox*
omitproplist_ecr.txt	Contains a list of object types and properties to be excluded from change reports.	object_type.property_name If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example: msExchSystemMailbox.* *.msExchEdgeSyncCredential *.msExchMailboxMoveTargetMDBLink *.adminDescription
omitreporterrors_ecr.txt	Contains a list of errors to be excluded from Activity Summaries.	Error message text For example, to omit the error “The HTTP service used by Public Folders is not available, possible causes are that Public stores are not mounted and the Information Store service is

File	Description	Syntax
		not running. ID no: c1030af3", add `*c1030af3*` to the file.

omitstorelist_ecr.txt	Contains a list of classes and attributes names to be excluded from Exchange snapshots.	`object_type.property_name`
		
		If there is no separator (.) between an object type and a property, the whole entry is treated as an object type.
		
		For example:
		
		`Exchange_Server.AdministrativeGroup`
		
		`Exchange_Server.AdministrativeNote`
		
		`Exchange_Server.CreationTime`

propnames_ecr2007.txt	Contains a list of human-readable names for object classes and attributes of Exchange 2007 to be displayed in change reports.	`classname.attrname=intelligiblename`
		
		For example:
		
		`msExchMDBAvailabilityGroup= Database Availability Group`

To exclude users or mailboxes from the Mailbox Access monitoring scope

Auditor allows specifying users and mailboxes that you do not want to monitor for non-owner mailbox access events. To do this, edit the mailboxestoexclude.txt, userstoexclude.txt, and agentomitusers.txt files.

Follow the steps to exclude data from Exchange Online monitoring scope

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Non-owner Mailbox Access Reporter for Exchange* folder.

Step 2 – Edit mailboxestoexclude.txt, userstoexclude.txt, or agentomitusers.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

You can also limit your reports by specific mailboxes. Edit the mailboxestoinclude.txt file to specify mailboxes.

File	Description	Syntax
mailboxestoexclude.txt	This file contains a list of mailboxes and folders that must be excluded from data collection.	Each entry must be a separate line. Wildcards (*) can be used to replace any number of characters. • To exclude the certain user's mailbox, enter `username@domainname`, e.g. `john.smith@acme.com` • To exclude the certian folder, enter `username@domainname/foldername`, e.g. `john.smith@acme.com/Drafts` • Use *to exclude multiple mailboxes or folders, e.g. `*/foldername` will exclude the specified folder when processing all mailboxes. Examples: `*admin*@corp.com` `*/Drafts` - exclude *Drafts* folder (for all mailboxes) `*/Testfolder/*` - exclude subfolders of *Testfolder* (for all mailboxes)

File	Description	Syntax
mailboxestoinclude.txt	This file contains a list of mailboxes that must be included when collecting data. For the mailboxes added to this list, the reports will contain only non-owner access events.	Specify email address to be included in the list as `username@domainname.` Example: `analyst@enterprise.com`
userstoexclude.txt	This file contains a list of users who must be excluded from reports if they perform non-owner access attempt for mailboxes (audit data on these users will still be stored in the state-in-time snapshots). If a user is removed from this list, the information on this user's actions can be viewed with the Report Viewer.	`DOMAIN\username`
agentomitusers.txt	This file contains a list of users who must be excluded from reports and snapshots. If a user is removed from this list, audit data on this user will only be available after the next data collection. Writing new users to this file affects reports and snapshots only if Network traffic compression is enabled.	`DOMAIN\username`

Exchange Online

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Exchange Online – Configure data source as required to be monitored

How to add Exchange Online Monitoring Plan

This instruction shows how to collect audit data from the Microsoft 365 tenant.

If you plan to use modern authentication, see the Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID topic for additional information on how to prepare Microsoft Entra ID app with required permissions. Make sure you have the following at hand:

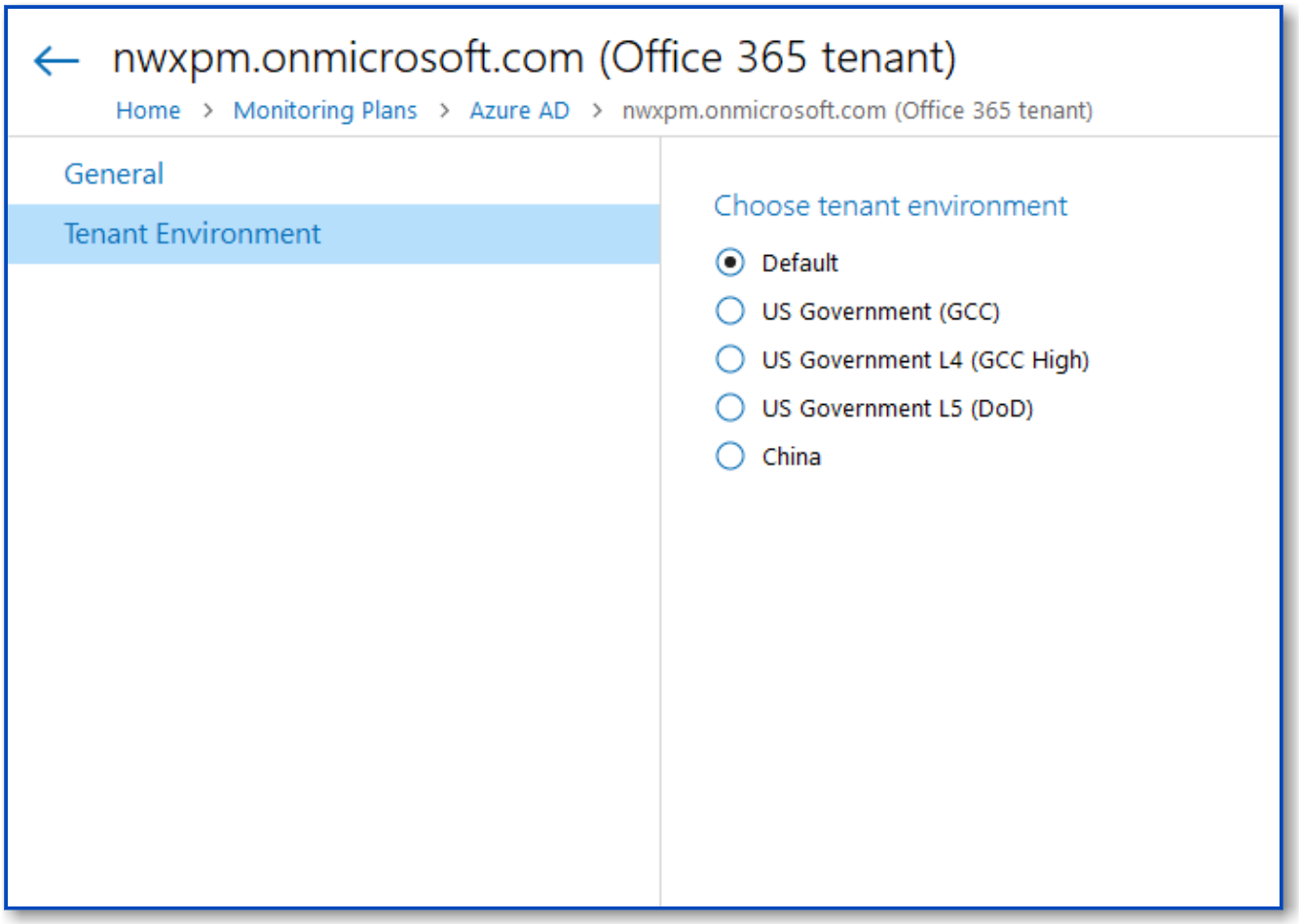
- Tenant name
- For modern authentication: Application (client) ID
- Application secret
- For basic authentication: User name and password

Types of data that can be collected by Netwrix Auditor from the Microsoft 365 tenant depend on the authentication option you choose.

Follow the steps to configure Office 365 tenant as a monitored item.

Step 1 – On the **General** page of the item properties, specify **Tenant name**:

- If you are going to use **Basic authentication**, you can proceed to the next step – **Tenant name** will be filled in automatically after it.
    - **NOTE:** Basic authentication is no longer possible for Exchange Online. For the already existing tenants it is still possible to use basic authentication for SharePoint Online and Microsoft Entra ID monitoring.
- If you are going to use **Modern authentication**, paste the obtained name. See the Using Modern Authentication with Microsoft Entra ID topic for additional information.



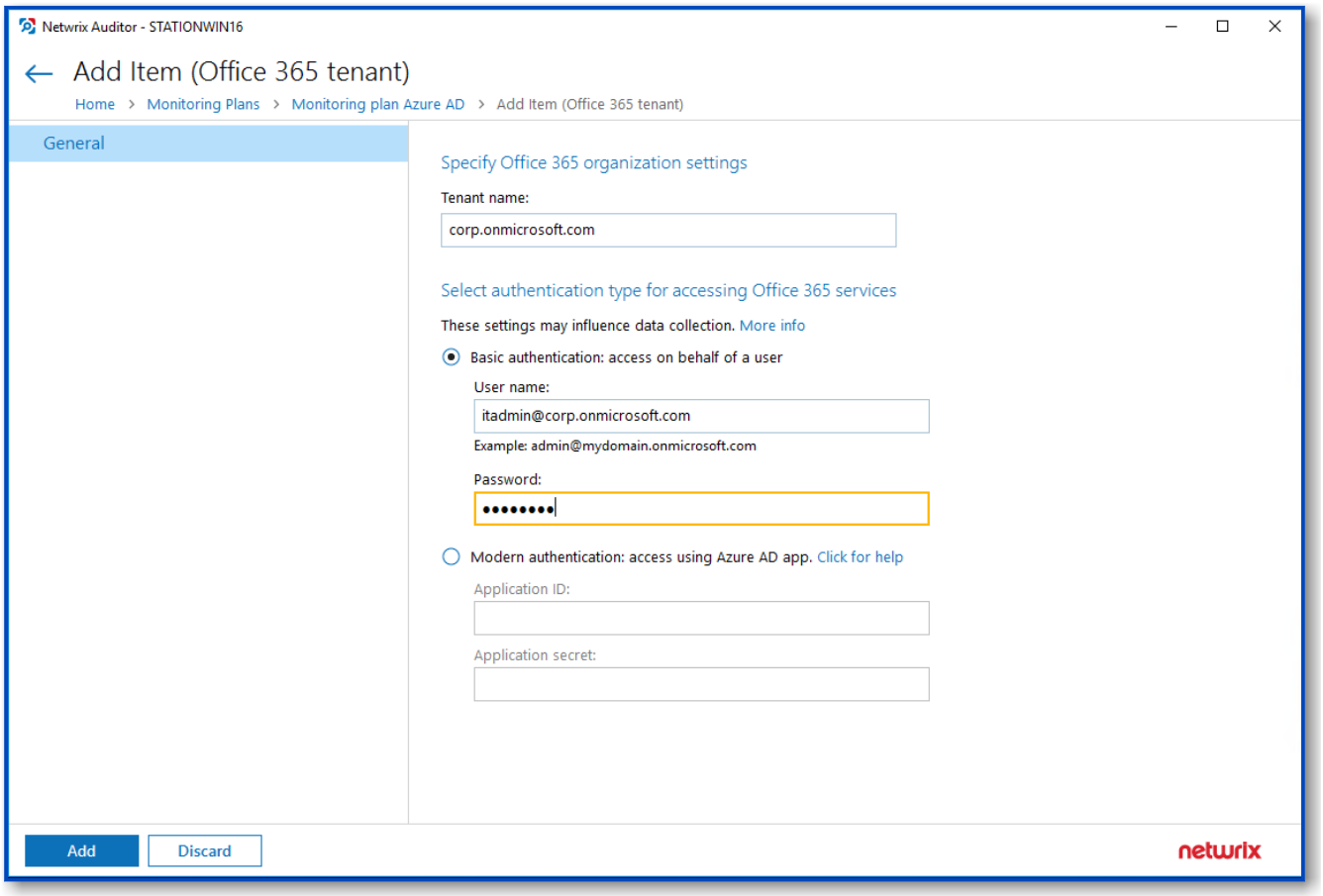
If you are using a government tenant, please click the **Tenant Environment** tab and select the desired tenant environment.

Step 2 – Select authentication method that will be used when accessing Office 365 services:

- Basic authentication:
  - Selected, Office 365 organization will be accessed on behalf of the user you specify.
  - Enter **User name** and **password**; use any of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*.
  - The **Tenant name** field then will be filled in automatically.
  - Make sure this user account has sufficient access rights. See Using Basic Authentication with Microsoft Entra ID topic for additional information.
- Modern authentication:

- Selected, Office 365 organization will be accessed using the Microsoft Entra ID (formerly Azure AD) app you prepared. Enter:
  - **Application ID**;
    - **Application secret**.
- See the Using Modern Authentication with Microsoft Entra ID for additional information.

Step 3 – Click the **Add** button.



You can use a single account to collect audit data for different Office 365 services (Microsoft Entra ID, Exchange Online, SharePoint Online); however, Netwrix recommends that you specify individual credentials for each of them.

If you plan to collect and report on the audit data for Exchange Online non-owner mailbox access, consider that the value shown in the "*Who*" field in reports and search results will be displayed in UPN format (unlike the earlier Netwrix Auditor versions). This refers to the following scenarios:

- All new installations

- Upgrade from the previous versions if:
  - Modern authentication is selected in the item settings after the upgrade.

    OR

  - Modern authentication has ever been selected in the item settings and reverted back to Basic later

Step 4 – Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the Exchange Online configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them.
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information.

Option	Description
Collect data on non-owner access to mailboxes	Enable monitoring of unauthorized access to mailboxes within your Exchange Online organization. Configure the following: • Notify users if someone gained access to their mailboxes—Select this checkbox if you want to notify users on non-owner access to their mailboxes. • Notify only specific users—Select this checkbox and click Add Recipient to specify the list of users who will receive notifications on non-owner access to their mailboxes. Users not included in this list will not be notified.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

See the Office 365 Tenant topic for additional information.

Exchange Online Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Exchange Online monitoring scope.

Follow the steps to exclude data from Exchange Online monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Exchange Online Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitlist.txt	The file contains a list of changes performed by cmdlets. To exclude a change from reports, search results and Activity Summaries, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`cmdlet`
		
		For example:
		
		`Enable-OrganizationCustomization`
		
		`New-AdminAuditLogSearch`
		
		`New-MailboxAuditLogSearch`
		
		`cmdlet.param`
		
		For example:
		
		`*.Identity`
		
		`*.DomainController`
		
		`*.Organization`
		
		`*.IgnoreDefaultScope`
		
		`*.Force`
		
		`*.Confirm`
		
		`*.Password`
		
		`*-ManagementRoleEntry.Parameters`
		
		`Remove-PublicFolder.Recurse`

omitpathlist.txt	Contains a list of paths to be excluded from reports, search results and Activity Summaries.	`path`
		
		For example:
		
		`SystemMailbox{*}`

File	Description	Syntax

		`DiscoverySearchMailbox{*}`
		
		`FederatedEmail.*`
		
		You can use a wildcard (*) to replace any number of characters in the path.

omituserlist.txt	Contains a list of user names to be excluded from reports, search results and Activity Summaries.	`domain\user`
		
		For example:
		
		`Enterprise\analyst`
		
		`email address`
		
		For example:
		
		`analyst@Enterprise.onmicrosoft.com`

propnames.txt	Contains a list of human-readable names for object classes and their and their properties to be displayed in search results, reports and Activity Summaries.	`cmdletobject=friendlyname`
		
		`cmdlet.param=friendlyname`
		
		For example:
		
		`RoleGroupMember = Role Group`
		
		`UMHuntGroup = Unified Messaging Hunt Group`

File Servers

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- File Servers – Configure data source as required to be monitored

Complete the following fields:

Option	Description	
General		
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.	
Specify actions for monitoring	Specify actions you want to track and auditing mode.	
	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

Option	Description	
		containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. 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 Long-Term Archive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. 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 Long-Term Archive.
	Actions reported by Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, etc. To track the copy action, enable successful read access and change auditing.	
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically	

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.

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 the File Servers topic for additional information.</td></tr>
<tr><td>Configure audit settings</td><td>You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary.

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.

Do not select the checkbox if you want to configure audit settings manually.

See the Supported Data Sources configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them.

Some settings cannot be configured automatically. The product has the following limitations depending on your file server type.

<table>
<tr><th>File Server</th><th>SACL Check</th><th>SACL Adjust</th><th>Policy Check</th><th>Policy Adjust</th><th>Log Check</th><th>Log Adjust</th></tr>
<tr><td>Windows</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>Dell Celerra\VNX\Unity</td><td>+</td><td>+</td><td>+</td><td>—</td><td>+</td><td>—</td></tr>
<tr><td>Dell Isilon</td><td>n/a</td><td>n/a</td><td>+</td><td>—</td><td>n/a</td><td>n/a</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>File Server</th><th>SACL Check</th><th>SACL Adjust</th><th>Policy Check</th><th>Policy Adjust</th><th>Log Check</th><th>Log Adjust</th></tr>
<tr><td>NetApp Data ONTAP 7 and 8 in 7-mode</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>NetApp Clustered Data ONTAP 8 and ONTAP 9</td><td>+</td><td>+</td><td>+</td><td>+</td><td>+</td><td>—</td></tr>
<tr><td>Nutanix Files</td><td>n/a</td><td>n/a</td><td>+</td><td>+</td><td>n/a</td><td>n/a</td></tr>
</table>
</td></tr>
<tr><td>Collect data for state-in-time reports</td><td>Configure Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information.

When auditing file servers, changes to effective access permissions can be tracked in addition to audit permissions. By default, Combination of file and share permissions is tracked. File permissions define who has access to local files and folders. Share permissions provide or deny access to the same resources over the network. The combination of both determines the final access permissions for a shared folder—the more restrictive permissions are applied. Upon selecting Combination of file and share permissions only the resultant set will be written to the Audit Database. Select File permissions option too if you want to see difference between permissions applied locally and the effective file and share permissions set. To disable auditing of effective access, unselect all checkboxes under Include details on effective permissions.

In the Schedule state-in-time data collection section, you can select a custom weekly interval for snapshots</td></tr>
</table>

Option	Description
	collection. Click Modify and select day(s) of week you want your snapshot to be collected. In the Manage historical snapshots section, you can click **Manage** and select the snapshots that you want to import to the Audit Database to generate a report on the data source's state at the specific moment in the past. You must be assigned the Global administrator or the Global reviewer role to import snapshots. Move the selected snapshots to the Snapshots available for reporting list using the arrow button. The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Users can also configure Only the latest snapshot is available for reporting in Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.
Users	
Specify monitoring restrictions	Select the users to be excluded from search results, reports and Activity Summaries. To add users to the list, click Add and provide user name in the domain\user format: *mydomain\user1*. • Use NetBIOS domain name format. • To exclude events containing “*System*” instead of initiator's account name in the “*Who*” column, enter "*System*" value to the list. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the Data source list. As a next step, click Add item to specify an object for monitoring.

Windows File Server
Dell Data storage
NetApp storage
Nutanix File Server

By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings.

Administrative hidden shares like default system root or Windows directory (*ADMIN$*), default drive shares (*D$, E$*), etc. will not be monitored. See the Add Items for Monitoring topic for additional information.

Remember, before adding your monitored items, examine the considerations, limitations and recommendations provided in the following sections:

- DFS-Related Constraints
- Supported File Servers and Devices
- State-in-Time Data
- Sensitive Data

Dell VNX VNXe

Dell VNX, VNXe, Celerra, and Unity NAS devices are collectively referred to as Dell Data Storage.

Complete the following fields:

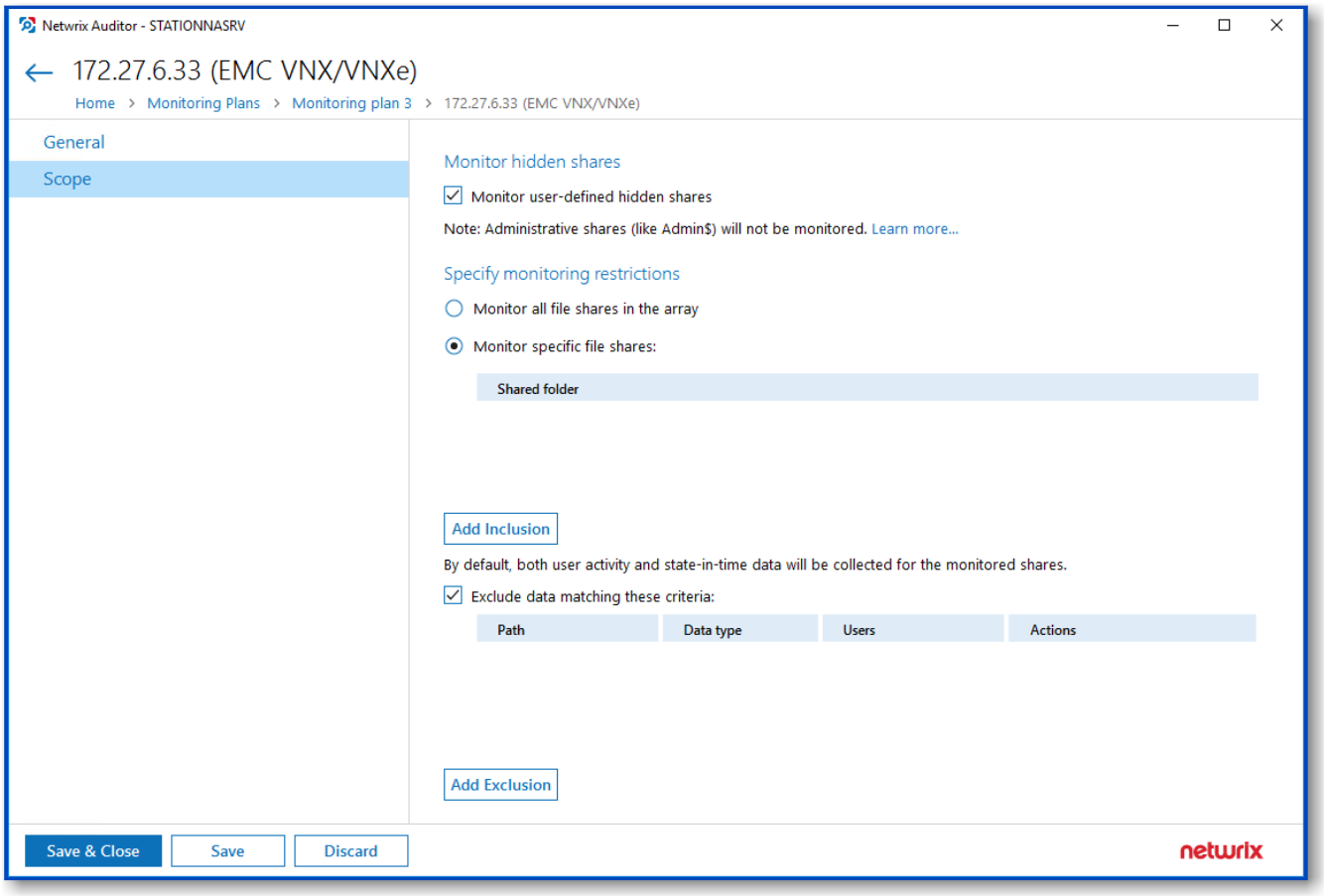
Option	Description
General	

Option	Description
Specify Dell VNX/VNXe, Celerra or Unity storage array	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
Scope	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. See the Fine-tune Monitoring Scope for additional information on how to narrow your monitoring scope. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular

Option	Description
	audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Fine-tune Monitoring Scope

To audit all file shares, under Specify monitoring restrictions, select Monitor all file shares in the array.



You can also create lists of specific file shares to include and/or exclude from being audited.

Include a File Share

Follow the steps to include a file share.

Step 1 – Under Specify monitoring restrictions, select Specific file shares.

Step 2 – Click Add Inclusion.

Step 3 – Provide UNC path to a shared resource. For example: *NewStation\Shared.*

Step 4 – Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).

Exclude Specific Data

Follow the steps to exclude specific data.

Click Add Exclusion. Then, in the Specify Filters dialog, do the following:

Step 5 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

Step 6 – You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 7 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.

Option	Description	Example
State-in-Time	Select to configure Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

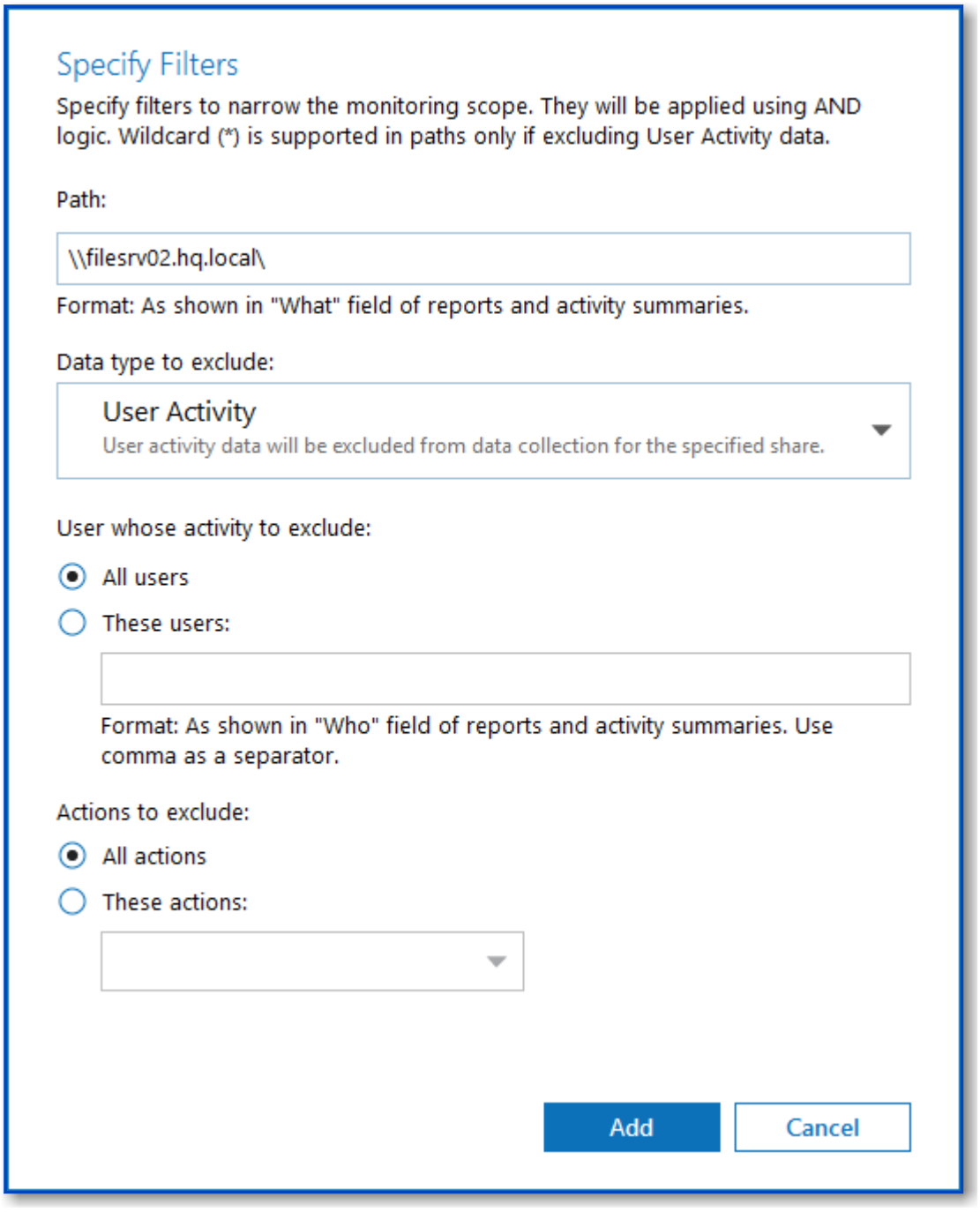
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users— Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



Step 3 – After configuring all filters, click **Add** to save them and return to the item settings.

Dell Isilon

Complete the following fields:

Option	Description
General	
Specify Dell Isilon storage array	Provide the IP address or the host name of the name server used to connect to your access zone. For example, *account.corp.lab*
Access Zone	Enter the name of access zone partition within your EMC Isilon cluster. For example, *zone_account*
OneFS web administration interface URL	Enter Dell Isilon web administration URL (e.g., *https://isiloncluster.corp.lab:8080*). This URL is used to get configuration details about your Isilon cluster via OneFS API.
File Share UNC path to audit logs	Path to the file share located on a Dell Isilon with event log files (e.g., *srv**netwrix_audit$**logs*\).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
Scope	

Option	Description
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. See the Fine-tune Monitoring ScopeFine-tune Monitoring Scopetopic for additional information about how to narrow your monitoring scope. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Configure the Scope

You can configure Netwrix Auditor to audit all file shares except for ones added as exclusions. For that, under Specify monitoring restrictions, select All file shares in the array. You can also create lists of specific file shares to include and/or exclude from being audited. Review the following for additional information:

- Add Inclusion
- Add Exclusion

Add Inclusion

Follow the steps to add inclusion.

Step 1 – Under Specify monitoring restrictions, select Specific file shares.

Step 2 – Click Add Inclusion.

Step 3 – Provide UNC path to a shared resource. For example: *NewStation\Shared.*

Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).

Add Exclusion

Follow the steps to add exclusion.

Click Add Exclusion. Then, in the Specify Filters dialog, do the following:

Step 4 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

Step 5 – You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 6 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.
State-in-Time	Select to configure Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

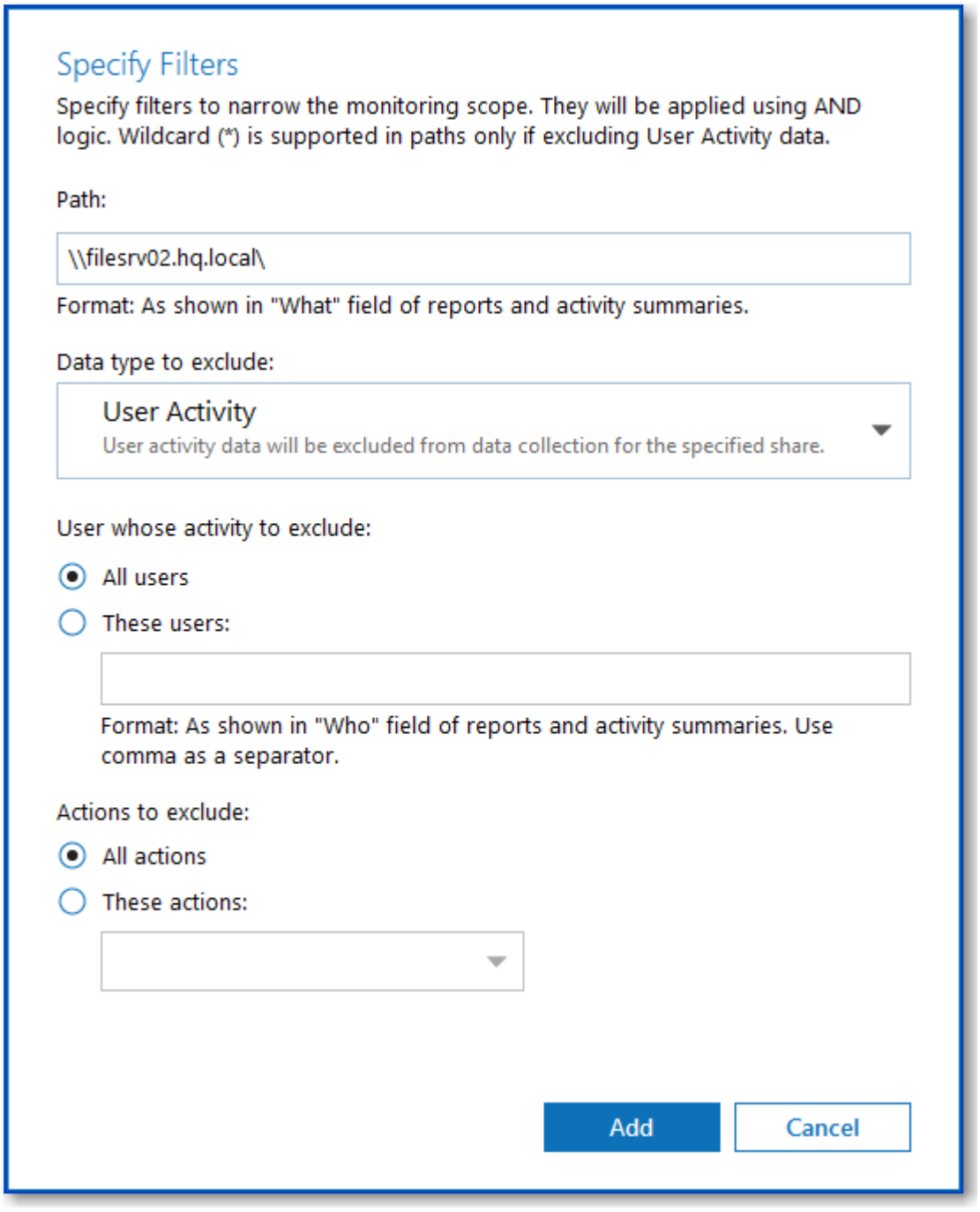
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users— Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



Step 3 – After configuring all filters, click **Add** to save them and return to the item settings.

NetApp

Complete the following fields:

Option	Description
General	
Specify NetApp file server	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network.
File share UNC path to audit logs	Select one of the following: • Detect automatically—If selected, a shared resource will be detected automatically. • Use this path—UNC path to the file share located on a NetApp Filer with event log files (e.g., *\\CORP\ETC$\log*).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
ONTAPI/ONTAP REST API	
Specify protocol for accessing ONTAPI/ONTAP REST API	Select one of the following: • Detect automatically—If selected, a connection protocol will be detected automatically. • HTTP • HTTPS

Option	Description
	Refer to Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to enable HTTP or HTTPS admin access. NOTE: ONTAP REST API works only over HTTPS protocol
Specify management interface	Select management interface to connect to ONTAPI/ ONTAP REST API. If you want to use custom management interface for ONTAPI/ONTAP REST API, select Custom and provide a server name by entering its FQDN, NETBIOS or IP address.
Specify account for connecting to ONTAPI/ONTAP REST API	Select an account to connect to NetApp and collect data through ONTAPI/ONTAP REST API. If you want to use a specific account (other than the one you specified on the General tab), select **Custom** and enter credentials. The credentials are case sensitive. Take into consideration that even if a custom account is specified, the account selected on the General tab must be a member of the Builtin\Administrators group and have sufficient permissions to access audit logs shared folder and audited shares. Data Collecting Account
Scope	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares

Option	Description
	used by printers to enable remote administration (PRINT$), etc. **CAUTION:** Monitoring of non-default hidden shares is not supported for NetApp servers in 7-mode.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Configure Scope how to narrow your monitoring scope. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Configure Scope

You can configure Netwrix Auditor to audit all file shares except for ones added as exclusions. For that, under Specify monitoring restrictions, select All file shares in the array. You can also create lists of specific file shares to include and/or exclude from being audited. Review the following for additional information:

Add Inclusion

Follow the steps to add inclusion.

Step 1 – Under Specify monitoring restrictions, select Specific file shares.

Step 2 – Click Add Inclusion.

Step 3 – Provide UNC path to a shared resource. For example: *NewStation\Shared.*

NOTE: Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).

Add Exclusion

Follow the steps to add exclusion.

Click Add Exclusion. Then, in the Specify Filters dialog, do the following:

Step 4 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

Step 5 – You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 6 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.
State-in-Time	Select to configure Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Auditor to collect state-in-time data for this folder.

Option	Description	Example
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

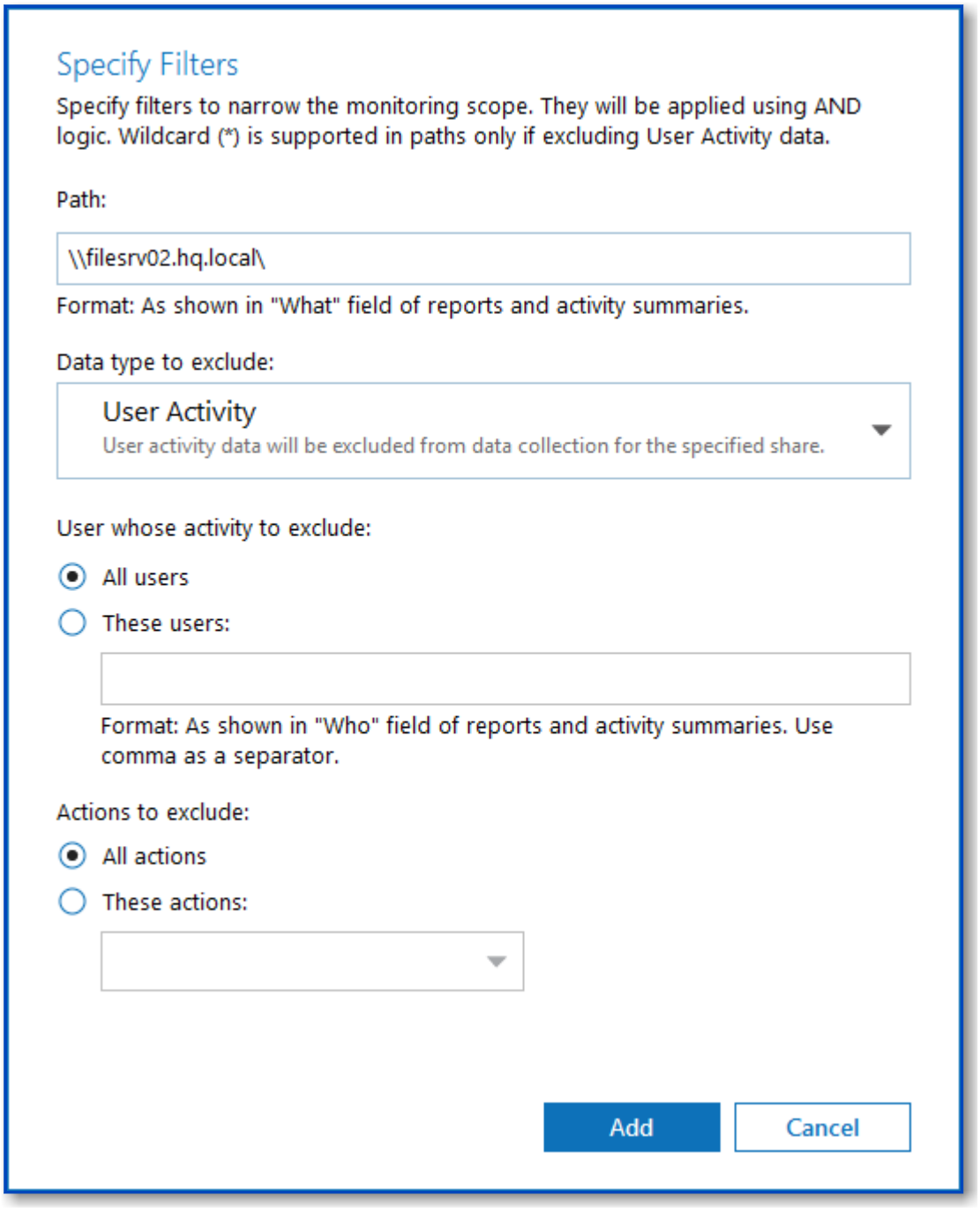
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users— Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



Step 3 – After configuring all filters, click **Add** to save them and return to the item settings.

Nutanix Files

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems

Complete the following fields:

Option	Description	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.	
Specify actions for monitoring	Specify actions you want to track and auditing mode.	
	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	

Option	Description	
	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. 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 Long-Term Archive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. 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 Long-Term Archive.
	Actions reported by Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, etc. To track the copy action, enable successful read access and change auditing.	

Option	Description
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the Supported Data Sources configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them. Netwrix Auditor can configure the following settings: • Policy Check • Policy Adjust
Collect data for state-in-time reports	Configure Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information. When auditing file servers, changes to effective access permissions can be tracked in addition to audit permissions. By default, Combination of file and share permissions is tracked. File permissions define who has access to local files and folders. Share permissions provide or deny access to the same resources over the

Option	Description
	network. The combination of both determines the final access permissions for a shared folder—the more restrictive permissions are applied. Upon selecting Combination of file and share permissions only the resultant set will be written to the Audit Database. Select File permissions option too if you want to see difference between permissions applied locally and the effective file and share permissions set. To disable auditing of effective access, unselect all checkboxes under Include details on effective permissions. In the Schedule state-in-time data collection section, you can select a custom weekly interval for snapshots collection. Click Modify and select day(s) of week you want your snapshot to be collected. In the Manage historical snapshots section, you can click **Manage** and select the snapshots that you want to import to the Audit Database to generate a report on the data source's state at the specific moment in the past. You must be assigned the Global administrator or the Global reviewer role to import snapshots. Move the selected snapshots to the Snapshots available for reporting list using the arrow button. The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Users can also configure Only the latest snapshot is available for reporting in Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Nutanix SMB Shares

Complete the following fields:

Option	Description
General	
Specify Nutanix File Server	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network. If you need to audit a 3-node cluster, it is recommended to use FQDN or NETBIOS name.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for more information.
Specify listening port for incoming connections	Provide the name of the TCP port to listen to notifications on the operations with Nutanix file shares. Default is **9898**. For details on how to open the port, refer to the Nutanix Ports topic.
Nutanix File Server REST API	
Specify account for connecting to Nutanix File Server REST API	Specify the account that will be used to connect to Nutanix REST API. This account should have sufficient privileges on the Nutanix File Server. For details, refer to Create User Account to Access Nutanix REST API.

Option	Description
Scope	
Monitor hidden shares	By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Refer to Configure Scope for detailed instructions on how to configure your monitoring scope. Currently, auditing is available for SMB shares only. Auditing of NFS shares is not supported due to known limitations.

Configure Scope

You can configure Netwrix Auditor to audit all file shares except for ones added as exclusions. For that, under Specify monitoring restrictions, select All file shares in the array. You can also create lists of specific file shares to include and/or exclude from being audited. Review the following for additional information:

Add Inclusion

Follow the steps to add inclusion.

Step 1 – Under Specify monitoring restrictions, select Specific file shares.

Step 2 – Click Add Inclusion.

Step 3 – Provide UNC path to a shared resource. For example: *NewStation\Shared.*

Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).

Add Exclusion

Follow the steps to add exclusion.

Click Add Exclusion. Then, in the Specify Filters dialog, do the following:

Step 4 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *corpsrv**shared*.

Step 5 – You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 6 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.
State-in-Time	Select to configure Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Auditor to

Option	Description	Example
		collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

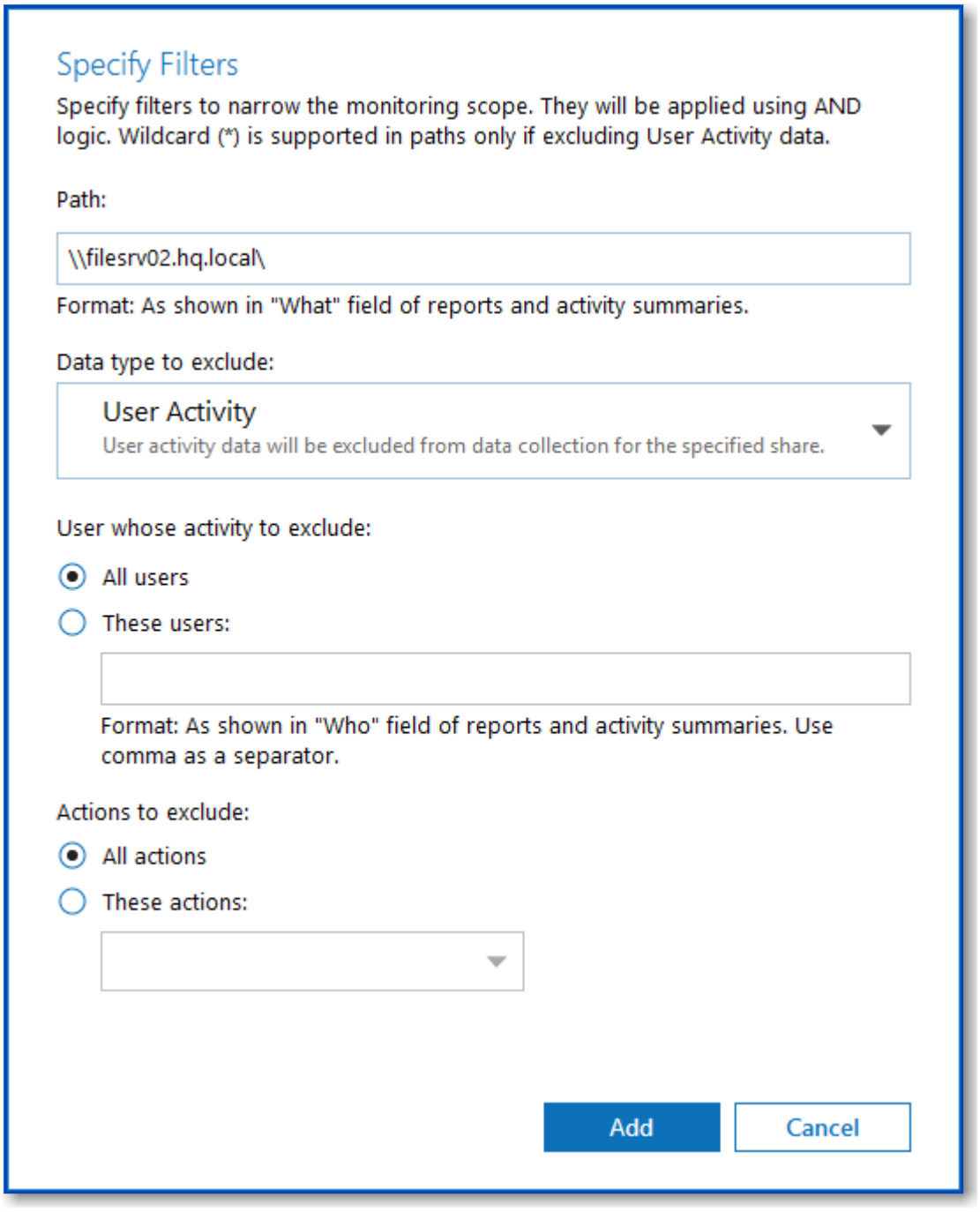
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users— Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



Step 3 – After configuring all filters, click **Add** to save them and return to the item settings.

Qumulo

Complete the following fields:

Option	Description
General	
Specify a file server	Provide UNC path to a file server. See the section below for special considerations. Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
Event Collection	
Specify a host or network resource	Provide UNC path to a file server or an IP range of servers you want to get activity events from. You can select to collect event data from the same server or provide a custom server or IP range.
Specify port and protocol for incoming connections	Use **Port** and **Protocol** to provide the port required for incoming connections (default is **UDP port 514**).
Scope	
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic.

Option	Description
	By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings. Remember that administrative hidden shares like default system root or Windows directory (ADMIN$), default drive shares (D$, E$), etc. will not be monitored. See the topics on the monitored items for details.

Synology

Complete the following fields:

Option	Description
General	
Specify a file server	Provide UNC path to a file server. See the section below for special considerations. Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

Option	Description
Event Collection	
Specify a host or network resource	Provide UNC path to a file server or an IP range of servers you want to get activity events from. You can select to collect event data from the same server or provide a custom server or IP range.
Specify port and protocol for incoming connections	Use **Port** and **Protocol** to provide the port required for incoming connections (default is **UDP port 514**).
Scope	
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings. Remember that administrative hidden shares like default system root or Windows directory (ADMIN$), default drive shares (D$, E$), etc. will not be monitored. See the topics on the monitored items for details.

Windows File Server

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections

- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems

Windows File Share

Complete the following fields:

Option	Description
General	
Specify Windows file share	Provide UNC path to a shared resource. See the section below for special considerations. Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.
Scope	

Option	Description
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. See the Configure Scope topic for additional information on how to narrow your monitoring scope. By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings. Remember that administrative hidden shares like default system root or Windows directory (ADMIN$), default drive shares (D$, E$), etc. will not be monitored. See the topics on the monitored items for details. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Configure Scope

You can narrow your monitoring scope by adding exclusions.

Click Add Exclusion. Then, in the Specify Filters dialog, do the following:

Step 1 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *corpsrv**shared*.

Step 2 – You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 3 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.
State-in-Time	Select to configure Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

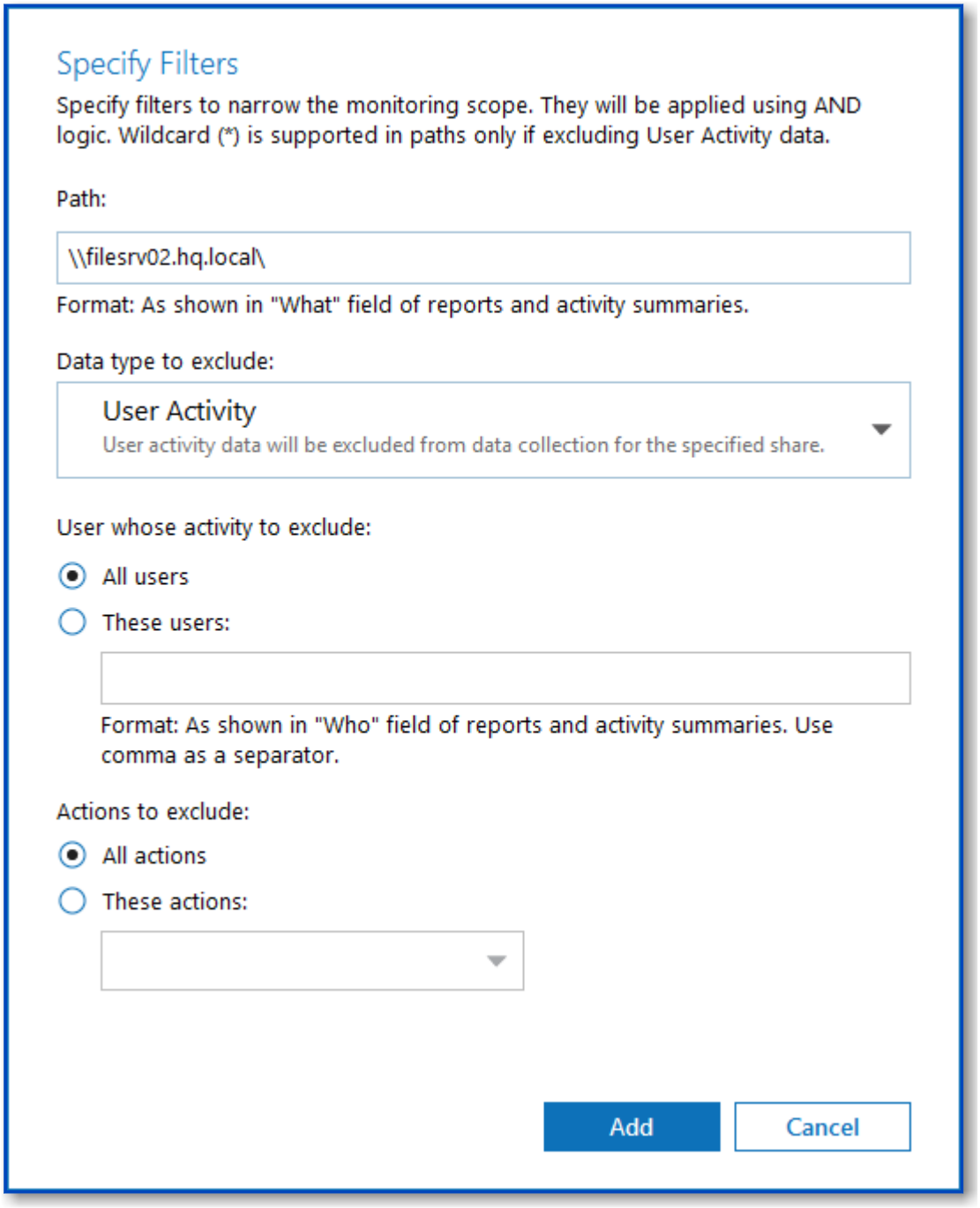
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users— Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



Step 3 – After configuring all filters, click **Add** to save them and return to the item settings.

Working with DFS File Shares

Netwrix Auditor supports auditing of DFS and clustered file servers if Object Access Auditing is enabled on DFS file shares or on every cluster node.

- When adding a cluster file server for auditing, it is recommended to specify a server name of the **Role** server or a UNC path of the shared folder located on the **Role** server.
- When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path of the whole namespace or UNC path of the DFS link (folder). For example:
  - *"\\domain\dfsnamespace\"* (domain-based namespace) or *"\\server\dfsnamespace\"* (in case of stand-alone namespace);
  - *"\\domain\dfsnamespace\link"* (domain-based namespace) or *"\\server\dfsnamespace\link"* (in case of stand-alone namespace).
- For recommendations on configuring DFS replication, refer to this Knowledge Base article.

Working with Mount Points

You can specify a mount point as a monitored item. However, consider the following:

- If a mount point represents a shared folder, then the objects in its root will be initially collected by Netwrix Auditor and appear as processed by *System* account. Wait for the next data collections - then all actions for these objects will be monitored in a normal way.
- To monitor the mount points targeted at the subfolder of a file share, provide network path to the target subfolder.

AD Container

Complete the following fields:

Option	Description
General	
Specify AD container	Specify a whole AD domain, OU or container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be audited within the chosen AD container: **Domain**

Option	Description
	controllers, Servers (excluding domain controllers), or **Workstations**. • Click **Exclude** to specify AD domains, OUs, and containers you do not want to audit. In the Exclude Containers dialog, click Add and specify an object. The list of containers does not include child domains of trusted domains. Use other options **(Computer, IP range** to specify the target computers.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. If using a group Managed Service Account (gMSA), you can specify only the account name in the *domain\account$* format. Password field can be empty. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information. Refer to the Permissions for Active Directory Auditing topic for more information on using Netwrix Privilege Secure as an account for data collection. A custom account must be granted the same permissions and access rights as the default account used for data collection. See theData Collecting Account topic for additional information.
Containers and Computers	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both

Option	Description
	default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Depending on the type of the object you want to exclude, select one of the following: • Add AD Container – Browse for a container to be excluded from being audited. You can select a whole AD domain, OU or container. • Add Computer – Provide the name of the computer you want to exclude as shown in the "*Where*" column of reports and Activity Summaries. For example, *backupsrv01.mydomain.local*. Wildcards (*) are not supported. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

IP Range

Complete the following fields:

Option	Description
General	
Specify IP range	Specify an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP subrange you want to exclude, and click **Add**.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
Scope	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.

Computer

For evaluation purposes, Netwrix recommends selecting Computer as an item for a monitoring plan. Once the product is configured to collect data from the specified items, audit settings (including Core and Compression services installation) will be applied to all computers within AD Container or IP Range.

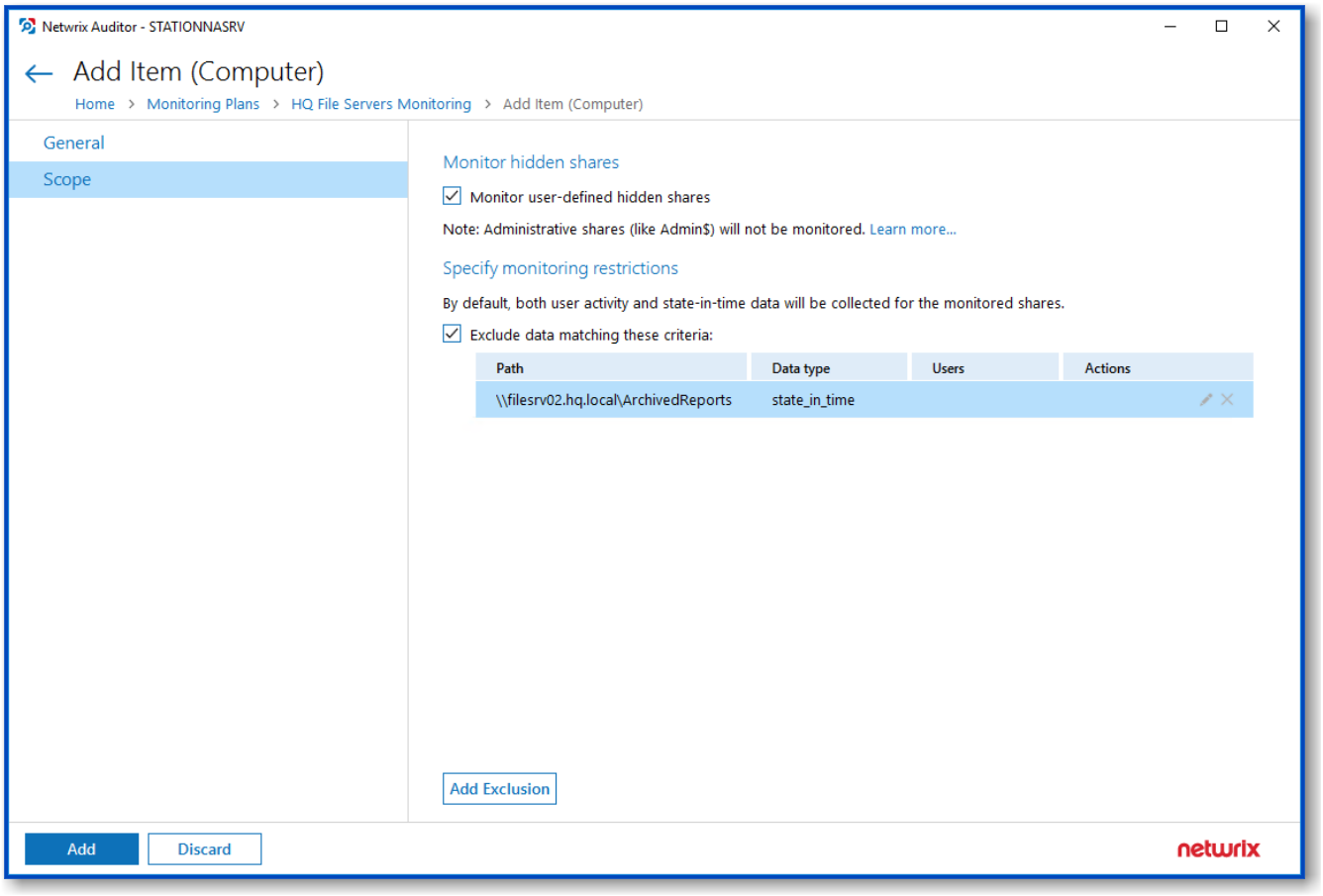
Complete the following fields:

Option	Description
General	
Specify a computer	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available: • User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information. • Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information. • Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.

Option	Description
Scope	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic.

Configure Scope

By default, both user activity and state-in-time data will be collected for the monitored item. However, you can narrow your monitoring scope by specifying certain locations, user accounts or actions to exclude .



Click Add Exclusion, then follow the steps in the Specify Filters dialog:

Step 1 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 2 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.

Option	Description	Example
	In this case,Netwrix Auditor does not adjust audit settings automatically for the selected folders.	
State-in-Time	Select to configure Netwrix Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Netwrix Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

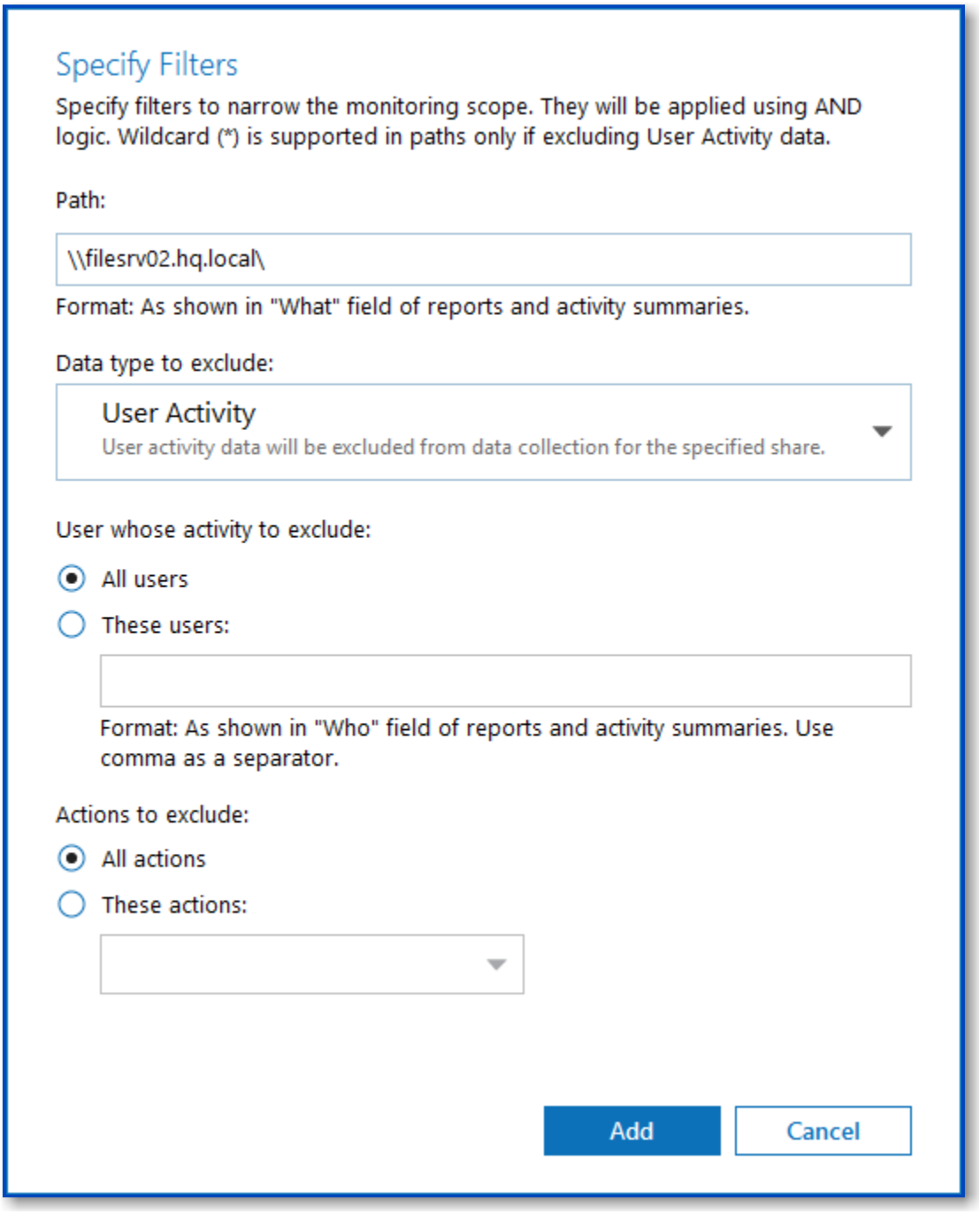
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users — Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*



After configuring all filters, click **Add** to save them and return to the item settings.

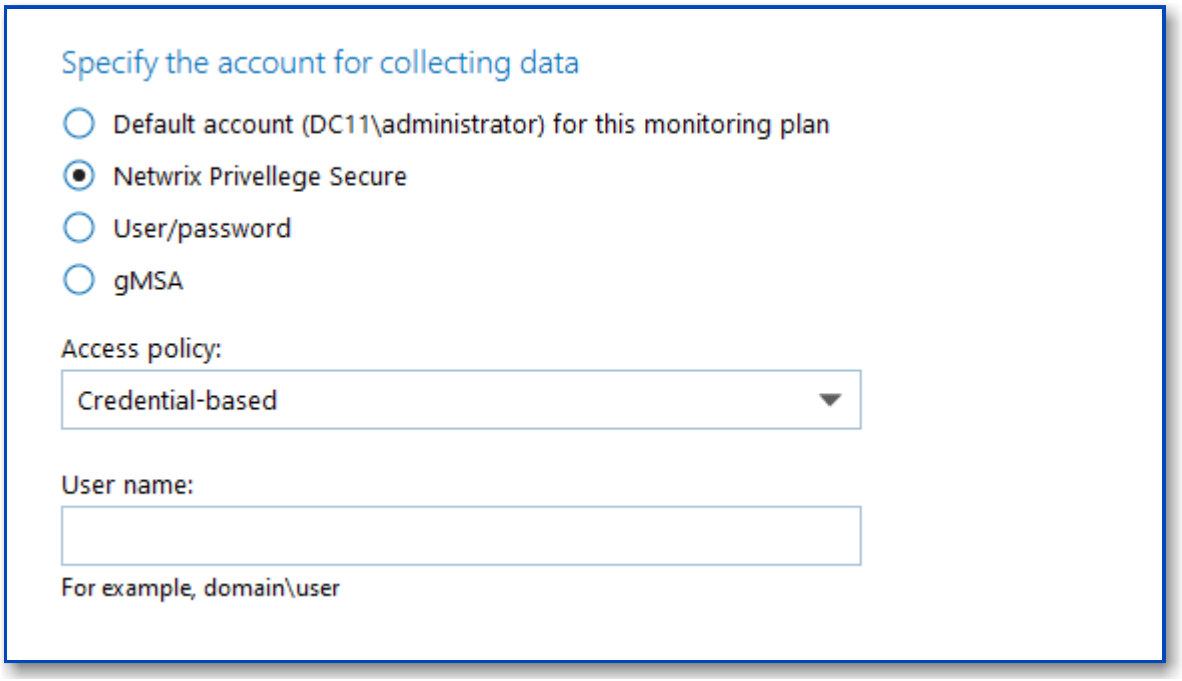
Use Netwrix Privilege Secure as a Data Collecting Account

Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

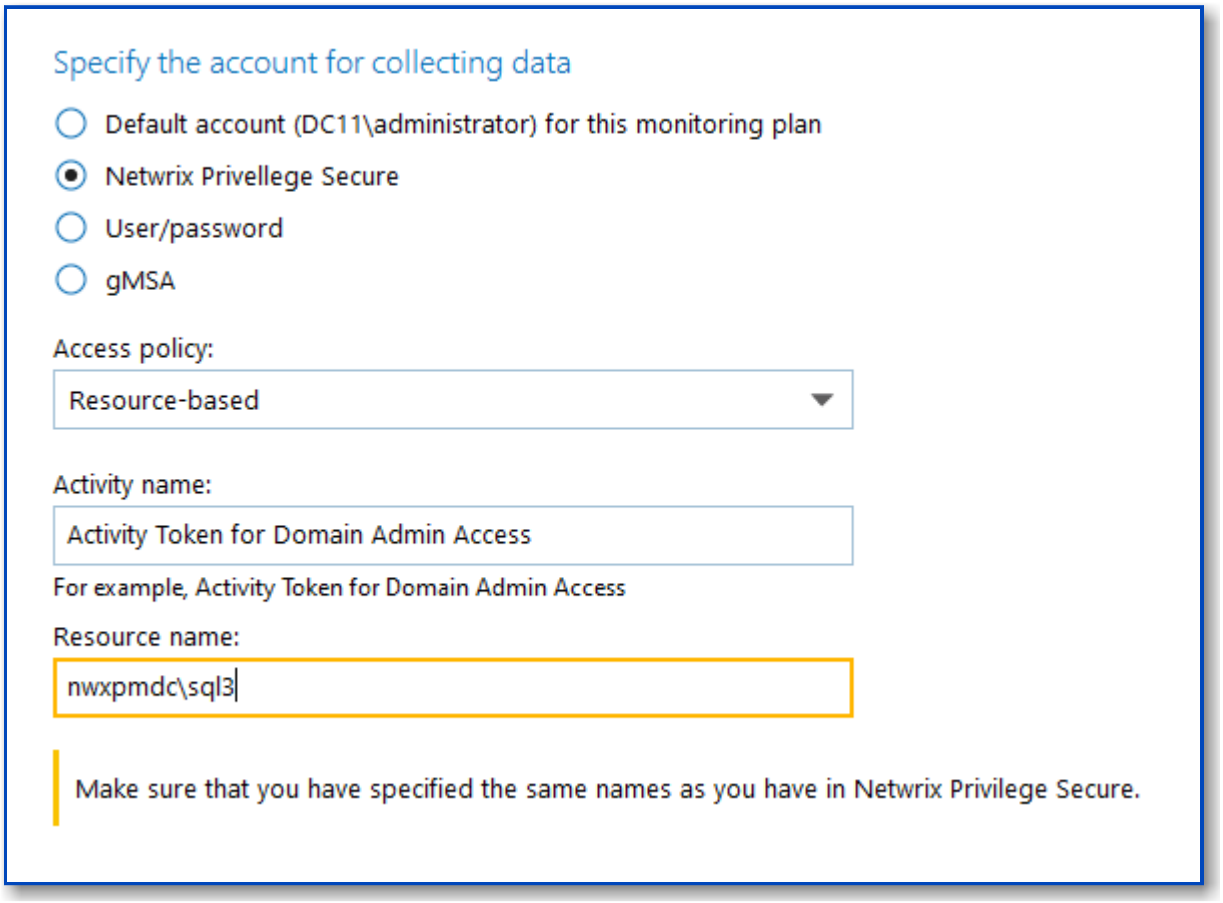
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

File Servers Monitoring Scope

You can specify data that you want to include into / exclude from the Windows File Server, NetApp Filer, and Dell Data Storage (formerly EMC) monitoring scope. For that, you can configure monitoring scope in Auditor client UI, as explained in the related section:

- File Servers
- Windows File Share

Besides, you can configure exclusions for file servers audit using the special txt files (omit lists), as explained below.

Monitoring scope restrictions set up in the UI will apply together with the exclusion settings configured in the *.txt files.

Follow the steps to exclude data from file server monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\File Server Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitcollectlist.txt	Contains a list of objects to be excluded from being monitored.	`Monitoring plan name,server name, resource path`
		
		Wildcards are not supported for the Server Name field. To disable filtering for this field, specify an empty string.
		
		For example:
		
		`*,,\\\\*\\System Volume Information*`

omiterrors.txt	Contains a list of errors and warnings to be omitted from logging to the Netwrix Auditor System Health event log.	`Monitoring plan name,server name,error text` For example:

File	Description	Syntax
		`*,productionserver1.corp.local, *Access is denied*`

omitreportlist.txt	Contains a list of objects to be excluded from reports and Activity Summary emails. In this case audit data is still being collected.	`Monitoring plan name,action,who,object type,resource path,property name`
		
		Wildcards are not supported for the action and property name fields. To disable filtering for these fields, specify an empty string.
		
		For example:
		
		`*,,CORP\\jsmith,*,*,`

omitstorelist.txt	Contains a list of objects to be excluded from being stored to the Audit Archive and showing up in reports. In this case audit data is still being collected.	`Monitoring plan name,action,who ,object type,resource path,property name`
		
		Wildcards are not supported for the Change Type and Property Name fields. To disable filtering for these fields, specify an empty string.
		
		For example:
		
		`*,,*,*,\\\ \productionserver1.corp.local\\builds\\*, Attributes`

File	Description	Syntax

omitstoreprocesslist.txt	Contains a list of processes to be excluded from being stored to the Audit Archive and showing up in reports.	`Monitoring plan name,resource path, executable path`
		
		Only local applications can be excluded.
		
		For example:
		
		`*,*,*notepad.exe`

Windows File Share

Complete the following fields:

Option	Description
General	
Specify Windows file share	Provide UNC path to a shared resource. See the section below for special considerations. Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).
Specify the account for collecting data	
Scope	

Option	Description
Specify monitoring restrictions	Refer to Configure Scope for detailed instructions on how to narrow your monitoring scope. By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). If you want to monitor user-defined hidden shares, select the related option in the monitored item settings. Remember that administrative hidden shares like default system root or Windows directory (ADMIN$), default drive shares (D$, E$), etc. will not be monitored. See the topics on the monitored items for details.

Configure Scope

You can narrow your monitoring scope by adding exclusions.

Click Add Exclusion. Then, in the Specify Filters dialog, do the following:

Step 3 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

Step 4 – You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 5 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.
State-in-Time	Select to configure Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

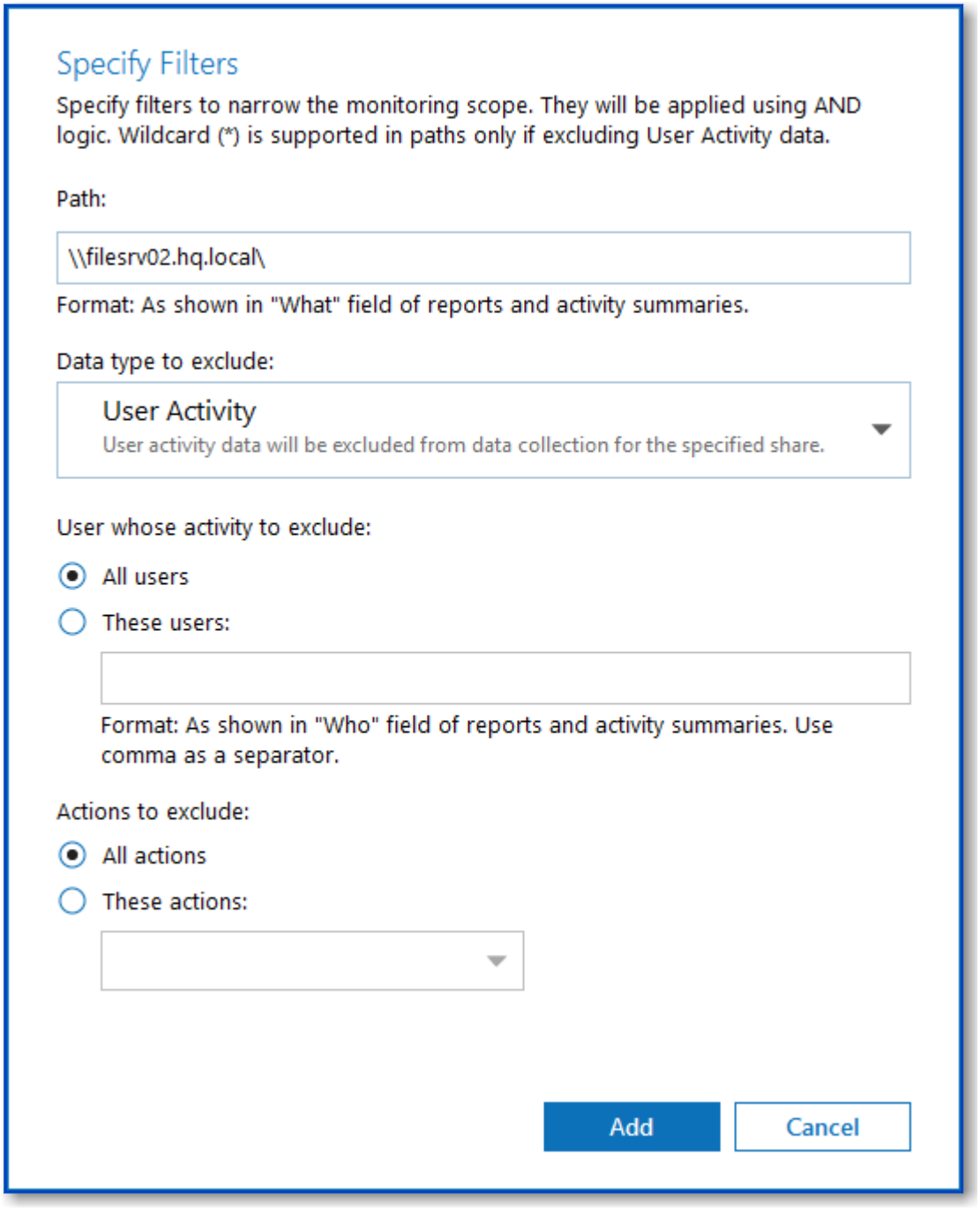
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users— Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



Step 3 – After configuring all filters, click **Add** to save them and return to the item settings.

Working with DFS File Shares

Netwrix Auditor supports auditing of DFS and clustered file servers if Object Access Auditing is enabled on DFS file shares or on every cluster node.

- When adding a cluster file server for auditing, it is recommended to specify a server name of the **Role** server or a UNC path of the shared folder located on the **Role** server.
- When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path of the whole namespace or UNC path of the DFS link (folder). For example:
  - "*domain**dfsnamespace*\" (domain-based namespace) or "*server**dfsnamespace*\" (in case of stand-alone namespace);
  - "*domain**dfsnamespace**link*" (domain-based namespace) or "*server**dfsnamespace**link*" (in case of stand-alone namespace).
- For recommendations on configuring DFS replication, refer to this Knowledge Base article.

Working with Mount Points

You can specify a mount point as a monitored item. However, consider the following:

- If a mount point represents a shared folder, then the objects in its root will be initially collected by Netwrix Auditor and appear as processed by *System* account. Wait for the next data collections - then all actions for these objects will be monitored in a normal way.
- To monitor the mount points targeted at the subfolder of a file share, provide network path to the target subfolder.

Group Policy

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Group Policy – Configure data source as required to be monitored

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Prerequisites	Netwrix Auditor will automatically look up additional system components and prompt you to install those that are missing. In case all required components have been already installed, this section will be omitted. See the Other Components topic for additional information.
Detect additional details	Specify additional information to include in reports and activity summaries. Select Group membershipif you want to include Group membership of the account under which the change was made.
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the Group Policy configuration topic for additional information about audit settings required to collect

Option	Description
	comprehensive audit data and the instructions on how to configure them.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Domain

Complete the following fields:

Option	Description
Specify Active Directory domain	Specify the audited domain name in the FQDN format. For example, "*company.local*".
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available: • User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information. • Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information. • Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege

Option	Description
	Secure. See the Netwrix Privilege Secure topic for additional information.

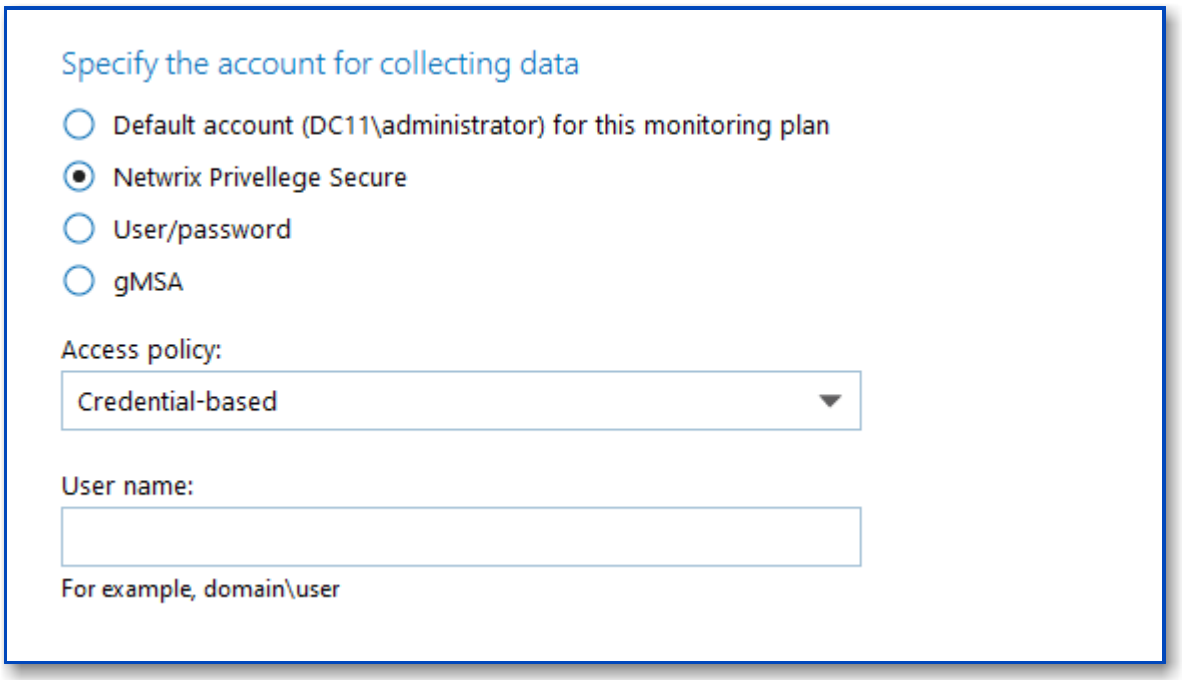
Use Netwrix Privilege Secure as a Data Collecting Account

Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

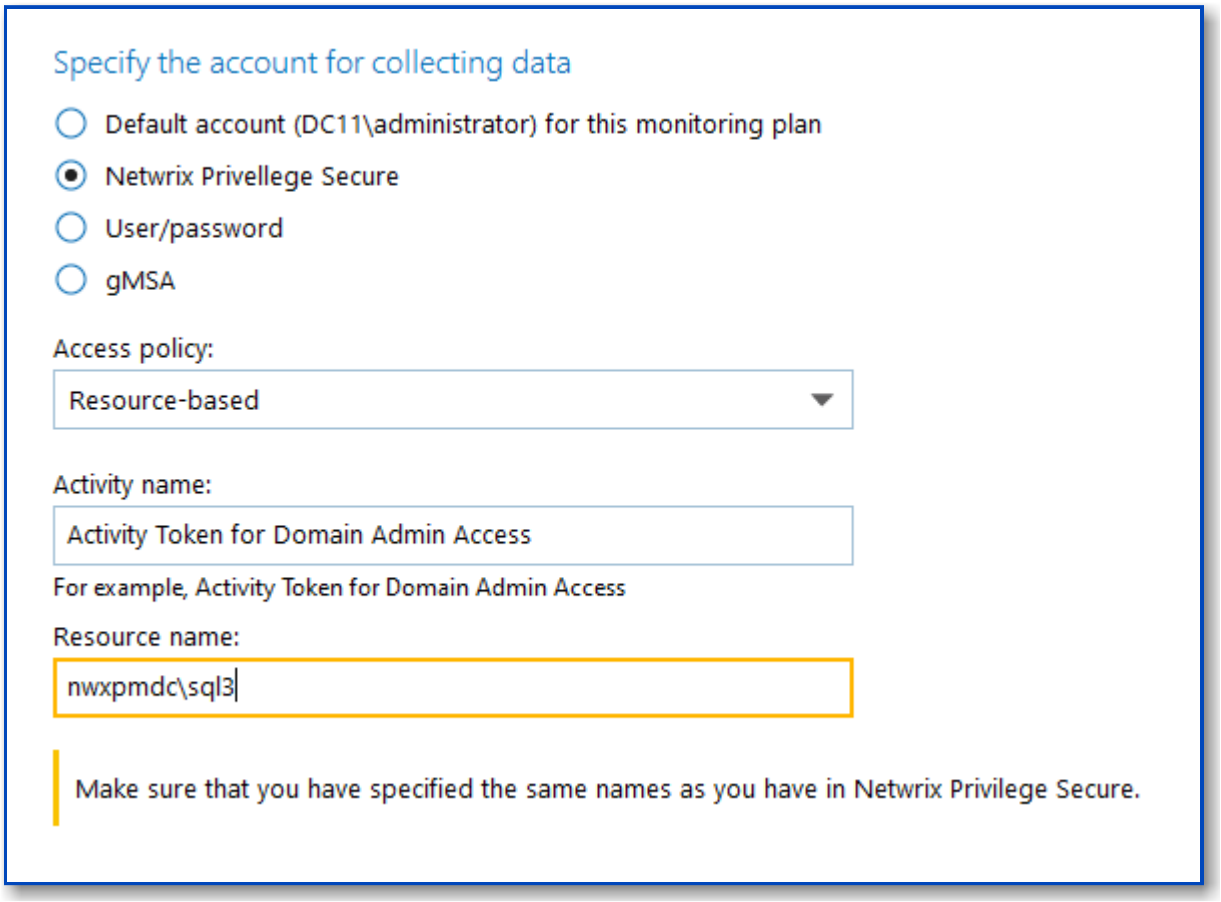
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

Group Policy Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Group Policy monitoring scope. To do it, edit the omitobjlist_gp.txt, omitproplist_gp.txt and omituserlist_gp.txt files.

Follow the steps to exclude data from the Group Policy monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitobjlist_gp.txt	The file contains a list of the Group Policy Object (GPO) names to be excluded from change reports.	`<object name>` For example, to exclude changes to the Default Domain Policy GPO, add the following line: `Default Domain Policy`.
omitproplist_gp.txt	The file contains a list of the Group Policy Object settings to be excluded from change reports.	`<settingname>` For example, to exclude data on changes made to the Maximum password length setting, add the following line: `Maximum password length`.
omituserlist_gp	The file contains a list of user names to be excluded from change reports.	`<domain\user>` For example, to exclude changes made by the user “usertest” in the domain “domaintest”, add the following line: `domaintest\usertest`.

Logon Activity

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Logon Activity – Configure data source as required to be monitored

Complete the following fields:

Option	Description
General	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Fine-tune logon activity monitoring	Specify interval for Netwrix Auditor to collect data on logon activity and add successful non-interactive logons to your auditing scope, if necessary.
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. This method is recommended for evaluation purposes in test environments. If any conflicts are detected with

Option	Description
	your current audit settings, automatic audit configuration will not be performed. Do not select the checkbox if you want to configure audit settings manually. See the Logon Activity configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them.
Users	
Specify monitoring restrictions	Select the users to be excluded from search results, reports and Activity Summaries. To add users to the list, click Add. Then, provide the user name in the domain\user format. For example: *mydomain**user1*. Consider the following: • Use NetBIOS domain name format. • You can provide the "*System*" value to exclude events containing the "*System*" instead of an account name in the "*Who*" column. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Domain

Complete the following fields:

Option	Description
Specify Active Directory domain	Specify the audited domain name in the FQDN format. For example, "*company.local*".
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available: • User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information. • Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information. • Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.

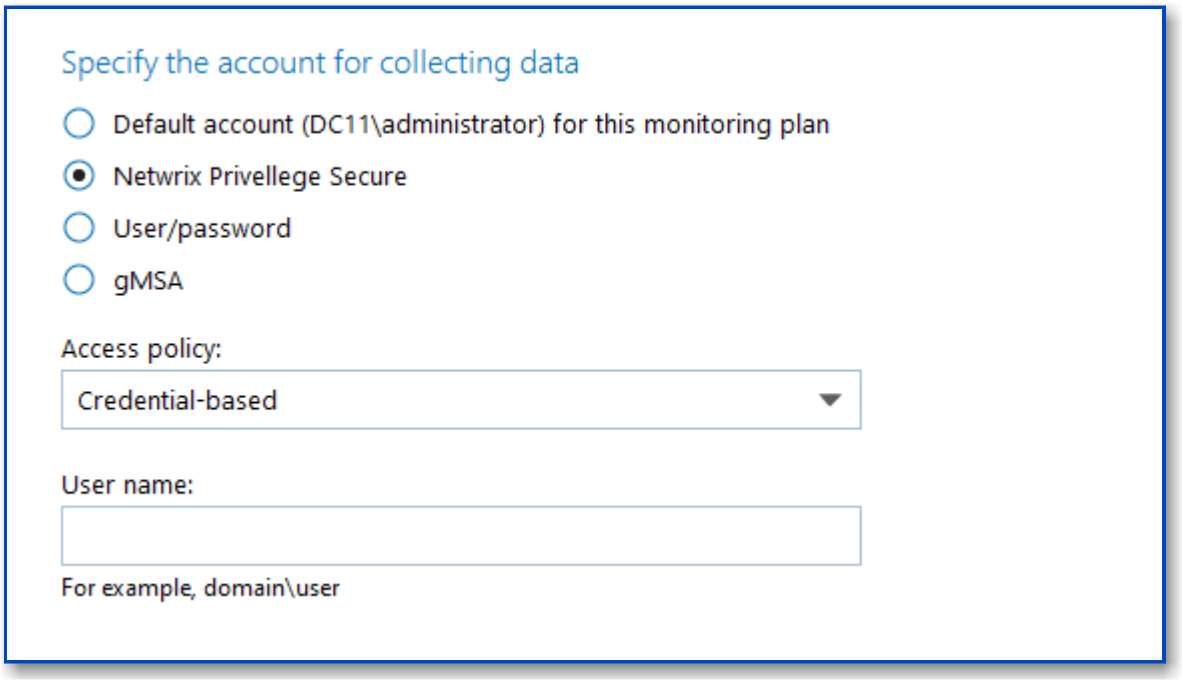
Use Netwrix Privilege Secure as a Data Collecting Account

Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

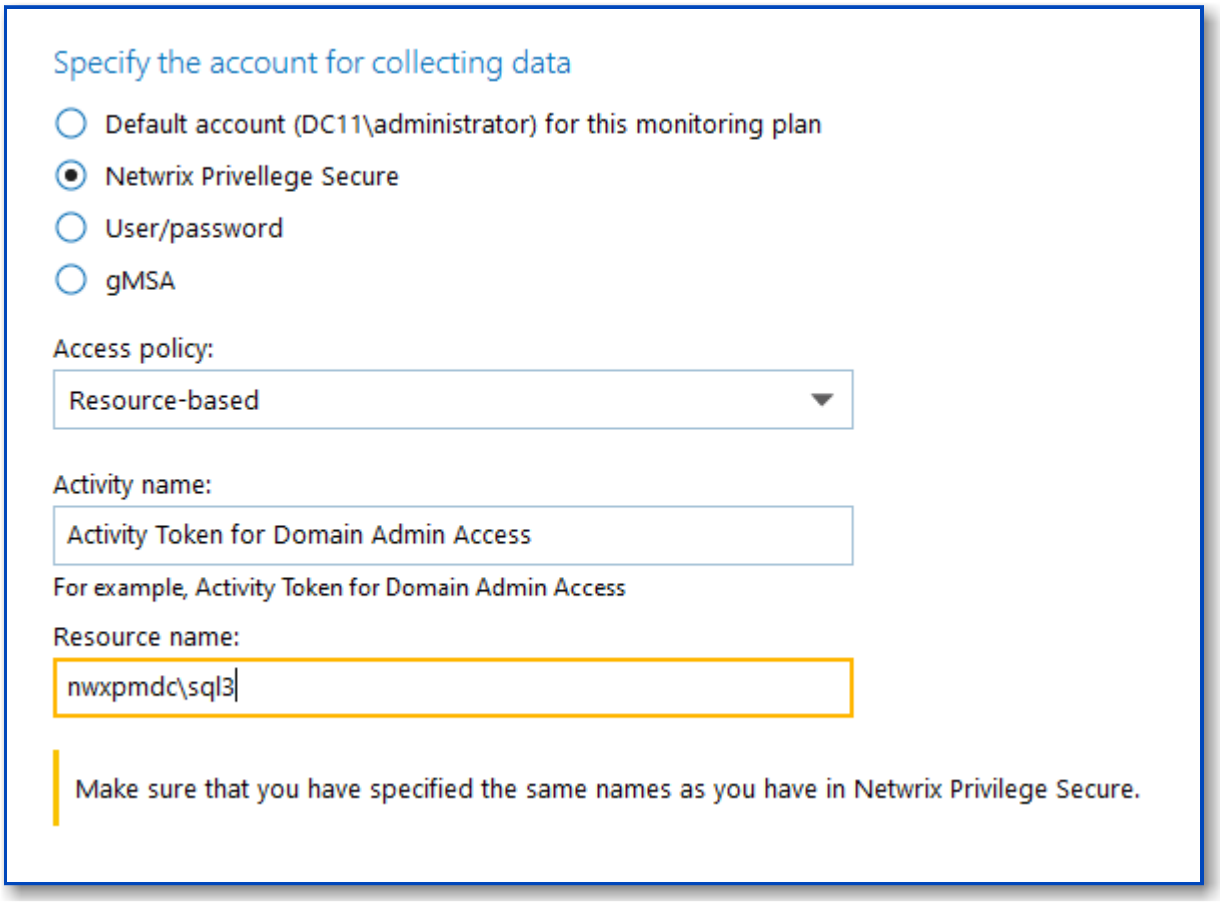
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

Logon Activity Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Logon Activity monitoring scope.

Follow the steps to exclude data from the Logon Activity monitoring scope:

Step 1 – Navigate to the *%working folder%\\NLA\Settings* folder and locate your monitoring plan GUID.

NOTE: If you have several monitoring plans for monitoring Logon Activity, configure omitlist for each monitoring plan separately.

Step 2 – Edit the Settings.cfg file based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

Configuration String	Description	Syntax

`<n n="DCOmitList">`	Contains a list of DCs to be excluded from being monitored.	`DC_name`
		
		For example:
		
		`<v v= "*ROOTDC1*"↗`

`<n n="Hubs">`	Determines whether to enable network traffic compression for a Domain Controller or not.
	
	If configured, overrides the Enable network traffic compression option in monitoring plan configuration.
		`<n n="localhost">`
		`<a n="DCWithCompression Service" t="258">`
		`<v v="DomainControllerN ameInFQDNFormat1"↗`
		`↙a>`
		`<a n="DCWithoutCompress ionService" t="258">`
		`<v v="DomainControllerN ameInFQDNFormat2"↗`
		`↙a>`
		`<a n="DataCollectionInt ervalInSeconds" v="0"↗`
		`↙n>`
		`↙n>`

`<n n="UserOmitList">`
`<a n="Names">`
	Contains a list of users to be excluded from being monitored. Allows specifying a user by name.	`User name`
		
		For example:
		
		`<v v="*NT AUTHORITY*"↗`

`<a n="SIDs">`	Contains a list of users to be excluded from being monitored. Allows specifying a user by security identifier (SID).	`User SID`
		
		For example:
		
		`<v v="*S-1-5-21-1180699209 -877415012-318292XXXX-XXX*"↗`

The file must be formatted in accordance with XML standard. The following symbols must be replaced with corresponding XML entities: & (ampersand), " (double quotes), ' (single quotes), < (less than), and > (greater than) symbols.

Symbol	XML entity
& e.g., Ally & Sons	& e.g., Ally & Sons
" e.g., Domain1\Users\"Stars"	" e.g., Domain1\Users\"Stars"
' e.g., Domain1\Users\O'Hara	' e.g., Domain1\Users\O'Hara
< e.g., CompanyDC<100	< e.g., CompanyDC<100
> e.g., ID>500	> e.g., ID>500

MS Teams

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- MS Teams – Configure data source as required to be monitored

How to Add Office365 Item

This instruction shows how to collect audit data from the Microsoft 365 tenant.

If you plan to use modern authentication, see the Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID topic for additional information on how to prepare Microsoft Entra ID app with required permissions. Make sure you have the following at hand:

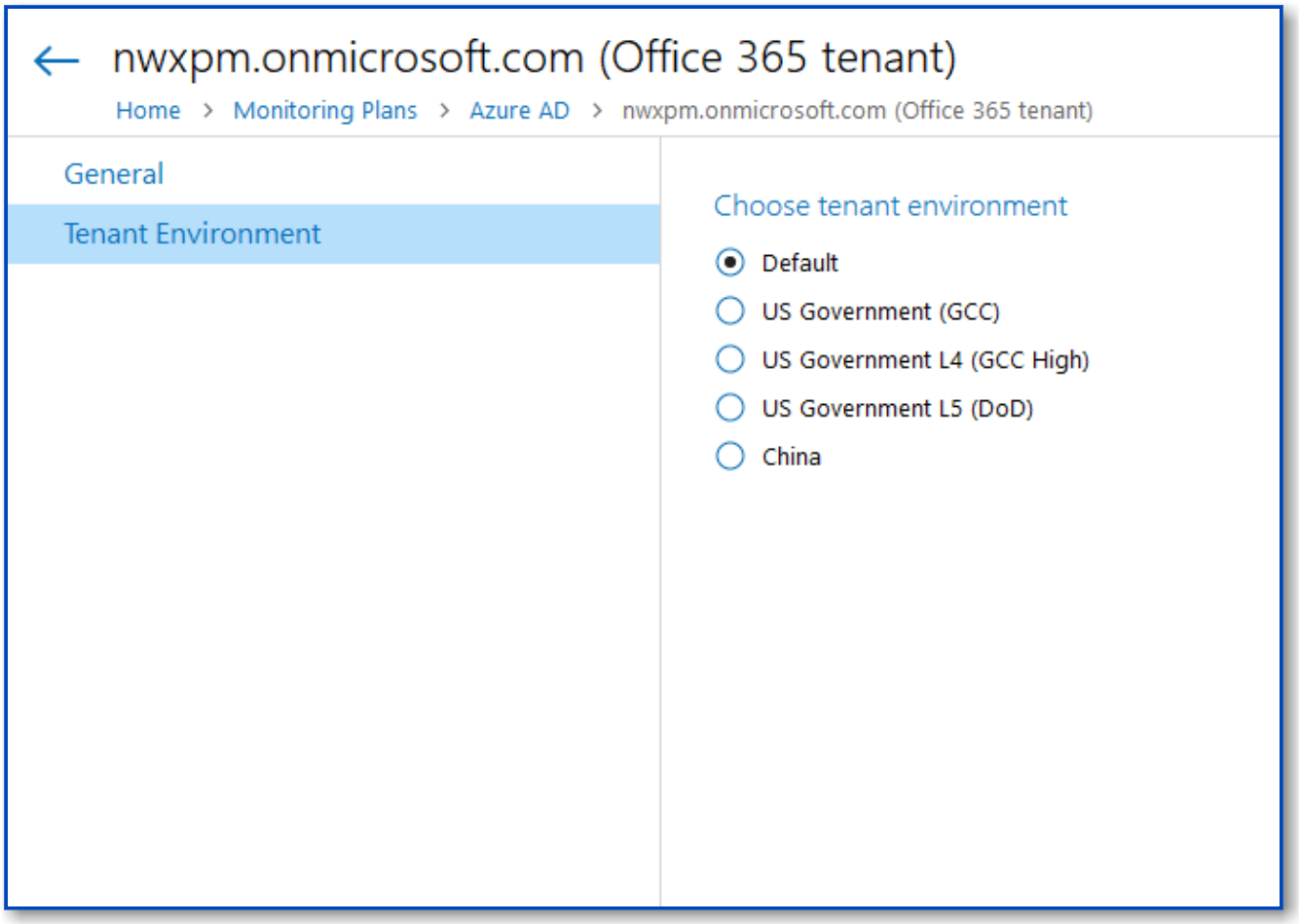
- Tenant name
- For modern authentication: Application (client) ID
- Application secret
- For basic authentication: User name and password

Types of data that can be collected by Netwrix Auditor from the Microsoft 365 tenant depend on the authentication option you choose.

Follow the steps to configure Office 365 tenant as a monitored item.

Step 1 – On the **General** page of the item properties, specify **Tenant name**:

- If you are going to use **Basic authentication**, you can proceed to the next step – **Tenant name** will be filled in automatically after it.
    - **NOTE:** Basic authentication is no longer possible for Exchange Online. For the already existing tenants it is still possible to use basic authentication for SharePoint Online and Microsoft Entra ID monitoring.
- If you are going to use **Modern authentication**, paste the obtained name. See the Using Modern Authentication with Microsoft Entra ID topic for additional information.



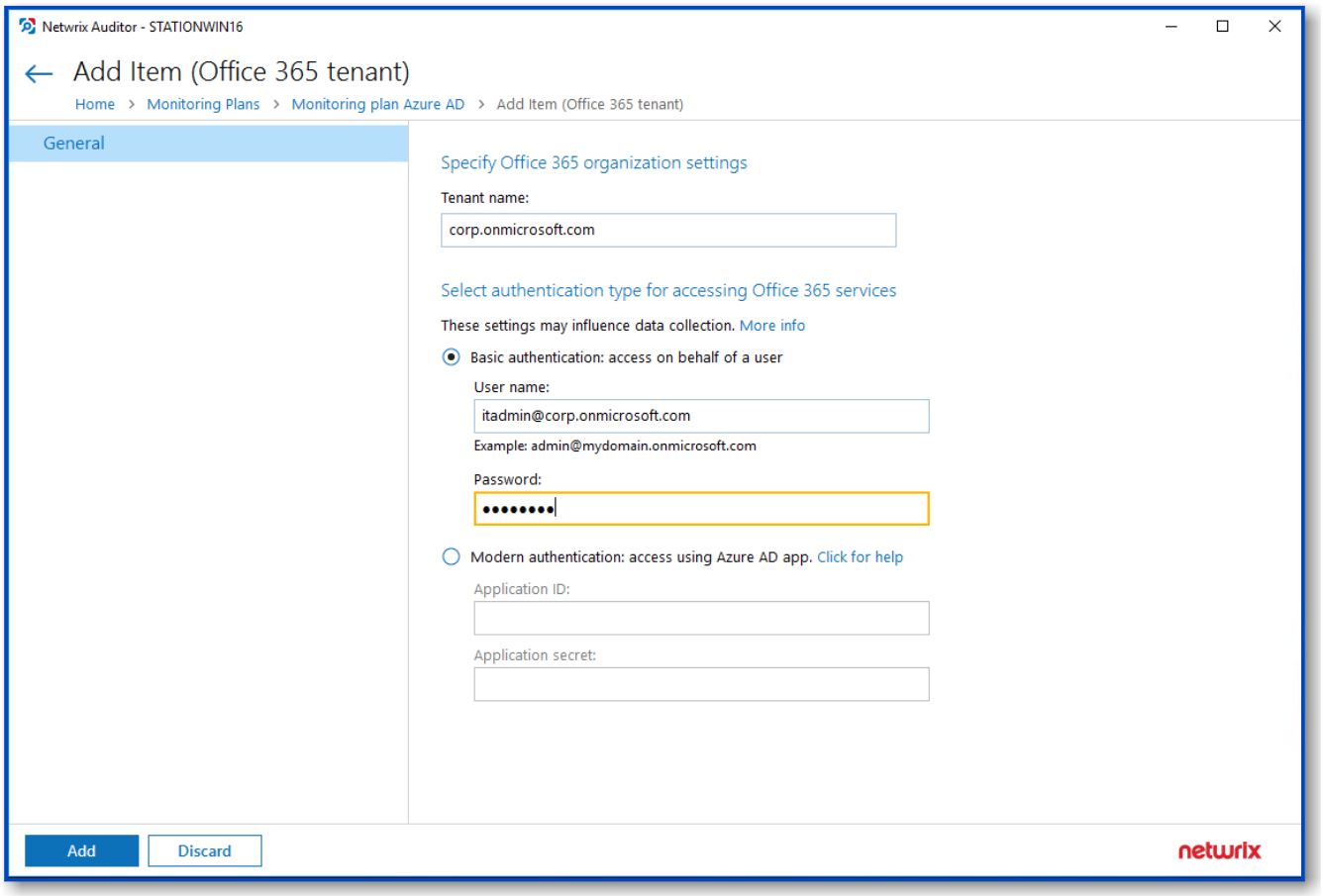
If you are using a government tenant, please click the **Tenant Environment** tab and select the desired tenant environment.

Step 2 – Select authentication method that will be used when accessing Office 365 services:

- Basic authentication:
  - Selected, Office 365 organization will be accessed on behalf of the user you specify.
  - Enter **User name** and **password**; use any of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*.
  - The **Tenant name** field then will be filled in automatically.
  - Make sure this user account has sufficient access rights. See Using Basic Authentication with Microsoft Entra ID topic for additional information.
- Modern authentication:

- Selected, Office 365 organization will be accessed using the Microsoft Entra ID (formerly Azure AD) app you prepared. Enter:
  - **Application ID**;
    - **Application secret**.
- See the Using Modern Authentication with Microsoft Entra ID for additional information.

Step 3 – Click the **Add** button.



You can use a single account to collect audit data for different Office 365 services (Microsoft Entra ID, Exchange Online, SharePoint Online); however, Netwrix recommends that you specify individual credentials for each of them.

Step 4 – Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information.

After that, you can use the Microsoft Entra ID management portal to revoke this privileged role and assign one of the non-privileged roles instead (for example, *Security Reader*).

Network Devices

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Network Devices – Configure data source as required to be monitored

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.

Cisco Meraki Dashboard

Complete the following fields:

Option	Description
Specify credentials to connect to Cisco Meraki Dashboard	Provide a name of your organization or an account used to connect to Cisco Meraki dashboard.
Select authentication type	There are two authentication options available to collect data from Cisco Meraki devices: • Access through API. You can access Cisco Meraki dashboard using API secret key if one-time password (OTP) MFA is required in your organization. In this case, you need to provide your API secret key. See Cisco Meraki documentation for additional information about Cisco Meraki API: Meraki Dashboard API. • Basic authentication: access on behalf of a user. Provide the name and password of the service account configured to access Cisco Meraki Dashboard. See the Configure Cisco Meraki Dashboard Account topic for additional information on how to configure the account used to collect data.

Syslog Device

Complete the following fields:

Option	Description
General	
Specify syslog host or network source	Select one of the following:

Option	Description
	• Host or network source name — Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network. • IP Range — Specify an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP subrange you want to exclude, and click **Add**.
Specify port and protocol for incoming connections	Use **Port** and **Protocol** to provide the port required for incoming connections (default is **UDP port 514**).
Devices	
Configure monitoring rules for required network devices: • **Cisco (ASA, IOS, FTD, Meraki)** • **Fortinet (FortiGate FortiOS)** • **Juniper (Junos OS)** • **Palo Alto (PAN-OS)** • **Sonic Wall (NS, SMA, WAF)** • **HPE (ArubaOS)** • **Pulse Secure**	

Oracle Database

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections

- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Oracle Database – Configure data source as required to be monitored

Complete the following fields:

Option	Description
General	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Monitor Oracle Database logon activity	Specify what types of logon events you want to monitor: successful or failed, performed through Windows and SQL authentication. • Failed logons • Successfullogons
Users	
Specify users to track their activity	Use controls in this section to populate the corresponding lists -click **Add** and specify user name and type (OS or database user). • Include—Add users to be included in the auditing scope. • Exclude—Add users to be excluded from the auditing scope by specifying their names and type (OS or database user). User names are case-sensitive.
Database Objects	

Option	Description
Data objects to monitor	Create rules for objects and actions that you want to audit: 1. Click Add Rule. 2. Specify a name of the Oracle database *Object* and *Schema*. 3. Select the necessary actions (successful or failed changes, successful or failed reads). 4. Click **Add**. Schema and object names are case sensitive.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Oracle Database Instance

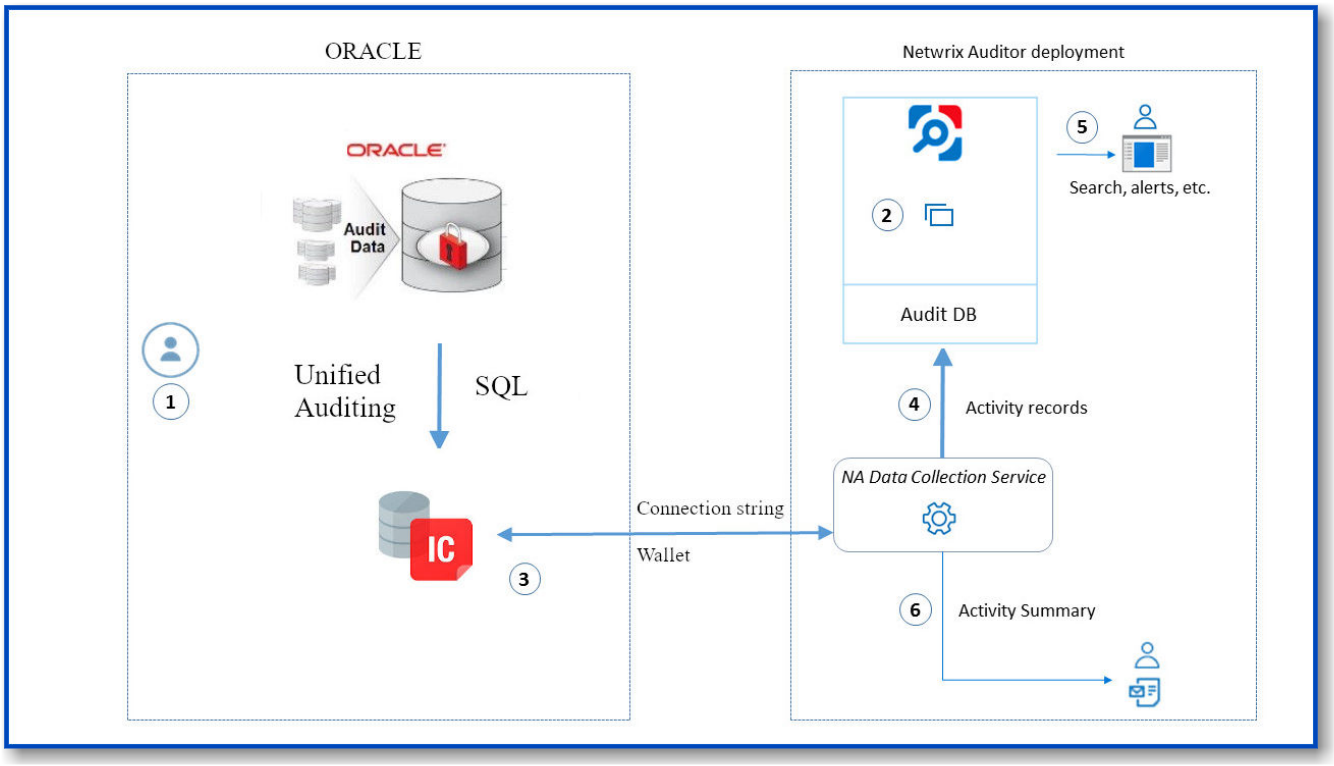
Complete the following fields:

Option	Description
Connection type	Select how the product connects to Oracle Database: • Oracle Database instance – select if you want to connect to a database by instance name. • Oracle Wallet – select if you want to use Oracle Wallet – password-protected container used to store authentication and signing credentials, including private keys, certificates, and trusted certificates needed by SSL.
Instance name	Provide connection details in the following format: *host:port/service_name.* Make sure audit settings are configured for your Oracle Database instance.

Option	Description
Wallet alias	Provide the alias you set while creating wallet. For example, "*MyOracle*". Alias name in Netwrix Auditor should exactly match the alias in the `tnsnames.ora` file. Configure Oracle Instant Client for HTTP Proxy Connections
Specify the account for collecting data **For Oracle Database instance connection type only.**	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

Data Collection from Oracle Database

On a high level, data collection process for Oracle databases works as follows:



1. Oracle administrator prepares a dedicated service account with sufficient permissions to collect data from Oracle Database. See the Permissions for Oracle Database Auditing topic for additional information.

2. Netwrix administrator does the following:

   - Creates a monitoring plan in Netwrix Auditor, specifying the service account (prepared at step 1) as a data collecting account in the Monitoring Plan wizard. Then s/he adds items to the monitoring plan – these are Oracle Databases to collect data from.
   - Configures alerts related to Oracle data source. Current version does not include predefined alerts for that data source, so follow the Create Alerts section to create and configure the necessary alerts.

   Remember to set the filter to “Data Source*equals* Oracle”.

3. Netwrix Auditor Data Collection Service starts periodic (every 10 min by default) data collection sessions. The results of each session include audit events that occurred since the previous data collection. Data is retrieved via Oracle Instant Client application. The product uses direct connection string or Oracle Wallet to connect to Oracle databases.

4. Netwrix Auditor Data Collection Service processes collected data into the proprietary format (Activity Records). Each Activity Record contains initiator’s account, time, action, and other details.

- To determine what has changed in the configuration, it compares a state snapshot from Oracle Server with the previously taken.
- To get '*Who*' (initiator) and '*When*' (date and time) information for the detected changes, the product uses Oracle events data.

Netwrix Auditor Serverthen writes the Activity Records to the audit database (default retention – 180 days) and long-term archive (default retention – 120 months).

5. Users can work with collected data in Netwrix Auditor client UI: run search, view reports, and so on. If you have configured alerting in Netwrix Auditor, then the activities that match the certain criteria will trigger the alerts. Recipients will be notified by email, and response actions will be taken, if configured.

6. Netwrix Auditor also generates an Activity Summary once a day (by default, at 3 AM) and sends it to the specified recipients. This email lists Oracle infrastructure changes and activities collected by Netwrix Auditor during the last 24 hours.

Oracle Database Monitoring Scope

You can fine-tune Netwrix Auditor by specifying users that you want to exclude from the Oracle Database monitoring scope.

Follow the steps to exclude data from the Oracle Database monitoring scope:

Step 1 – In Auditor, navigate to your Oracle Database monitoring plan and click Edit.

Step 2 – In the right pane, select Edit data source.

Step 3 – Navigate to Users tab and click Add next to Exclude.

Step 4 – In the Add User dialog, type name of the user you want to exclude and select its type (OS user or Database user).

Step 5 – Click Add to exclude selected user from being monitored.

SharePoint

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections

- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- SharePoint – Configure data source as required to be monitored

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Detect additional details	Specify additional information to include in reports and activity summaries. Select Group membershipif you want to include Group membership of the account under which the change was made.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the SharePoint configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them.
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information.

Option	Description
	In the **Manage historical snapshots** section, you can click **Manage** and select the snapshots that you want to import to the Audit Database to generate a report on the data source's state at the specific moment in the past. You must be assigned the **Global administrator** or the **Global reviewer** role to import snapshots. Move the selected snapshots to the Snapshots available for reporting list using the arrow button. The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Users can also configure Only the latest snapshot is available for reporting in Auditor . If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Troubleshoot SharePoint Auditing

Problem	Description	KB article
The "Timeout Expired" error appears during the agent's deployment.	The agent failed to be deployed due to one of the following reasons: • One or several servers are unreachable • The SPAdminV4 service is not started on any of the servers. • The servers within the farm are located in different time zones. http://support.microsoft.com/kb/2655727	www.Netwrix.com/kb/1868

Problem	Description	KB article
	• Your SharePoint farm exceeds the recommended capacity limits. http://technet.microsoft.com/en-us/library/cc262787 Increase DeployTimeout value in *%ProgramData%\Netwrix\NetwrixAuditor for SharePoint\ Configuration\ <managed_object_name>\ Commonsettings.config* and restart the agent service.	

SharePoint Farm

Complete the following fields:

Option	Description
General	
Specify SharePoint farm for monitoring	Enter the SharePoint Central Administration website URL.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

Option	Description
Core Service	
Deploy Netwrix Auditor for SharePoint Core Service	Select deployment method for the Core Service. Select one of the following: • Automatically—The installation will run under the account used to collect data on the SharePoint farm wizard completion. 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 SharePoint 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 Permissions for SharePoint Auditing topic for more information. • Manually—See the Netwrix Auditor Installation and Configuration Guide for more information.

Option	Description
	During the Netwrix Auditor for SharePoint Core Service installation / uninstallation your SharePoint sites may be unavailable.
Changes	
Audit SharePoint farm configuration changes	Configuration changes are always audited.
Audit SharePoint permissions and content changes	Select change types to be audited with Netwrix Auditor. Netwrix Auditor allows auditing the entire SharePoint farm. Alternatively, you can limit the auditing scope to separate web applications and site collections. To do it, select Specific SharePoint objects and do one of the following: • Click Add, provide the URL to web application or site collection and select object type (Web application or Site collection). • Click Import, select object type (Web application or Site collection), encoding type, and browse for a file that contains a list of web applications and sites. Netwrix Auditor ignores changes to system data (e.g., hidden and system lists or items are not audited). Netwrix Auditor also ignores the content changes to sites and objects on the site collections located on Central Administration web application, but the security changes that occurred there are tracked and reported anyway.
Activity	
Specify monitoring restrictions	Specify restriction filters to narrow your SharePoint monitoring scope (search results, reports and Activity

Option	Description
	Summaries). For example, you can exclude site collections document libraries and lists from being audited as they contain public non sensitive data. All filters are applied using AND logic. Click Add and complete the following fields: • User – provide the name of the user as shown in the "*Who*" column of reports and Activity Summaries. Example: *mydomain\user1*. • Object URL – provide URL of the objects as shown in the "*What*" column of reports and Activity Summaries. Example: *http://sitecollection/list/document.docx*. • Action Type – select what types of actions performed by selected users under the object you want to monitor. Available values: *All*, *Changes*, *Reads*. You can use a wildcard (*) to replace any number of characters in filters. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.
Read Access	
Audit SharePoint read access	Configure Netwrix Auditor to track read access to lists and list items within your SharePoint farm except for Central Administration web sites. Select Sites only if you want to enable read access auditing on SharePoint sites only. Enable Sites and subsites to track read access on each subsite. Then, do one of the following: • Click Add and provide URL to a SharePoint site. • Click Import, select encoding type, and browse for a file that contains a list of sites.

Option	Description
	Read access auditing significantly increases the number of events generated on your SharePoint and the amount of data written to the AuditArchive.

SharePoint Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the SharePoint monitoring scope.

Follow the steps to exclude data from the SharePoint monitoring scope:

Step 1 – Navigate to the *%working folder%\Netwrix Auditor for SharePoint\Configuration\GUID* folder, where omit lists are located.

If you have several monitoring plans for monitoring SharePoint farms, configure omit lists for each monitoring plan separately.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omiteventloglist.txt	Contains a list of event IDs to be excluded from the Netwrix Auditor System Health event log.	`event ID`
		For example:
		`1001`
		Only add known error or warning events, otherwise you may lose important data.

File	Description	Syntax

omitscreadaccesslist.txt	Contains a list of site collections for which the product will not monitor read access attempts.	`http(s)://URL`
		
		Enter the root web site URLs.
		
		If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs to specify a child site collection.
		
		For example:
		
		`http://sharepointsrv:3333/`

omitscstorelist.txt	Contains a list of site collections to be excluded from audit data collection.	`http(s)://URL`
		
		Enter the root web site URLs.
		
		If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs to specify a child site collection.
		
		For example:
		
		`https://siteColl*`

omitsitscstorelist.txt	Lists site collections to exclude from being monitored and reported in state-in-time report.	`http(s)://URL` Enter root web site URLs. If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of

File	Description	Syntax

		these URLs to specify a child site collection.
		
		You can use a wildcard (*) to replace any number of characters.
		
		Examples:
		
		`http://siteCollection1:3333/`
		`https://siteColl*`

omitsitstorelist.txt	Contains SharePoint lists and list items that you want to exclude from being audited.	URI Reference
		
		URI Reference does not include site collection URL. For example, to exclude the list item with URL *http://sitecollection/list/document.docx*, specify only "*list/document.docx*" instead of full URL.
		
		Wildcard (*) is supported to replace any number of characters.
		
		Examples:
		
		`*list/document.docx`
		`*/_catalogs/*`
		`*/_vti_inf.html`
		`*/Style Library*`
		`*/SitePages*`

omituserviewstorelist.txt	Contains a list of user or service accounts to be excluded from read access monitoring.	`Login name` For example: SHAREPOINT\System
omitviewstorelist.txt	Contains lists and list items to be excluded from being monitored for read access.	`URI Reference` Only specify URI reference to a list or list item without `https:\\<siteCollection_name>` part. For example:

File	Description	Syntax
		`*list/document.docx`

omitwastorelist.txt	Contains a list of web applications to be excluded from audit data collection.	`http(s)://URL`
		
		Enter the root web site URLs. If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs.
		
		For example:
		
		`http://webApplication1:3333/`

SharePoint Online

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- SharePoint Online – Configure data source as required to be monitored

How to Add Office365 Item

This instruction shows how to collect audit data from the Microsoft 365 tenant.

If you plan to use modern authentication, see the Configuring Microsoft Entra ID App for Auditing Microsoft Entra ID topic for additional information on how to prepare Microsoft Entra ID app with required permissions. Make sure you have the following at hand:

- Tenant name

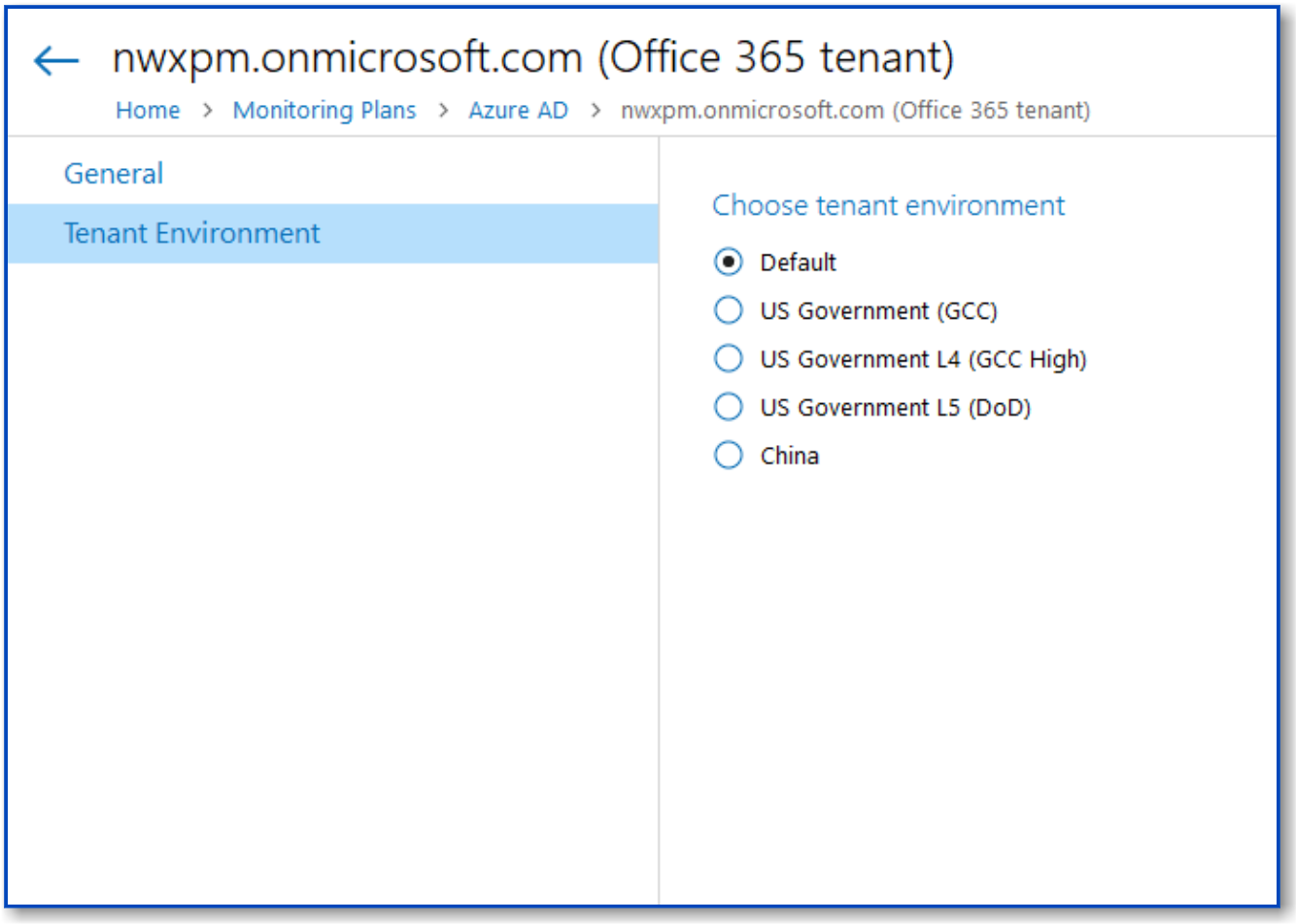
- For modern authentication: Application (client) ID
- Application secret
- For basic authentication: User name and password

Types of data that can be collected by Netwrix Auditor from the Microsoft 365 tenant depend on the authentication option you choose.

Follow the steps to configure Office 365 tenant as a monitored item.

Step 1 – On the **General** page of the item properties, specify **Tenant name**:

- If you are going to use **Basic authentication**, you can proceed to the next step – **Tenant name** will be filled in automatically after it.
    - **NOTE:** Basic authentication is no longer possible for Exchange Online. For the already existing tenants it is still possible to use basic authentication for SharePoint Online and Microsoft Entra ID monitoring.
- If you are going to use **Modern authentication**, paste the obtained name. See the Using Modern Authentication with Microsoft Entra ID topic for additional information.



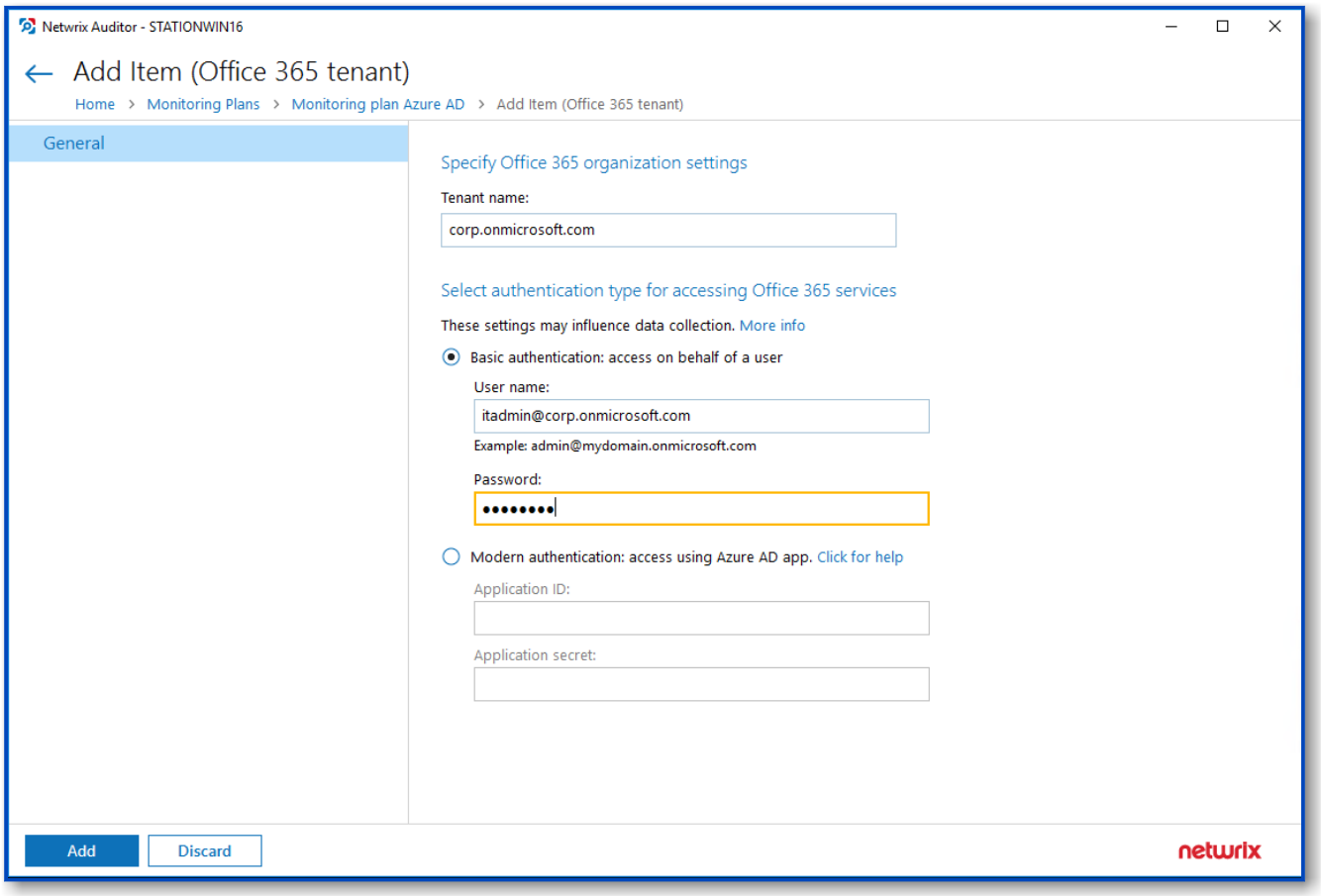
If you are using a government tenant, please click the **Tenant Environment** tab and select the desired tenant environment.

Step 2 – Select authentication method that will be used when accessing Office 365 services:

- Basic authentication:
  - Selected, Office 365 organization will be accessed on behalf of the user you specify.
  - Enter **User name** and **password**; use any of the following formats: *user@domain.com* or *user@domain.onmicrosoft.com*.
  - The **Tenant name** field then will be filled in automatically.
  - Make sure this user account has sufficient access rights. See Using Basic Authentication with Microsoft Entra ID topic for additional information.
- Modern authentication:

- Selected, Office 365 organization will be accessed using the Microsoft Entra ID (formerly Azure AD) app you prepared. Enter:
  - **Application ID**;
    - **Application secret**.
- See the Using Modern Authentication with Microsoft Entra ID for additional information.

Step 3 – Click the **Add** button.



You can use a single account to collect audit data for different Office 365 services (Microsoft Entra ID, Exchange Online, SharePoint Online); however, Netwrix recommends that you specify individual credentials for each of them.

Step 4 – Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Audit SharePoint Online configuration and content changes	Configuration and content changes are always audited.
Audit SharePoint Online read access	Configure Auditor to monitor SharePoint Online read access.
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your SharePoint Online configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database. For that, in the Manage historical snapshots section, click **Manage** and select the snapshots that you want to import. To import snapshots, you must be assigned the Global administrator or the Global reviewer role . Move the selected snapshots to the Snapshots available for reporting list using the arrow button. When finished, click **OK**.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

See the Permissions for SharePoint Online Auditing topic for additional information.

SharePoint Online Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the SharePoint Online monitoring scope.

Follow the steps to exclude data from the SharePoint monitoring scope:

Step 1 – Navigate to the *%ProgramData%\Netwrix Auditor\Netwrix Auditor for SharePoint Online\Configuration* folder and locate your monitoring plan.

If you have several monitoring plans for monitoring SharePoint Online, configure omitlists for each monitoring plan separately.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitstorelist.txt	Contains a list URLs of SharePoint Online objects to be excluded from audit data collection.	`https://URL`
		For example:
		`https://Corp.sharepoint.com/*`

omiteventloglist.txt	Contains a list of event IDs to be excluded from the Netwrix Auditor System Health event log.	`event ID` For example:

File	Description	Syntax
		`1001` Only add known error or warning events, otherwise you may lose important data.

omitreadstorelist.txt	Contains the SharePoint Online lists, documents, etc., to be excluded from being monitored for read access.	`https://URL`
		
		For example:
		
		`https://Corp.sharepoint.com/*`
		
		`*list/document.docx`

omituserreadstorelist.txt	Contains a list of user accounts to be excluded from read access monitoring.	Provide user name in the UPN format. For example: `account@example.*.com`
OmitSitScStoreList.txt	Contains a list of SharePoint Online site collections to be excluded from state-in-time data collection.	Enter root web site URLs. For example: `https://URL`
OmitSitStoreList.txt	Contains SharePoint Online lists and list items to be excluded from state-in-time data collection.	Enter list or list item URI (Unique resource identifier, or endpoint) reference. Note that URI Reference does not include site collection URL. For example, to exclude a list item with the `https://`

File	Description	Syntax
		`sitecollection.sharepoint.com/list/document.docx`, URL, you should specify the corresponding endpoint (URI), i.e. `list/document.docx`.

SQL Server

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- SQL Server – Configure data source as required to be monitored

To configure SQL Server data source settings, use the following property tabs:

- General settings
- Users
- Data
- Audit SELECT

When finished, review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the Data source list.

As a next step, click Add item to specify an object for monitoring. See the Add Item to the SQL Server topic for additional information.

General settings

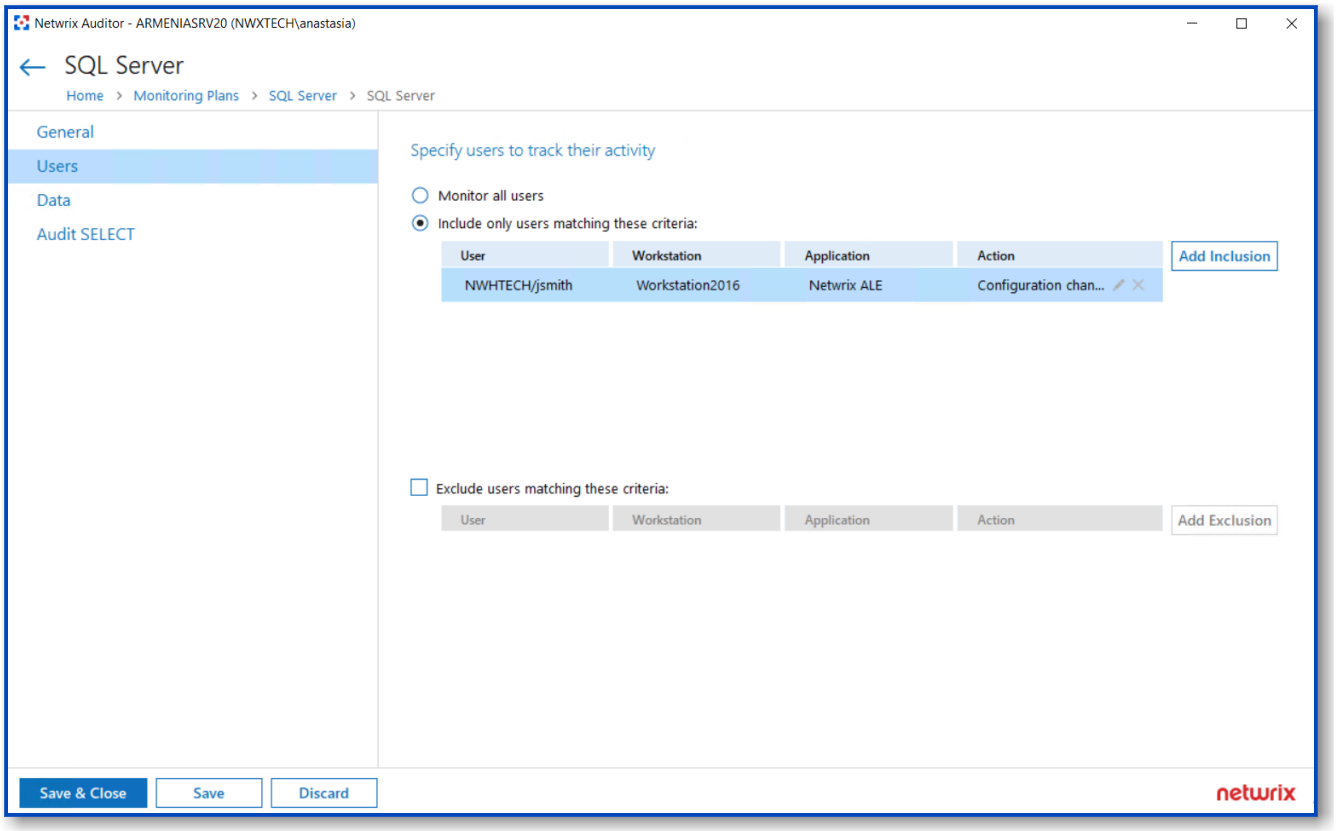
On the **General** tab, you can configure the following settings for SQL Server data source:

Option	Description
General	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Monitor SQL Server configuration changes	Always enabled, as SQL Server configuration changes are always monitored.
Monitor SQL Server logon activity	Specify what types of logon events you want to monitor: successful or failed, performed through Windows and SQL authentication. • Failed logons • Successfullogons
Collect data for state-in-time reports	Configure Netwrix Auditor to store the snapshots of your SQL Server instance configuration — you will require them for state-in-time reports generation. See State–In–Time Reports for more information. **CAUTION:** The State-in-Time functionality is not available for SQL Server Availability Groups. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.

Option	Description
	To import snapshots, you must be assigned the Global administrator or the Global reviewer role in Netwrix Auditor. 1. In the Manage historical snapshots section, click **Manage** and select the snapshots that you want to import. 2. Move the selected snapshots to the Snapshots available for reporting list using the arrow button. 3. When finished, click **OK**. See also Using historical data.

Users

On the **Users** tab, you can configure the following settings for SQL Server data source:



Options	Description
Specify users to track their activity	Select the option you need to fine-tune your SQL Server monitoring scope. • **Monitor all users** • **Include only users matching these criteria** • **Exclude users matching these criteria** For example, you may need to track only actions performed by administrative accounts, or exclude the activity initiated by ordinary applications. If so, data should be filtered accordingly before it appears in search results, reports and Activity Summaries. You can create either inclusion or exclusion lists. All filters are applied using AND logic. To create a filter for user activity monitoring, select the related option and click the button on the right.

Options	Description
	Specify the following: • User — enter the initiator's account as it appears in the "*Who*" column of reports and Activity Summaries, for example: *mydomain\user1*. For events containing “*System*” in the “*Who*” column you can enter "*System*" . • Workstation where activity was initiated — enter the workstation name as it is shown in the "*Workstation*" column of reports and Activity Summaries, for example: *StationWin2016*. • Application that initiated the activity — enter the application name as shown next to "*Application name*" in details of reports and Activity Summaries. You can use a wildcard (*) to replace any number of characters in filters. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Data

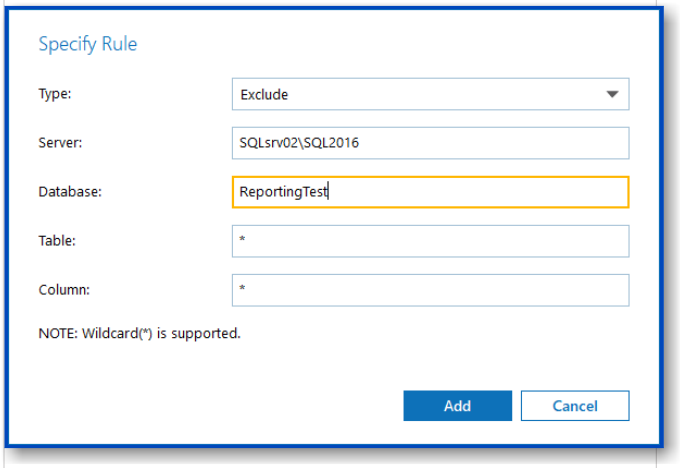
On the **Data** tab, you can configure the following settings for SQL Server data source.

Remember, when auditing SQL Server availability on groups, the only supported data collection mode is the '*Do not use triggers* ' mode.

Option	Description

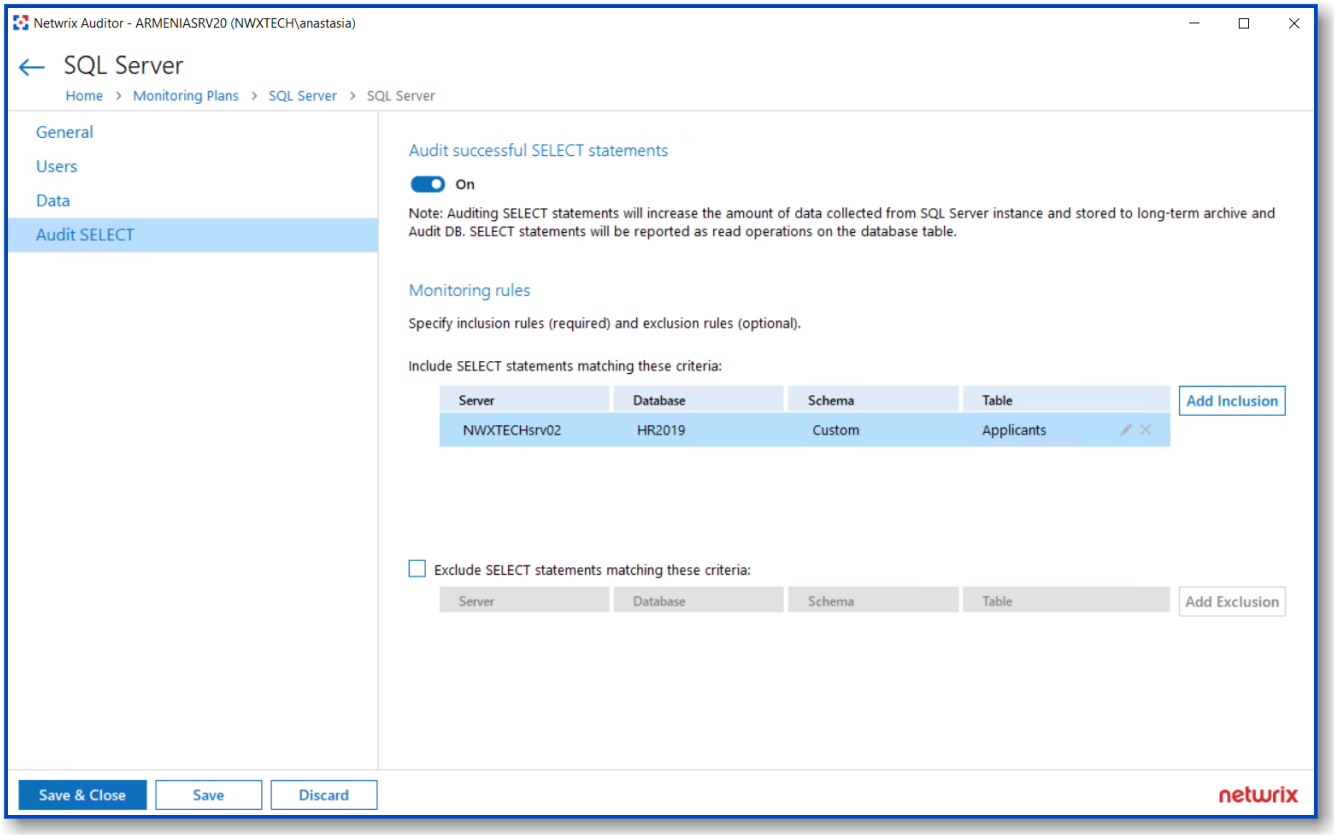
Option	Description
Monitor changes to data in the database tables	Enable monitoring of changes to data stored in the database tables hosted on the SQL Server. If you plan to enable this option, make sure the account that runs the *SQL Server service* on the monitored instance has at least *read* permissions in the Active Directory domain (e.g., it does not run under a local user account). Otherwise, enabling this option may lead to issues when altering databases on the monitored SQL Server instances.
Data collection mode	
Do not use triggers	Default mode for a new installation of Netwrix Auditor. Data will be collected using the SQL Server traces. This mode allows you to get a sufficient level of detail in the reports and search results without producing additional load on your SQL Server instance. Thus, it is recommended for highly-transactional servers. When using this mode, consider that the "*What*" field of the Activity Record with "*Object type*" = "*Data*" may show incorrect data. The issues occur because the product applies data categories to an entire SQL Server table and not to rows.
Use triggers for detailed monitoring	However, if you require a very detailed reporting on the data changes, you can select this mode. It will be also selected by default if you are upgrading your Netwrix Auditor deployment. Data will be collected using a set of triggers. For more information on this technology, see https://kb.netwrix.com/728 .

Option	Description
	It is recommended to use this setting carefully, as collecting large amount of details from a highly-transactional server may affect its performance. Using this mode may lead to issues when altering databases on the monitored SQL Server instances. The issues occur only if the SQL Server service account does not have *Read* permissions in the Active Directory domain (e.g., a local user account). When using this mode, consider that the "*What*" field of the Activity Record with "*Object type*" = "*Data*" may show incorrect data. The issues occur because the product applies data categories to an entire SQL Server table and not to rows. Switching from the configured triggerless mode may lead to a data loss. The workaround is to force data collection right after enabling the triggers.
Changes (per transaction) to collect and report:	Specify how many changes per a database transaction you want to be collected. For example, you can limit this number to 10 changes per transaction, or collect all changes. It is recommended to adjust this setting carefully, as collecting large number of changes from a highly-transactional server may affect its performance.
Monitoring rules	To specify what data changes must be monitored, create at least one **inclusion rule**. Exclusion rules are optional. Click **Add Rule** and configure the following:

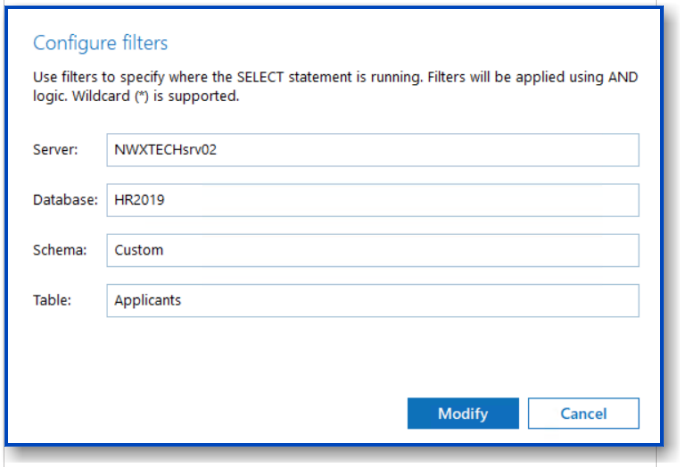
Option	Description
	 • Type — Select rule type: include or exclude. • Server — Specify a name of the monitored SQL Server instance where the required database resides. Use the *server_name\instance_name* format, for example, *SQLsrv11\SQLExpress2016*. **NOTE:** If you are going to configure monitoring rules for SQL Server Availability Groups, provide the name of your Availability Group item in this field. • Database — Specify the database whose data changes you want to monitor. • Table — Specify database table to monitor. • Column—Specify table column name. The following column types are currently not supported: `text`, `ntext`, `image`, `binary`, `varbinary`, `timestamp`, `sql_variant`. These filters will be applied using AND logic. Wildcard (*) is supported and can be used to replace any number of characters.

Audit SELECT

Use the settings in this section to configure how the successful SELECT statements should be audited.



Option	Description
Audit successful SELECT statements	Enable monitoring of successful SELECT statements for the database tables. Successful SELECT statement execution will be reported as Read operation on the database table. Auditing SELECT statements will increase the amount of data collected from the SQL Server instance and stored to long-term archive and audit database. Plan for your resources accordingly.

Option	Description
Monitoring rules	To specify what data changes will be monitored, you must create at least one **inclusion rule**. Exclusion rules are optional. Click **Add Inclusion** and specify the following:  • Server — specify target SQL Server instance in the server\instance format. **NOTE:** If you are going to configure monitoring rules for SQL Server Availability Groups, provide the name of your Availability Group item in this field. • Database — specify target database • Schema — specify database schema • Table — specify database table you will monitor Wildcard (*) is supported and can be used to replace any number of characters. Filters will be applied using AND logic, that is, only SELECT statements matching all specified criteria will be monitored. So, in the example above, the program will track and report only the successful SELECT statements executed against the *Applicants* table of the *HR2019* database with *Custom* schema, hosted on the *SQLsrv02\TestInstance*.

Option	Description
	When finished, click **Add**. If needed, configure the exclusion rules in a similar way.

Add Item to the SQL Server

Perform the following steps to add an item to the SQL Server monitoring plan.

Step 1 – Create a monitoring plan for the SQL Server.

Step 2 – Double-click SQL Server monitoring plan.

Step 3 – Click **Add Item**.

Step 4 – Select one of the items from the drop-down list:

- SQL Server Instance
- SQL Server Availability Group

Step 5 – Click **Add**.

Item is added and SQL Server monitoring plan is ready to use.

SQL Server Instance

Complete the following fields:

Option	Description
Specify SQL Server instance	Specify the name of the SQL Server instance.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other

Option	Description
	than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

Use a combination of server role, environment, instance name (including "DEFAULT" for default instances), and a unique identifier.

Example:

- Production default instance: PROD-SQL-01
- Development named instance: DEV-SQL-01\DEVINSTANCE
- Test named instance on a specific port: TEST-SQL-01\TESTINSTANCE:1440

NOTE: When dealing with SQL Server instances, Always On Availability Group (AG) instances, and a mix of default and non-default instances along with specified ports, it's important to craft names that provide clear identification.

SQL Server Availability Group

Complete the following fields:

Option	Description
Availability group listener	Provide a name of an availability group listener in FQDN or NetBIOS format. The listener is a virtual network name (VNN) that you can connect to in order to access a database in a primary or secondary replica of an Always On availability group. A listener allows you to connect to a replica without having to know the physical instance name of the SQL Server.

Option	Description
	Ensure that the requirements to the DNS name and Windows permissions requirements are met. See Configure a listener for an Always On availability group for additional information.
Availability group name	Enter a name of your SQL Server availability group.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

Extend the SQL Server instance name with a replica role (Primary/Secondary), AG identifier, and a unique identifier.

Example:

- For: `PROD-SQL-01-AG1`

SQL Server Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the SQL Server monitoring scope.

Follow the steps to exclude data from the SQL Server monitoring scope.

Step 1 – Navigate to the *%Netwrix Auditor install folder%\SQL Server Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.

- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitarlist.txt	Lists activity records to exclude from showing up in reports, search, and activity summaries.
	
	This omit list does not affect triggerless data collection mode, SELECT statements auditing and SQL logons monitoring. Use the *omitlogonlist.txt* to exclude SQL logons from monitoring. Use the *omitreadaccess.txt* to exclude SELECT statements from monitoring.
		Specify the following fields of the activity records to exclude:
		
		`Monitoring plan name, SQL Server instance,object type, account,workstation,application na`
		
		Wildcard (*) is supported and can replace any number of characters.
		
		For the account, workstation, application name fields, you can specify a mixed expression that contains both a value and a wildcard (e.g., Admin*).
		
		For example:
		
		`SQLPlan,Ent-SQL,Table,guest,WksSQL`

omiterrorlist.txt	Contains a list of errors and warnings to be excluded from logging to the Netwrix Auditor System Health event log.	`Monitoring plan name,item name,error text`
		
		Wildcard (*) is supported and can replace any number of characters.
		
		For example:
		
		`*,sqlserver1.corp.local, *Access is denied*`

omitlogonlist.txt	Contains a list of logons to exclude from monitoring.	`monitoring plan name,SQL Server instance,logon type,account,workstation ,application name`

File	Description	Syntax
		For the `account`, `workstation`, `application name` fields, you can specify a mixed expression that contains both a value and a wildcard (e.g., `Admin*`). The following logon types are supported: • `NtLogon` — Successful logon attempt made through Windows authentication. • `SqlLogon` — Successful logon attempt made through SQL Server authentication. • `NtFailedLogon` — Failed logon attempt made through Windows authentication. • `SqlFailedLogon` — Failed logon attempt made through SQL Server authentication. For example: `DB_M0,Ent-SQL,SQLFailedLogon,guest,WksSQL,MyInternalApp`

omitobjlist.txt	Contains a list of object to exclude from showing up in reports, search results and activity summaries.
	
	Audit data, however, will still be collected and saved to Long-Term Archive.
	
	This omit list does not affect SELECT statements auditing, data changes auditing and logon activity auditing.
		`object_type_name`
		
		Available object types can be found in the "Object type" column in reports.
		
		For example:
		
		`Database`

File	Description	Syntax
	Use the *omitlogonlist.txt* to exclude logon activity from monitoring. Use the *omitreadaccess.txt* to exclude SELECT statements from monitoring.	`Column`
omitpathlist.txt	Specify the resource paths to objects that you want to exclude from showing up in search, reports and activity summaries. Audit data, however, will still be collected and saved to Long-Term Archive. This omit list does not affect triggerless data collection mode, SELECT statements auditing and logon activity auditing. Use the *omitlogonlist.txt* to exclude logon activity from monitoring. Use the *omitreadaccess.txt* to exclude SELECT statements from monitoring.	`server_instance:resource_path` where: • `server_instance` — SQL Server instance, use * for all servers • `resource_path` — resource path as shown in the "**What**" column of SQL Server report, or in search results Wildcard * is supported and can replace any part of the path. For example, to exclude information about databases whose names start with "tmp" on the SQL Server instance "PROD.SQL2012": `PROD.SQL2012:Databases\tmp*`.
omitproplist.txt	Contains a list of attributes to be excluded from being monitored and stored to the Audit Archive.	`object_type_name.property_name.attribute_name` where: • `object_type_name`—Can be found in the found in the Object Type column in change reports.

File	Description	Syntax
		• `property_name`—Can be found in the Details column (property name is bold). • `attribute_name`—Can be found in the Details column (attribute name is not bold). If an object does not have an attribute name, use the * character. For example to exclude information about the Size attribute of the Database File property in all databases: `Database.Database File.Size`.

omitstorelist.txt	Contains a list of SQL Server objects that you want to exclude from data collection and reporting.
	This list is only relevant to operations with SQL Server objects; it does not affect triggerless data collection mode, SELECT statements auditing and logon activity auditing. To configure exclusions for logon activity auditing (Windows or SQL logons), use the *omitlogonlist.txt*. Use the *omitreadaccess.txt* to exclude SELECT statements from monitoring.
		`server_instance:resource_path`
		where:
		• `server_instance` — SQL Server instance. For all instances, use wildcard (*).
		• `resource_path` — path as shown in the "**What**" column of SQL Server report, or in search results. Wildcard (*) can be used to replace any number of characters.
		For example, to exclude information about server roles on the SQL Server instances whose names start with *njsqlsrv23*, enter:
		`njsqlsrv23*:Security\Server Roles\*`

File	Description	Syntax
omittracelist.txt	If you do not want the product to enable SQL tracing on some of your SQL Server instances, specify their names in this omitlist. In this case the "Who", "Workstation" and "When" values will not be reported correctly (except for content changes). This omit list does not affect triggerless data collection mode, SELECT statements auditing and logon activity auditing. Use the *omitlogonlist.txt* to exclude logon activity from monitoring. Use the *omitreadaccess.txt* to exclude SELECT statements from monitoring.	Enter the name of SQL Server instance, use * for all servers: `server\instance name` Wildcard (*) is supported and can replace any number of characters, e.g., MYSERVER_SQL* Examples: * *\SQLExpress MYSERVER*

propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in the change reports.	`object_type_name.property_name=friendlyname`
		
		For example:
		
		`*.Date modified=Modification Time`

User Activity

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems

- User Activity – Configure data source as required to be monitored

Complete the following fields:

Option	Description
General	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Notify users about activity monitoring	You can enable the message that will be displayed when a user logs in and specify the message text.
Record video of user activity within sessions	• If disabled, only user session events will be collected (regardless of whether the user is idle or not). • If enabled, the product will both collect user session events and record video of user activity. By default, this option is disabled.
Video Recording **For these settings to become effective, enable video recording on the General tab.**	
Adjust video quality	Optimize video file by adjusting the following: • File size and video quality • Save video in grayscale • CPU load and Video smoothness.
Adjust video duration	Limit video file length by adjusting the following: • Recording lasts for <...> minutes—Video recording will be stopped after the selected time period.

Option	Description
	• User has been idle for <...> minutes—Video recording will be stopped if a user is considered inactive during the selected time period. If the Record video of user activity within sessions option is enabled, the User Sessions report shows active time calculated without including user idle period. Mind that a computer is considered to be idle by Windows if there has not been user interaction via the mouse or keyboard for a given time and if the hard drives and processors have been idle more than 90% of that time. • Free disk space is less than <...> MB—Video recording will be stopped when upon reaching selected disk space limit. • Consider user activity — Select one of the following: ◦ Stop if user has been idle for <...> minutes. Select if you want video recording for a user to be stopped after the specified time period. ◦ Continue video recording regardless of the user idle state. When selected, Netwrix Auditor continues video recording for idle users.
Set a retention period to clear stale videos	When the selected retention period is over, Netwrix Auditor deletes your video recordings.
Users	
Specify users to track their activity	Select the users whose activity should be recorded. You can select **All users** or create a list of **Specific users or user groups**. Certain users can also be added to **Exceptions** list.

Option	Description
Applications	
Specify applications you want to track	Select the applications that you want to monitor. You can select All applications or create a list of Specific applications. Certain applications can also be added to Exceptions list.
Monitored Computers	
For a newly created monitoring plan for User Activity, the list of monitored computers is empty. Add items to your monitoring plan and wait until Netwrix Auditor retrieves all computers within these items. See Add Items for Monitoringfor more information. The list contains computer name, its current status and last activity time.	

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

How to Include/Exclude Applications

To create a list of application to include in / exclude from monitoring, you will need to provide:

- Titlie — application title as shown on top of the application window, for example, **MonthlyReport.docx - Word**.
    - Title can also be found in the "*What*" column of related Netwrix Auditor reports and search results, for example, in the **User Sessions** report.
- Description — as shown in the Description column on theDetails tab of Windows Task Manager.
    - Using Description can help to filter out several components of a single application — for example, all executables having *TeamViewer 14* description belong to the same app (see the screenshot above).

To create a list of inclusions / exclusions for applications:

Step 1 – Click Add on the right of the list.

Step 2 – Enter application title and description you have identified.

Wildcards (*?) are supported and applied as follows:

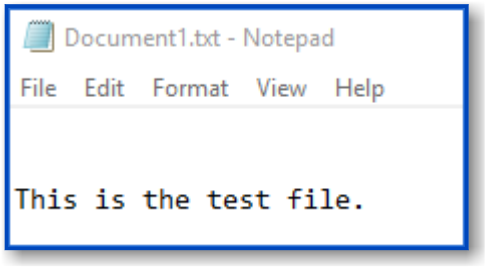
- * - *Notepad* (the "Title" filter) will exclude all Notepad windows.
- *colo?r** (the "Title" filter) will exclude all application window titles containing "*color*" or "*colour*".

Same logic applies to the inclusion rules.

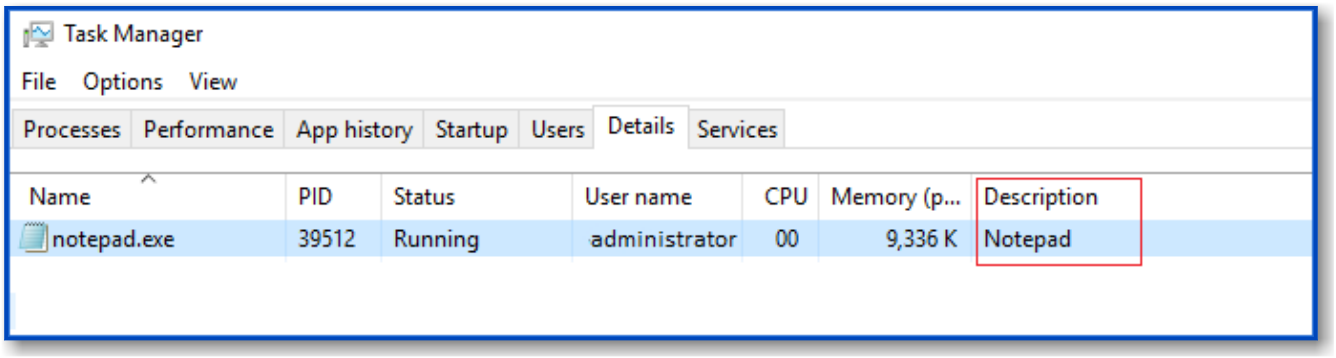
Example

To exclude the Notepad application window with "*Document1*" open, add the following filter values:

- In the Title filter enter "*Document1.txt - Notepad*":



- In the Description filter, enter the corresponding value, here it will be "*Notepad*".



IP Range

Complete the following fields:

Option	Description
General	
Specify IP range	Specify an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP subrange you want to exclude, and click **Add**.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.
Scope	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.

AD Container

Complete the following fields:

Option	Description
General	
Specify AD container	Specify a whole AD domain, OU or container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be audited within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Click **Exclude** to specify AD domains, OUs, and containers you do not want to audit. In the Exclude Containers dialog, click Add and specify an object. The list of containers does not include child domains of trusted domains. Use other options **(Computer, IP range** to specify the target computers.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. If using a group Managed Service Account (gMSA), you can specify only the account name in the *domain\account$* format. Password field can be empty. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.

Option	Description
	Refer to the Permissions for Active Directory Auditing topic for more information on using Netwrix Privilege Secure as an account for data collection. A custom account must be granted the same permissions and access rights as the default account used for data collection. See theData Collecting Account topic for additional information.
Containers and Computers	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Depending on the type of the object you want to exclude, select one of the following: • Add AD Container – Browse for a container to be excluded from being audited. You can select a whole AD domain, OU or container. • Add Computer – Provide the name of the computer you want to exclude as shown in the "*Where*" column of reports and Activity Summaries. For example, *backupsrv01.mydomain.local*.

Option	Description
	Wildcards (*) are not supported. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Computer

For evaluation purposes, Netwrix recommends selecting Computer as an item for a monitoring plan. Once the product is configured to collect data from the specified items, audit settings (including Core and Compression services installation) will be applied to all computers within AD Container or IP Range.

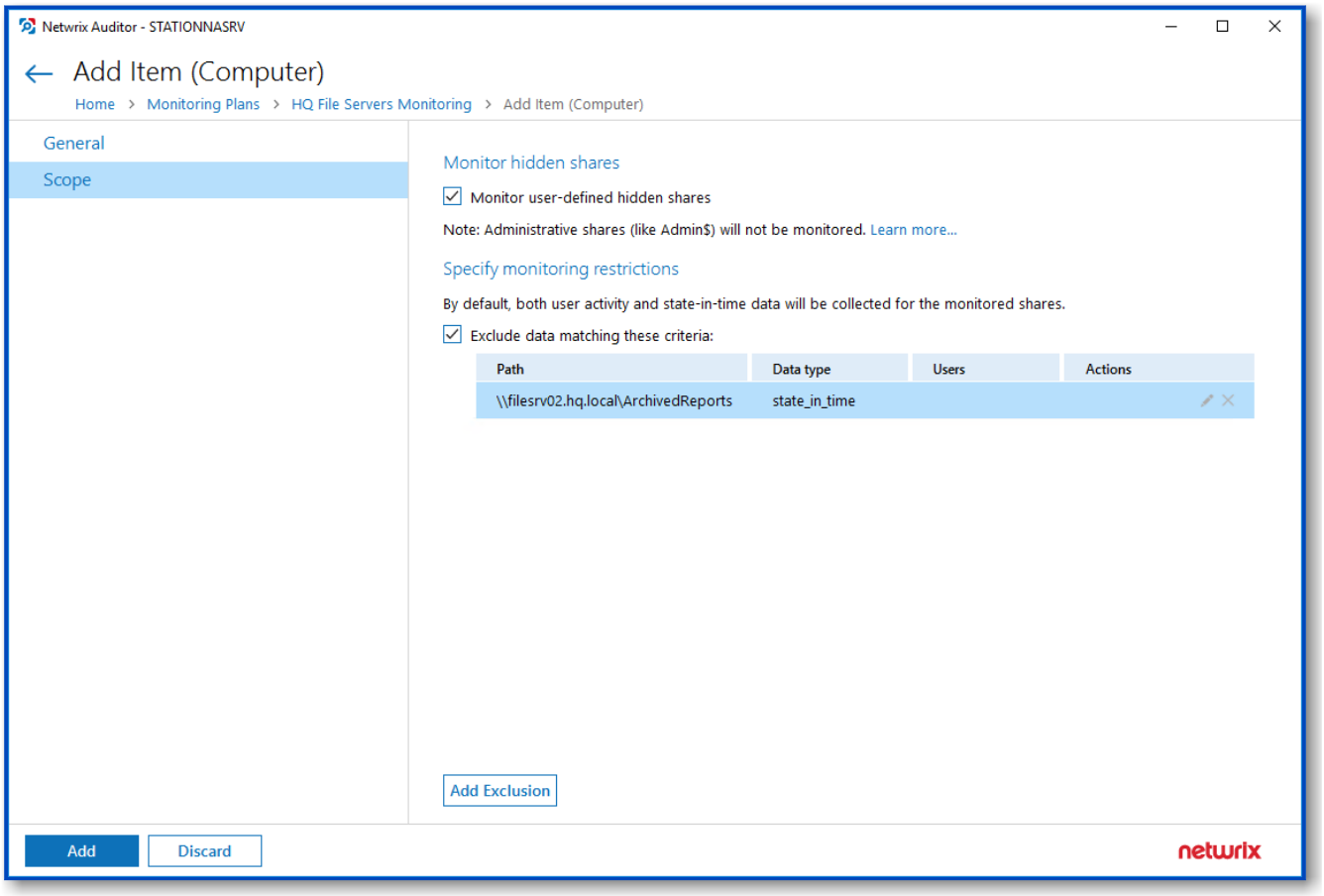
Complete the following fields:

Option	Description
General	
Specify a computer	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click Browse to select a computer from the list of computers in your network.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available: • User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the

Option	Description
	Data Collecting Account topic for additional information. • Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information. • Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.
Scope	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic.

Configure Scope

By default, both user activity and state-in-time data will be collected for the monitored item. However, you can narrow your monitoring scope by specifying certain locations, user accounts or actions to exclude .



Click Add Exclusion, then follow the steps in the Specify Filters dialog:

Step 1 – Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

You can use a wildcard (*) only if you need to exclude user activity on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

Step 2 – Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. In this case,Netwrix Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.
State-in-Time	Select to configure Netwrix Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Netwrix Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

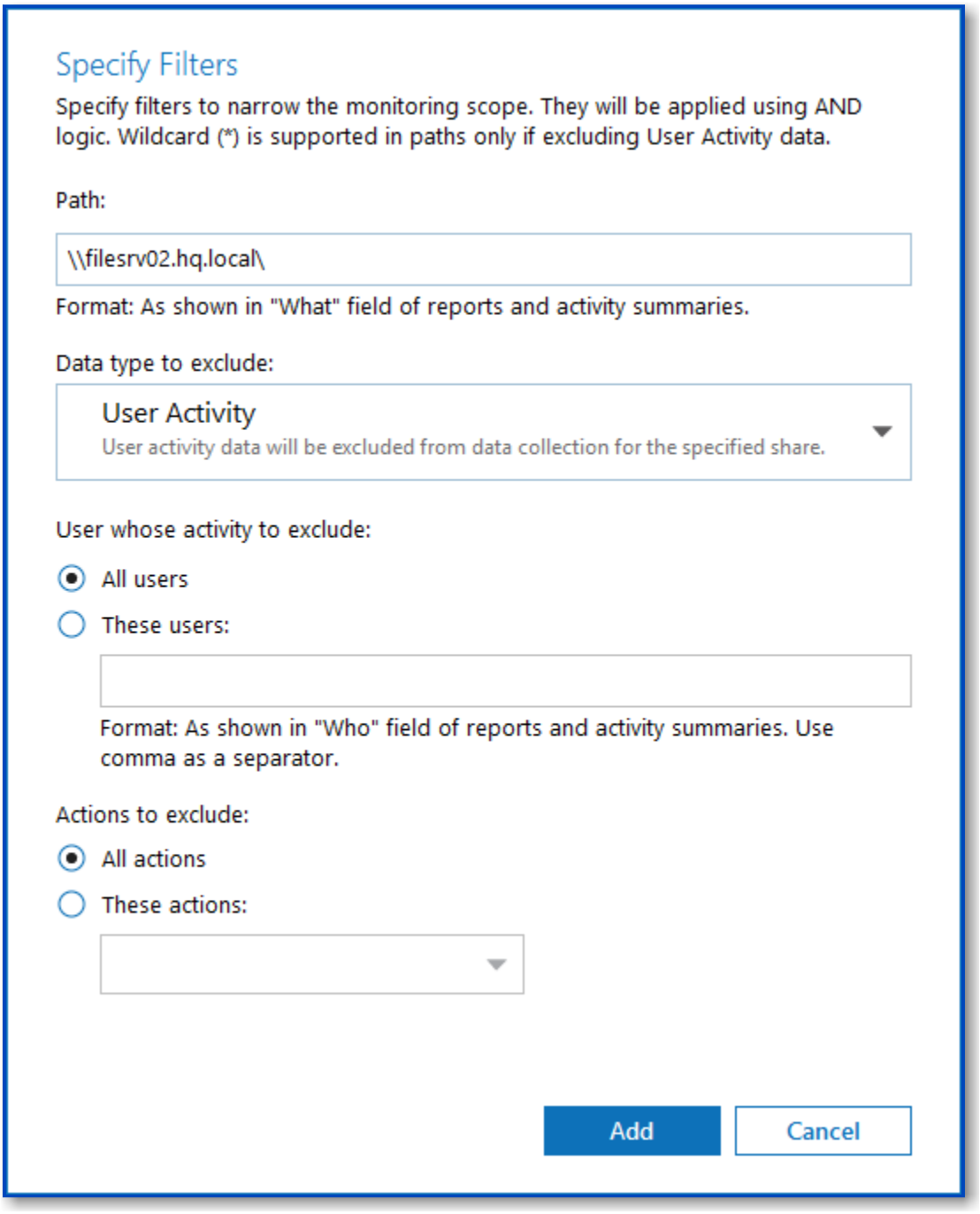
Follow the steps to exclude specific user activity.

Step 1 – Specify what user accounts should be excluded:

- All Users — Select to exclude the activity of any user on the file share you specified.
- These users — Select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.

Step 2 – Specify what actions should be excluded:

- All actions — Exclude all actions of the selected users
- These actions — Use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*



After configuring all filters, click **Add** to save them and return to the item settings.

VMware

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- VMware – Configure data source as required to be monitored

For this data source, specify the options you need:

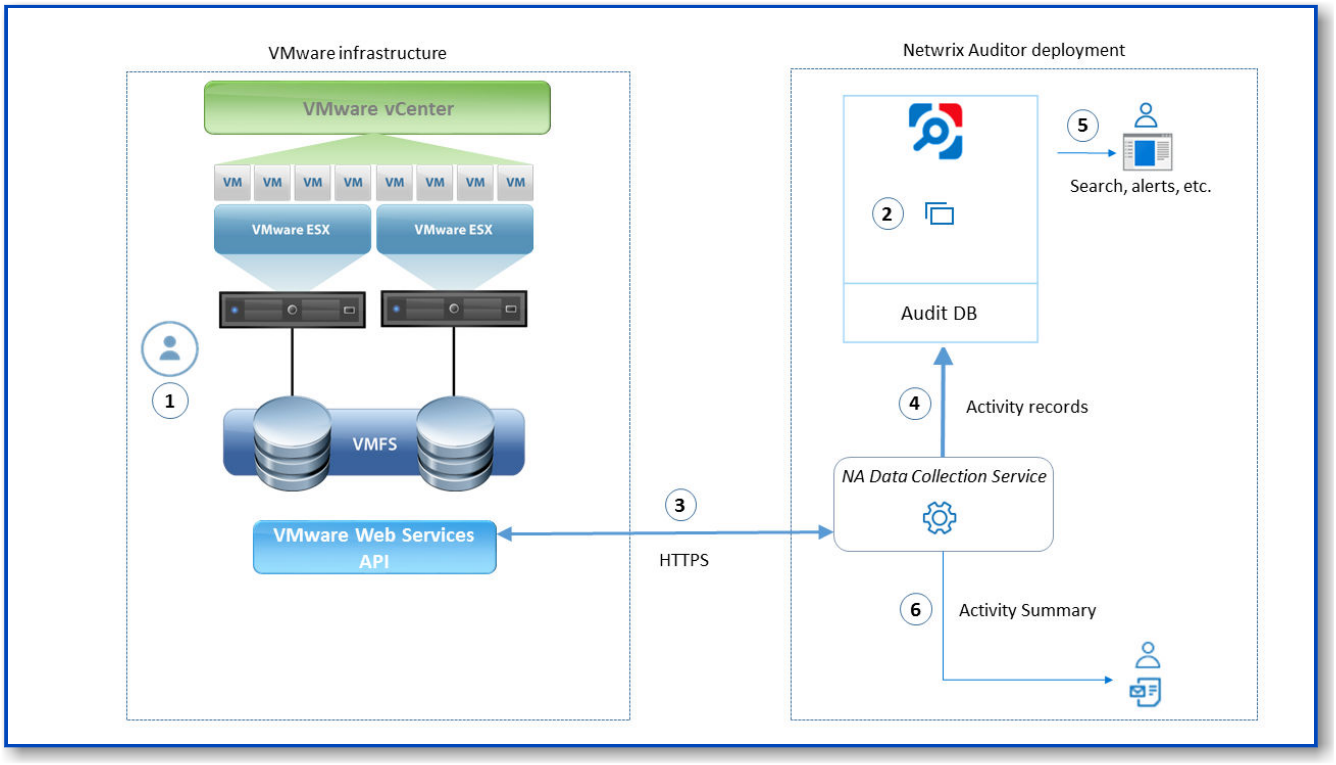
Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Monitor VMware configuration changes	Configuration changes are always monitored for VMware data source. See the Data Collection from VMware Servers topic for additional information.
Monitor VMware logon activity	Specify what types of logon events you want to monitor for VMware infrastructure.
Monitor SSO users/groups on vCenter and Local users on ESXi sever	Select Enable monitoring if you want to audit the following users and groups: • vCenter Single Sign-On (SSO) Users. The product collects data from vCenter. • Localos users. For these users, the product collects data from ESXi and vCenter.

Option	Description
	• VMware groups. The product collects data from vCenter. To audit users and groups, vCenter 6.5 and above required. Check that your data collecting account has all required rights and permissions. See the Permissions for VMware Server Auditing topic for additional information.
Collect data for state-in-time reports	Configure Auditor to store daily snapshots of your VMware system configuration required for further state-in-time reports generation. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database. To import snapshots, you must be assigned the Global administrator or the Global reviewer role . Follow the steps to import snapshots. **Step 1 –** In the Manage historical snapshots section, click Manage. **Step 2 –** Select the snapshots that you want to import. **Step 3 –** Move the selected snapshots to the Snapshots available for reporting list using the arrow button. **Step 4 –** When finished, click OK.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Data Collection from VMware Servers

On a high level, data collection process for VMware servers works as follows:



VMware administrator prepares a dedicated service account with sufficient permissions to collect data from VMware servers. This account must have at least **Read Only role** on those servers. For more information on VMware vSphere roles and permissions assignment, refer to this VMware article.

Netwrix administrator does the following:

- Creates a monitoring plan in Netwrix Auditor, specifying the service account (prepared at step 1) as a data collecting account in the **Monitoring Plan wizard**. Then s/he adds items to the monitoring plan – these are VMware servers to collect data from.
- Configures alerts related to VMware data source. Current version does not include predefined alerts for that data source, so follow the Create Alerts to create and configure the necessary alerts.
    - Remember to set the filter to "**Data Source***equals***VMware**".
- **Netwrix Auditor Data Collection Service**starts periodic (every 15 min) data collection sessions. The results of each session include:

- VMware infrastructure snapshot collected from the monitored items, i.e. VMware vCenter or ESX(i) host
- VMware events that occurred since the previous data collection. Data is retrieved via **VMware web services API** using HTTPS protocol.

- **Netwrix Auditor Data Collection Service** processes collected data into the proprietary format (Activity Records). Each Activity Record contains initiator's account, time, action, and other details.
  - To determine what has changed in the configuration, it compares a state snapshot from VMware server with the previously taken.
  - To get '*Who*' (initiator) and '*When*' (date and time) information for the detected changes, the product uses VMware events data.
- Netwrix Auditor Server then writes the Activity Records to the audit database (default retention – 180 days) and long-term archive (default retention – 120 months).
- Users can work with collected data in Netwrix Auditor client UI: run search, view reports, and so on. If you have configured alerting in Netwrix Auditor, then the activities that match the certain criteria will trigger the alerts. Recipients will be notified by email, and response actions will be taken, if configured.

Netwrix Auditor also generates an Activity Summary once a day (by default, at 3 AM) and sends it to the specified recipients. This email lists VMware infrastructure changes and activities collected by Netwrix Auditor during the last 24 hours.

VMware ESX/ESXi/vCenter

Complete the following fields:

Option	Description
General	
Specify VMware ESX, ESXi, or vCenter for monitoring	Specify the ESX or ESXi host URL, or vCenter Server URL.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other

Option	Description
	than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See Permissions for VMware Server Auditing topic for more information.
Virtual Machines	
Specify monitoring restrictions	Select the virtual machines to be excluded from search results, reports and Activity Summaries. To add VMs to the list, click Add. Then provide the full path of the machine to exclude. Consider the following: • To exclude a single VM, provide its full path as shown in the "*What*" column of reports and Activity Summary, for example: *Vcenters\VCenterServer021\VMs\vm01*. • To exclude several VMs, you can define a mask using a wildcard, for example: ◦ *\TestVM* — exclude VMs with names starting with *TestVM* (e.g., *TestVM01, TestVM_new*), located anywhere. ◦ *TestVM* — exclude VMs with names containing *TestVM* (e.g., *MyTestVM02*). In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

VMware Monitoring Scope

You can fine-tune Netwrix Auditor by specifying various data types that you want to exclude/include from/in the VMware reports.

Follow the steps to exclude data from the VMware monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Vmware Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitproplist.txt	Contains a list of object types and properties to be excluded from change reports.	`object_type.property_name` If there is no separator (.) between an object type and aproperty, the whole entry is treated as an object type. For example, to exclude the config.flags.monitorType property from reports, add the following line: `*.config.flags.monitorType`.

hidepropvalues.txt	Contains a list of object types and properties to be excluded from the reports when the property is set to certain value.	`object_type.property_name=property_value:object_type.hidden_property`
		
		For example, to exclude the config.cpuAllocation.shares.level property when it equals to *"Low"*, add the following line:
		`*.config.cpuAllocation.shares .level=low:`

File	Description	Syntax
		`*.config.cpuAllocation.shares.shares.`

proplist.txt	Contains a list of human-readable names for object types and properties to be displayed in the reports.	`inner_type:object_type.property=intelligiblename`
		
		`Inner_type` is optional.
		
		For example, if you want the configStatus property to be displayed in the reports as Configuration Status, add the following line:
		`*.configStatus=Configuration Status.`

omitstorelist.txt	Contains a list of objects to be excluded from being saved to data storage and showing up in reports. Audit data will still be collected.	Monitoring plan name, who, where, object type, what, property name, property value For example, to exclude internal logons: `*,*,*,Logon,*,UserAgent,VMware vim-java*` The following characters must be preceded with a backslash (\) if they are a part of an entry value: * , \ ? Characters may be also specified with hex value using *xnnnn* template.

File	Description	Syntax
		The spaces are trimmed. If they are required, use hex notation. For example: `Word\x0020 where \x0020` (with space at the end) means blank character.

Windows Server

NOTE: Prior to configuring your monitoring plan, please read and complete the instructions in the following topics:

- Protocols and Ports Required – To ensure successful data collection and activity monitoring configure necessary protocols and ports for inbound and outbound connections
- Data Collecting Account – Configure data collecting accounts as required to audit your IT systems
- Windows Server – Configure data source as required to be monitored

Complete the following fields:

Option	Description
General	
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Auditor to collect and store audit data.
Monitor changes to system components	Select the system components that you want to audit for changes. Review the following for additional information: • General computer settings—Enables auditing of general computer settings. For example, computer name or workgroup changes.

Option	Description
	• Hardware—Enables auditing of hardware devices configuration. For example, your network adapter configuration changes. • Add/Remove programs—Enables auditing of installed and removed programs. For example, Microsoft Office package has been removed from the audited Windows Server. • Services—Enables auditing of started/stopped services. For example, the Windows Firewall service stopped. • Audit policies—Enables auditing of local advanced audit policies configuration. For example, the Audit User Account Management advanced audit policy is set to "*Failure*". • DHCP configuration—Enables auditing of DHCP configuration changes. • Scheduled tasks—Enables auditing of enabled / disabled / modified scheduled tasks. For example, the GoogleUpdateTaskMachineUA scheduled task trigger changes. • Local users and groups—Enables auditing of local users and groups. For example, an unknown user was added to the Administrators group. • DNS configuration—Enables auditing of your DNS configuration changes. For example, your DNS security parameters' changes. • DNS resource records—Enables auditing of all types of DNS resource records. For example, A-type resource records (Address record) changes. • File shares—Enables auditing of created / removed / modified file shares and their properties. For example, a new file share was created on the audited Windows Server. • Removable media—Enables auditing of USB thumb drives insertion.
Specify data collection method	You can enable **network traffic compression.** If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data

Option	Description
	transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. 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. Do not select the checkbox if you want to configure audit settings manually. See the Windows Server configuration topic for additional information about audit settings required to collect comprehensive audit data and the instructions on how to configure them.
Collect data for state-in-time reports	Configure Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See the State–In–Time Reports topic for additional information. When auditing file servers, changes to effective access permissions can be tracked in addition to audit permissions. By default, Combination of file and share permissions is tracked. File permissions define who has access to local files and folders. Share permissions provide or deny access to the same resources over the network. The combination of both determines the final access permissions for a shared folder—the more restrictive permissions are applied. Upon selecting Combination of file and share permissions only the resultant set will be written to the Audit Database. Select File permissions option too if you want to see difference between permissions applied locally and the effective file and share permissions set. To disable

Option	Description
	auditing of effective access, unselect all checkboxes under Include details on effective permissions. In the Schedule state-in-time data collection section, you can select a custom weekly interval for snapshots collection. Click Modify and select day(s) of week you want your snapshot to be collected. In the Manage historical snapshots section, you can click **Manage** and select the snapshots that you want to import to the Audit Database to generate a report on the data source's state at the specific moment in the past. You must be assigned the Global administrator or the Global reviewer role to import snapshots. Move the selected snapshots to the Snapshots available for reporting list using the arrow button. The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Users can also configure Only the latest snapshot is available for reporting in Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.
Activity	
Specify monitoring restrictions	Specify restriction filters to narrow your Windows Server monitoring scope (search results, reports and Activity Summaries). For example, you can exclude system activity on a particular objects on all computers. All filters are applied using AND logic. Click Add and complete the following fields: • User who initiated the change: – provide the name of the user whose changes you want to ignore as shown in the "*Who*" column of reports and Activity Summaries. Example: *mydomain\user1*.

Option	Description
	You can provide the "*System*" value to exclude events containing the "*System*" instead of an account name in the "*Who*" column. • Windows Server which setting was changed: – provide the name of the server in your IT infrastructure whose changes you want to ignore as shown in the "*What*" column of reports and Activity Summaries. Example: *winsrv2016-01.mydomain.local*. • Setting changed: – provide the name for unwanted settings as shown in the "*What*" column in reports and Activity Summaries. Example: *System Properties**. You can use a wildcard (*) to replace any number of characters in filters. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See the Add Items for Monitoring topic for additional information.

Computer

Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select account type you want to use and enter credentials. The following choices are available:

- User/password. The account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

- Group Managed Service Account (gMSA). You should specify only the account name in the domain\account$ format. See the Use Group Managed Service Account (gMSA) topic for additional information.
- Netwrix Privilege Secure. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information.

IP Range

Complete the following fields:

Option	Description
General	
Specify IP range	Specify an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP subrange you want to exclude, and click **Add**.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. A custom account must be granted the same permissions and access rights as the default account used for data collection. See the Data Collecting Account topic for additional information.

AD Container

Complete the following fields:

Option	Description
General	
Specify AD container	Specify a whole AD domain, OU or container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be audited within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Click **Exclude** to specify AD domains, OUs, and containers you do not want to audit. In the Exclude Containers dialog, click Add and specify an object. The list of containers does not include child domains of trusted domains. Use other options **(Computer, IP range** to specify the target computers.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. If using a group Managed Service Account (gMSA), you can specify only the account name in the *domain\account$* format. Password field can be empty. Starting with version 10.7, you can implement the integration between Netwrix Auditor and Netwrix Privilege Secure. See the Netwrix Privilege Secure topic for additional information. Refer to the Permissions for Active Directory Auditing topic for more information on using Netwrix Privilege Secure as an account for data collection. A custom account must be granted the same permissions and access rights as the default account

Option	Description
	used for data collection. See theData Collecting Account topic for additional information.
Containers and Computers	
Monitor hidden shares	By default, Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Depending on the type of the object you want to exclude, select one of the following: • Add AD Container – Browse for a container to be excluded from being audited. You can select a whole AD domain, OU or container. • Add Computer – Provide the name of the computer you want to exclude as shown in the "*Where*" column of reports and Activity Summaries. For example, *backupsrv01.mydomain.local*. Wildcards (*) are not supported. In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion

Option	Description
	settings configured in the *.txt files. See the Monitoring Planstopic for additional information.

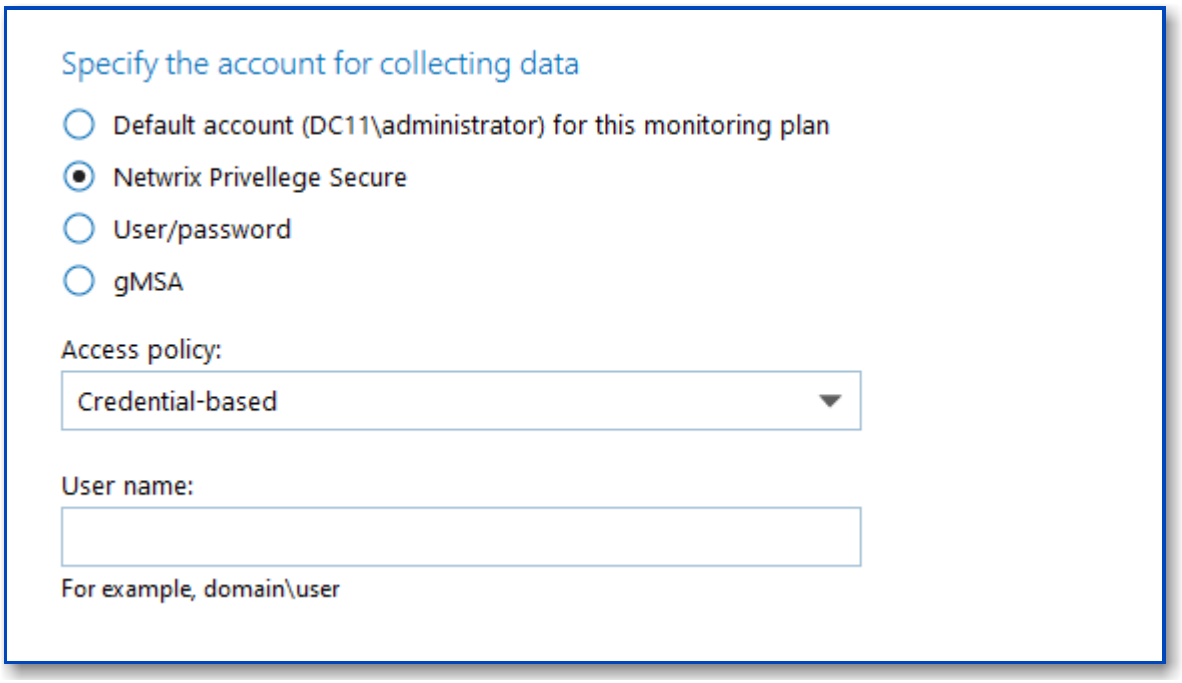
Use Netwrix Privilege Secure as a Data Collecting Account

Starting with version 10.7, you can use Netwrix Privilege Secure to manage the account for collecting data, after configuring the integration. See the Netwrix Privilege Secure topic for additional information about integration and supported data sources. In this case, the credentials will not be stored by Netwrix Auditor. Instead, they will be managed by Netwrix Privilege Secure and provided on demand, ensuring password rotation or using temporary accounts for data collection.

Follow the steps to use Netwrix Privilege Secure as an account for data collection.

Step 1 – Select the desired item.

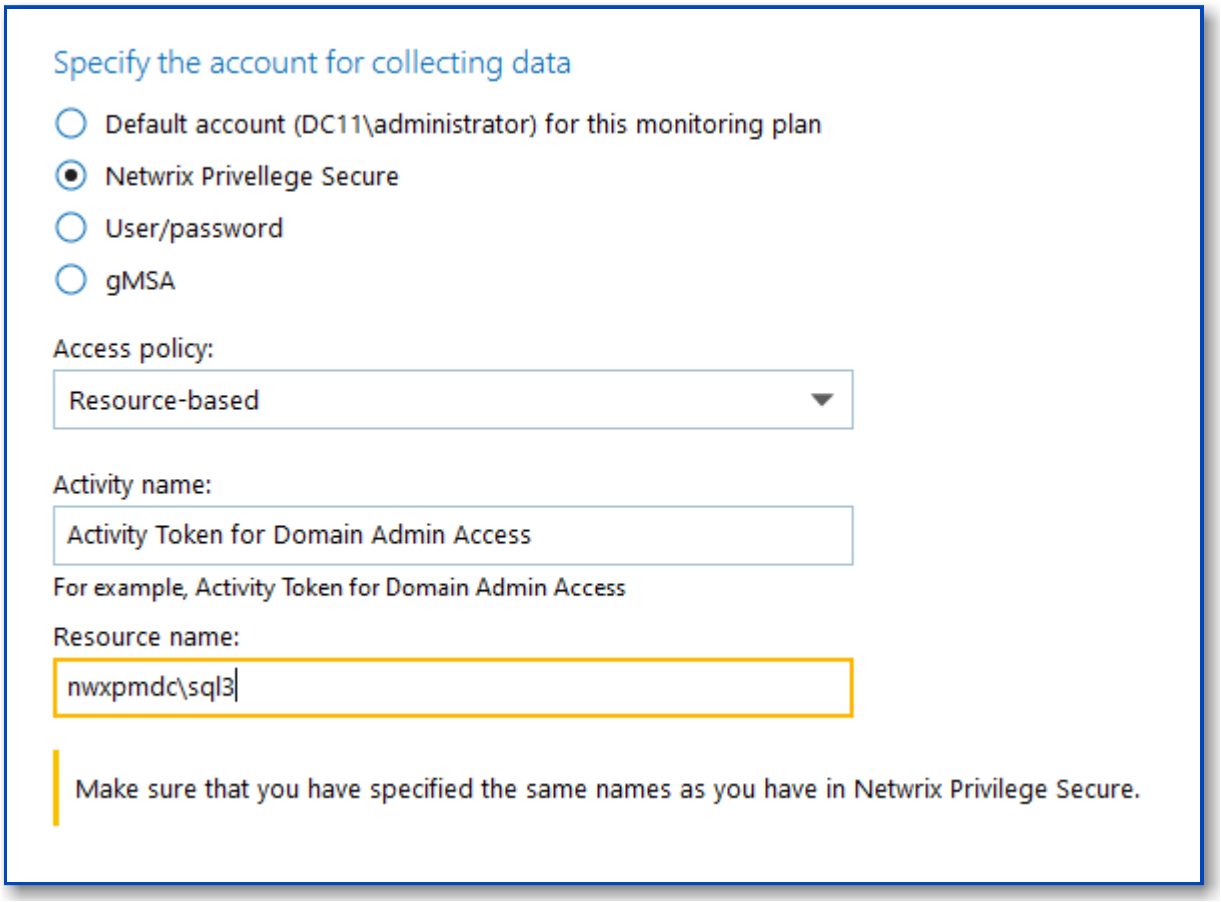
Step 2 – In the item configuration menu, select Netwrix Privilege Secure as an option for data collection.



Step 3 – Select the type of the Access Policy you want to use in Netwrix Privilege Secure. Credential-based is the default option. Refer to the Netwrix Privilege Secure documentation to learn more about Access Policies.

In this case, you need to provide the username of the account managed by Netwrix Privilege Secure, and to which Netwrix Auditor has the access through a Credential-based access policy.

NOTE: Netwrix recommends using different credentials for different monitoring plans and data sources.



The second option is Resource-based. To use this option, you need to provide the Activity and Resource names, assigned to Netwrix Auditor in the corresponding Resource-based policy. Make sure that you specified the same names as in Netwrix Privilege Secure.

The Resource name in this case is where the activity will be performed. For example, if you grant the data collecting account the access to a local Administrators group - the resource is the server where the permission will be granted.

Netwrix Privilege Secure is ready to use as an account for data collection.

Windows Server Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Windows Server monitoring scope.

Follow the steps to exclude data from the Windows Server monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Windows Server Auditing* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- Wildcards (* and ?) are supported. A backslash (\) must be put in front of (*), (?), (,), and (\) if they are a part of an entry value.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitcollectlist.txt	Contains a list of objects and their properties to be excluded from being monitored.
	
	If you want to restart monitoring these objects, remove them from the omitcollectlist.txt and run data collection at least twice.
		`monitoring plan name,server name,class name,property name,property value`
		
		`class name` is a mandatory parameter, it cannot be replaced with a wildcard. `property name` and `property value` are optional, but cannot be replaced with wildcards either.
		
		For example:
		
		`**,server,MicrosoftDNS_Server`
		`**,*,StdServerRegProv`

omiterrors.txt	Contains a list of errors/warnings to be omitted from logging to the Netwrix Auditor System Health event log.	`monitoring plan name,server name,error text` For example:

File	Description	Syntax
		`*,productionserver1.corp.local,*Access is denied*`

omitreportlist.txt	Contains a list of objects to be excluded from reports and Activity Summary emails. In this case audit data is still being collected.	`monitoring plan name,who,where,object type,what,property name`
		
		For example:
		
		`*,CORP\\jsmith,*,*,*,*`

omitsitcollectlist.txt	Contains a list of objects to be excluded from State-in-time reports.	`monitoring planname,server name,class name,property name,property value`
		
		`class name` is a mandatory parameter, it cannot be replaced with a wildcard. `property name` and `property value` are optional, but cannot be replaced with wildcards either.
		
		For example:
		
		`*,server,MicrosoftDNS_Server`
		
		`*,*,StdServerRegProv`

omitstorelist.txt	Contains a list of objects to be excluded from being stored to the Audit Archive and showing up in reports. In this case audit data is still being collected.	`monitoring plan name,who,where,object type,what,property name`
		
		For example:
		
		`*,*,*,Scheduled task,Scheduled Tasks\`

File	Description	Syntax
		\User_Feed_Synchronization*,*

Fine-Tune Your Plan and Edit Settings

At any time, you can review your plan settings and fine-tune Audit Database, notification and data collection settings.

To modify most plan settings, you must be assigned the Global administrator role in the product or the Configurator role on the plan. The Global reviewer or this plan's Reviewer can modify Activity Summary recipients. See the Role-Based Access and Delegation topic for additional information.

Follow the steps to edit your plan settings:

Step 1 – Select a plan in the All Monitoring Plans list and click Edit.

Step 2 – In the right pane, select Edit settings.

Step 3 – In the Plan Settings page, review the tabs and modify the settings.

Option	Description
General	
Name **Description**	Update a plan name or its description.
Data Collection	

Option	Description
Specify the account for collecting data • **Not specified** • **User/Password** • **gMSA**	Specify a new user name and a password for the account that Auditor will use to collect data. Make sure the account has sufficient permissions to collect data. See the Data Collecting Account topic for additional information about the rights and permissions, and instructions on how to configure them.
Audit Database	
Disable security intelligence and make data available only in activity summaries	Keep this checkbox cleared if you want Auditor to write data to the Audit Database.
Use default SQL Server settings	Select this checkbox to write data to a SQL Server instance with connection parameters as shown in **Settings** > **Audit Database**. See the Audit Database topic for additional information.
Specify custom connection parameters	Specify this option to use non-default settings (e.g., use a different authentication method or user). Make sure to store data on the same SQL Server instance. Otherwise some data may become unavailable for search and reporting.
Notifications	
Specify Activity Summary delivery schedule	Configure how often you want to receive an Activity Summary. By default, it is delivered once a day, at 3

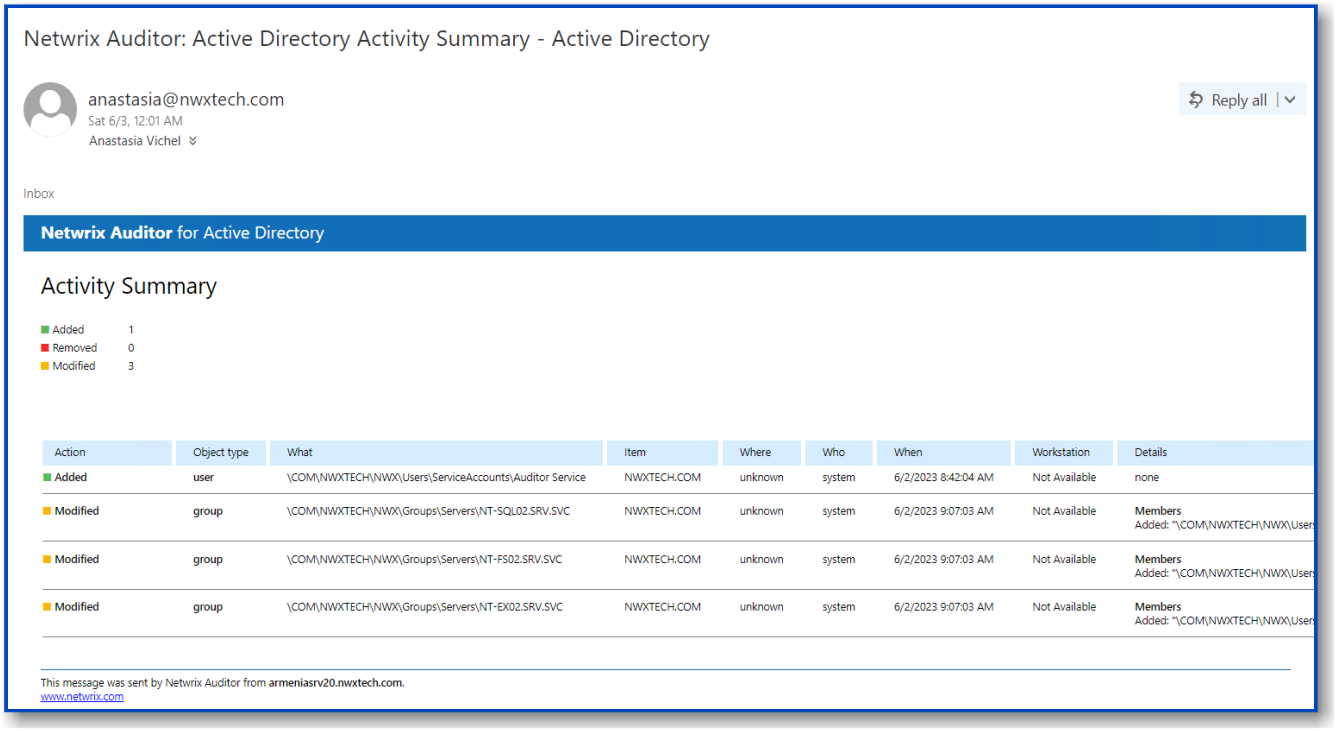
Option	Description
	AM. You can specify custom delivery time and frequency (e.g., every 6 hours starting 12 AM — at 12 AM, 6 AM, 12 PM, 6 PM).
Customize notifications	By default, Activity Summary lists changes and activity in email body. For most data sources, if an Activity Summaries contains more than 1,000 activity records, these records are sent as a CSV attachment, bigger attachments are compressed in ZIP files. • Attach Activity Summary as a CSV file — You can configure Auditor to always send emails with attachments instead of listing activity and changes in email body. • Compress attachment before sending — You can configure Auditor to always compress attachments in a ZIP file, irrespective of its size and number of activity records.
Specify the recipients who will receive daily activity summaries	Modify a list of users who will receive daily activity summaries. Click Add Recipient and provide email address.

Activity Summary Email

Activity Summary email is generated automatically by Netwrix Auditor and lists all changes / recorded user sessions that occurred since the last Activity Summary delivery. By default, for most data sources an Activity Summary is generated daily at 3:00 AM and delivered to the specified recipients. You can also launch data collection and Activity Summary generation manually.

Notifications on user activity and event log collection (Event Log Collection Status) are a bit different and do not show changes.

The following Activity Summary example applies to Active Directory. Other Activity Summaries generated and delivered by Netwrix Auditor will vary slightly depending on the data source.



Netwrix Auditor: Active Directory Activity Summary - Active Directory

anastasia@nwxtech.com
Sat 6/3, 12:01 AM
Anastasia Vichel

Reply all

Inbox

Netwrix Auditor for Active Directory

Activity Summary

Added 1
Removed 0
Modified 3

Action	Object type	What	Item	Where	Who	When	Workstation	Details
Added	user	\COM\NWXTECH\NWX\Users\ServiceAccounts\Auditor Service	NWXTECH.COM	unknown	system	6/2/2023 8:42:04 AM	Not Available	none
Modified	group	\COM\NWXTECH\NWX\Groups\Servers\NT-SQL02.SRV.SVC	NWXTECH.COM	unknown	system	6/2/2023 9:07:03 AM	Not Available	Members Added: "\COM\NWXTECH\NWX\User
Modified	group	\COM\NWXTECH\NWX\Groups\Servers\NT-FS02.SRV.SVC	NWXTECH.COM	unknown	system	6/2/2023 9:07:03 AM	Not Available	Members Added: "\COM\NWXTECH\NWX\User
Modified	group	\COM\NWXTECH\NWX\Groups\Servers\NT-EX02.SRV.SVC	NWXTECH.COM	unknown	system	6/2/2023 9:07:03 AM	Not Available	Members Added: "\COM\NWXTECH\NWX\User

This message was sent by Netwrix Auditor from **armeniasrv20.nwxtech.com**.
www.netwrix.com

The example Activity Summary provides the following information on Active Directory changes:

Column	Description
Action	Shows the type of action that was performed on the object. • Added • Removed • Modified • Activated (User Activity)
Object Type	Shows the type of the modified AD object, for example, 'user'.

Column	Description
What	Shows the path to the modified AD object.
Item	Shows the item associated with the selected monitoring plan.
Where	Shows the name of the domain controller where the change was made.
Who	Shows the name of the account under which the change was made.
When	Shows the exact time when the change occurred.
Workstation	Shows the name / IP address of the computer where the user was logged on when the change was made.
Details	Shows the before and after values of the modified AD object.

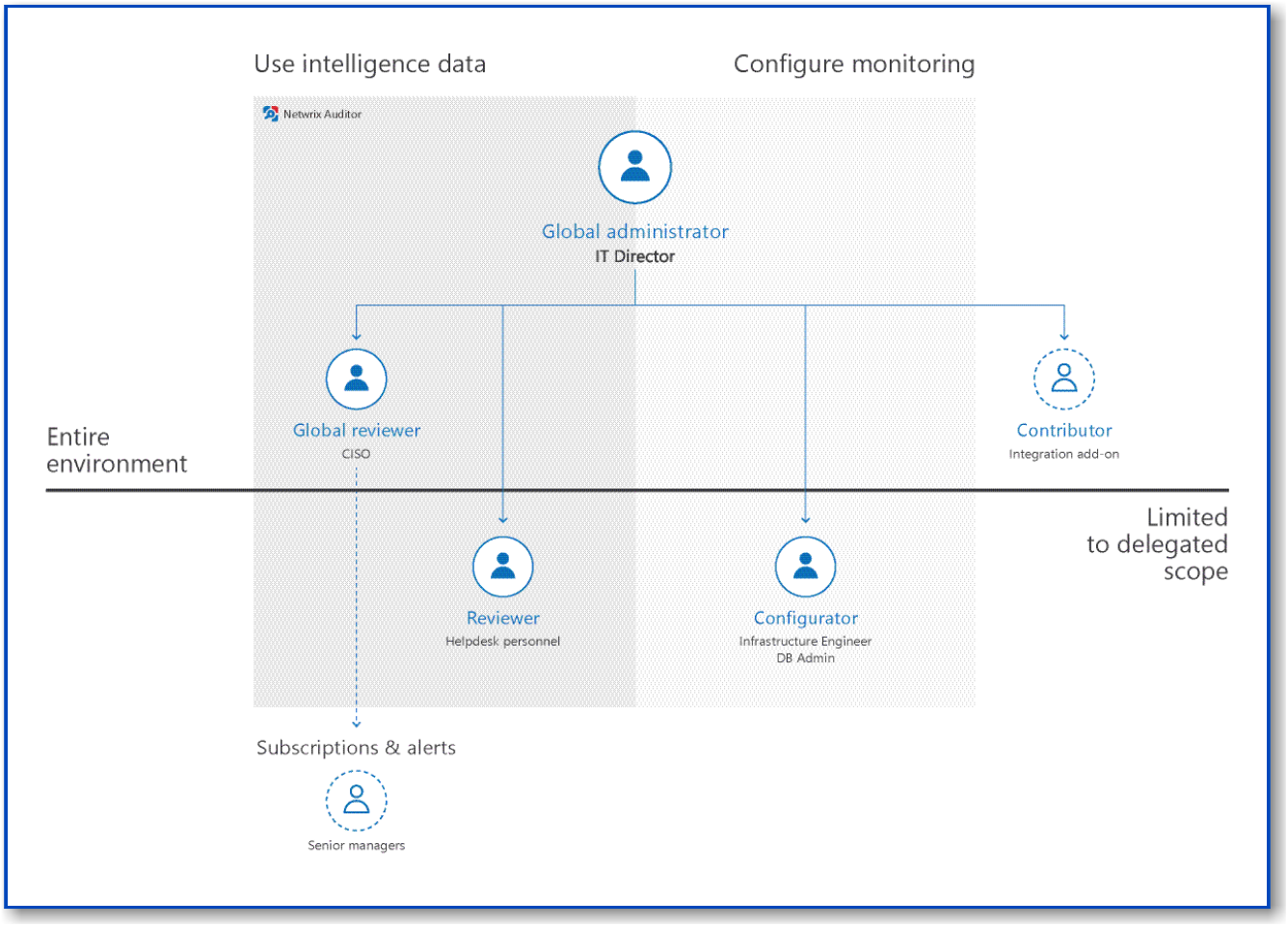
To initiate an on-demand Activity Summary delivery, navigate to the Monitoring Plans section, select a plan, click Edit, and then select Update. A summary will be delivered to the specified recipient, listing all activity that occurred since the last data collection.

To disable Activity Summary Emails, you need to disable notifications in the settings. See the Notifications topic for additional information.

Role-Based Access and Delegation

Security and awareness of *who* has access to *what* is crucial for every organization. Besides notifying you on *who* changed *what*, *when* and *where*, and *who* has access to *what* in your IT infrastructure, Netwrix pays attention to safety of its own configuration and collected data.

To keep the monitoring process secure, Netwrix suggests configuring role-based access. Delegating control ensures that only appropriate users can modify the product configuration or view audit data, based on your company policies and the user's job responsibilities.



Roles are described briefly in the table below and explained in detail in the next topic.

Role	Access level	Recommended use
Global administrator	Full control. Access to global settings, monitoring plan configuration, collected data, access delegation, etc.	The role should be assigned to a very limited number of employees—typically, only the owner of the Auditor Server host in your environment. By default, the user who installed Auditor is assigned the Global administrator role. All members of the local Administrators group are Global administrators too.
Configurator	Access to monitoring plan configuration within the delegated scope: a monitoring plan or a folder with monitoring plans	The role is appropriate for system administrators, infrastructure engineers, and members of operations team who manage network and services in your organization but should not have access to sensitive data.
Global reviewer	Access to all data collected by Auditor and intelligence and visibility features.	The role is appropriate for key employees who need to review audit data collected across various data sources—typically, IT managers, chief information security officer, and so on.
Reviewer	Access to data collected by Auditor and intelligence and visibility features within the delegated scope.	The role is appropriate for members of security team and helpdesk personnel who are responsible for mitigating risks in a certain sector of your environment (e.g., domain, file share). This role is granted to specialists who use the Integration API to

Role	Access level	Recommended use
		retrieve data from the Audit Database.
Contributor	Write access to Auditor Server and Audit Database.	This service role is granted to specialists who use the Integration API to write data to the Audit Database. This role is also granted to service accounts or any accounts used for interaction with Auditor Server (e.g., add-on scripts).

Compare Roles

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Launch Auditor client	+	+	+	+	+
Delegate control, grant and revoke permissions	+	–	–	–	–
View global settings	+	Some	Some	Some	Some
Modify global settings (including default Audit Database,	+	–	–	–	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
licenses, retention settings, etc.)					
Monitoring plan configuration					
List folders	+	+	+	+	+
Add, remove, rename folders	+	–	–	Some Only under assigned folders provided that directly assigned roles do not conflict.	–
List monitoring plans, review status	+	+	+	+	+
Add, remove, rename monitoring plans	+	–	–	Some Only under assigned folders provided that directly assigned roles do not conflict.	–
Modify monitoring plan settings	+	Some	Some Add and remove Activity Summary recipients within	Some Restricted to the delegated scope	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
		Add and remove Activity Summary recipients	the delegated scope	(folder or monitoring plan)	
List data sources and items in monitoring plan	+	+	+	+	+
Add, modify, remove data sources, enable or disable auditing	+	–	–	Some Restricted to the delegated scope (folder or monitoring plan)	–
Add, modify, remove items in monitoring plan	+	–	–	Some Restricted to the delegated scope (folder or monitoring plan)	–
Manage state-in-time data, upload snapshots to the Audit Database	+	+	–	–	–
Intelligence					
List reports	+	+	+	+	+

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Generate reports	+	+	Some Restricted to the delegated scope (folder or monitoring plan)	–	–
List report subscriptions	+	+	+	+	+
Create, modify, remove subscriptions	+	+	–	–	–
See search results	+	+	Some Restricted to the delegated scope (folder or monitoring plan)	–	–
List, create, modify, delete custom reports	+	+	+	+	- (only can *list*)
List alerts	+	+	+	+	+
Create, modify, delete alerts	+	+	–	–	–
Import investigation data from the	+	–	–	–	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Long-Term Archive					
View investigation data	+	+	–	–	–
View Behavior Anomalies list	+	+	–	–	–
Review user profile	+	+	–	–	–
Update anomaly status	+	+	–	–	–
Risk Assessment Overview dashboard and drill-down reports					
View Risk Assessment Overview results (dashboard, drill-down reports)	+	+	Some Restricted to delegated scope (folder or monitoring plan)	-	-
Modify risk level thresholds	+	+	-	-	-
Customize risk indicators	+	+	-	-	-

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Auditor Integration API					
Write Activity Records	+	–	–	–	+
Retrieve Activity Records	+	+	+ Restricted to the delegated scope (folder or monitoring plan)	–	–

Assign Roles

Netwrix Auditor allows assigning roles on the product as a whole, or within a specific *scope*. A scope can be limited to a single monitoring plan or to the contents of a folder. This helps to ensure that only authorized personnel has access to the relevant data. For example, database administrators (DBAs) should not access Active Directory management data, and domain administrators do not need permissions to view database schema changes or update data collection settings, and so on.

Understanding Scopes

Scopes for different Auditor roles are as follows:

Scope	Roles
Global (All monitoring plans)	Global administrator Global reviewer Contributor
Folder level	Configurator Reviewer
Plan level	Configurator Reviewer

Follow the steps to delegate control to some scope, review, or revoke assigned roles.

Step 1 – On the main Auditor page, navigate to the **Monitoring Plans** section.

Step 2 – Browse your monitoring plans tree and select the scope you want to delegate to a user (e.g., All monitoring plans root folder, a folder, or a monitoring plan).

Step 3 – Click **Delegate**.

Review roles that are already defined for this scope.

Do one of the following:

To...	Do...
Assign a role	1. Select Add User. 2. In the dialog that opens, specify a user (or a group) and a role.

To...	Do...
Revoke a role assignment	• Click  next to the user.

Step 4 – Click **Save** or **Save&Close**.

Browser Role on Report Server

Along with adding a new Global administrator, Global reviewer or Reviewer role, Auditor will automatically assign this user the Browser role on the Report Server (SSRS).

The Browser role is required to generate reports. It is granted on all reports — or within a delegated scope.

If for some reason Auditor is unable to grant the Browser role, configure it manually. See the SQL Server Reporting Services topic for additional information.

Default Role Assignments

By default, several accounts and local groups are assigned the following roles:

Account or group name	Role	Details
Local Administrators	Global administrator	
Local service accounts	Global administrator	Global administrator Auditor uses system accounts for data processing and interaction between product components.
Auditor Administrators	Global administrator	

Account or group name	Role	Details
Auditor Client Users	Global reviewer	

Delegating Control via Windows Group Membership

During the Auditor Server installation, Netwrix Auditor Administrators and Netwrix Auditor Client Users groups are created automatically. To delegate control via group membership, you need to add users to these groups on the computer where Auditor Server resides.

Users will be granted roles with extended permissions. You may need to limit their scope to a specific monitoring plan.

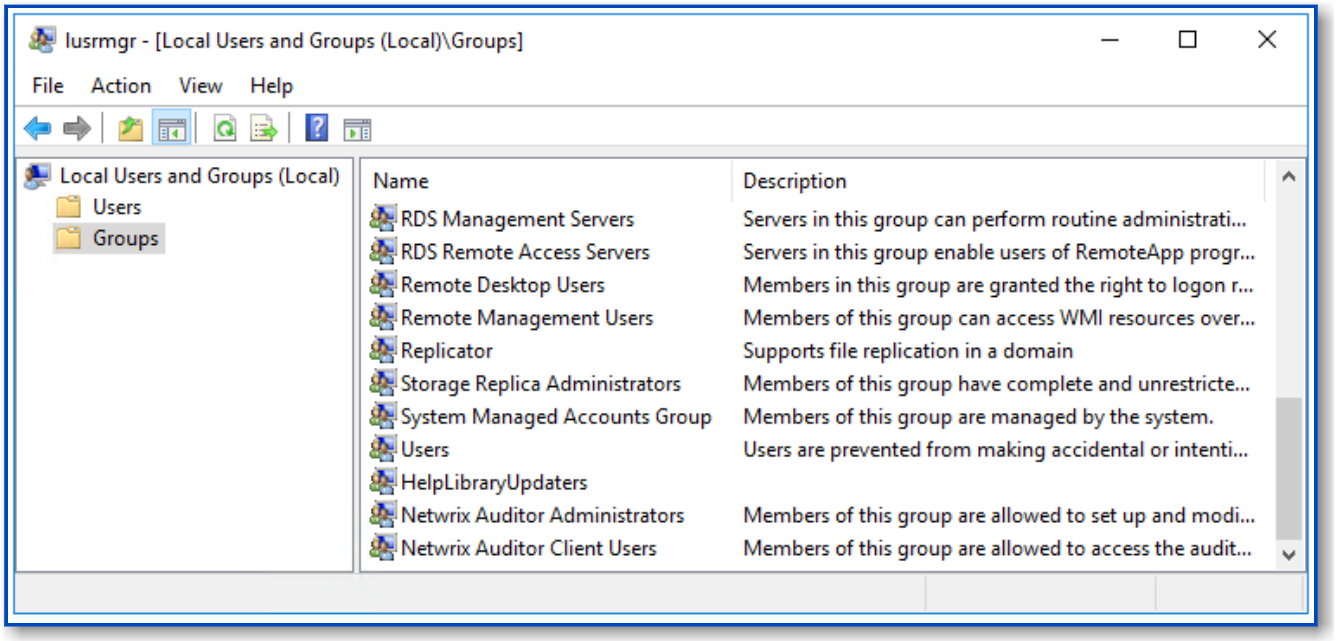
Follow the steps to add an account to a group.

Step 1 – On the computer where Auditor Server is installed, start the Local Users and Computers snap-in.

Step 2 – Navigate to the **Groups** node and locate the Netwrix Auditor Administrators or Netwrix Auditor Client Users group.

Step 3 – In the group properties, click **Add**.

Specify users you want to be included in this group.



NOTE: For additional information about User Activity video access management, see the Configure Video Recordings Playback Settings topic.

Provide Access to a Limited Set of Data

By default, only users designated in Auditor are allowed to view its configuration and collected data. This policy ensures that only authorized and trustworthy users access sensitive data and make changes.

However, in some cases, organizations need to provide certain employees with access to a limited set of audit data. For example, an auditor might need to review particular access reports once or twice a year. You can provide these users (recipients) with means to review the data they need without actually running Auditor. This ensures that dedicated specialists have access to the data while preventing data breaches and ensuring that sensitive data is not being distributed across the whole company.

Netwrix recommends granting limited access permissions to employees who need to:

- Review audit data periodically in accordance with company policy
- Review audit data accumulated over time
- Be notified only in case of a rare incident

To grant limited access to audit data, you can:

Do..	Recommended use
Schedule email report subscriptions	This is helpful when you want to share information with a group of employees, external consultants, auditors, and so on. Reports are sent according to a specified schedule and recipients can review them, but they do not have any other means to access audit data. Basically, this option is enough for employees who are interested in a high-level summary—for example, an auditor who performs monthly access rights attestation on critical folders or a senior manager.
Publish reports to file shares	This scenario works great for a helpdesk with several departments. Assume, each department has its own field of responsibility and must not disclose

Do..	Recommended use
	information to other departments. You can configure Auditor to publish reports to folders that can be accessed by employees from a specific department only. You might set up the following folders and permissions: • The user support team has access to a folder with reports on account lockouts and password resets. • File server helpdesk personnel have access to a different folder with daily reports listing all file removals. • The helpdesk supervisor has access to both folders.
Configure alerts	This is helpful for rare occasions when you have to notify some senior specialists about critical system state that has to be addressed immediately, e.g., CISO must mitigate risks in the event of massive deletions in the sensitive data storage.

View and Search Collected Data

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient interactive search interface enables you to investigate incidents and browse data collected across the entire IT infrastructure. When running a search, you are not limited to a certain data source, change type, or object name. You can create flexible searches that provide you with precise results on *who* changed *what*, and *when* and *where* each change was made.

To review collected data, you must be assigned the **Global administrator** or **Global reviewer** Netwrix Auditor role. Users with the **Reviewer** role on a certain plan or folder have limited access to data—only within their delegated scope. See the Role-Based Access and Delegation topic for additional information.

This functionality is currently available for the following data sources:

- Active Directory
- Microsoft Entra ID (formerly Azure AD)
- Exchange

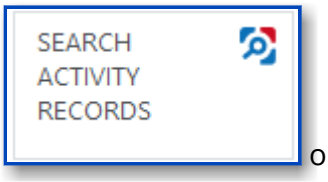
- Exchange Online
- File Servers (Windows File Servers, EMC, and NetApp)
- Network Devices
- Oracle Database
- SharePoint
- SharePoint Online
- SQL Server
- VMware
- Windows Server
- Group Policy
- Logon Activity
- User Activity (Video)
- Netwrix API—data imported to the Audit Database from other sources using Netwrix Auditor Integration API

- Netwrix Auditor Self-Audit

- Netwrix Data Classification. See Sensitive Data Discovery for more information.

Netwrix Auditor executes interactive search queries against data stored in the audit databases, that is, on data collected in the last 180 days (default retention period). If you want to investigate incidents that occurred more than 180 days ago, then you should import that data from the Long-Term Archive. See Investigations topic for additional information.

Browsing Your Audit Data

On the main Netwrix Auditor page, click 

on the left.

You can add any elements (a dashboard, report, alert, risk, etc.) to the Auditor Home screen to access them instantly. See the Navigation and Customize Home Screen topics for additional information.

There you can use the UI controls to run the variety of search queries that will fecth you exactly the data you need.

- To view all audit data stored in all Audit Databases by all monitoring plans, click **Search** button in the center.

  Be aware that this type of search query may take time due to a large amount of data. Thus, it is recommended that instead of retrieveing a massive data set, you pre-configure your search query using filters.

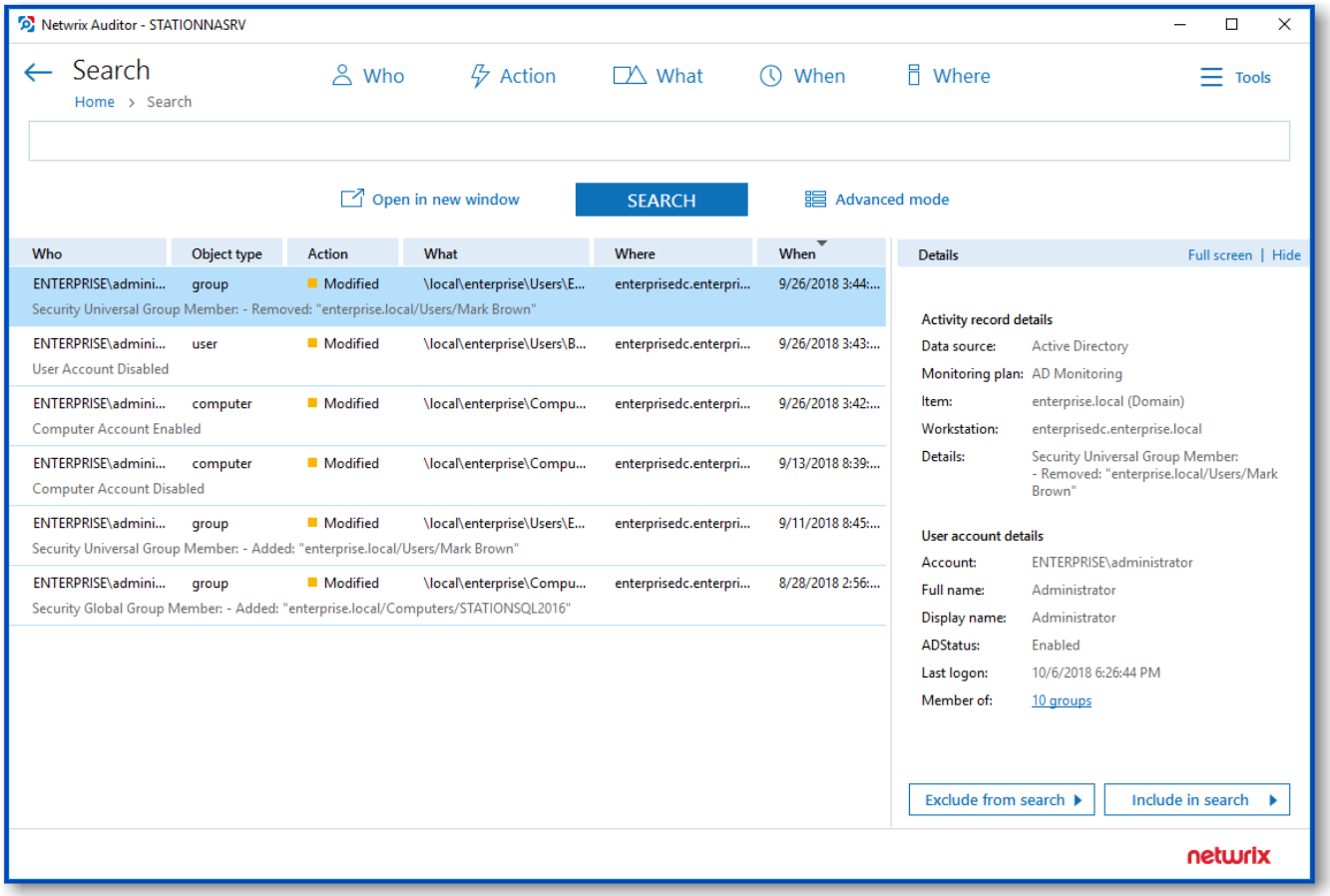
By default, Netwrix Auditor shows only the top 2,000 entries in the search results.

- To pre-configure your search query before you click Search, you can add filters. Then the search query will return only data matching your filtering criteria. See Use Filters in Simple Mode for details.

  You can also use advanced filtering capabilities based on regular expressions (they involve filter fields and conditions). See Use Filters in Advanced Mode for details.

- By default, search results are open in the same window, so the subsequent search results will overwrite the previous search results. To view them in different windows, click Open in new window.
- In addition, you can customize your view by selecting columns to display.

Use search results for your own needs: save, share, create search-based alerts, subscribe to periodic delivery of search query results, etc. See Make Search Results Actionnable for more information.



You can also use the **Search** window to examine details for the selected activity record, or watch a video recording (for User Ativity data).

Examining Activity Record in Detail

To work with a certain activity record:

1. Select the activity record which details you want to review. Its key fields and user (initiator) account details will be displayed in the right pane.
2. To display all fields and copy them if necessary, click the Full screen... link on the right.

   If you are examining User Activity entries, click the Show video... link below the entry. Review details and play a video by clicking the Show video on the right.

3. You can instruct Netwrix Auditor to include or exclude this activity record from the search query results, as described in the Include and Exclude Data

Customize View

Having reviewed the search results, you can modify the way the data is presented, for example, hide a column or change its position, or hide the Details pane on the right.

To modify view:

1. Navigate to Tools
2. Click Select columns. The dialog that opens shows the search columns currently selected for display.
3. Check the columns you want to include and clear unwanted ones.

4. Set the order of displayed columns using arrows on the right.

5. Click **Hide details** if you want to hide the Details pane with the activity record and user (initiator) account details.

6. To restore the original view configuration, click Restore Default.

Include and Exclude Data

Having reviewed the search results, you can proceed with your investigation by excluding or including data. Excluding a filter value is helpful if you want to skip it in your search results (e.g.,

a service account or trusted user account). On the other hand, including a filter value ensures that only the entries containing it will be shown (e.g., a suspicious user or potentially violated folder).

To include or exclude data

1. Review your search results and locate an entry with data you want to exclude or include.
2. Select this entry and review details.
3. Click Exclude from search or Include to search and specify a filter value from the list.
4. Click Search to update the search results.

Your exclusions and inclusions will automatically be added to the search filters, limiting the amount of data shown in the results pane.

Make Search Results Actionnable

You can export your search query results, save them as a custom report, subscribe to periodic delivery of this search results, create a search-based alert.

Navigate to Tools in the top right corner of the Search window and select the required action.

Use...	To...
Save as report	Save your search results as custom reports.
Create alert	Create an alert with the same set of filters you have just specified for your search.
Subscribe	Create subscription for periodic delivery of the search query results. Subscription to the search results is not the same as creation of a custom report using this search.
Export data	Save your search results as a *.pdf* or *.csv* file. All audit data from your search query results will be exported

Use...	To...
	(unlike the interactive view which is limited to the top 2,000 entries). When exporting large amount of data (e.g., changes made by a newly retired employee during the last 8 months), it is recommended to use *.csv* format.

Troubleshooting Tips

If you do not see the expected information in search results, try the following:

- Verify the Audit Database retention and SQL Server settings.
- Make sure that data collection is configured properly in the monitoring plan settings.
- Check the required audit settings in your monitored infrastructure.
- Verify the data collecting account.

See next:

- Use Filters in Advanced Mode

Use Filters in Simple Mode

Filters are used to narrow your search results. To create a unique set of filters, you can:

- Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., Who*: Administrator* AND Action*: Added*).
- Specify several values in the same filter to search for any of them (e.g., Action*: Modified* ORAction*: Removed*). To do this, select a filter again and specify a new value.

  Spaces do not separate values, so the whole expression will be included in your search as a single value. For example, if you want to search for any of three names, do not enter *Anna Mark Bill* but instead create a separate filter entry for each name.

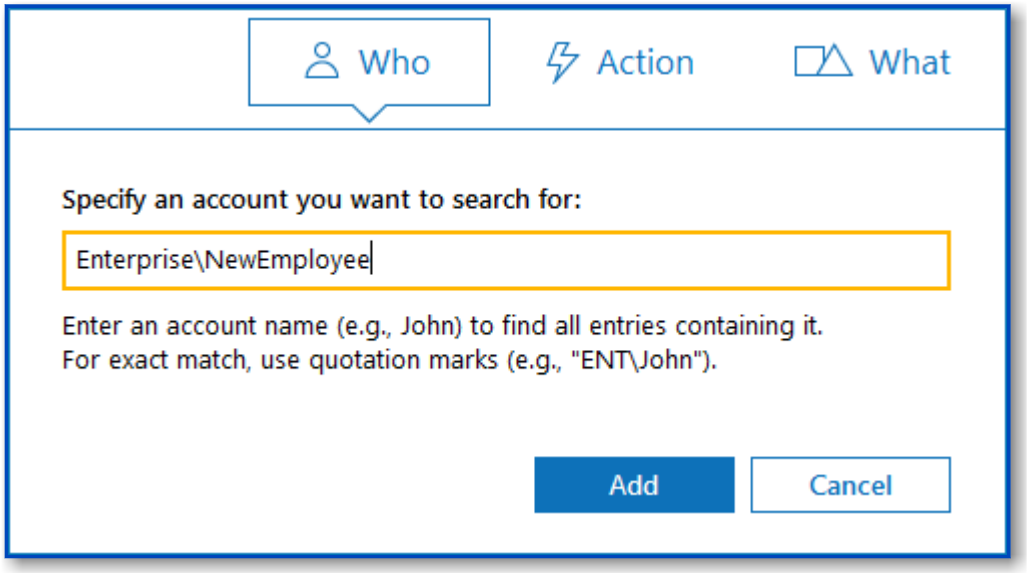
Filter Types

Filter	Description
Who	Filter data by user (initiator) account. Specify an account name (e.g., *John*) to find all entries containing it (e.g., *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*, *John@domain.com*). For exact match, use quotation marks and provide a user name in Domain\User or UPN format (e.g., *“Domain1\John”* or *"John@domain.com"*) .
Action	Filter data by action type (Added, Removed, etc.) Select an action type from the list (Added, Removed, Modified, Read). For additional actions, navigate to Advanced mode. Apply Additional Filters
What	Specify an object name (e.g., *Policy*) to find all entries containing it (e.g., *HiSecPolicy*, *\\FileSserver\Share\NewFolder\NewPolicy.docx*, *http://sharepoint/sites/collection1/Lists/Policy*). Netwrix Auditor searches across all data sources. For an exact match, use quotation marks and provide an object name in the format that is typical for your data source (e.g., “*HiSecPolicy*”).
When	Filter data by the time interval when the change occurred. Specify a timeframe or provide a custom date range. Netwrix Auditor allows you to see changes that occurred today, yesterday, in the last 7 or 30 days, or within the specified date range.

Filter	Description
Where	Specify a resource name (e.g., *Enterprise*) to find all entries containing it (e.g., *Enterprise-SQL*, *FileStorage.enterprise.local*). The resource name can be a FQDN or NETBIOS server name, Active Directory domain or container, SQL Server instance, SharePoint farm, VMware host, etc. Netwrix Auditor searches across all data sources. For an exact match, use quotation marks and provide a resource name in the format that is typical for your data source (e.g., *"Enterprise-SQL"*).

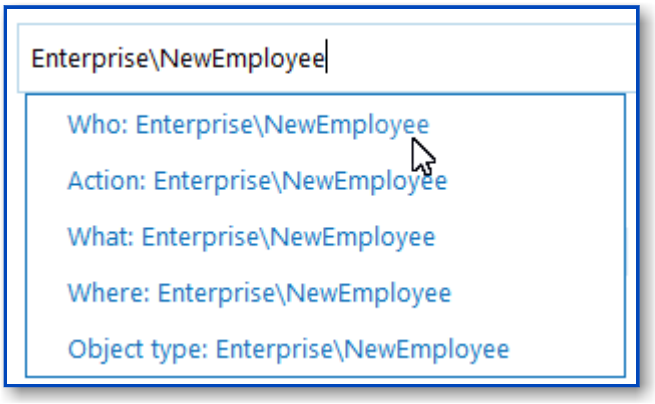
To add a filter to your search

1. Click a filter type icon. Enter a value you want to search for.



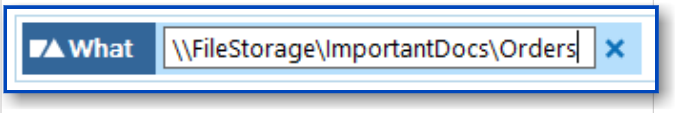
Alternatively, you can type a value directly into the Search field.

- For exact match, use quotation marks.
- To further restrict your search, right-click the value and select a filter from the pop-up menu. To search across all columns in the results view (everywhere—Who, What, Where, Action, etc.), leave it as is.



2. Click Search to apply your filters. By default, all entries that contain the filter value are shown.

Modifying and Removing Filters

To...	Do...
Modify filter	Double-click the filter and type a new value.  If you need to modify the When filter, delete it and add a new value, or navigate to the Advanced mode (Simple mode does not support its modification).
Remove filter	Click the Close icon next to it.

Exporting and Importing Filters

To export or import filters as regular expressions, use the **Tools** menu commands:

To...	Use...
Export	**Copy search** — copies the search filters that are currently applied to your search. This can be helpful if you want to share your search with a colleague (e.g., by pasting it in an email) or to modify a saved search query with your current filters.
Import	**Paste search** — pastes the search filters you copied before. These can be filters copied from a previous search or those someone shared with you.

Use Filters in Advanced Mode

Netwrix Auditor provides an advanced set of filters and match type operators that enable you to customize your searches even more precisely.

Switch to Advanced mode to review your current search in details and modify it if necessary. Click Add to add a new filter to your search.

Review the following for additional information:

- Apply Additional Filters
- Search Conditions

Apply Additional Filters

Expand the Filter list to find additional filters or filter values. The most commonly used filters are described in Use Filters in Simple Mode. Review the following for additional information:

Filter	Description	Example
Action	Limits your search to the selected actions only. Specify an action from the Value list or type it yourself. The Action filter in the Advanced mode contains	You are investigating suspicious user activity. You have already identified the intruder and now you want to see if any files were deleted or moved, and emails sent.

<table>
<tr><th>Filter</th><th>Description</th><th>Example</th></tr>
<tr><td></td><td>actions besides those available in basic mode (added, modified, removed, and read). Reported actions vary depending on the data source and object type.<table>
<tr><td>• Added</td><td>• Add (Failed Attempt)</td></tr>
<tr><td>• Removed</td><td>• Remove (Failed Attempt)</td></tr>
<tr><td>• Modified</td><td>• Modify (Failed Attempt)</td></tr>
<tr><td>• Read</td><td>• Read (Failed Attempt)</td></tr>
<tr><td>• Moved</td><td>• Move (Failed Attempt)</td></tr>
<tr><td>• Renamed</td><td>• Rename (Failed Attempt)</td></tr>
<tr><td>• Checked in</td><td>• Checked out</td></tr>
<tr><td>• Discard check out</td><td>• Successful Logon</td></tr>
</table></td><td>Since you are interested in specific actions only, set the Action filter to Removed, Moved, and Sent.</td></tr>
</table>

Filter	Description	Example
	• Failed Logon • Logoff • Copied • Sent • Session start • Session end • Activated	
Object type	Limits your search to objects of a specific type only. Specify an object type from the Value list or type it yourself. This filter modifies the What filter. The value list is prepopulated with the most frequent object types.	You noticed that some domain policies were changed and you want to investigate this issue. Your What filter is set to *Policy*, and so you keep receiving search results such as *HiSecPolicy,* \ *FS**Share**NewPolicy.docx*, *http://corp/sites/col1/Lists/Policy.* These entries correspond to different object types and data sources. Since you are looking for GPOs only, select GroupPolicy from the Value list.
Data source	Limits your search to the selected data source only. Specify a data source from the Value list or type it yourself.	You are investigating suspicious user activity. A user specified in the Who filter made a lot of changes across your IT infrastructure, so the search results became difficult to review. Since you are only interested in the way this user's activity could affect your Active Directory domain and Exchange organization, set the Data

Filter	Description	Example
		source filter to Active Directory and Exchange to limit the search results.
Monitoring plan	Limits your search to the selected plan only. Specify the name from the Value list or type it yourself.	You are investigating suspicious user activity. A user specified in the Who filter made a lot of changes across your IT infrastructure, so the search results became difficult to review. Since you are only interested in the way this user's activity could affect file shares audited within a single plan, set the Monitoring plan filter to *"My servers"* to limit the search results.
Item	Limits your search to the selected item only. This filter can be helpful if have several items of the same type in your monitoring plan (e.g., two Active Directory domains). Specify the name from the Value list or type it yourself.	Your monitoring plan is configured to track domains and includes your secured corporate domain and a domain for temporary employees. You are investigating who logged in your secured corporate domain outside business hours. You can set the Item filter to this domain name to limit the search results and exclude logons to computers from a less important domain.
Working hours	Limits your search results to entries that occurred within the specified hours. You can use this filter together with When if you need, for example, to search for activity in the non-business hours during the last week.	You are investigating an incident and want to know who accessed sensitive data outside business hours. You can set this filter as *Not equal to* and specify the time interval from *8:00 AM* to *6:00 PM*. Filtered data will include only operations that occurred outside this interval, that is, during non-business hours.

Filter	Description	Example
Data categories	Limits your search results to entries that contain sensitive data comply with a classification rule. You can use this filter together with Equal to PCIDSS to, for example, to search for sensitive files that contain data regulated by the PCIDSS.	You are searching all documents containing cardholder data that can potentially be mapped with the PCIDSS compliance standard. You can set this filter *as equal to* and specify the value as *PCIDSS*. Filtered data will contain only files that match this criteria. This filter shows activity records collected from the following data sources: • Windows File Servers • ShrePoint • SharePoint Online
Details	Limits your search results to entries that contain the specified information in the Details column. The Details column normally contains data specific to your target, e.g., assigned permissions, before and after values, start and end dates. This filter can be helpful when you are looking for a unique entry.	You discovered that a registry key was updated to *"242464"*. Now you want to investigate who made the change and what the value was before. You can set the Details filter to *242464* to find this change faster.
Before*	Limits your search results to entries that contain the specified before value in the Details column.	You are investigating an incident in which the SAM-account-name attribute was changed for an account in your Active Directory domain. You can set the Before filter to the previous name (e.g., *John2000*) to find the new name faster.

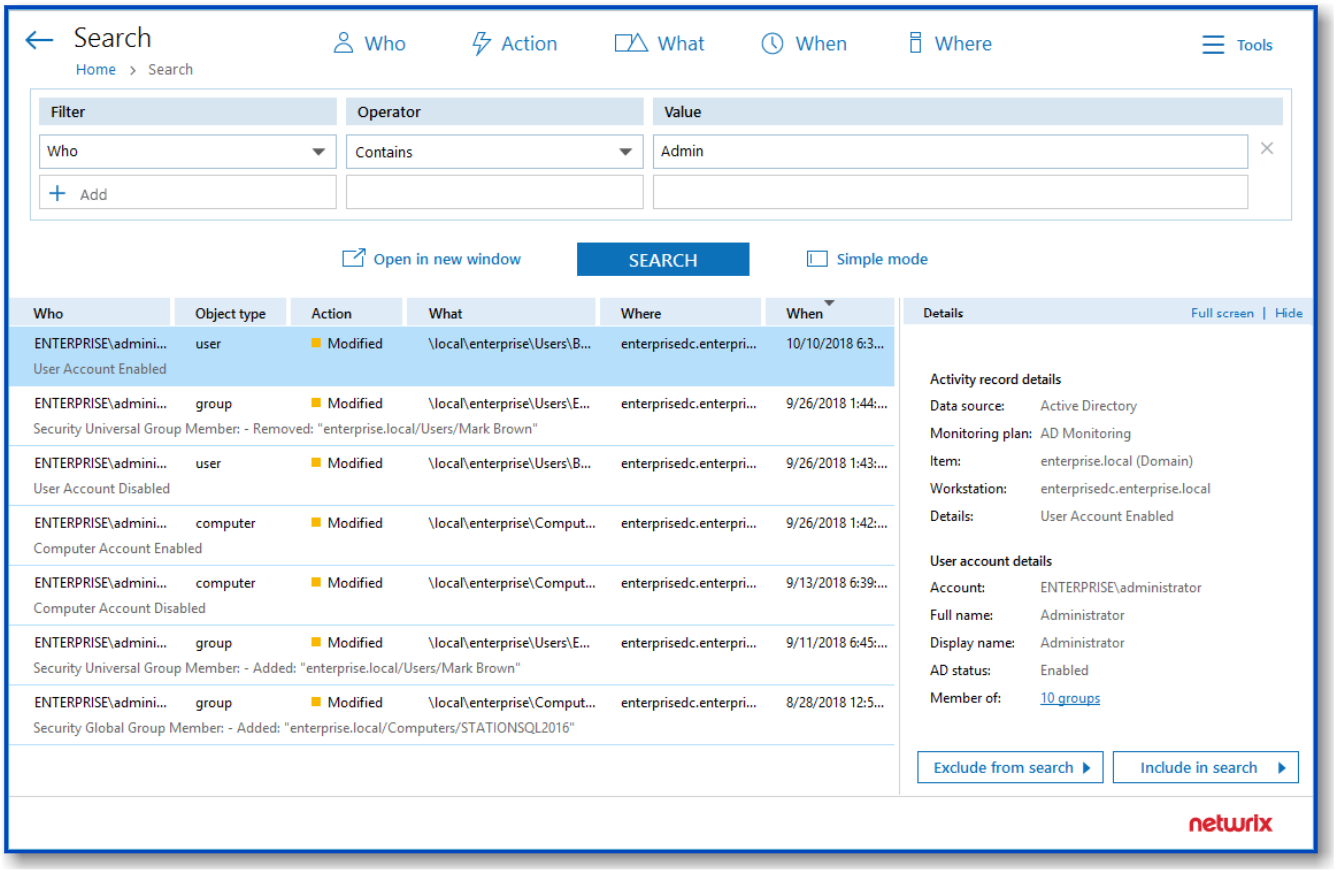
Filter	Description	Example
After*	Limits your search results to entries that contain the specified after value in the Details column.	You are investigating a security incident and want to know who enabled a local Administrator account on your Windows Server. You can set the After filter to this account's current state (e.g., *Enabled*) to find this change faster.
Everywhere	Limits your search results to entries that contain the specified value in any column.	You are investigating a security incident. You have already identified the intruder (e.g., *BadActor*) and now you want to see all actions made by intruder's account or with it. Since the intruder can be the actor (Who), the object (What), or can even show up in details, set the Everywhere filter to intruder's name.

* 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.

* – 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.

Search Conditions

When you apply filters at search, you can specify operators that should be used as conditions for data you want to retrieve and compare with the certain filter value. A condition can be, for example, Contains, Starts with, and so on.



The following operators can be used to specify search conditions:

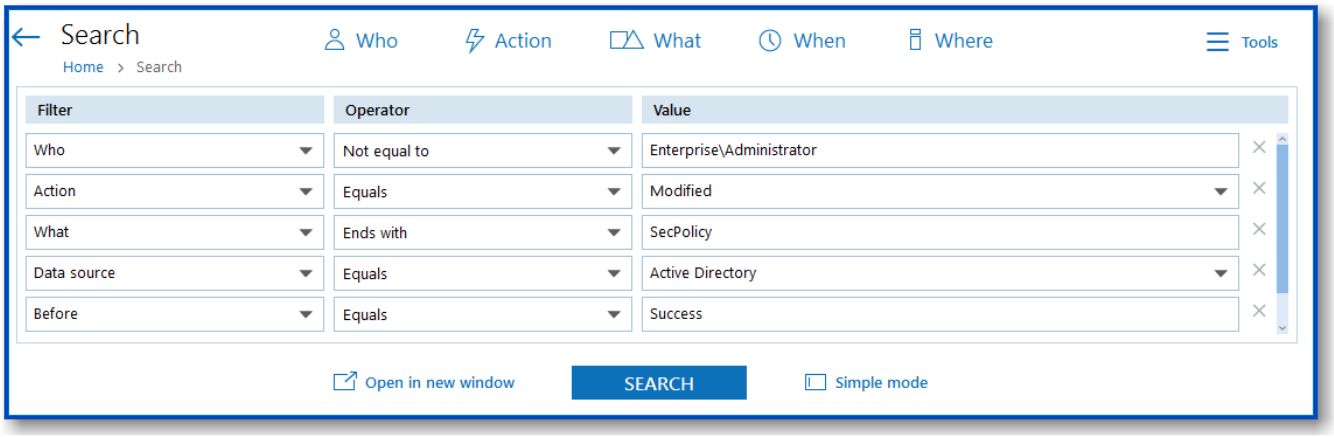
Operator	Description	Example
Contains	This operator shows all entries that contain a value specified in the filter.	If you set the Who filter to contains *John*, you will get the following results: *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*, *John@domain.com*.
Equals	This operator shows all entries with the exact value specified. Make sure to provide a full object name or path. To apply this operator when adding filters in the Simple mode, provide	Use this operator if you want to get precise results, e.g., \ *FS\Share\NewPolicy.docx*.

Operator	Description	Example
	a value in quotation marks (e.g., *"Domain1\John"*).	
Not equal to	This operator shows all entries except those with the exact value specified. In the Search field in the Simple mode, this operator appears as not, e.g., Who not for the Who filter.	If you set the Who filter to not equal to *Domain1\John*, you will exclude the exact user specified and find all changes performed by other users, e.g., *Domain1\Johnson, Domain2\John*.
Starts with	This operator shows all entries that start with the specified value.	If you set the Who filter to starts with *Domain1\John*, you will find all changes performed by *Domain1\John*, *Domain1\Johnson*, and *Domain1\Johnny*.
Ends with	This operator shows all entries that end with the exact specified value.	If you set the Who filter to ends with *John*, you will find all changes performed by *Domain1\John*, *Domain2\Dr.John*, *Domain3\John*.
Does not contain	This operator shows all entries except those that contain the specified value. In the Search field in the Simple mode, this operator appears as not, e.g., Who not for the Who filter.	If you set the Who filter to does not contain *John*, you will exclude the following users: *Domain1\John*, *Domain2\Johnson*, and *Johnny@domain.com*.
In group	This operator relates to the Who filter. It instructs Netwrix Auditor to show only data for the accounts included in the specified group.	If you set the In group condition for Who filter to *Domain\Administrators*, only the data for the accounts included in that group will be displayed.
Not in group	This operator relates to the Who filter. It instructs Netwrix Auditor to	If you set the Not in group condition for Who filter to *Domain\Administrators*, only the

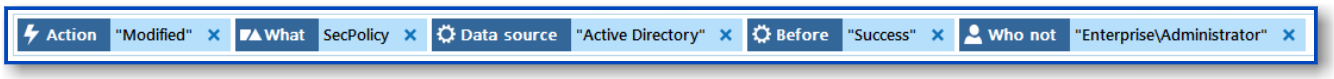
Operator	Description	Example
	show only data for the accounts not included in the specified group.	data for the accounts not included in that group will be displayed.

When you add a new search filter, the Contains operator is used by default.

To modify conditions for the selected filters, make sure you have switched to the Advanced search mode.



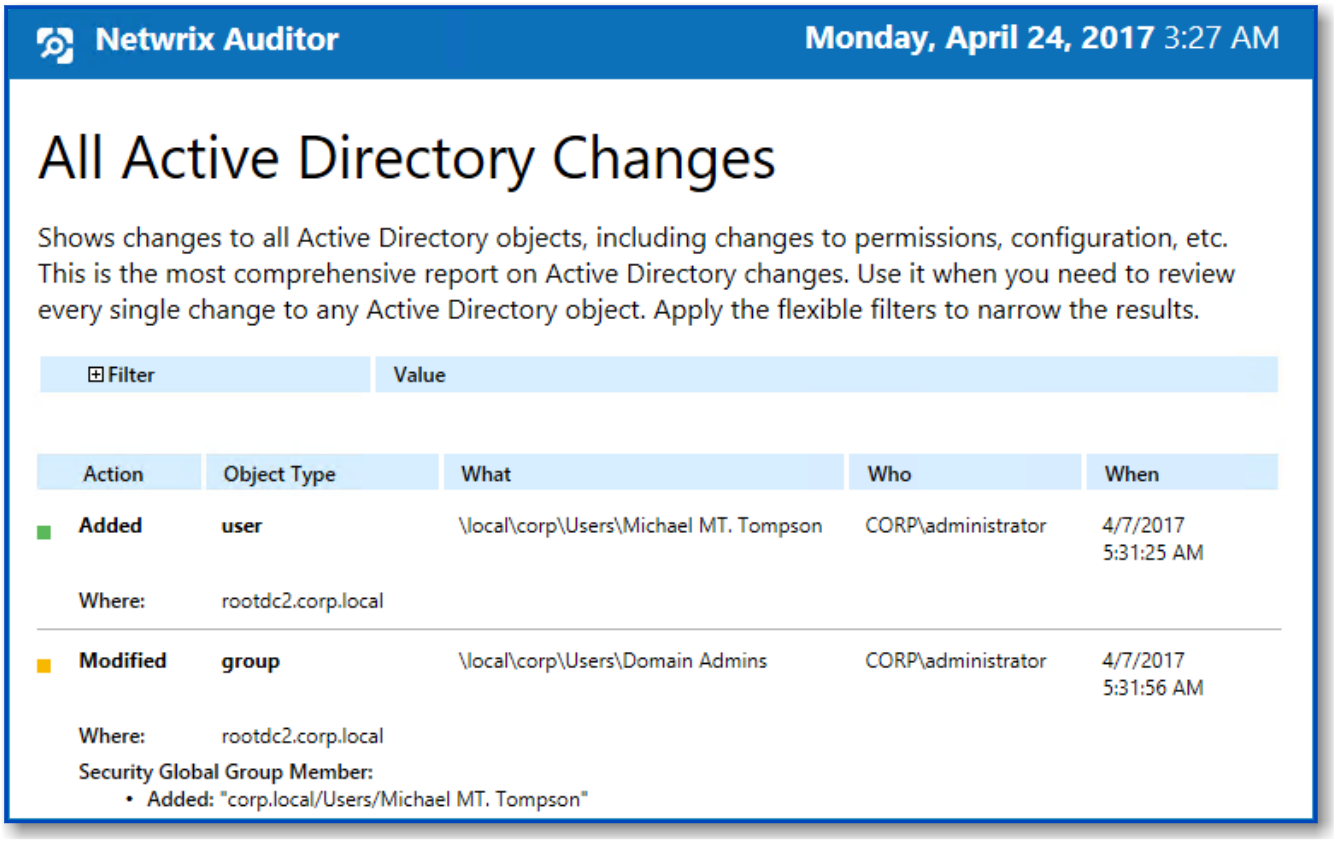
The image below represents the same search filters as they are shown in the Search field in the Simple mode.



Reports

Netwrix Auditor provides a variety of reports for each data source. This helps you keep track of all changes in your IT infrastructure and validate compliance with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.). You can also create your custom reports based on the Interactive Search technology.

To review intelligence data, you must be assigned the Global administrator or Global reviewer role in the product. The users assigned the Reviewer role on a certain plan or folder have a limited access to data—only within a delegated scope. See the Role-Based Access and Delegation topic for additional informatuion.



Review general report types available in Netwrix Auditor to meet your specific business needs:

Report type	Description
Predefined reports	Predefined reports pack contains over a hundred SSRS-based reports grouped by business categories and data sources. Predefined reports are helpful if you are looking for a ready-to-use template for your business needs. See the Predefined Reports topic for additional information.
Compliance reports	For your convenience, specific reports are grouped into folders by corresponding international standards and regulations such as security controls, information security, etc. See the Compliance Reports topic for additional information.
Custom reports	For your convenience, the Reports section has been enhanced with Custom reports. Initially, the product provides templates for the best common workflows

Report type	Description
	within Auditor. Later, you can always create custom report from interactive search and find them here. See the Custom Search-Based Reports topic for additional information.

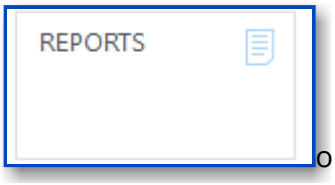
View Reports

To view reports, users need the following:

1. Sufficient access rights in Netwrix Auditor, which are provided through role assignment:
   - Users with *Reviewer* role can generate the reports for their delegated scope only, and view them in any Netwrix Auditor client or in a web browser.
   - Users with *Global administrator* or *Global reviewer* role can also create subscriptions to reports.
2. The Browser role on the SSRS Report Server. See the SQL Server Reporting Services topic for additional information.

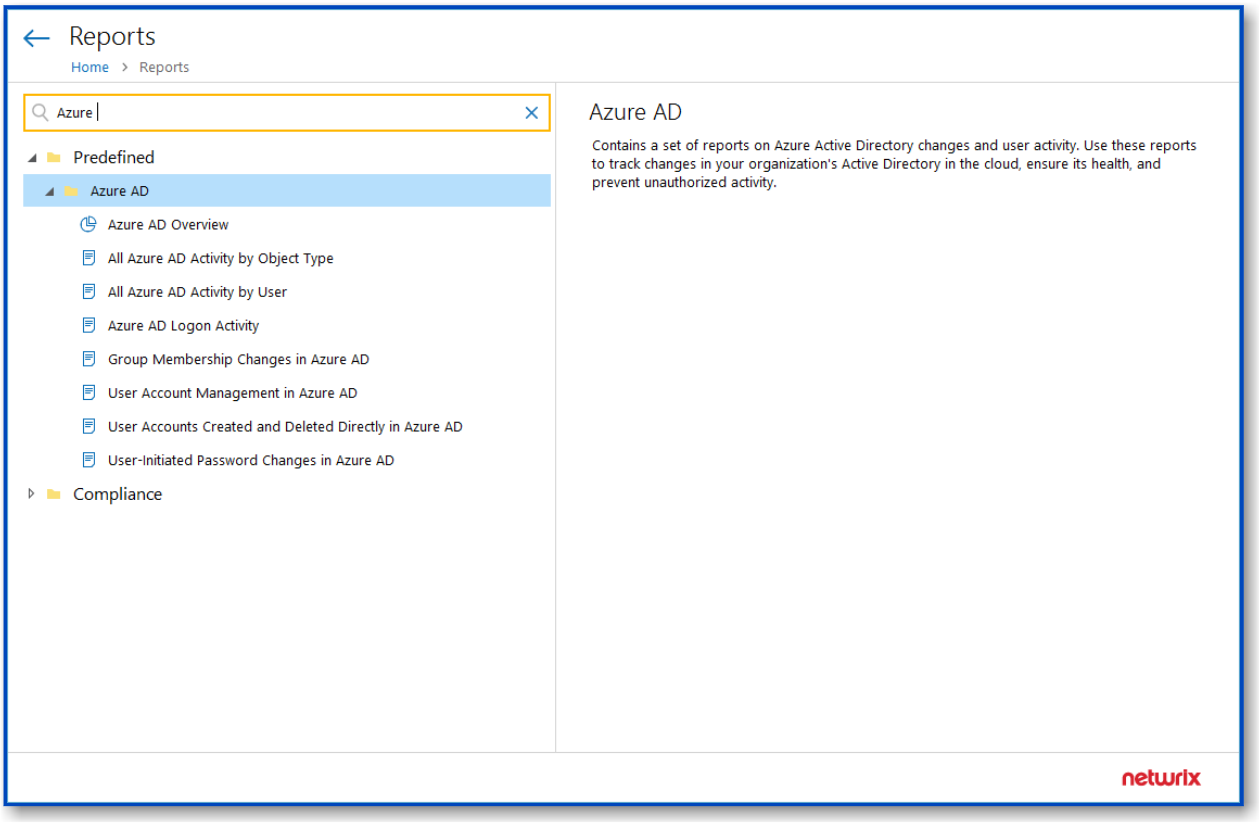
To view a report

You can add any elements (a dashboard, report, alert, risk, etc.) to the Auditor Home screen to access them instantly. See the Navigation and Customize Home Screen topics for additional information.

1. In Netwrix Auditor Home screen, click 

on the left, and in the tree on the left select the report you need.

   To speed up the process, you can use the **Search** field, entering the keyword to search by.



2. Click View button in the right pane.

To learn how to subscribe to a report, see Create Subscriptions.

Troubleshooting

If no data is displayed in the report, you may need to do the following:

1. Make sure that the Audit Database settings are configured properly in the monitoring plan, and that data is written to databases that reside on the default SQL Server instance. See the Audit Database topic for additional information.
2. For SSRS-based reports - verify that SSRS (SQL Server Reporting Services) settings are configured properly. See the Audit Database topic for additional information.
3. For state-in-time reports - verify that the monitoring plan that provides data for the report has the corresponding option selected. See the Create a New Monitoring Plan topic for additional information.

Customize Report with Filters

Report filters allow you to display changes matching certain criteria. For example, you can filter changes by audited domain or object type. Filtering does not delete changes, but modifies the report view allowing you to see changes you are interested in. Filters can be found in the upper part of the Preview Report page.

To apply filters

1. Navigate to Reports and generate a report.
2. Apply required filters to the report and click View Report. For example, you can update report timeframe, change *Who* and *Where* values, apply sorting, etc.

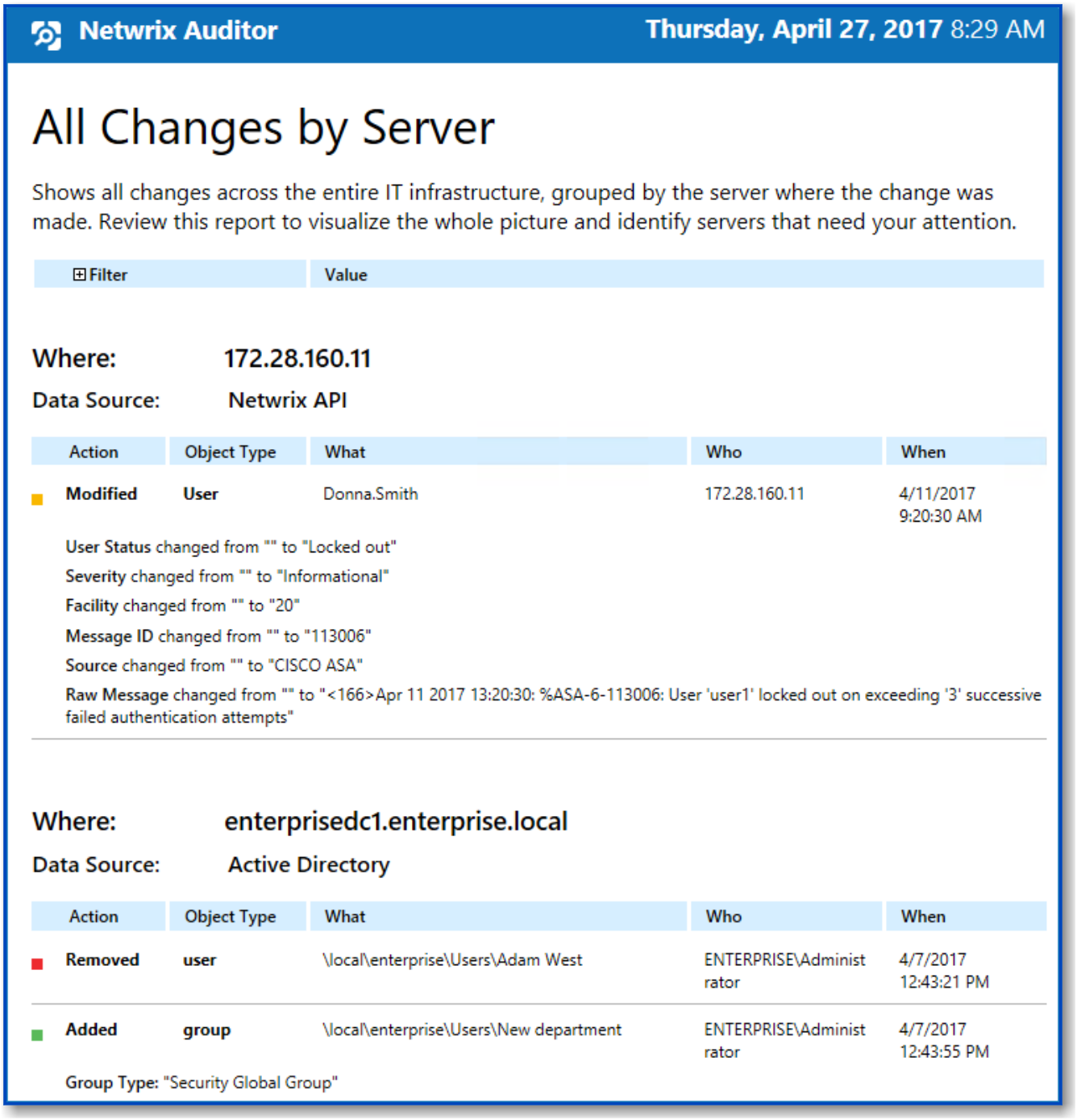
Wildcards are supported. For example, type *%corp\administrator%* in the in the Who domain\user field if you want to view changes made by the corp\administrator user only .

Do not use % in the exclusive filters (e.g., Who (Exclude domain\user)). Otherwise, you will receive an empty report.

escape_characters are not supported.

The example below applies to the All Changes by Server report and shows the before and after views of the report. The filters may vary slightly depending on the audited system and report type.

The report without filtering:



Netwrix Auditor Thursday, April 27, 2017 8:29 AM

All Changes by Server

Shows all changes across the entire IT infrastructure, grouped by the server where the change was made. Review this report to visualize the whole picture and identify servers that need your attention.

Filter	Value

Where: 172.28.160.11

Data Source: Netwrix API

Action	Object Type	What	Who	When
Modified	**User**	Donna.Smith	172.28.160.11	4/11/2017 9:20:30 AM

User Status changed from "" to "Locked out"

Severity changed from "" to "Informational"

Facility changed from "" to "20"

Message ID changed from "" to "113006"

Source changed from "" to "CISCO ASA"

Raw Message changed from "" to "<166>Apr 11 2017 13:20:30: %ASA-6-113006: User 'user1' locked out on exceeding '3' successive failed authentication attempts"

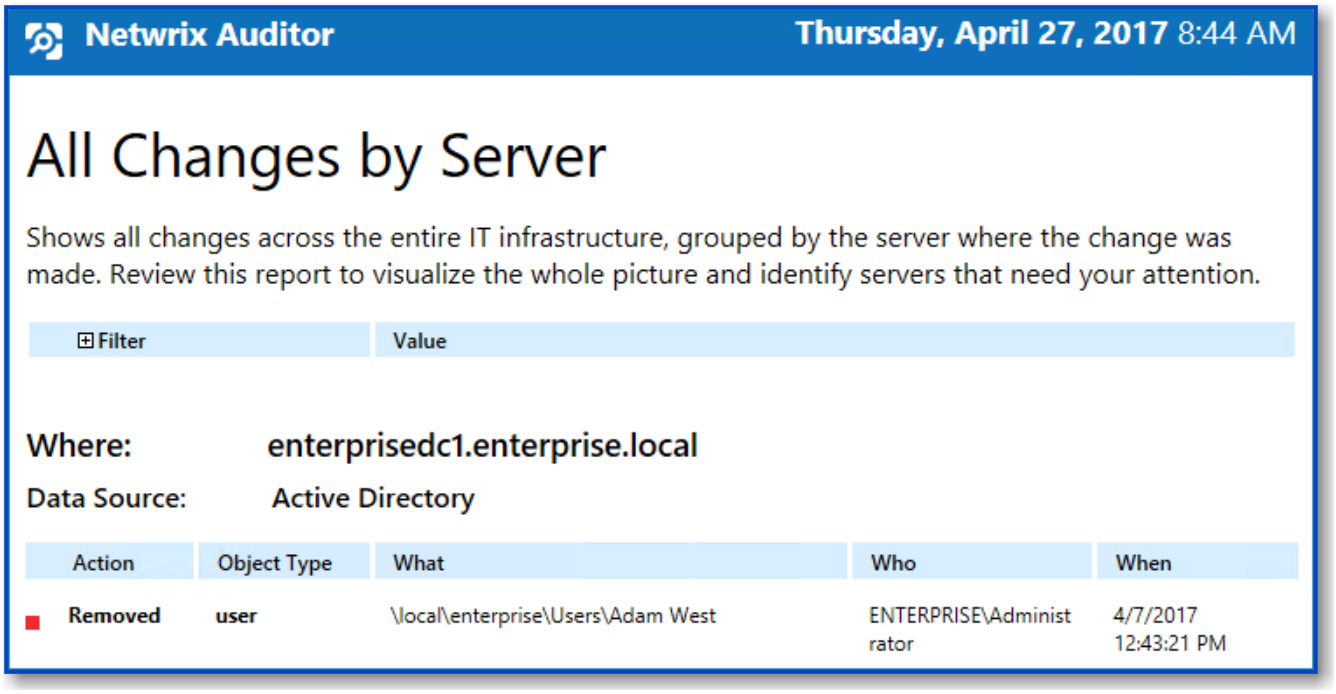
Where: enterprisedc1.enterprise.local

Data Source: Active Directory

Action	Object Type	What	Who	When
Removed	**user**	\local\enterprise\Users\Adam West	ENTERPRISE\Administrator	4/7/2017 12:43:21 PM
Added	**group**	\local\enterprise\Users\New department	ENTERPRISE\Administrator	4/7/2017 12:43:55 PM

Group Type: "Security Global Group"

The report below displays changes for all audited systems made by the CORP\Administrator user on the ROOTDC2 domain controller for a month sorted by the action type.

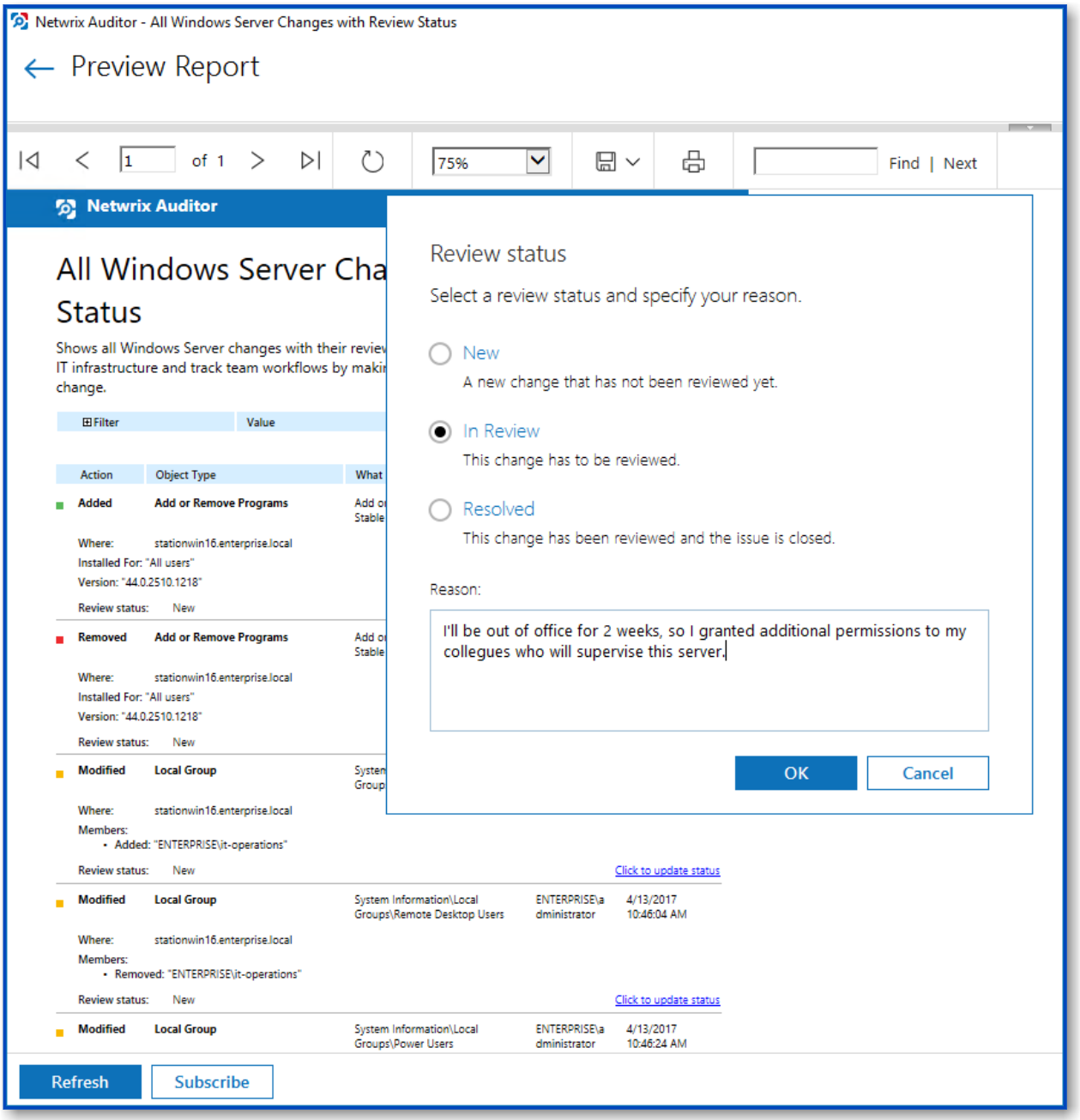


Interactive Reports for Change Management Workflow

Change management is one of the critical processes for many companies referring to such areas as requesting, planning, implementing, and evaluating changes to various systems. For your change management workflow, Netwrix Auditor offers several reports with interactive capabilities – not only they list changes in your infrastructure but also allow you to track, analyze, assign appropriate status and comment on these changes.

This capability can supplement your organization's workflow of monitoring and resolving potential issues through the following automated course of action:

1. The reported changes to the monitored environment are assigned the New status by default.
2. If a change seems unauthorized, or requires further analysis, you can click the Click to update status link next to the change detailed data:



3. In the **Review status** dialog for selected change, set its status to In Review and provide a reason.
4. Once the change has been approved of, or rolled back, you can set its status to Resolved.

This capability is supported for the following reports:

Data source	Report location
Entire IT infrastructure	Organization Level Reports

Data source	Report location
Active Directory	Active Directory → Active Directory Changes → All Active Directory Changes with Review Status
Exchange	Exchange → All Exchange Server Changes with Review Status
SharePoint	SharePoint → All SharePoint Changes with Review Status
Windows Server	Windows Server → Windows Server Changes → All Windows Server Changes with Review Status
Group Policy	Active Directory → Group Policy Changes → All Group Policy Changes with Review Status

In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the Monitoring Plans section.

They list

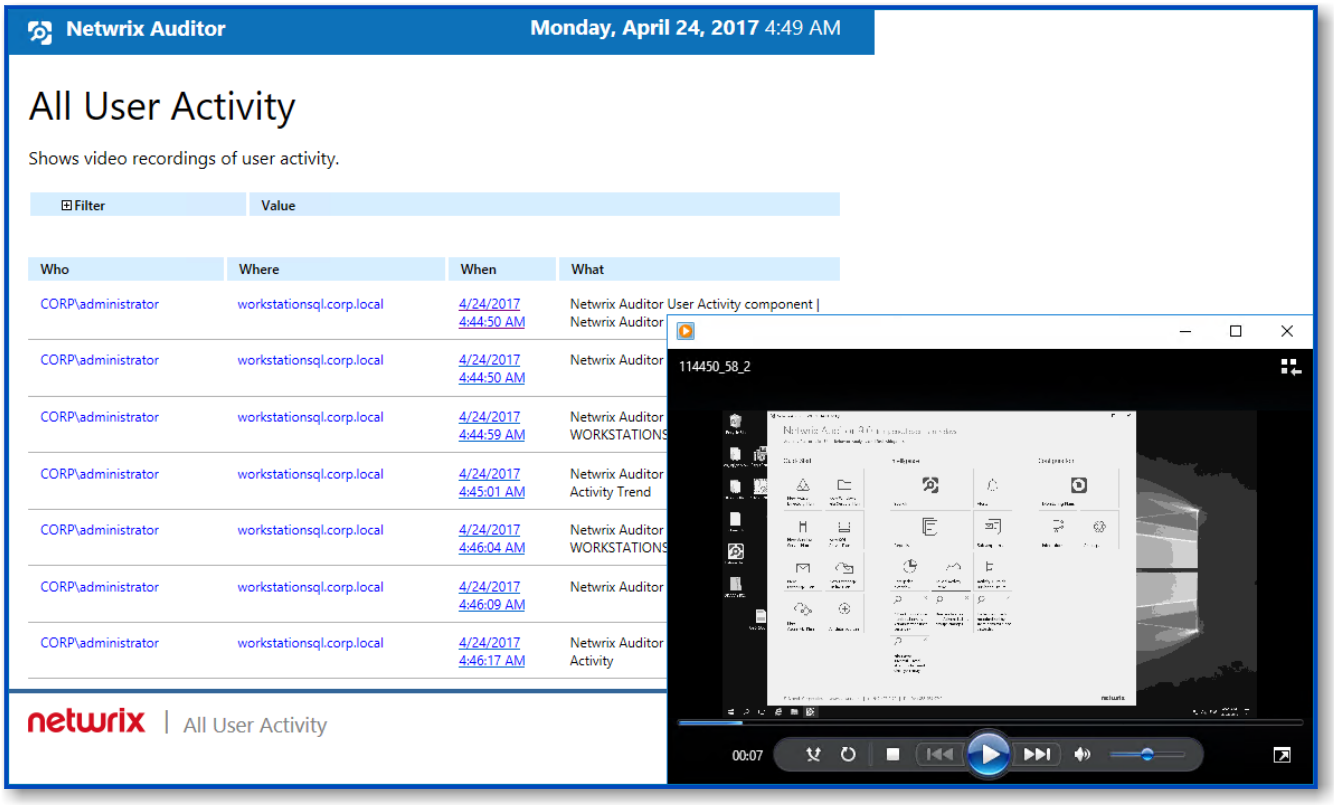
Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any report you want to receive on a regular basis. See the Subscriptions topic for additional information.

Reports with Video

Netwrix Auditor can be configured to capture video of user activity on the monitored computers that helps analyze and control changes made there. When you click a link, a video player opens and playback of the recorded user activity starts, showing launched applications, actions, etc.

To view reports with video, navigate to Reports → User Activity.

In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the Monitoring Plans section.



Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any report you want to receive on a regular basis. See the Subscriptions topic for additional information.

Follow the steps to play a video:

Step 1 – Navigate to **Reports** → **User Activity**. Select any report and click View.

Step 2 – Click a link in the **When** column.

To open User Activity report for the selected user or server, you can also click the link in the Who and Where columns of the All Users Activity report.

Predefined Reports

Netwrix Auditor is shipped with 250+ ready-to-use reports designed by Netwrix industry experts. To find a report that is right for you, check out the predefined report types available in the product.

- Enterprise Overview—A dashboard with a set of widgets that provide quick access to important statistics across the audited IT infrastructure. They allow you to see the activity

trends by date, user, data source, server or audited IT system, and drill through to detailed reports for further analysis. The Enterprise Overview dashboard aggregates the information on changes from all data sources and provides a centralized overview. System-specific dashboards reflect all changes across all monitoring plans where audit of this target system is enabled. See the Enterprise Overview Dashboard topic for additional information.

- Organization level reports—High-level reports that aggregate data from all data sources and monitoring plans. They list all activity that occurred across the audited IT infrastructure. Enterprise Overview provides bird's eye view of changes and activity from all data sources and provides a centralized overview. See the Organization Level Reports topic for additional information.
- Overview diagrams—System-specific diagram reports that aggregate audit data for an auditing system. They provide a high-level overview of changes within a selected time period. Overviews consist of four charts, showing the activity trends by date, user, object type or server, and drill through to detailed reports for further analysis.
- Change and activity reports—System-specific reports that aggregate audit data for a specific data source within specified monitoring plans. These reports show detailed data on changes and activity and provide grouping, sorting and filtering capabilities. Each report has a different set of filters allowing you to manage collected data in the most convenient way. See the Change and Activity Reports topic for additional information.
- State-in-time reports—System-specific reports that aggregate data for a specific data source within a specified individual monitoring plan and allow reviewing the point-in-time state of the data source. These reports are based on daily snapshots and help you paint a picture of your system configuration at a specific moment in time. Currently, the Windows Server State-in-Time report set provides baselining functionality that help identify aberrant servers. See the State–In–Time Reports topic for additional information.
- Changes with video reports—Windows server-based reports that provide video recordings of user activity on audited computers. See the Reports with Video topic for additional information.
- Changes with review status reports—Both system-specific and overview reports that can be used in the basic change management process. These reports allow setting a review status for each change and providing comments. See the Interactive Reports for Change Management Workflow topic for additional information.

Review the following for additional information:

- See the View Reports topic for additional information on how to find the report you need and view reports in a web browser.

- See the View Reports topic for additional information on how to apply filters to reports.

Enterprise Overview Dashboard

Enterprise Overview dashboard provide a high-level overview of activity trends by date, user, server, object type or audited system in your IT infrastructure. They allow you to see the activity

trends by date, user, object type, server or audited IT system, and drill through to detailed reports for further analysis. The Enterprise diagram aggregates data on all Managed Objects and all audited systems, while system-specific diagrams provide quick access to important statistics within one audited system.

The current version of Netwrix Auditor contains the following diagrams:

- Enterprise (aggregates data on all audited systems listed below)
- Active Directory
- Exchange
- File Servers
- SharePoint
- SQL Server
- VMware
- Windows Server

If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Auditor Global administrator to import that data from the Long-Term Archive.

All diagrams provide the drill-down functionality, which means that by clicking on a segment, you will be redirected to a report with the corresponding filtering and grouping of data that renders the next level of detail.

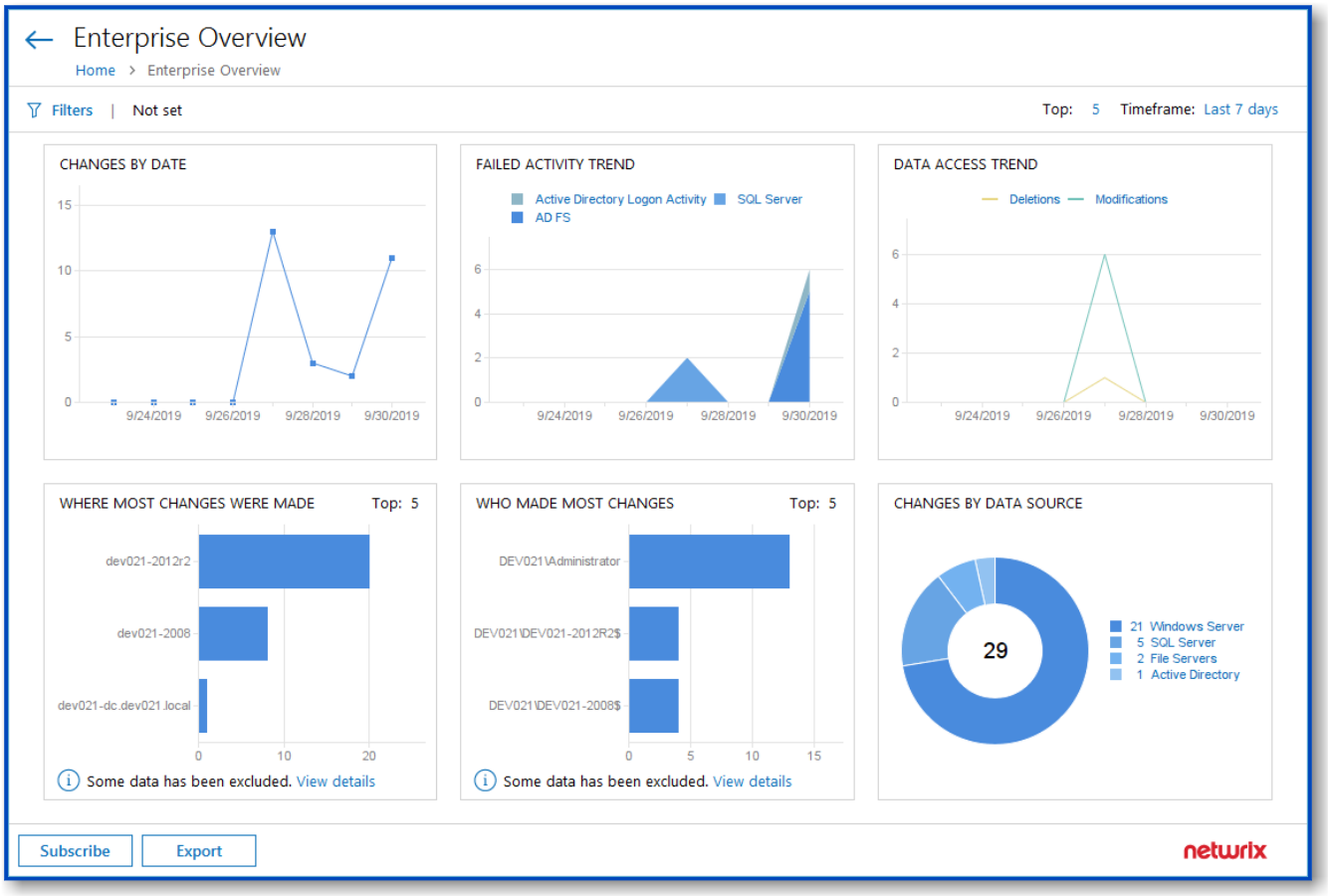
Follow the steps to review a diagram:

- On the Auditor home screen, click the **Reports** tile and open the Enterprise Overview section. Click a tile to open a corresponding diagram.

- Navigate to Reports and select one of the following locations:

Title	Location
Enterprise	Organization Level Reports
Active Directory Overview	Active Directory ® Active Directory Changes
Exchange Overview	Exchange
File Servers Overview	File Servers ® File Servers Activity
SharePoint Overview	SharePoint
SQL Server Overview	SQL Server
VMware Overview	VMware
Windows Server Overview	Windows Server ® Windows Server Changes

The example below applies to Enterprise.



Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any report you want to receive on a regular basis. See the Subscriptions topic for additional information.

Organization Level Reports

Organization Level reports aggregate data on all monitoring plans and list changes and activity that occurred across all data sources. Also, this folder includes a report on Auditor self-audit - it provides detailed information on changes to monitoring plans, data sources and audited items.

Organization Level reports can be found in the Organization Level Reports folder under the Reports node.

This folder includes:

Report	Details
Enterprise Overview	Dashboard report with diagrams showing all activities and changes across the monitored data sources. See also: Enterprise Overview Dashboard
All Activity with Review Status	Shows all activity across the entire IT infrastructure, including changes, read access and logons. Features interactive review status to supplement your change management workflow. See also: Interactive Reports for Change Management Workflow.
All Changes by Data Source	Shows all changes across your IT infrastructure, grouped by data source.
All Changes by Server	Shows all changes across the entire IT infrastructure, grouped by the server where the change was made.
All Changes by User	Shows all changes across your IT infrastructure, grouped by the user who made the change.
All Integration API Activity	Shows all activity records imported with Netwrix Auditor Integration API.
Self-Audit	Help to ensure that the scope of data to be audited is complete and all changes are in line with the workflows adopted by your organization.

Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any report you want to receive on a regular basis. See the Subscriptions topic for additional information.

Data Discovery and Classification Reports

Follow the steps to review Data Discovery and Classification reports:

Step 1 – Navigate to **Reports** > **Data Discovery and Classification** and select a report you are interested in.

Step 2 – Click View.

Data Discovery and Classification reports grouped by data sources.

The table below lists the reports available for Data Discovery and Classification:

Report	Description
File Servers	
Activity reports	
Activity Related to Sensitive Files and Folders	This report lists all access attempts to files and folders that contain certain categories of sensitive data at the moment.
State-in-time reports	
Most Accessible Sensitive Files and Folders	This report shows the number of users that effectively have access to sensitive files or folders, sorted in descending order. Use this report to identify data at high risk and plan for corrective actions accordingly.
Overexposed Files and Folders	This report shows sensitive files and folders accessible by the specified users or groups, based on the combination of folder and share permissions. Use this report to identify data at high risk and plan for corrective actions accordingly.
Sensitive Files and Folders by Owner	This report shows ownership of files and folders that are stored in the specified file share and contain selected categories of sensitive data. Use this report to determine the owners of particular sensitive data.
Files and Folders Categories by Object	This report shows files and folders that contain specific categories of sensitive data. Use this report to see whether a specific file or folder contains sensitive data.
Sensitive Files Count by Source	This report shows the number of files that contain specific categories of sensitive data. Use this report to estimate amount of your sensitive data in each

Report	Description
	category, plan for data protection measures and control their implementation.
Sensitive File and Folder Permissions Details	This report shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.
SharePoint	
Activity reports	
Activity Related to Sensitive Data Objects	This report shows changes and read operations on SharePoint sites and documents that contain sensitive information. Use this report to detect suspicious activity around your sensitive data.
State-in-time reports	
Sensitive Data Objects by Site Collection	For each SharePoint site collection listed, this report shows the categories of sensitive data stored there and the number of documents in each category. Use this report to reveal the number of sensitive files stored in your SharePoint site collections.
Sensitive Data Objects	For each site collection listed, this report shows the SharePoint objects (sites, lists and documents) that have been classified as containing sensitive information. Use this report to plan and control data protection measures for sensitive information stored on your SharePoint.

Report	Description
Sensitive Data Object Permissions	For each SharePoint object (site, list or document) listed, this report shows the user accounts that have access to this object, their effective permissions and how those permissions were granted (for example, permissions can be granted directly, via group membership or using SharePoint policy). Use this report to control access to SharePoint objects that contain sensitive data.
Overexposed Sensitive Data Objects	For each user account listed, this report shows the SharePoint objects (sites, lists and documents) containing sensitive data that the user can access based on their effective permissions. Use this report to identify overexposed data and plan measures to mitigate your risk.
Most Exposed Sensitive Data Objects	Lists the SharePoint objects (sites, lists and documents) containing sensitive data that can be accessed by the most users (or even Everyone), based on effective permissions. Use this report to identify data at high risk and plan corrective actions.

Requirements for Data Discovery and Classification Reports

The table below contains requirements to run Data Discovery and Classification reports. These are reports that help you to reduce the risk of data leaks and non-compliance by ensuring that all sensitive data resides in safe locations, that it isn't overexposed and that user activity around it is in line with security policies.

Applicable for:

- File Servers
- SharePoint
- SharePoint Online

Report	Requirement
File Servers	
Activity Related to Sensitive Files and Folders	• Monitoring plan for File Server data source with activity audit enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
File and Folder Categories by Object	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Most Accessible Sensitive Files and Folders	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Overexposed Files and Folders	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match);

Report	Requirement
	• Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Sensitive File and Folder Permissions Details	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Sensitive Files and Folders by Owner	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Sensitive Files and Folders by Source	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
SharePoint	
Activity Related to Sensitive Data Objects	• Monitoring plan for SharePoint data source with activity audit enabled in Netwrix Auditor;

Report	Requirement
	• Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Overexposed Sensitive Data Objects	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Sensitive Data Object Permissions	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.
Sensitive Data Objects by Site Collection	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.

Report	Requirement
Sensitive Data Objects	• Monitoring plan for File Server data source with 'Collect data for State-In-Time reports' feature enabled in Netwrix Auditor; • Netwrix Data Classification instance configured to crawl from the same source (naming must exactly match); • Sensitive Data Discovery correctly configured on the Netwrix Auditor Server.

Make Reports Handy

In addition to reviewing reports, you can customize them with filters and create report subscriptions. Review the following for additional information:

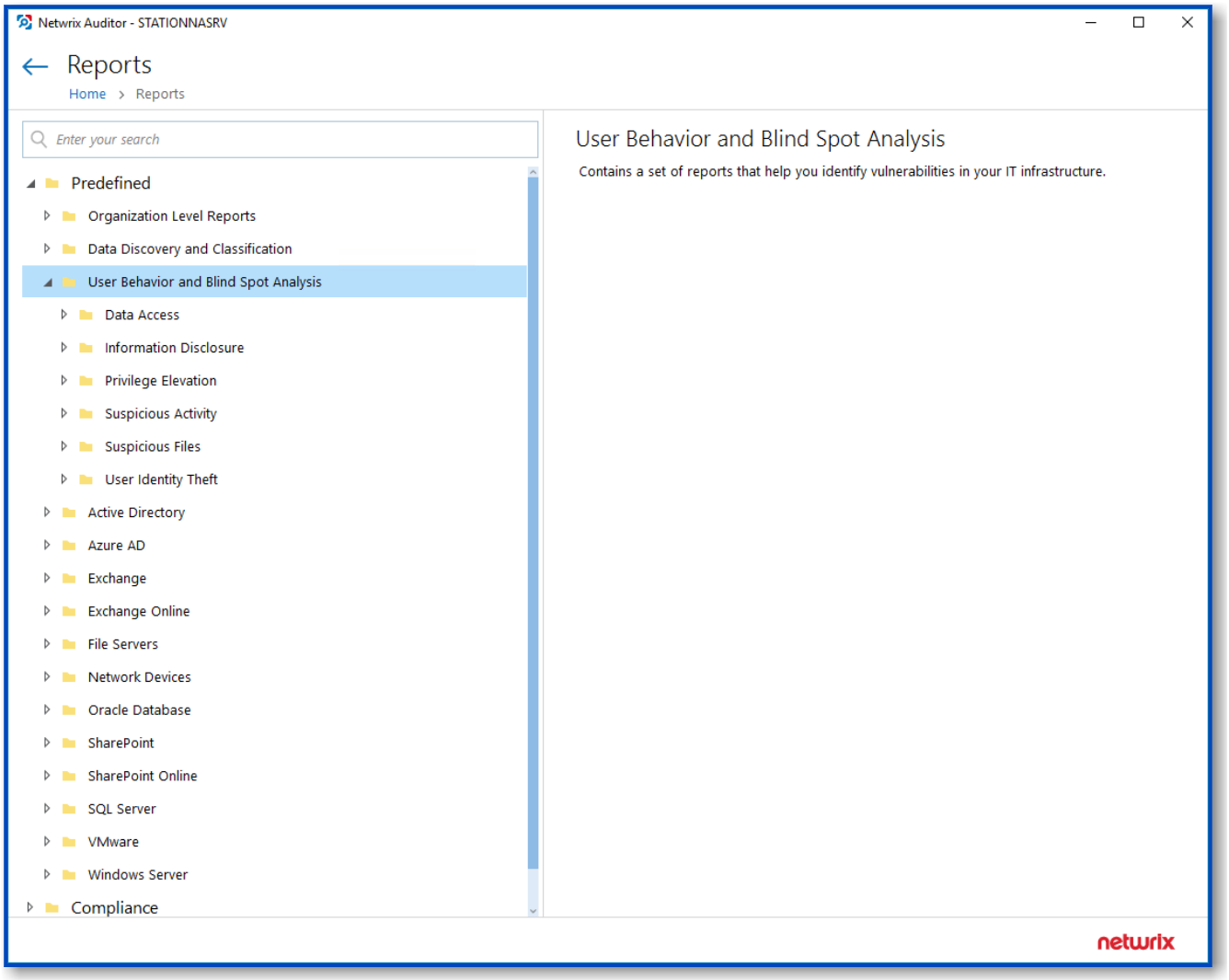
- View Reports
- Create Subscriptions

User Behavior and Blind Spot Analysis Reports

The User Behavior and Blind Spot Analysis report pack contains a set of smart reports that help you identify vulnerabilities and easily answer questions such as:

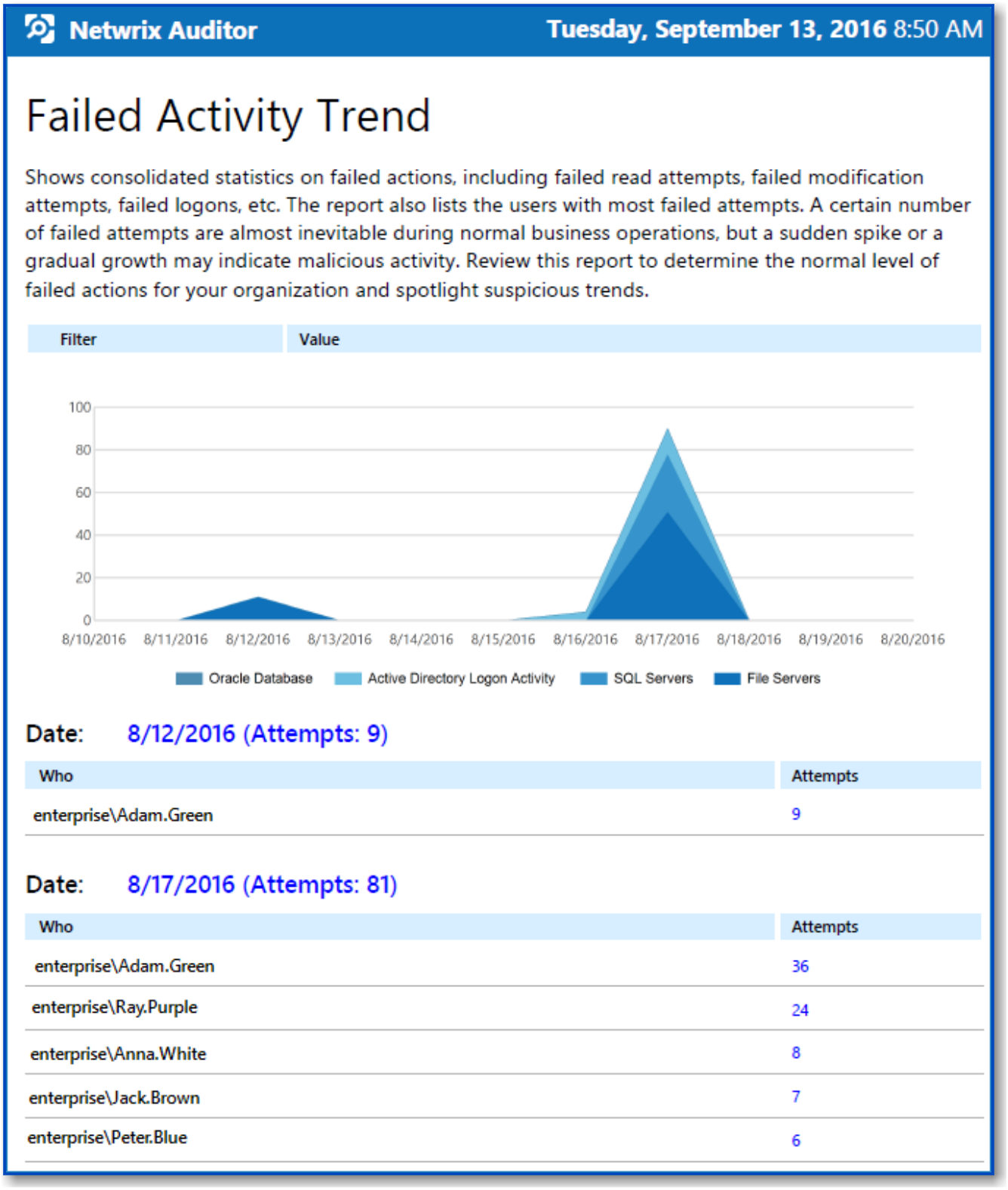
- Has there been any abnormal access to sensitive data?
- Is anyone accessing stale data?
- Have there been any unusual spikes in failed activity?
- Who is active outside of business hours and what are they doing?
- Has anyone put harmful files on corporate data storage?
- Are there any files likely to contain credentials, Social Security numbers, PHI or other sensitive data?

Analytics reports can be found in the User Behavior and Blind Spot Analysis folder under the Predefined node.



If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Auditor Global administrator to import that data from the Long-Term Archive.



Netwrix Auditor Tuesday, September 13, 2016 8:50 AM

Failed Activity Trend

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts. A certain number of failed attempts are almost inevitable during normal business operations, but a sudden spike or a gradual growth may indicate malicious activity. Review this report to determine the normal level of failed actions for your organization and spotlight suspicious trends.

Filter	Value

Date: 8/12/2016 (Attempts: 9)

Who	Attempts
enterprise\Adam.Green	9

Date: 8/17/2016 (Attempts: 81)

Who	Attempts
enterprise\Adam.Green	36
enterprise\Ray.Purple	24
enterprise\Anna.White	8
enterprise\Jack.Brown	7
enterprise\Peter.Blue	6

Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any

report you want to receive on a regular basis. See the Subscriptions topic for additional information.

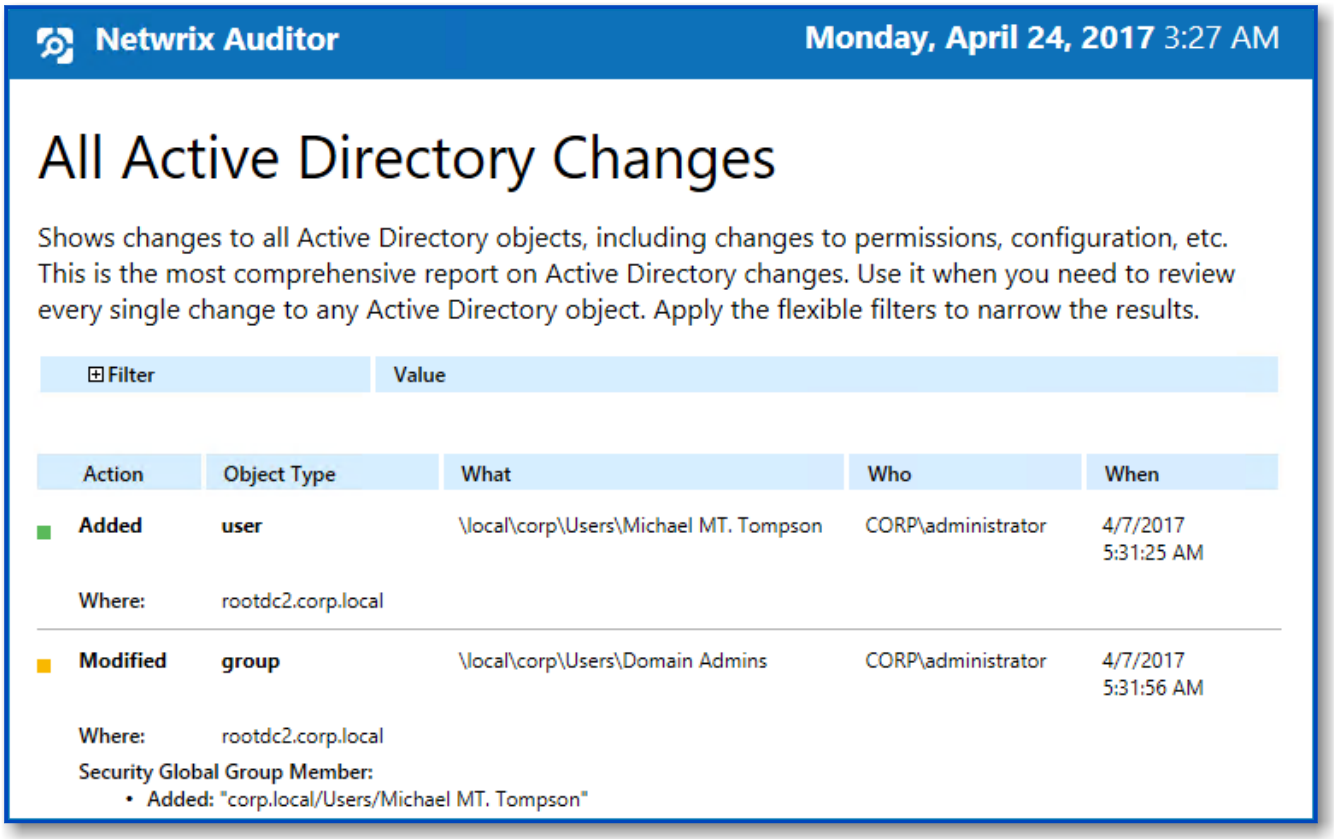
Change and Activity Reports

Change and activity reports provide information on changes to different aspects of the audited environment. Depending on the data source, navigate to one of the following locations, or use the search field to look for the keywords you need:

Data source	Report location
Active Directory	**Active Directory → Active Directory Changes**
Active Directory Federation Services	**Active Directory Federation Services (AD FS)**
Microsoft Entra ID Plans	Microsoft Entra ID Plans
Group Policy	Active Directory → Group Policy Changes
Exchange	Exchange
Exchange Online	Exchange Online
File Servers	File Servers → File Servers Activity
Oracle Database	Oracle Database

Data source	Report location
SharePoint	SharePoint
SharePoint Online	SharePoint Online
SQL Server	SQL Server
VMware	VMware
Windows Server	Windows Server → Windows Server Changes
Event Log	Windows Server → Event Log
IIS	Windows Server→ Event Log
Logon Activity	**Active Directory → Logon Activity**
Integration API	Organization Level Reports
Netwrix Auditor self-audit	Organization Level Reports

In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the Monitoring Plans section.



Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any report you want to receive on a regular basis. See the Subscriptions topic for additional information.

State–In–Time Reports

The state-in-time reports functionality allows generating reports on the system's state at a specific moment of time in addition to change and activity reports. State-in-time reports are based on the daily configuration snapshots, and reflect a particular aspect of the audited environment.

This functionality is currently available for the following data sources:

- Active Directory
- Azure AD
- File Servers
- Exchange Online
- MS Teams
- Windows Server
- SharePoint

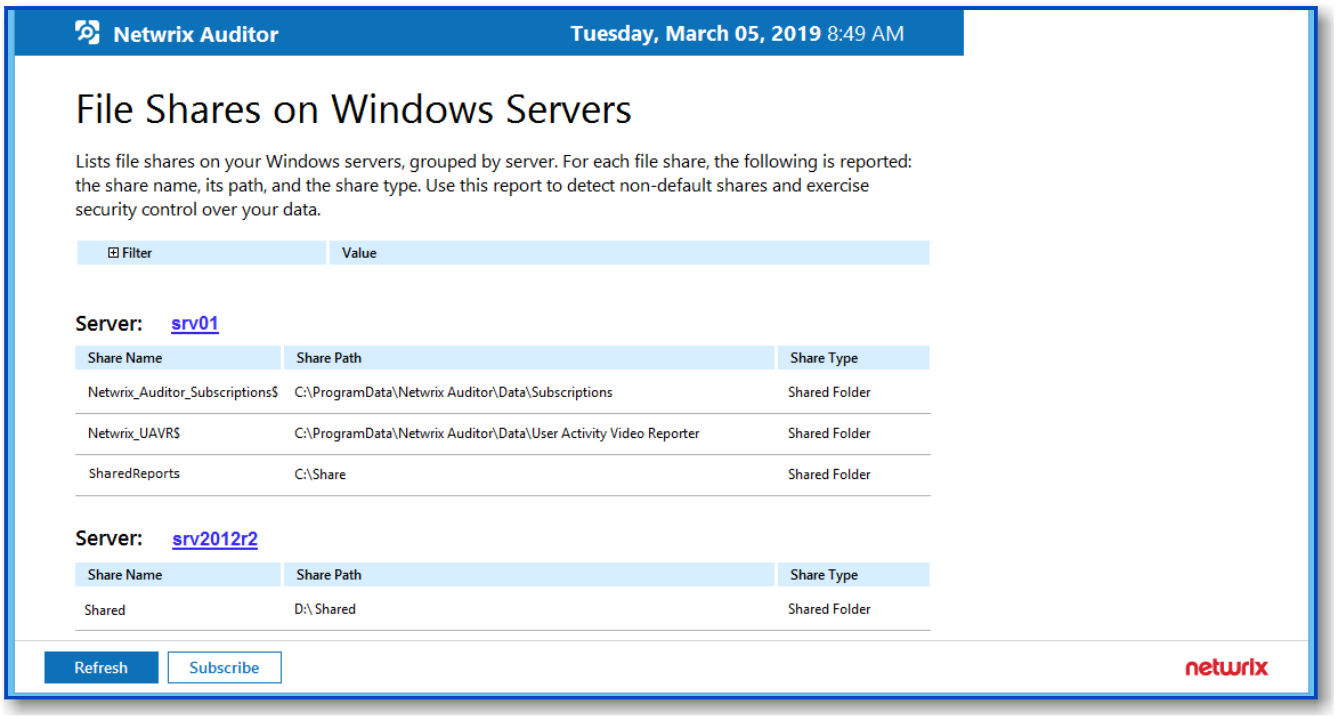
- SharePoint Online
- SQL Server
- Group Policy
- VMware

NOTE: The State-in-Time Functionality is not available for SQL Server Availability Groups.

To provide data for state-in-time reports, remember to select the **Collect data for state-in-time reports** option when you configure a monitoring plan for the selected data source. See the Settings for Data Collection topic for additional information.

The state-in-time reports are available under the Reports node. Depending on the data source, navigate to the corresponding subfolder, for example, **Predefined** → **Active Directory** →**Active Directory — State-in-Time**.

In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the Monitoring Plans section.



Each report has a set of filters which help organize audit data in the most convenient way. See the View Reports topic for additional information. You can also create a subscription to any report you want to receive on a regular basis. See the Subscriptions topic for additional information.

By default, state-in-time reports reflect the current state of the data source. If you want to generate a report to assess your system at a particular moment in the past, you can select the corresponding snapshot from the Snapshot Date filter.

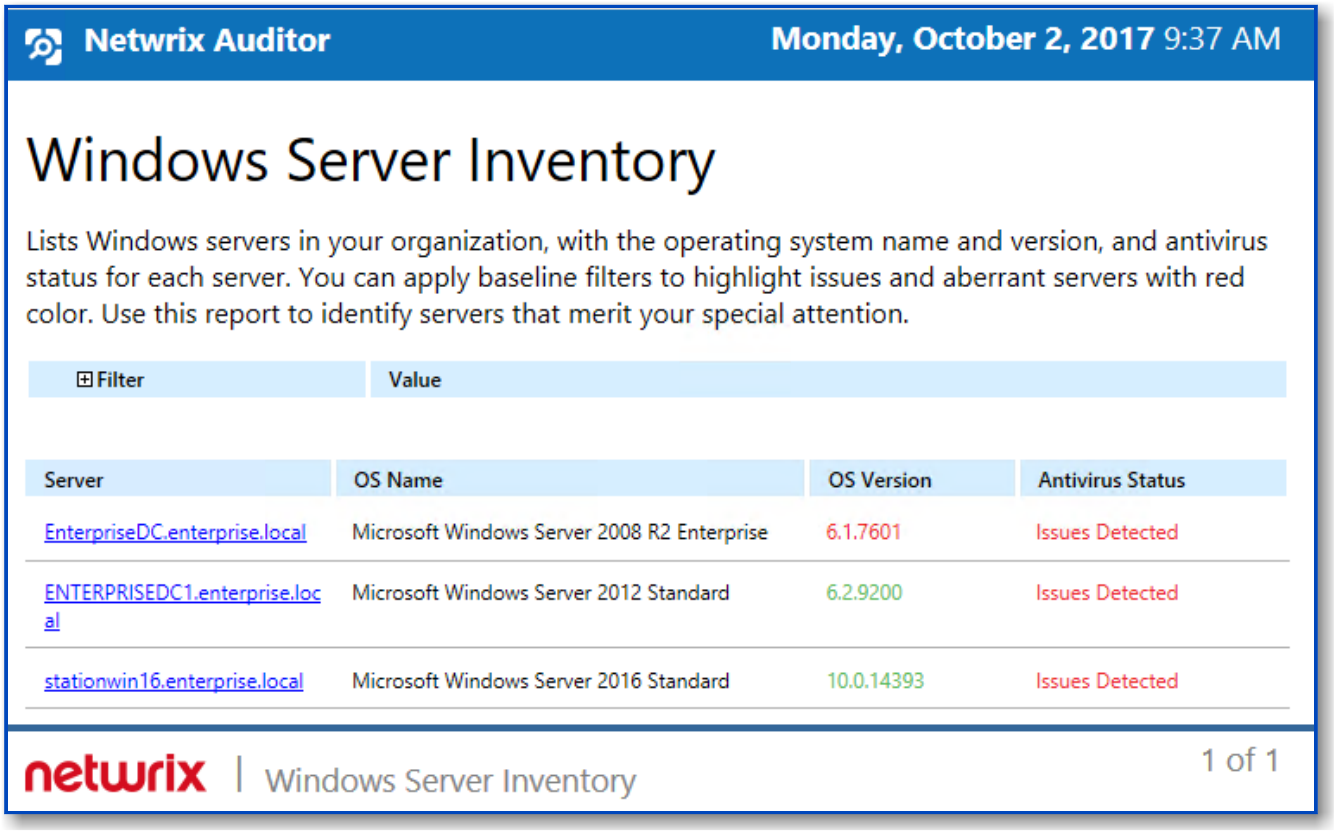
To be able to generate reports based on different snapshots, ask your Auditor Global administrator to import historical snapshots to the Audit Database, otherwise only the Current Session option is available in the drop-down list.

NOTE: Importing historical snapshots is not available for Office 365.

When auditing file servers, changes to both access and audit permissions are tracked. To exclude information on access permissions, contact your Auditor Global administrator or Configurator of this plan.

Baseline Reports

Most reports in Windows Server—State-in-Time folder allow you to specify baselines. A *baseline* defines a certain safe level or state. If a server parameter falls below it, it is a considered a threat or at least merits your special attention. With baselines specified right in report filters, you can easily identify servers that are different from your corporate policies or best practices. Risks are marked with red color and are easy to spot in the report.



You can specify baseline values specific to your organization in one of the following ways:

- As a baseline filter value in the report filters. Baselines in the field should be separated by commas.

  While inputting text inline is easy, your baseline values will not be preserved for the next report generation. You will have to input them every time you generate a report. This method is recommended you plan to subscribe to this report.

- In a special file stored on the computer where your Audit Database resides.

  To secure your baseline values for the next report runs, create a text file with baselines; baselines in this file should on a separate line. In the report, provide a link to this file inside the baseline filter. You should create a separate file for each baseline. In this case, the baselines will be reused every time you run the report.

  Make sure the account running your SQL Server instance service with Audit Database has permissions to access the baseline file. Otherwise, Netwrix Auditor will not be able to process them.

Active Directory State-In-Time Reports

Examine the Active Directory state-in-time data on the user account attributes:

- User Accounts - Attributes

To instruct Netwrix Auditor to collect data needed for the report, make sure that **Collect data for state-in-time reports** option is selected in the corresponding monitoring plan properties. See Settings for Data Collection.

User Accounts - Attributes

This report shows specific AD attributes for the accounts that meet the specified filtering criteria. Use this report to discover user accounts with settings that violate company policies or applicable compliance standards.

Supported object types and attributes are listed in the Active Directory section.

For this report to function properly, you must enable the **Collect data for state-in-time reports** option for the data source in the monitoring plan settings. See Create a New Monitoring Plan

Tips to Work with Report

1. Set desired filters in the report header. Filters
2. Select as many Accounts details to show as needed. Selected details are shown in the table view for each account that comply filtering criteria.
3. Filter on Sort by to bring important accounts' data to front.
4. Add filters by specific attribute values to narrow your report scope. In this case, the report shows only accounts that contains these values. Reported Attributes
5. The report is limited by 2000 records. To view all, create subscription to the report. The subscription (email attachment or file uploaded to a file share) will contain complete data.
6. If you have more than 2000 entities within the report scope, sorting might work incorrectly. Apply filters to narrow your report scope.

Please consider that if you are going to export the report in .csv format or want to subscribe to the .csv report, the file will contain the full list of available attributes regardless of which filters you specified. Unseleted attributes have no values.

Filters

You can narrow your reporting scope using multiple filters. Review the full list of available filters and values:

- **Monitoring plan** — name of the monitoring plan set to collect data from the AD domain you need.
- Item — name of the item within your monitoring plan.
- Account details to show — set of AD attributes to display in the report for each account.
- Sort by — list of available sorting parameters.
- Attribute/Value — list of available AD attributes with the ability to provide specific value. Review the full list here: Reported Attributes

Reported Data

For the account(s) you selected using filters, the summary section includes:

- **Total account count** — total number of accounts that meet selected filtering criteria.

- **Enabled accounts** —total number of enabled accounts that meet selected filtering criteria.
- **Disabled accounts** —total number of disabled accounts that meet selected filtering criteria.

Reported Attributes

The following account attributes are reported:

Attribute	Description	Possible values	Filtering
Account			
Account enabled	Shows whether an account enabled or not.	Yes No	+
Account locked	Shows whether an account locked or not.	Yes No	+
Canonical name	Equals the Canonical-Name attribute. See the corresponding Microsoft article for more information: Canonical-Name attribute.	Example: *USRegion.OrgName.com/Finance/JDoe*	+
Display name	Equals the Display-Name attribute. See the corresponding Microsoft article for more information: Display-Name attribute.	Example: *John Smith*	+
Logon name (sAMAccountName)	Equals the sAMAccountName attribute. See the corresponding Microsoft article for more information: sAMAccountName.	Example: *JSmith*	+
Logon name (UPN)	Equals the userPrincipalName attribute. See the corresponding Microsoft article for more information: User-Principal-Name attribute.	Example: *JSmith@domain.com*	+
Parent OU/container	Shows the path to account's parent object (OU or container)	Example:	+

Attribute	Description	Possible values	Filtering
		test.corp.local/ UserAccounts/user with all properties	
Member of	Shows direct AD group membership for the account. The report is limited to 10 groups. To view all groups the account is member of, export the report to .CSV file.	Example: *Domain Admins, Backup Operators* Clicking the Expand group membership link opens a detailed report on the user's effective group membership.	+
Employee details			
First name	Shows the first name.	Example: *John*	+
Last name	Shows the last name.	Example: *Smith*	+
Job title	Equals the Title attribute. See the corresponding Microsoft article for more information: Title attribute (AD Schema).	Example: *Manager*	+
Department	Shows the name for the department in which the user works.	Example: *Sales*	+
Telephone number	Equals the Telephone-Number attribute. See the corresponding Microsoft article for more information: Telephone-Number attribute.	Example: *949-555-1234*	+
Email address	Equals the E-mail-Addresses attribute. See	Email address	+

Attribute	Description	Possible values	Filtering
	the corresponding Microsoft article for more information: E-mail-Addresses attribute.	*Example: JSmith@domain.com*	
Manager	Shows manager specified for the account.	Display name (default) If empty, the report shows common name.	+
Manager email address	Equals the manager / mail attribute.	Email address *Example: JSmith@domain.com*	+
Office	Equals the Physical-Delivery-Office-Name attribute. See the corresponding Microsoft article for more information: Physical-Delivery-Office-Name attribute.	Example: *London Office*	+
Company	Equals the Company attribute. See the corresponding Microsoft article for more information: Company attribute.	Example: *Corporation*	+
Street address	Shows address based on the Street-Address and postOfficeBox attributes.	Example: *The Main Road; 10*	+
City	Shows the locality, such as the town or city, in the user's address.	Example: *NewLondon*	+
State/province	Equals the State-Or-Province-Name attribute. See the corresponding Microsoft article for more	Example: *New York*	+

Attribute	Description	Possible values	Filtering
	information: State-Or-Province-Name attribute.		
ZIP/postal code	Equals the Postal-Code attribute. See the corresponding Microsoft article for more information: Postal-Code attribute.	Example: *61441*	+
Country/region	Shows the country/region in which the user is located.	Example: *Ireland*	+
Security			
Account cannot be delegated	Shows whether the account can be delegated or not based on the User-Account-Control attribute. See the corresponding Microsoft article for more information: User-Account-Control attribute.	Yes No	+
Account expiration date	Equals the Account-Expires attribute. See the corresponding Microsoft article for more information: Account-Expires attribute.	Date	–
Password age	Shows password age for the account based on the Pwd-Last-Set attribute. See the corresponding Microsoft article for more information: Pwd-Last-Set attribute.	Number of days N/A — if password never set When the filter applied, the report shows above or equal results	+
Password expired	Shows whether the account has the "*Password expired*" flag set under the AccountControl attribute.	Yes No	+

Attribute	Description	Possible values	Filtering
Password last changed	Equals the Pwd-Last-Set attribute. See the corresponding Microsoft article for more information: Pwd-Last-Set attribute.	Date	–
		Never – if password never set	+
Password never expires	Shows whether the account has the "*Password never expires*" flag set on the Account tab in properties.	Yes No	+
Password not required	Shows whether the account has the "*Password not required*" flag set under the AccountControl attribute. Such account may have empty password.	Yes No	+
User cannot change password	Shows whether the account has the "*User cannot change password*" flag set on the Account tab in properties.	Yes No	+
User must change password	Shows whether the account has the "*User must change password*" flag set on the Account tab in properties.	Yes No	+
Other			
Creation date	Shows account creation date.	Date	–
Days inactive	Shows the number of days the account is considered to be inactive.	Days When the filter applied, the report shows above or equal results	+
Description	Contains account description if provided.	Example: *Sales Manager*	+

Attribute	Description	Possible values	Filtering
Last logon	Shows the date of account's last logon.	Date Never A user's last logon time is updated only once every 9-14 days, so some data may be outdated.	-
Last modified	Equals the When-Changed attribute. See the corresponding Microsoft article for more information: When-Changed attribute.	Date The Last modified attribute is considered as last object's modification date and not appears immediately. So some data may be outdated.	–
Logon script path	Equals the Script-Path attribute. See the corresponding Microsoft article for more information: Script-Path attribute.	Example: *C:\Powershellscripts\old scripts\script.ps1*	+
Recipient type	Shows recipient type based on the msExchRecipientTypeDetails attribute.	Mail user User Mailbox	+
Working (logon) hours	Shows time interval based on the Logon-Hours attribute. See the corresponding Microsoft article for more information: Logon-Hours attribute.	Specified time interval (in hours).	–

Related Reports

Clicking an Account name link opens the Account Permissions in Active Directory report.

Clicking a Expand group membership link opens the Effective Group Membership report for this account.

Usage Example

An IT administrators wants to find all user accounts from the OU named *Finance* that are currently locked out and disabled with information about their managers to contact them in case of any questions. This OU is included in the monitoring plan named *Active Directory Monitoring*. They need to set report filters as follows:

- Monitoring plan: Active Directory Monitoring
- In the Account details to show filter, select Manager.
- Attribute 1: Parent OU/container - equals | Value: Domain.com/Finance
- Attribute 2: Account enabled | Value: No
- Attribute 3: Account locked | Value: Yes
- All other filter values can be left default.

A security manager wants to find administrators of the *corp.local* domain with incorrect password settings (password not required). Service accounts (*svc_%*) must be skipped in the report. This domain is included in the monitoring plan named *Active Directory Monitoring*. He or she needs to set report filters as follows:

- Monitoring plan: Active Directory Monitoring
- Item: corp.local
- In the Account details to show filter, select Member of, Password not required.
- Attribute 1: Member of - equals | Value: Domain Admins
- Attribute 2: Password not required| Value: Yes
- Attribute 3: Logon name (sAMAccountName) - not equal to | Value: svc_%
- All other filter values can be left default.

Microsoft Entra ID State-In-Time Reports

To instruct Netwrix Auditor to collect data needed for the report, make sure that **Collect data for state-in-time reports** option is selected in the corresponding monitoring plan properties. See Create a New Monitoring Plan.

User Accounts - Attributes

The report shows specific AD attributes for the Microsoft Entra ID (formerly Azure AD) accounts that meet the specified filtering criteria. Use this report to discover Microsoft Entra ID accounts with settings that violate company policies or applicable compliance standards.

For this report to function properly, you must enable the **Collect data for state-in-time reports** option for the data source in the monitoring plan settings. See the Settings for Data Collection topic for more information.

Tips to Work with Report

1. Set desired filters in the report header. See the Filters topic for more information.
2. Select as many Accounts details to show as needed. Selected details are shown in the table view for each account that comply filtering criteria.
3. Filter on Sort by to bring important accounts' data to front.
4. Add filters by specific attribute values to narrow your report scope. In this case, the report shows only accounts that contains these values. See the Reported Attributes topic for more information.
5. The report is limited by 2000 records. To view all, create subscription to the report. The subscription (email attachment or file uploaded to a file share) will contain complete data.
6. If you have more than 2000 entities within the report scope, sorting might work incorrectly. Apply filters to narrow your report scope.

Filters

You can narrow your reporting scope using multiple filters. Review the full list of available filters and values:

- **Monitoring plan** — name of the monitoring plan set to collect data from the AD domain you need.
- Time zone — select you time zone.
- Item — name of the item within your monitoring plan.
- Sort by — list of available sorting parameters.
- Account enabled — select whether you want to see disabled accounts or not.
- Department — provide the name of the department if needed.
- Attribute/Value — list of available AD attributes with the ability to provide specific value.

Reported Data

For the account(s) you selected using filters, the summary section includes:

- **Total account count** — total number of accounts that meet selected filtering criteria.
- **Enabled accounts** —total number of enabled accounts that meet selected filtering criteria.
- **Disabled accounts** —total number of disabled accounts that meet selected filtering criteria.

Reported Attributes

The following account attributes are reported:

Attribute (display name in report)	Microsoft Entra ID attribute mapping	Possible values	Description
Account enabled	accountEnabled	Yes/No	Specifies, whether the user account is enabled or disabled: the "true" value indicates that the account is enabled.
Change password on next sign in	passwordProfile	Yes/No	Specifies the password profile for a user. The password in the profile must satisfy the minimum requirements as specified by the passwordPolicies property. By default, a strong password is required.
Change password on next sign in with MFA	passwordProfile	Yes/No	Specifies the password profile for the user. The password in the profile must satisfy the minimum requirements as specified by the passwordPolicies property. By default, a strong password is required.
City	city	Example: "*London*"	The city where a user is located. Maximum length 128.

Attribute (display name in report)	Microsoft Entra ID attribute mapping	Possible values	Description
Cloud-only	onPremisesSyncEnabled	Yes/No	true if this object is synced from any on- premises directory; false if this object was originally synced from any on-premises directory but is no longer synced; null if this object has never been synced from any on-premises directory (default).
Country	country	Example: "*US*"	The country/region in which the user is located. Example: "US" or "UK". Maximum length 128.
Creation date	createdDateTime	1/21/2021 4:08:00 PM	The created date of the user object.
Department	department	Example: "*Accounting and Finance*"	The name for the department in which the user works. Maximum length is 64 characters.
Display name	displayName	Example: "*John Smith*"	The name displayed in the address book for the user. This is usually the combination of the user's first name, middle initial and last name. This property is required when a user is created and it cannot be cleared during updates. Maximum length is 256 characters.
First name	givenName	Example: "*John*"	The given name (first name) of the user. Maximum length is 64 characters.
Is licensed	–	–	–
Last DirSync time	onPremisesLastSyncDateTime	Example: *3/20/2021 2:13:00 PM*	M Indicates the last time at which the object was synchronized with the on-premises directory; for example: "2013- 02-16T03:04:54Z". The

Attribute (display name in report)	Microsoft Entra ID attribute mapping	Possible values	Description
			Timestamp type represents date and time information using ISO 8601 format and is always in UTC time.
Last name	surname	Example: "*Smith*"	The user's surname (family name or last name). Maximum length is 64 characters.
Licenses	–	Example: *OFFICE 365 E1*	–
Manager	manager	Example: "*JamesWilliams*"	The user or contact that is this user's manager.
Manager email	–	Example: *JWilliams@gmail.com*	–
Office	physicalDeliveryOfficeName (officeLocation)	Example: *1068*	The office location in the user's place of business. Maximum length is 128 characters.
Password last change	lastPasswordChangeDateTime	Example: *4/6/2021 6:17:00 PM*	The time when this Microsoft Entra ID Plans user last changed their password. The date and time information uses ISO 8601 format and is always in UTC time.
Password never expires	passwordPolicies	Yes/No	Specifies password policies for the user. This value is an enumeration with one possible value being “DisableStrongPassword”, which allows weaker passwords than the default policy to be specified. “DisablePasswordExpiration” can also be specified. The two may be specified together; for example: "DisablePasswordExpiration, DisableStrongPassword".

Attribute (display name in report)	Microsoft Entra ID attribute mapping	Possible values	Description
Phone number	businessPhones	Example: *+1-202-555-155*	The telephone numbers for the user. Although this is a string collection, only one number can be set for this property.
Role membership	–	Example: "*Exchange Service Administrator, Company Administrator*"	–
Sign in names	identities	*Example: "user_company.com#EXT#@office.onmicrosoft.com"*	Represents the identities that can be used to sign into this user account. An identity can be provided by Microsoft (also known as a local account), by organizations, or by social identity providers such as Facebook, Google, and Microsoft, and tied to a user account. May contain multiple items with the same signInType value. https://docs.microsoft.com/en-us/graph/api/resources/objectid entity?view=graph-rest-1.0
Strong password required	passwordPolicies	Yes/No	Specifies password policies for the user. This value is an enumeration with one possible value being “DisableStrongPassword”, which allows weaker passwords than the default policy to be specified. “DisablePasswordExpiration” can also be specified. The two may be specified together; for example:

Attribute (display name in report)	Microsoft Entra ID attribute mapping	Possible values	Description
			"DisablePasswordExpiration, DisableStrongPassword".
Title	jobTitle	Example: "*Business development manager*"	The user's job title. Max length is 128.
User principal name	userPrincipalName	Example: "*user_company.com#EXT#@officenwxqc.onmicrosoft.com*"	The user principal name (UPN) of wxq the user. The UPN is an Internet- style login name for the user based on the Internet standard RFC 822. By convention, this should map to the user's email name. The general format is alias@domain, where the domain must be present in the tenant's collection of verified domains. This property is required when a user is created. The verified domains for the tenant can be accessed from the verifiedDomains property of organization. NOTE: While this property can contain accent characters, they can cause access issues to first-party applications for the user.
User type	userType	Example: "*Member*"	A string value that can be used to classify user types in your directory, such as "Member" and "Guest".

File Servers State-In-Time Reports

This section contains limitations and considerations for File Server State-in-Time reports generation.

Limitations

1. For the following File Server State-in-Time reports wildcard *%* is not supported for the "*Object Path*" field:
    - Account permissions
    - Duplicate files
    - Empty folders
    - Excessive Access Permissions
    - Excessive Access Permissions with Account Details
    - Files and Folders by Owner
    - Folder and File Permission Details
    - Folder and File Permissions with Account Details
    - Folder Permissions
    - Folder Permissions with Account Details
    - Folder Summary Report
    - Largest Files
    - Potential Data Owners by Folder
    - Stale Data by Folder
    - Top Owners by Total File Size
2. For the Folder TreeView State-in-Time report, the wildcard *%* is supported.

SQL Server State-In-Time Reports

These are reports on the SQL Server state-in-time data, including roles, permissions and other configuration settings:

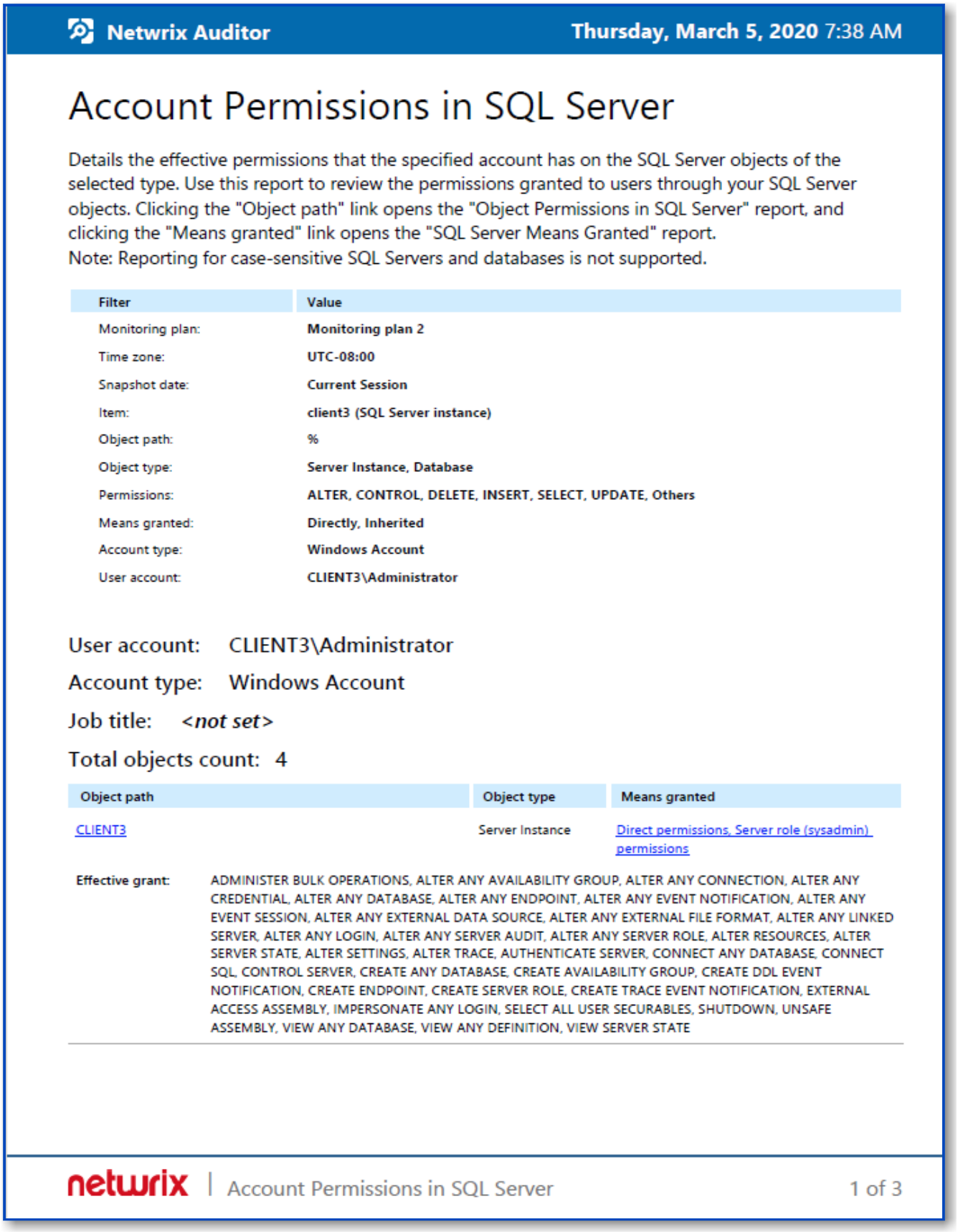
- Account Permissions in SQL Server

- Object Permissions in SQL Server
- SQL Server Databases
- SQL Server Means Granted
- SQL Server-Level Roles

To instruct Netwrix Auditor to collect data needed for these reports, make sure that **Collect data for state-in-time reports** option is selected in the corresponding monitoring plan properties. See the Settings for Data Collection topic for additional information. By default, data collection will run daily at 4 AM.

Account Permissions in SQL Server

Details the effective permissions that the specified account has on the SQL Server objects of the selected type. Use this report to review the permissions granted to users through your SQL Server objects.



Netwrix Auditor Thursday, March 5, 2020 7:38 AM

Account Permissions in SQL Server

Details the effective permissions that the specified account has on the SQL Server objects of the selected type. Use this report to review the permissions granted to users through your SQL Server objects. Clicking the "Object path" link opens the "Object Permissions in SQL Server" report, and clicking the "Means granted" link opens the "SQL Server Means Granted" report.
Note: Reporting for case-sensitive SQL Servers and databases is not supported.

Filter	Value
Monitoring plan:	**Monitoring plan 2**
Time zone:	**UTC-08:00**
Snapshot date:	**Current Session**
Item:	**client3 (SQL Server instance)**
Object path:	**%**
Object type:	**Server Instance, Database**
Permissions:	**ALTER, CONTROL, DELETE, INSERT, SELECT, UPDATE, Others**
Means granted:	**Directly, Inherited**
Account type:	**Windows Account**
User account:	**CLIENT3\Administrator**

User account: CLIENT3\Administrator

Account type: Windows Account

Job title: *<not set>*

Total objects count: 4

Object path	Object type	Means granted
CLIENT3	Server Instance	Direct permissions, Server role (sysadmin) permissions

Effective grant: ADMINISTER BULK OPERATIONS, ALTER ANY AVAILABILITY GROUP, ALTER ANY CONNECTION, ALTER ANY CREDENTIAL, ALTER ANY DATABASE, ALTER ANY ENDPOINT, ALTER ANY EVENT NOTIFICATION, ALTER ANY EVENT SESSION, ALTER ANY EXTERNAL DATA SOURCE, ALTER ANY EXTERNAL FILE FORMAT, ALTER ANY LINKED SERVER, ALTER ANY LOGIN, ALTER ANY SERVER AUDIT, ALTER ANY SERVER ROLE, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS, ALTER TRACE, AUTHENTICATE SERVER, CONNECT ANY DATABASE, CONNECT SQL, CONTROL SERVER, CREATE ANY DATABASE, CREATE AVAILABILITY GROUP, CREATE DDL EVENT NOTIFICATION, CREATE ENDPOINT, CREATE SERVER ROLE, CREATE TRACE EVENT NOTIFICATION, EXTERNAL ACCESS ASSEMBLY, IMPERSONATE ANY LOGIN, SELECT ALL USER SECURABLES, SHUTDOWN, UNSAFE ASSEMBLY, VIEW ANY DATABASE, VIEW ANY DEFINITION, VIEW SERVER STATE

netwrix | Account Permissions in SQL Server 1 of 3

Reported data

The report has a summary section with general information on the selected account, and the details section presented in the table format.

The summary section shows:

- **User account**— name or SID of the account
- **Account type** —possible values:
  - Windows Account
  - Login SQL Authentication
  - DB SQL User with password
- **Job title** —reported for Active Directory users as set in their corresponding attribute. If not set, <*not set*> is reported.
- **Total objects count** — total number of objects that this account has access to.

The detailed information under summary includes:

- **Object path** — monitored object path as formatted by Netwrix Auditor in the activity records (see '*What*' field in the reports, search results and activity summaries). For example, if reporting on the database hosted on selected SQL Server, the path will be as follows: *Databases\database_name*.
- **Object type** — monitored object type; for the full list of supported object types, refer to SQL Server topic.
- **Means granted** —how access permissions were granted to this account, e.g., *Direct permissions* or *Server role permissions*.

- **Effective grant** —the effective set of permissions granted to this account on the selected object.

Filters

This report has the following filters:

- **Monitoring plan** — name of the monitoring plan set to collect data from the SQL Server you need.
- **Time zone** — time zone where Netwrix Auditor server is located, for example, UTC-08:00. This value is filled in automatically.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current*

Session). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in SQL Server
- **Item**— name of the SQL Server instance monitored with selected monitoring plan.
- **Object path** — path to the monitored object, as formatted by Netwrix Auditor in the activity records (see '*What*' field in the reports, search results and activity summaries). Wildcard (*) is supported. For example, to report on the database hosted on selected SQL Server, specify the path as follows: *Databases\database_name*.
- **Object type**— type of the monitored object that provided data for this report. Possible values: *Database*, *Server Instance*.
- **Permissions** —access permissions whose assignment you want to be reported for selected account.
- **Means granted** —how access permissions were granted to this account. You can select *Directly*, *Inherited*, or both (default setting).
- **Account type** —possible values: *Windows Account*, *Login SQL Authentication*, *DB SQL User with password*.
- **User account**—name or SID of the account whose permission assignments are reported.

Considerations and limitations

- Reporting for case-sensitive SQL Servers and databases is not supported.
- Permissions for INFORMATION_SCHEMA granted via *master db* will not be reported.
- The report will not show the RESTORE capability for the database owner.
- When calculating effective rights and permissions, the following will not be considered:
  - Ownership chaining
  - Cross DB ownership chaining
  - Trustworthy database
  - SQL Server agent fixed database roles

Related reports

- Clicking a Object permissions link opens the Object Permissions in SQL Server report.
- Clicking a Means granted link opens the **SQL Server Means Granted** report.

Usage example

Database administrators in the *Corp* organization need to discover what kind of permissions a certain user has on the **SQLSrv01\SQLServer2016** instance. This instance is included in the monitoring plan named *SQL Servers Monitoring*.

To examine the relevant data, they generated the **Account Permissions in SQL Server** report with the filters set as follows:

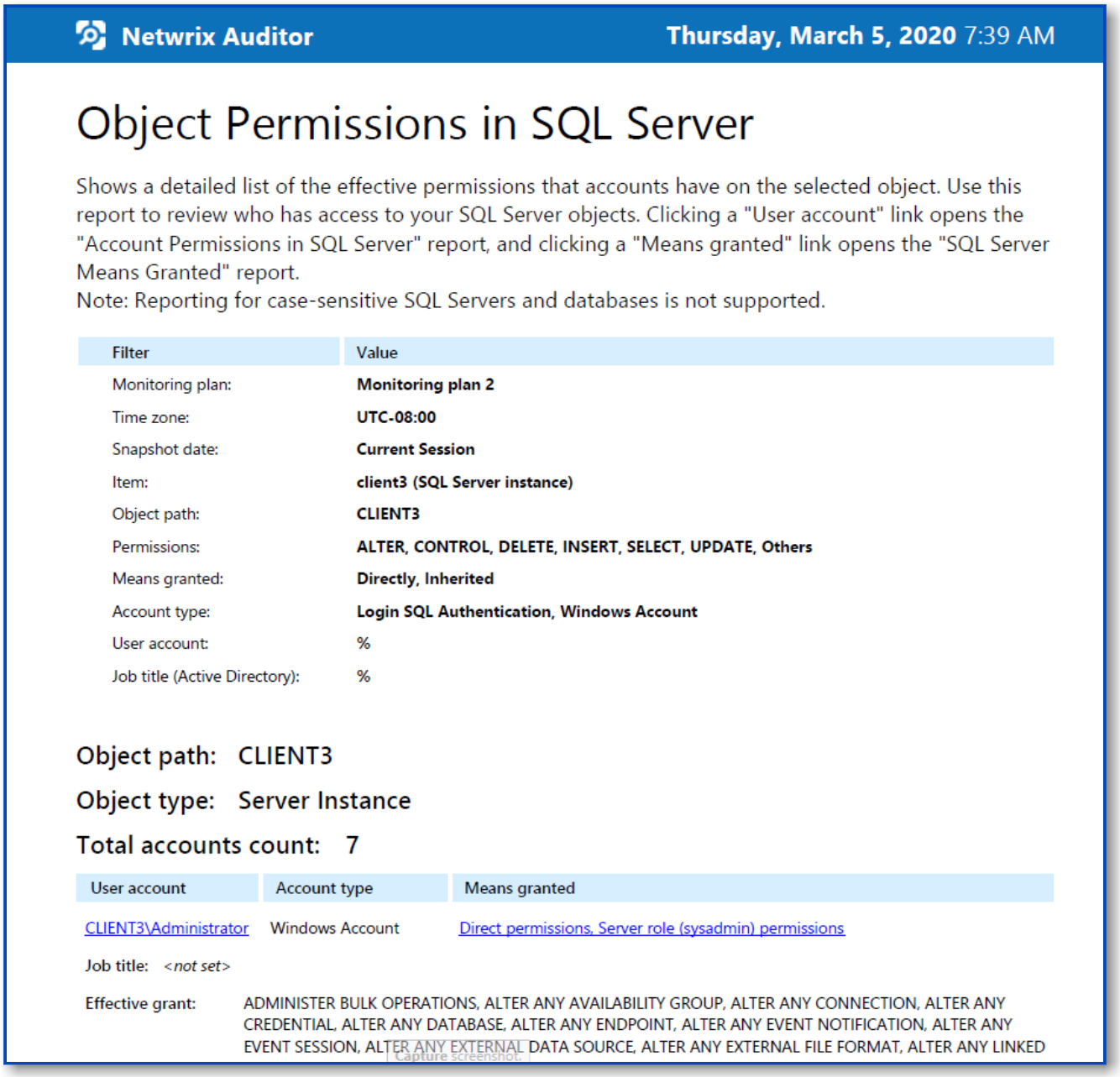
- **Monitoring plan:***SQL Servers Monitoring*
- **Snapshot date:***Current Session*
- **Item:***SQLSrv01\SQLServer2016*
- **User account:** *Corp\Ian.Harris*

The report revealed that this user has access permissions for the master database. To discover how they were granted, click the link in the **Means granted** field.

Object Permissions in SQL Server

This report shows a detailed list of the effective permissions that accounts have on the selected object. Use this report to review who has access to your SQL Server objects.

Supported object types and attributes are listed in the SQL Server section.



Netwrix Auditor Thursday, March 5, 2020 7:39 AM

Object Permissions in SQL Server

Shows a detailed list of the effective permissions that accounts have on the selected object. Use this report to review who has access to your SQL Server objects. Clicking a "User account" link opens the "Account Permissions in SQL Server" report, and clicking a "Means granted" link opens the "SQL Server Means Granted" report.
Note: Reporting for case-sensitive SQL Servers and databases is not supported.

Filter	Value
Monitoring plan:	**Monitoring plan 2**
Time zone:	**UTC-08:00**
Snapshot date:	**Current Session**
Item:	**client3 (SQL Server instance)**
Object path:	**CLIENT3**
Permissions:	**ALTER, CONTROL, DELETE, INSERT, SELECT, UPDATE, Others**
Means granted:	**Directly, Inherited**
Account type:	**Login SQL Authentication, Windows Account**
User account:	%
Job title (Active Directory):	%

Object path: CLIENT3

Object type: Server Instance

Total accounts count: 7

User account	Account type	Means granted
CLIENT3\Administrator	Windows Account	Direct permissions, Server role (sysadmin) permissions

Job title: *<not set>*

Effective grant: ADMINISTER BULK OPERATIONS, ALTER ANY AVAILABILITY GROUP, ALTER ANY CONNECTION, ALTER ANY CREDENTIAL, ALTER ANY DATABASE, ALTER ANY ENDPOINT, ALTER ANY EVENT NOTIFICATION, ALTER ANY EVENT SESSION, ALTER ANY EXTERNAL DATA SOURCE, ALTER ANY EXTERNAL FILE FORMAT, ALTER ANY LINKED

Reported data

The report has a summary section with general information on the selected SQL Server object, and the details section presented in the table format.

The summary section shows:

- **Object path** — monitored object path as formatted by Netwrix Auditor in the activity records (see '*What*' field in the reports, search results and activity summaries). For example, if reporting on the database hosted on selected SQL Server, the path will be as follows: *Databases\database_name*.
- **Object type** — monitored object type; for the full list of supported object types, refer to SQL Server topic.
- **Total account count** — total number of accounts that have access to this object.

The detailed information under summary includes:

- **User account** —name or SID of the account that has permissions on the selected object.
- **Account type** —possible values:
  - Windows Account
  - Login SQL Authentication
  - DB SQL User with password
- **Means granted** —how access permissions were granted to this account, e.g., *Direct permissions* or *Server role permissions*.
- **Job title** —reported for Active Directory users as set in their corresponding attribute. If not set, <*not set*> is reported.
- **Effective grant** —the effective set of permissions granted to this account on the selected object.

Covering rules do not need to be applied, since **Effective grant** permissions are reported automatically using these rules.

Filters

This report has the following filters:

- **Monitoring plan** — name of the monitoring plan set to collect data from the SQL Server you need.
- **Time zone** — time zone where Netwrix Auditor server is located, for example, UTC-08:00. This value is filled in automatically.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current Session*). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in the SQL Server topic.
- **Item**—name of the SQL Server instance monitored with selected monitoring plan.
- **Object path** —path to the monitored object, as formatted by Netwrix Auditor in the activity records (see '*What*' field in the reports, search results and activity summaries). Wildcard (*) is supported. For example, to report on the database hosted on selected SQL Server, specify the path as follows: *Databases\database_name*.
- **Permissions** —access permissions which assignment you want to be reported for the selected object.

- **Means granted** —how access permissions were granted to this account. You can select *Directly*, *Inherited*, or both (default setting).
- **User account**—name or SID of the account that has permissions on the selected object. Default is *%* (all accounts).
- **Account type** —possible values: *Windows Account*, *Login SQL Authentication*, *DB SQL User with password*.
- **Job title (Active Directory)** —reported for Active Directory users as set in their corresponding attribute. Default is *%* (any title).

Considerations and limitations

- Reporting for case-sensitive SQL Servers and databases is not supported.
- The report will not show the RESTORE capability for the database owner.
- When calculating effective rights and permissions, the following will not be considered:
  - Ownership chaining
  - Cross DB ownership chaining
  - Trustworthy database
  - SQL Server agent fixed database roles
- Some permissions may not be reported correctly due to the known issues. See Release Notes for details.

Related reports

- Clicking a User account link opens the Account Permissions in SQL Server report.
- Clicking a Means granted link opens theSQL Server Means Granted report.

Usage example

Database administrators need to discover who currently has access permissions to **FinReports** database stored on the **SQLSrv01\SQLServer2016** instance. This instance is included in the monitoring plan named *SQL Servers Monitoring*.

To examine the relevant data, they need to generate **Object Permissions in SQL Server** report with the filters set as follows:

- **Monitoring plan:** *SQL Servers Monitoring*
- **Snapshot date:** *Current Session*
- **Item:** *SQLSrv01\SQLServer2016*
- **Object path:** *Databases\FinReports*

All other filter values can be left default.

SQL Server Databases

This report lists the properties of databases and database snapshots hosted on the selected SQL Server instance. Use this report for your SQL Server database inventory.

Netwrix Auditor Thursday, March 5, 2020 7:41 AM

SQL Server Databases

Lists all databases and database snapshots for the selected SQL Server instance. The details for each database include its name, restrict access mode, state, size, shrink status, encryption status, last full backup date, data file path and log file path. All database snapshots include the database snapshot name, source database name, restrict access status and state. Use this report for SQL Server database inventory.
Note: Reporting for case-sensitive SQL Servers and databases is not supported.

Filter	Value
Monitoring plan:	**Monitoring plan 2**
Time zone:	**UTC-08:00**
Snapshot date:	**Current Session**
Item:	**client3 (SQL Server instance)**
Database name:	%

Database name	Restrict access	State	Size (MB)	Shrink enabled	Encryption	Last full backup date
master	MULTI_USER	ONLINE	6.00	No	No	None
Data file path:	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\master.mdf					
Log file path:	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\mastlog.ldf					

Database name	Restrict access	State	Size (MB)	Shrink enabled	Encryption	Last full backup date
ReportServer	MULTI_USER	ONLINE	15.31	No	No	None
Data file path:	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\ReportServer.mdf					
Log file path:	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\ReportServer_log.ldf					

Database name	Restrict access	State	Size (MB)	Shrink enabled	Encryption	Last full backup date
ReportServerTempDB	MULTI_USER	ONLINE	5.25	No	No	None
Data file path:	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\ReportServerTempDB.mdf					
Log file path:	C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\ReportServerTempDB_log.ldf					

netwrix | SQL Server Databases 1 of 1

Reported data

For each database, the following information is reported:

- **Database name**
- **Restrict access** mode— as set in the database properties **>Options>State**. Possible values are: *Multi_user* (for *Multiple*), *Restricted*, *Single*. See this Microsoft article for details.
- **State**— as set in the database properties**>Options>State**. See this Microsoft article for details
- **Size (MB)**
- **Shrink enabled**— as set in the database properties **>Options>Automatic>Auto Shrink**. See this Microsoft article for details.
- **Encryption status**— as set in the database properties **>Options>State**. See this Microsoft article for details.
- **Last full backup date**— local date and time for the audited SQL Server instance.

In some cases, the backup time will be displayed in server ticks.

- **Data file path**— .MDF file path.
- **Log file path**— .LDF file path.

For each database snapshot, the following information is reported:

- **Database snapshot name**
- **Source database name**
- **Restrict access** mode — as set in the database properties at snapshot creation time.
- **State** — as set in the database properties at snapshot creation time.

Filters

This report has the following filters:

- **Monitoring plan** — name of the monitoring plan set to collect data from the SQL Server instance hosting the required database.
- **Item** — name of the item within your monitoring plan, here — SQL Server instance.
- **Time zone** — time zone where Netwrix Auditor server is located, for example, UTC-08:00. This value is filled in automatically.
- **Database name** — database to report on. Default is all databases on selected SQL Server instance (*%*).

Considerations and recommendations

Reporting for case-sensitive SQL Servers and databases is not supported.

Usage example

Database administrators in the *Corp* organization need to perform an inventory of the **SQLSrv01\SQLServer2016** instance. This instance is included in the monitoring plan named *SQL Servers Monitoring*.

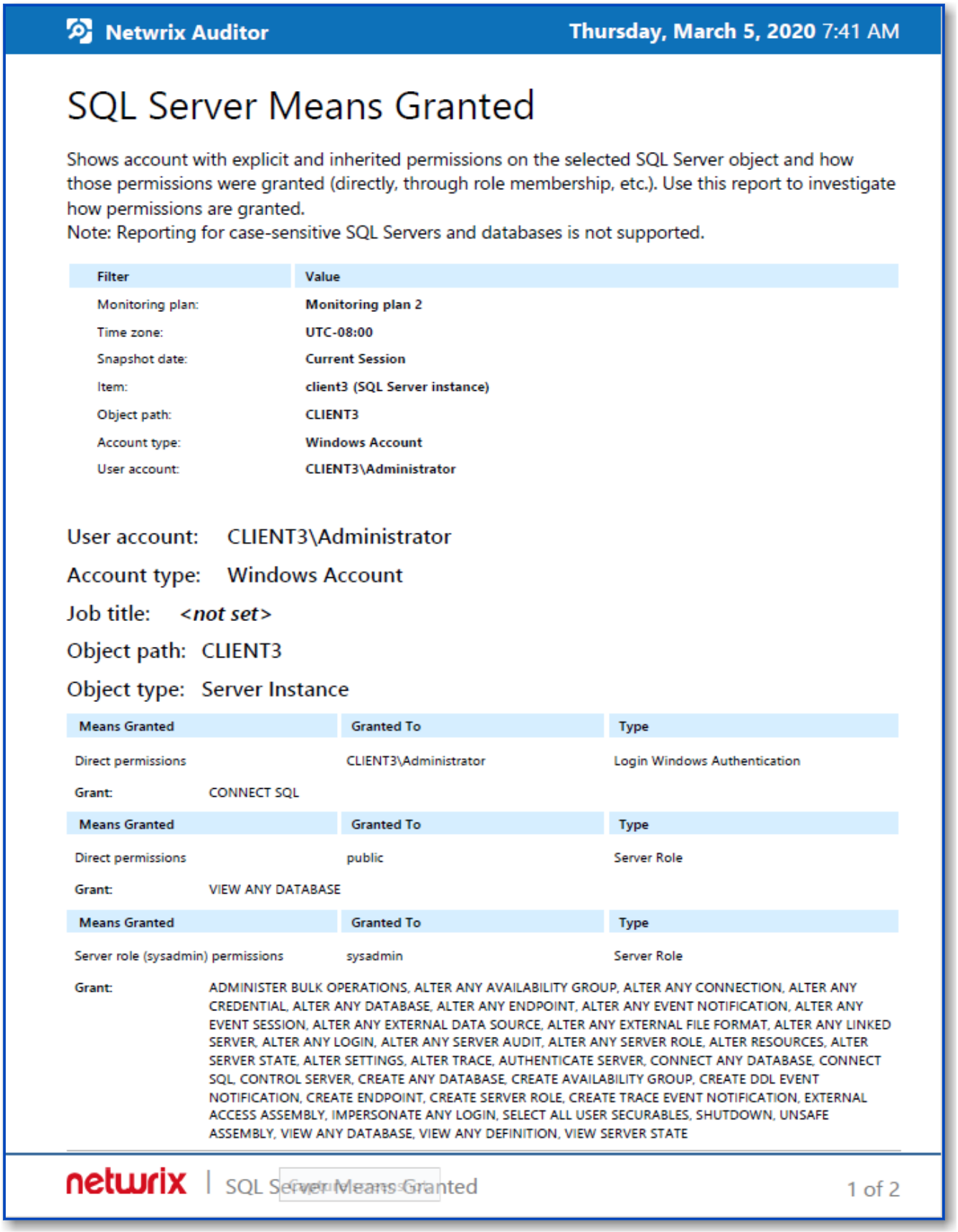
To examine the relevant data, they generated the **SQL Server Databases** report with the default filters.

SQL Server Means Granted

This report shows accounts with explicit and inherited permissions on the selected SQL Server object and how those permissions were granted (directly, through role membership, etc.). Use this report to investigate how permissions are granted.

Supported object types and attributes are listed in the SQL Server section.

To instruct Netwrix Auditor to collect data needed for this report, make sure that **Collect data for state-in-time reports** option is selected in the monitoring plan properties.



Netwrix Auditor Thursday, March 5, 2020 7:41 AM

SQL Server Means Granted

Shows account with explicit and inherited permissions on the selected SQL Server object and how those permissions were granted (directly, through role membership, etc.). Use this report to investigate how permissions are granted.
Note: Reporting for case-sensitive SQL Servers and databases is not supported.

Filter	Value
Monitoring plan:	**Monitoring plan 2**
Time zone:	**UTC-08:00**
Snapshot date:	**Current Session**
Item:	**client3 (SQL Server instance)**
Object path:	**CLIENT3**
Account type:	**Windows Account**
User account:	**CLIENT3\Administrator**

User account: CLIENT3\Administrator

Account type: Windows Account

Job title: *<not set>*

Object path: CLIENT3

Object type: Server Instance

Means Granted	Granted To	Type
Direct permissions	CLIENT3\Administrator	Login Windows Authentication
Grant: CONNECT SQL		

Means Granted	Granted To	Type
Direct permissions	public	Server Role
Grant: VIEW ANY DATABASE		

Means Granted	Granted To	Type
Server role (sysadmin) permissions	sysadmin	Server Role
Grant: ADMINISTER BULK OPERATIONS, ALTER ANY AVAILABILITY GROUP, ALTER ANY CONNECTION, ALTER ANY CREDENTIAL, ALTER ANY DATABASE, ALTER ANY ENDPOINT, ALTER ANY EVENT NOTIFICATION, ALTER ANY EVENT SESSION, ALTER ANY EXTERNAL DATA SOURCE, ALTER ANY EXTERNAL FILE FORMAT, ALTER ANY LINKED SERVER, ALTER ANY LOGIN, ALTER ANY SERVER AUDIT, ALTER ANY SERVER ROLE, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS, ALTER TRACE, AUTHENTICATE SERVER, CONNECT ANY DATABASE, CONNECT SQL, CONTROL SERVER, CREATE ANY DATABASE, CREATE AVAILABILITY GROUP, CREATE DDL EVENT NOTIFICATION, CREATE ENDPOINT, CREATE SERVER ROLE, CREATE TRACE EVENT NOTIFICATION, EXTERNAL ACCESS ASSEMBLY, IMPERSONATE ANY LOGIN, SELECT ALL USER SECURABLES, SHUTDOWN, UNSAFE ASSEMBLY, VIEW ANY DATABASE, VIEW ANY DEFINITION, VIEW SERVER STATE		

netwrix | SQL Server Means Granted 1 of 2

Reported data

The report has a summary section with general information on the selected SQL Server object, and the details section presented in the table format.

The summary section shows:

- **User account** — name or SID of the account that has permissions on the selected object.

- **Account type** —possible values:
  - Windows Account
  - Login SQL Authentication
  - DB SQL User with password
- **Job title** —reported for Active Directory users as set in their corresponding attribute. If not set, <*not set*> is reported.
- **Object path** —path to the monitored object, as formatted by Netwrix Auditor in the activity records (see '*What*' field in the reports, search results and activity summaries). For example, when reporting on the database hosted on selected SQL Server, the path will be as follows: *Databases\database_name*.
- **Object type** — monitored object type; for the full list of supported object types, refer to SQL Server.

The detailed information under summary includes:

- **Means granted** —how access permissions were granted to this account, e.g., *Direct permissions* or *Server role permissions*.
- **Granted to**— the security principal to which the access permissions were granted, e.g. *sysadmin*.
- **Type**— the security principal type, e.g. *Server role*.
- **Grant** —the set of permissions granted to this account on the selected object by all means.

Covering rules do not need to be applied, since **Grant** permissions are reported automatically using these rules.

Filters

This report has the following filters:

- **Monitoring plan** — name of the monitoring plan set to collect data from the SQL Server you need.

- **Time zone** — time zone where Netwrix Auditor server is located, for example, UTC-08:00. This value is filled in automatically.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current Session*). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in SQL Server.
- **Item**—name of the SQL Server instance monitored with selected monitoring plan.
- **Object path** —path to the monitored object, as formatted by Netwrix Auditor in the activity records (see '*What*' field in the reports, search results and activity summaries). Wildcard (*) is supported. For example, to report on the database hosted on selected SQL Server, specify the path as follows: *Databases\database_name*.
- **User account**—name or SID of the account that has permissions on the selected object. Default is *%* (all accounts).
- **Account type** —possible values: *Windows Account*, *Login SQL Authentication*, *DB SQL User with password*.

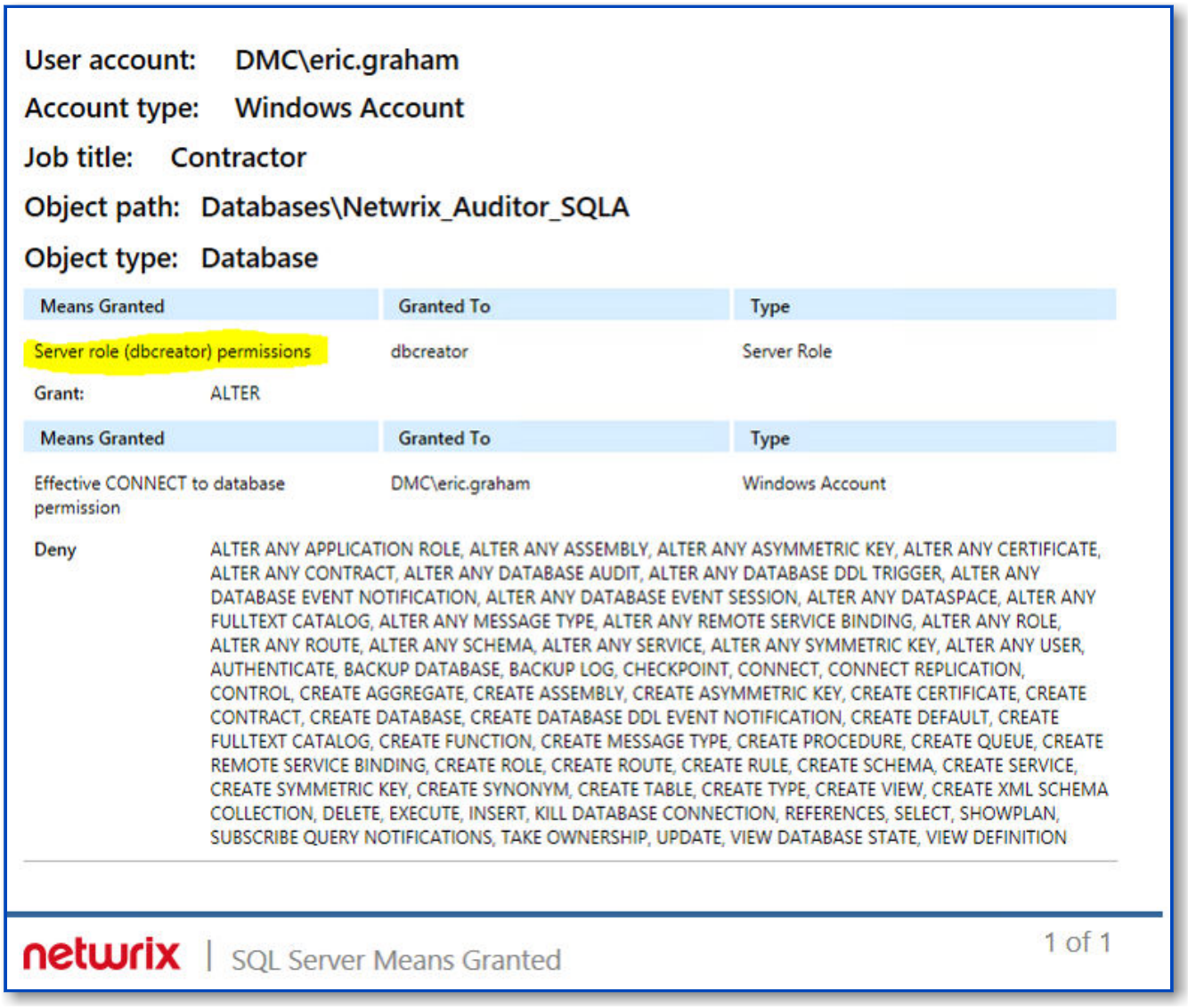
Considerations and limitations

- Reporting is not supported for the following objects:
  - Case-sensitive SQL Servers and databases
  - Read-only Filegroups
  - Contained databases.
- Permissions assigned using **With Grant option** are not reported (see this Microsoft article on that means).
- When calculating effective rights and permissions, the following will not be considered:
  - Ownership chaining
  - Cross DB ownership chaining
  - Trustworthy database
  - SQL Server agent fixed database roles

Usage example

When examining the **Object Permissions in SQL Server** report, database administrators in the *Corp* organization discovered that the accounts with Contractor job title has access to the

SQLSrv01\SQLServer2016 instance. To explore how this could happen, they drilled down to the **SQL Server Means Granted** report for that account by clicking the link in the **Means granted** field for that account.



User account: DMC\eric.graham
Account type: Windows Account
Job title: Contractor
Object path: Databases\Netwrix_Auditor_SQLA
Object type: Database

Means Granted	Granted To	Type
Server role (dbcreator) permissions	dbcreator	Server Role
Grant: ALTER		

Means Granted	Granted To	Type
Effective CONNECT to database permission	DMC\eric.graham	Windows Account
Deny	ALTER ANY APPLICATION ROLE, ALTER ANY ASSEMBLY, ALTER ANY ASYMMETRIC KEY, ALTER ANY CERTIFICATE, ALTER ANY CONTRACT, ALTER ANY DATABASE AUDIT, ALTER ANY DATABASE DDL TRIGGER, ALTER ANY DATABASE EVENT NOTIFICATION, ALTER ANY DATABASE EVENT SESSION, ALTER ANY DATASPACE, ALTER ANY FULLTEXT CATALOG, ALTER ANY MESSAGE TYPE, ALTER ANY REMOTE SERVICE BINDING, ALTER ANY ROLE, ALTER ANY ROUTE, ALTER ANY SCHEMA, ALTER ANY SERVICE, ALTER ANY SYMMETRIC KEY, ALTER ANY USER, AUTHENTICATE, BACKUP DATABASE, BACKUP LOG, CHECKPOINT, CONNECT, CONNECT REPLICATION, CONTROL, CREATE AGGREGATE, CREATE ASSEMBLY, CREATE ASYMMETRIC KEY, CREATE CERTIFICATE, CREATE CONTRACT, CREATE DATABASE, CREATE DATABASE DDL EVENT NOTIFICATION, CREATE DEFAULT, CREATE FULLTEXT CATALOG, CREATE FUNCTION, CREATE MESSAGE TYPE, CREATE PROCEDURE, CREATE QUEUE, CREATE REMOTE SERVICE BINDING, CREATE ROLE, CREATE ROUTE, CREATE RULE, CREATE SCHEMA, CREATE SERVICE, CREATE SYMMETRIC KEY, CREATE SYNONYM, CREATE TABLE, CREATE TYPE, CREATE VIEW, CREATE XML SCHEMA COLLECTION, DELETE, EXECUTE, INSERT, KILL DATABASE CONNECTION, REFERENCES, SELECT, SHOWPLAN, SUBSCRIBE QUERY NOTIFICATIONS, TAKE OWNERSHIP, UPDATE, VIEW DATABASE STATE, VIEW DEFINITION		

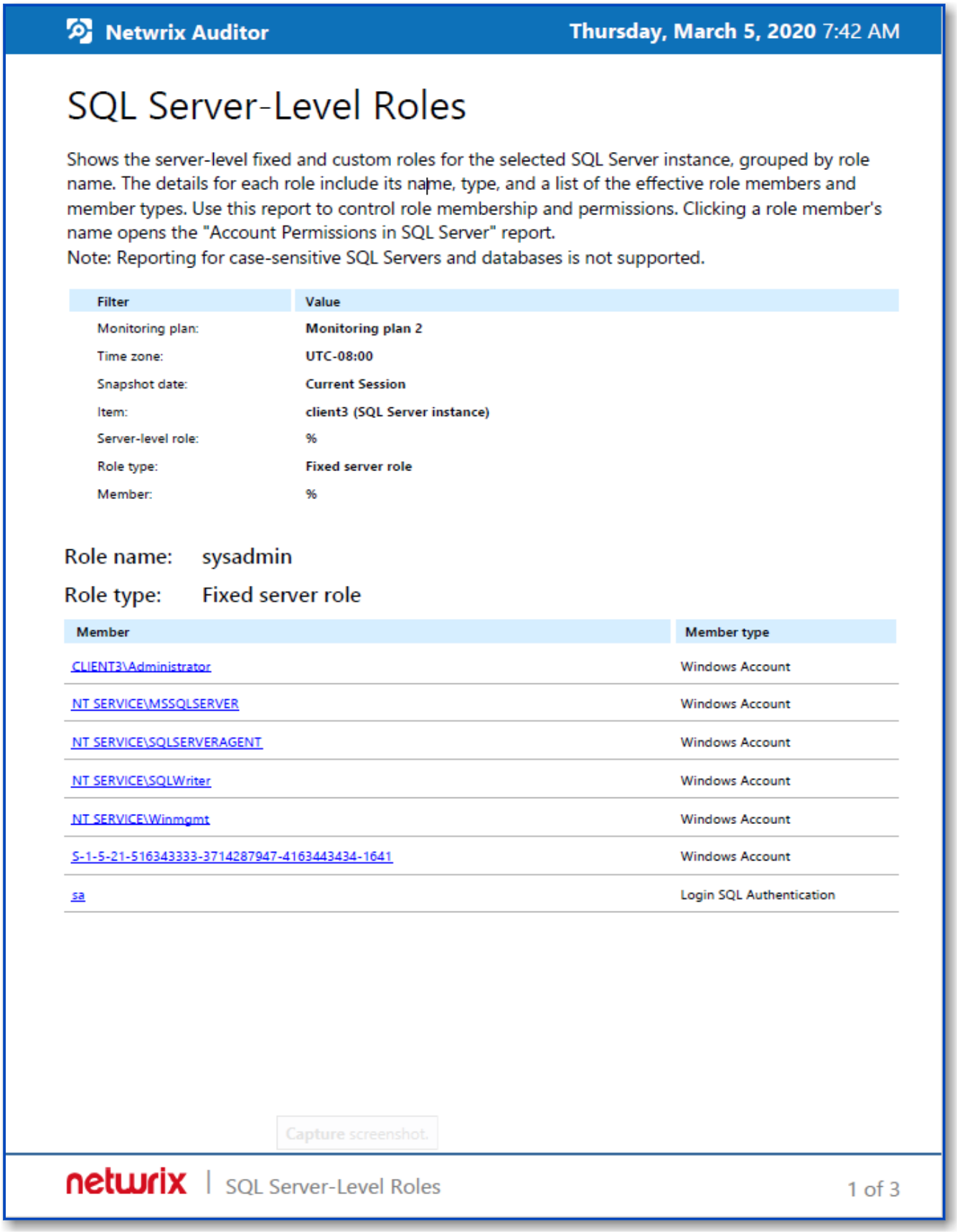
netwrix | SQL Server Means Granted 1 of 1

SQL Server-Level Roles

This report shows the server-level fixed and custom roles for the selected SQL Server instance, grouped by role name. The details for each role include its name, type, and a list of the effective role members and member types. Use this report to control role membership and permissions.

To read more about SQL server-level roles, refer to this Microsoft article.

To instruct Netwrix Auditor to collect data needed for this report, make sure that **Collect data for state-in-time reports** option is selected in the monitoring plan properties. See Settings for Data Collection.



Netwrix Auditor Thursday, March 5, 2020 7:42 AM

SQL Server-Level Roles

Shows the server-level fixed and custom roles for the selected SQL Server instance, grouped by role name. The details for each role include its name, type, and a list of the effective role members and member types. Use this report to control role membership and permissions. Clicking a role member's name opens the "Account Permissions in SQL Server" report.
Note: Reporting for case-sensitive SQL Servers and databases is not supported.

Filter	Value
Monitoring plan:	**Monitoring plan 2**
Time zone:	**UTC-08:00**
Snapshot date:	**Current Session**
Item:	**client3 (SQL Server instance)**
Server-level role:	%
Role type:	**Fixed server role**
Member:	%

Role name: sysadmin

Role type: Fixed server role

Member	Member type
CLIENT3\Administrator	Windows Account
NT SERVICE\MSSQLSERVER	Windows Account
NT SERVICE\SQLSERVERAGENT	Windows Account
NT SERVICE\SQLWriter	Windows Account
NT SERVICE\Winmgmt	Windows Account
S-1-5-21-516343333-3714287947-4163443434-1641	Windows Account
sa	Login SQL Authentication

Capture screenshot.

netwrix | SQL Server-Level Roles 1 of 3

Reported data

The report has a summary section with general information on the selected SQL Server object, and the details section presented in the table format.

The summary section shows:

- **Role name**
- **Role type** — *Fixed server role* or *Custom role*

The detailed information under summary includes the list of effective members for this role, where:

- **Member** — role member name.
- **Member type** —possible values:
  - Windows Account
  - Login SQL Authentication
  - DB SQL User with password

Filters

This report has the following filters:

- **Monitoring plan** — name of the monitoring plan set to collect data from the SQL Server you need.
- **Time zone** — time zone where Netwrix Auditor server is located, for example, UTC-08:00. This value is filled in automatically. time zone where Netwrix Auditor server is located, for example, UTC-08:00.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current Session*). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in SQL Server.
- **Item**— name of the SQL Server instance monitored with selected monitoring plan.
- **Server-level role** —select the role that you want to explore.
- **Role type** — *Fixed server role* or *Custom role*.
- **Member**— role member name.

Considerations and limitations

- Reporting for case-sensitive SQL Servers and databases is not supported.

Related reports

- Clicking a role member (account) link opens the Account Permissions in SQL Server report.

Usage example

Database administrators in the *Corp* organization need to discover what fixed server roles a certain user has on the **SQLSrv01\SQLServer2016** instance. This instance is included in the monitoring plan named *SQL Servers Monitoring*.

To examine the relevant data, they generated the **SQL Server-Level Roles** report with the filters set as follows:

- **Monitoring plan:***SQL Servers Monitoring*
- **Snapshot date:***Current Session*
- **Item:***SQLSrv01\SQLServer2016*
- **Server-level role:** %
- **Role type:** Fixed server role
- **Member:***Corp\Jim.White*

VMware State-In-Time Reports

These are reports on the VMware vCenter state-in-time data, including account permissions and object permissions:

- Account Permissions in vCenter
- Detailed Account Permissions in vCenter
- Object Permissions in vCenter

To instruct Netwrix Auditor to collect data needed for these reports, make sure that **Collect data for state-in-time reports** option is selected in the corresponding monitoring plan properties. See the Settings for Data Collection topic for more information.

Account Permissions in vCenter

Shows vCenter objects that user or group has explicit or inherited permissions on (either granted directly or through group membership). Use this report to see who has permissions to what and prevent rights elevation.

Supported object types and attributes are listed in the VMware topic.

For this report to function properly, you must enable the **Collect data for state-in-time reports** option for the data source in the monitoring plan settings. See the Settings for Data Collection topic for more information.

Filters

You can narrow your reporting scope using multiple filters. Review the full list of available filters and values:

- **Monitoring plan** — name of the monitoring plan set to collect data from the AD domain you need.
- Time zone — is set automatically.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current Session*). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in VMware
- Item — name of the item within your monitoring plan.
- Inherited — select whether to show inherited permissions or not.
- Role – select the name of the VMware role you want to see in the report.

- User (domain\account) – select a specific user to be displayed in the report.

Related Reports

- Clicking a Object path link opens the Object Permissions in vCenter report.
- Clicking a Role link opens the detailed report on privileges for the account report.
- Clicking the Defined in link opens the object permissions on vCenter level report.

Detailed Account Permissions in vCenter

Shows detailed list of privileges that the specified account has on the VMware objects. Use this report to prevent unnecessary privileges assigned to custom roles.

Supported object types and attributes are listed in the VMware topic.

For this report to function properly, you must enable the **Collect data for state-in-time reports** option for the data source in the monitoring plan settings. See the Settings for Data Collection topic for more information.

Filters

You can narrow your reporting scope using multiple filters. Review the full list of available filters and values:

- **Monitoring plan** — name of the monitoring plan set to collect data from the AD domain you need.
- Time zone — is set automatically.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current Session*). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in VMware
- Item — name of the item within your monitoring plan.
- Role – select the name of the VMware role you want to see in the report.
- Object path — path to the monitored object, as formatted by Netwrix Auditor in the activity records.
- User (domain\account) – select a specific user to be displayed in the report.
- Inherited — select whether to show inherited permissions or not.

Object Permissions in vCenter

Shows accounts with explicit or inherited permissions on a specific object in your vCenter (either granted directly or through group membership). Use this report to see who has permissions to what and prevent rights elevation.

Supported object types and attributes are listed in the VMware topic.

For this report to function properly, you must enable the **Collect data for state-in-time reports** option for the data source in the monitoring plan settings. See the Settings for Data Collection topic for more information.

Filters

You can narrow your reporting scope using multiple filters. Review the full list of available filters and values:

- **Monitoring plan** — name of the monitoring plan set to collect data from the AD domain you need.
- Time zone — is set automatically.
- **Snapshot date** —select the date of state-in-time snapshot you want to report on. By default, the report includes data obtained during the latest data collection session (*Current Session*). To report on other snapshots, make sure they are available through import. For details, see **Manage historical snapshots** option description in VMware
- Item — name of the item within your monitoring plan.
- Role – select the name of the VMware role you want to see in the report.
- **Object path** —path to the monitored object, as formatted by Netwrix Auditor in the activity records .

- User (domain\account) – select a specific user to be displayed in the report.

Related Reports

- Clicking a User account link opens the Account Permissions in vCenter report.
- Clicking a Role link opens the detailed report on privileges for the account report.
- Clicking the Defined in link opens the object permissions on vCenter level report.

Compliance Reports

For your convenience, besides grouping by data source the reports are grouped by compliance standards. Auditor provides out-of-box reports that allow validating compliance with different standards and regulations, including but not limited to:

- FERPA
- FISMA/NIST SP800-53 rev4

- GDPR

- GLBA
- HIPAA
- ISO/IEC 27001
- NERC
- PCI DSS v3.2
- SOX
- CJIS

Each compliance folder provides overview on a selected standard, to read it, click on the folder name. Click Read More to learn more about mapping between these standards and Auditor reports.

In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the Monitoring Plans section.

Review the following for additional information:

- See the View Reports topic for additional information on how to find the report you need and view reports in a web browser.

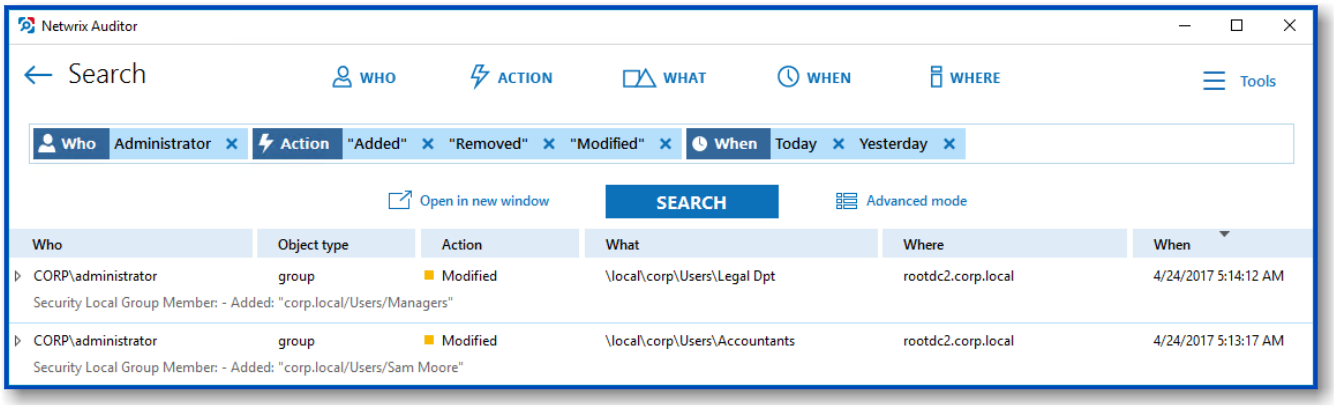
Custom Search-Based Reports

Netwrix Auditor allows you to save your favorite searches as reports to access them instantly. For your convenience, the product provides predefined templates for some popular usage scenarios. You can save your custom report or use one of the templates provided by Netwrix. Navigate to Reports → Custom to review these reports. Click View to generate the selected report.

Moreover, custom reports are shared between all Netwrix Auditor clients that have access to the same Netwrix Auditor Server (the main component responsible for collecting and processing audit data).

For your convenience, you can create additional folders for your custom reports. Select Add Folder under the Custom section and specify the name for a new folder. Then, select a custom report and move it to the new folder.

The example custom report results apply to AD or Group Policy modifications by administrator.



Review the following for additional information:

- To save a search as a custom report
- To modify a custom report
- To subscribe to a custom report
- To delete a custom report

To save a search as a custom report

1. On the main Netwrix Auditor page, navigate to Search.
2. Apply filters and click Search.

   View and Search Collected Data how to apply filters when searching audit data.
3. Navigate to Tools and select Save as report.
4. In the Specify a name for your custom report dialog, specify a name. Make sure to specify a unique name.

To modify a custom report

1. On the main Netwrix Auditor page, navigate to Reports → Custom.
2. Select one of the custom reports in the list and review filters.
3. Click View to open search.
4. Modify filters and click Search.

   View and Search Collected Data how to apply filters when searching audit data.

5. Navigate to Tools and select Save as report.
6. In the Specify a name for your custom report dialog, specify a name. Netwrix Auditor automatically offers a previously used name so that this custom report will be overwritten. If you want to save both searches, specify a unique name for a modified search.

To subscribe to a custom report

1. Navigate to Reports → Custom and select the report you want to subscribe to.
2. Click Subscribe and complete the Add Subscription to Search wizard.

To delete a custom report

- Navigate to Reports → Custom, select a report and click Delete.

Subscriptions

Subscriptions enable you to schedule email delivery of a variety of reports or set of specific search criteria. Subscriptions are helpful if you are a rare guest of Netwrix Auditor and you only need to get statistics based on individual criteria. For example, an IT manager can easily provide auditors with weekly reports to prove compliance with regulations.

You can configure subscriptions to reports (including dashboards) risk assessment overview and interactive search.

You can add any elements (a dashboard, report, alert, risk, etc.) to the Auditor Home screen to access them instantly. See the Navigation and Customize Home Screen topics for additional information.

Subscription to Reports

This subscription type has the following key features:

- Predefined change reports to monitor important cases for all data sources.
- State-in-Time reports to monitor data source state at a specific moment of time.

- Predefined User Behavior and Blind Spot Analysis report pack with complex logic to identify vulnerabilities (e.g., data access, suspicious files, etc.).
- Organization level reports to visualize what is happening in your environment.
- Reports with review status to track team workflow.
- Compliance reports to stay compliant with different standards.

Subscription to Search Results

This subscription type has the following key features:

- Flexible set of filters to modify search for your business use and create another subscription based on the existing one.
- Advanced filters to make your results context match.
- The History option to verify that the subscription is configured properly.
- On-demand delivery to send the subscription to a recipient at any moment.

Subscription to Risk Assessment Overview

This subscription type has the following key features:

- Risk assessment overview based on the latest state-in-time data to monitor the state of your Active Directory users and computers, as well as files and folders and other data at a specific moment.
- Automatically calculated metrics to identify risks and potential vulnerabilities (sensitive data, malicious files, etc.).
- Filters for monitoring plans and risk categories to receive exactly the data you need.
- Subscription options - delivery by email or upload to the specified file share.
- History option to verify that the subscription was configured properly and delivered successfully.
- On-demand delivery (Run Now) to send the subscription to a recipient at any moment.

Subscription emails may vary slightly depending on the file delivery method and subscription type.

Subscription to Behavior Anomalies

This subscription type is similar to the predefined reports.

Review the following for additional information:

- Create Subscriptionshow to create new subscriptions.
- Review and Manage Subscriptionshow to manage subscriptions.

Create Subscriptions

To create new subscriptions and manage existing subscriptions, you must be assigned the Global administrator or Global reviewer role in the product. See the Role-Based Access and Delegation topic for additional information.

1. Do one of the following depending on subscription type:

To...	Do...
Subscribe to a report	On the main Auditor page, navigate to Reports. Specify the report that you want to subscribe to and click Subscribe.
Subscribe to Behavior anomalies dashboard report	On the main Auditor page, navigate to Behavior anomalies, then in the dashboard window click Subscribe.
Subscribe to search	1. Navigate to Search and set appropriate search criteria. See the Use Filters in Simple Mode topic for additional information. Click Search. 2. Navigate to Tools and select Subscribe.
Subscribe to risk assessment overview	On the main Auditor page, navigate to Risk assessment and in the dashboard window click Subscribe.

2. On the Add Subscription page, complete the following fields:

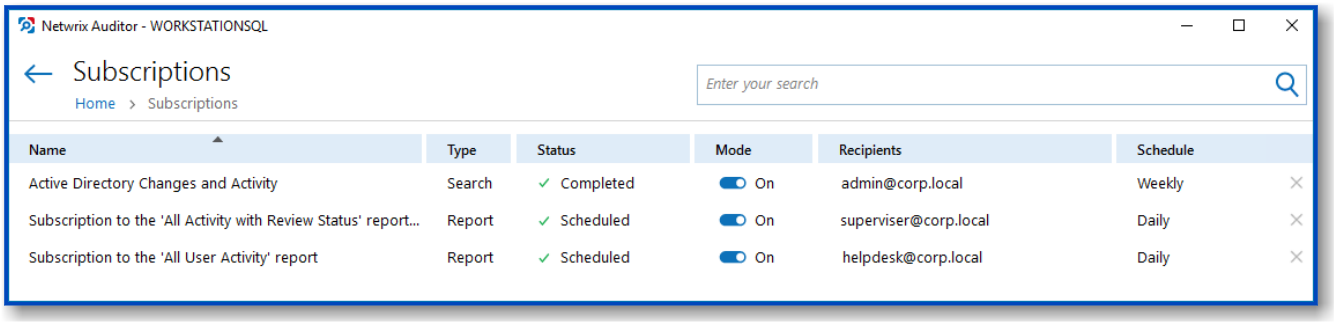
Option	Description
General	
Subscription name	Enter the name for the subscription.
Report name ***OR*** **Email subject**	For report subscription—You cannot edit report name. For subscription to search and risk assessment overview—Specify email subject to identify subscription emails from Auditor. For example, "*Successful read attempts on important file shares*".
Send empty subscriptions when no activity occurred **Available for report and search subscriptions only.**	Slide the switch to Yes if you want to receive a report even if no changes occurred.
Specify delivery options	• File format—Configure reports to be delivered as the pdf or csv files for search subscriptions; and pdf, docx, csv or xls files for report subscriptions. Available for report and search subscriptions only. • File delivery—Select delivery method: ◦ Attach to email—Select this option to receive data as email attachments. The maximum size of the attachment file is 50 MB. Attachments larger than 50MB will be uploaded to *<NAservername>*\Netwrix_Auditor_Subscriptions$\LostAndFound\ folder on Netwrix Auditor server. They will be

Option	Description
	available for 7 days. Check the subscription email to get the files. ◦ Upload to a file share—Select this option to save data on the selected file share. Click Browse to select a folder on the computer that hosts Auditor Server or specify a UNC path to a shared network resource. Make sure that the recipients have sufficient rights to access it and the Long-Term Archive service account has sufficient rights to upload reports. See the File-Based Repository for Long-Term Archive topic for additional information. **NOTE:** Make sure that the AD Computer account for the Auditor host server also has read access on the file share where the Subscriptions are being uploaded.
Other tabs	
Recipients	Shows the number of recipients selected and allows specifying emails where reports are to be sent. Expand the Recipients list and click Add to add more recipients.
Schedule	Allows specifying report delivery schedule (daily, certain days of week, a certain day of a certain month). By default, risk assessment overview and search subscription delivery is scheduled to 7.00 am daily, report subscription delivery - to 8.00 am daily.

Option	Description
Filters	• For report subscription—Specify the report filters, which vary depending on the selected report. • For subscription to risk assessment overview—Select one or several monitoring plans and risk categories whose data you want to be included. By default, you will receive data on all risk categories, provided by all monitoring plans configured for risk assessment. • For search subscription—Specify filters in the same way as for search. See the Use Filters in Advanced Mode topic for additional information. For search subscription, you can also select a parameter to sort actions by and the sorting order.
History **For search and risk assessment subscriptions only.**	• Contains subscription generation details (intervals, status, last run time, start type). If the subscription failed, expand its details to understand and resolve error, then click the Try again link. • Allows for on-demand subscription delivery—for that, click Run Now. On successful subscription generation you will receive the results that match your criteria for the scheduled period.

Review and Manage Subscriptions

On the main Netwrix Auditor page, navigate to Subscriptions to review a list of your subscriptions.



The table below provides instructions on how to manage your subscriptions.

To...	Do...
Browse subscriptions	Type the target subscription name in the search bar in the upper part of the Subscriptions window and click the Search icon to review results.
Enable or disable subscriptions	Pick a subscription and select On or Off in the Mode column.
Modify subscriptions	Select the subscription that you want to modify and click Edit at the bottom of the Subscriptions window. Update the subscription and save your changes.
Remove subscriptions	Click  icon next to the selected subscription.

Alerts

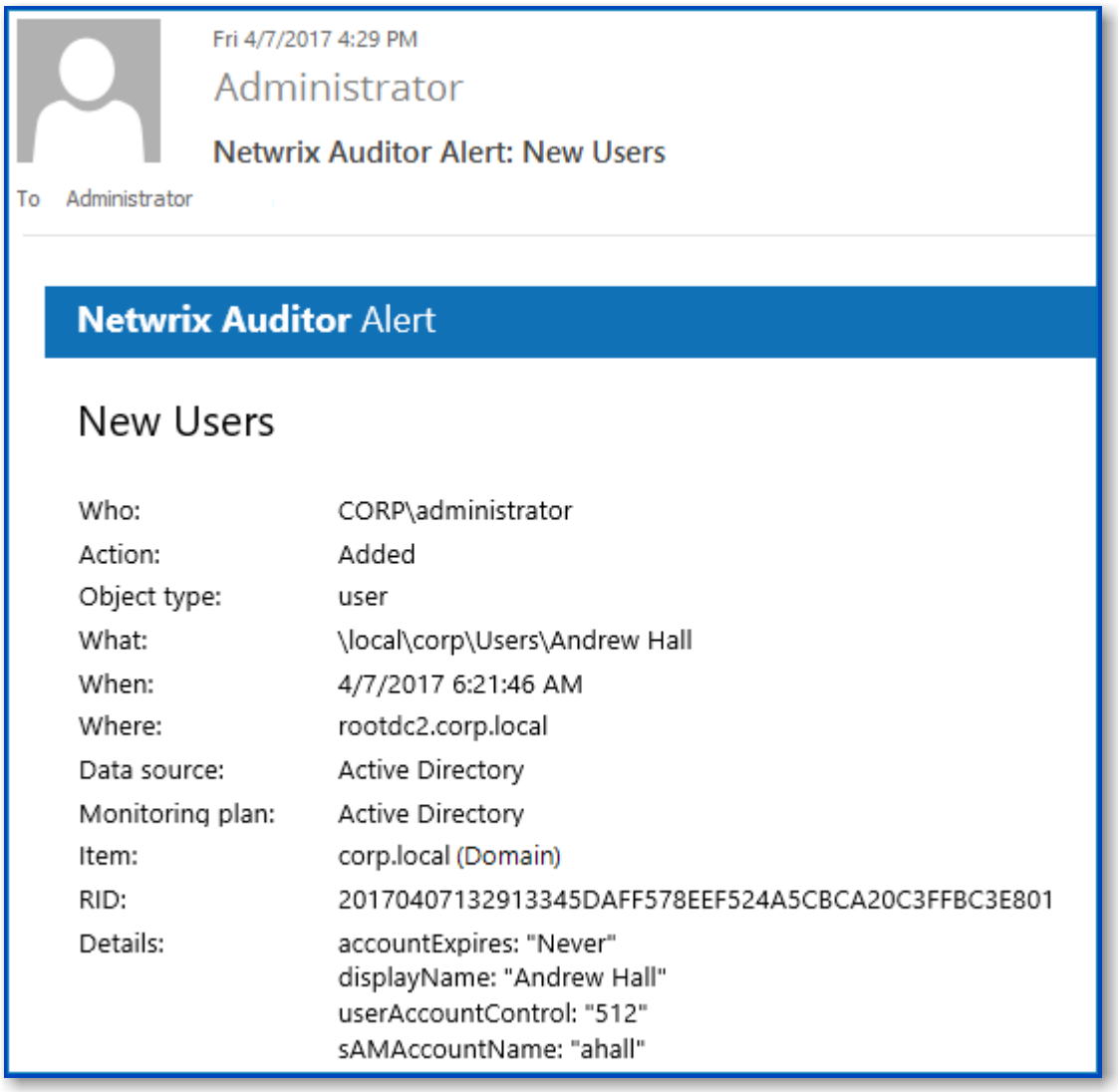
If you want to be notified about suspicious activity, you can configure alerts that will be triggered by specific events. Alerts are sent after the specified action has been detected. Alerts are helpful if you want to be notified about actions critical to your organization security and have to mitigate risks once the suspicious action occurs.

Review the following to take advantage of the Alerts functionality:

- See theManage Alerts topic for additional information on how to edit and enable existing predefined alerts, and create new alerts based on the predefined ones.

- See the Create Alerts topic for additional information on how to create custom alerts with your personal filters.
- If you need to be alerted on specific events in your Event Logs or non-owner mailbox access attempts, see the Create Alerts for Event Log and Create Alerts for Non-Owner Mailbox Access Events topics for additional information.

The example alert is triggered when a new user is created in the monitored domain.



Fri 4/7/2017 4:29 PM

Administrator

Netwrix Auditor Alert: New Users

To Administrator

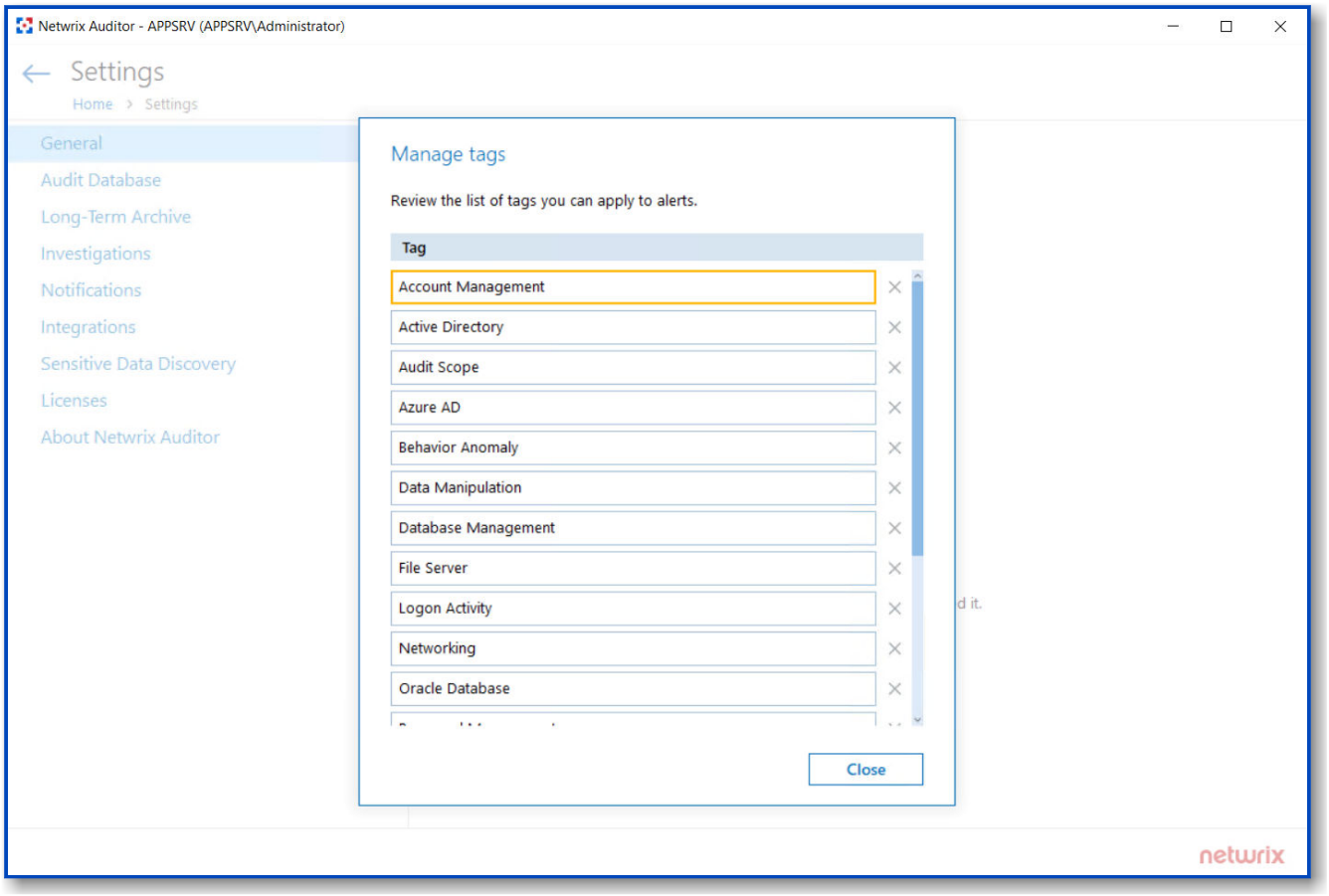
Netwrix Auditor Alert

New Users

Who:	CORP\administrator
Action:	Added
Object type:	user
What:	\local\corp\Users\Andrew Hall
When:	4/7/2017 6:21:46 AM
Where:	rootdc2.corp.local
Data source:	Active Directory
Monitoring plan:	Active Directory
Item:	corp.local (Domain)
RID:	20170407132913345DAFF578EEF524A5CBCA20C3FFBC3E801
Details:	accountExpires: "Never" displayName: "Andrew Hall" userAccountControl: "512" sAMAccountName: "ahall"

Tags

Netwrix Auditor allows you to apply tags when creating an alert. Applying tags to alerts allows you to distinguish one alert from another or create groups of similar alerts.



The Tags page contains a complete list of alerts that were created in the product. Currently, you cannot assign or create tags on this page.

To apply tags to an alert, navigate to alert settings and locate the Apply tags section on the General tab. See the Create Alerts topic to receive information about tags applying.

Alerts Overview Dashboard

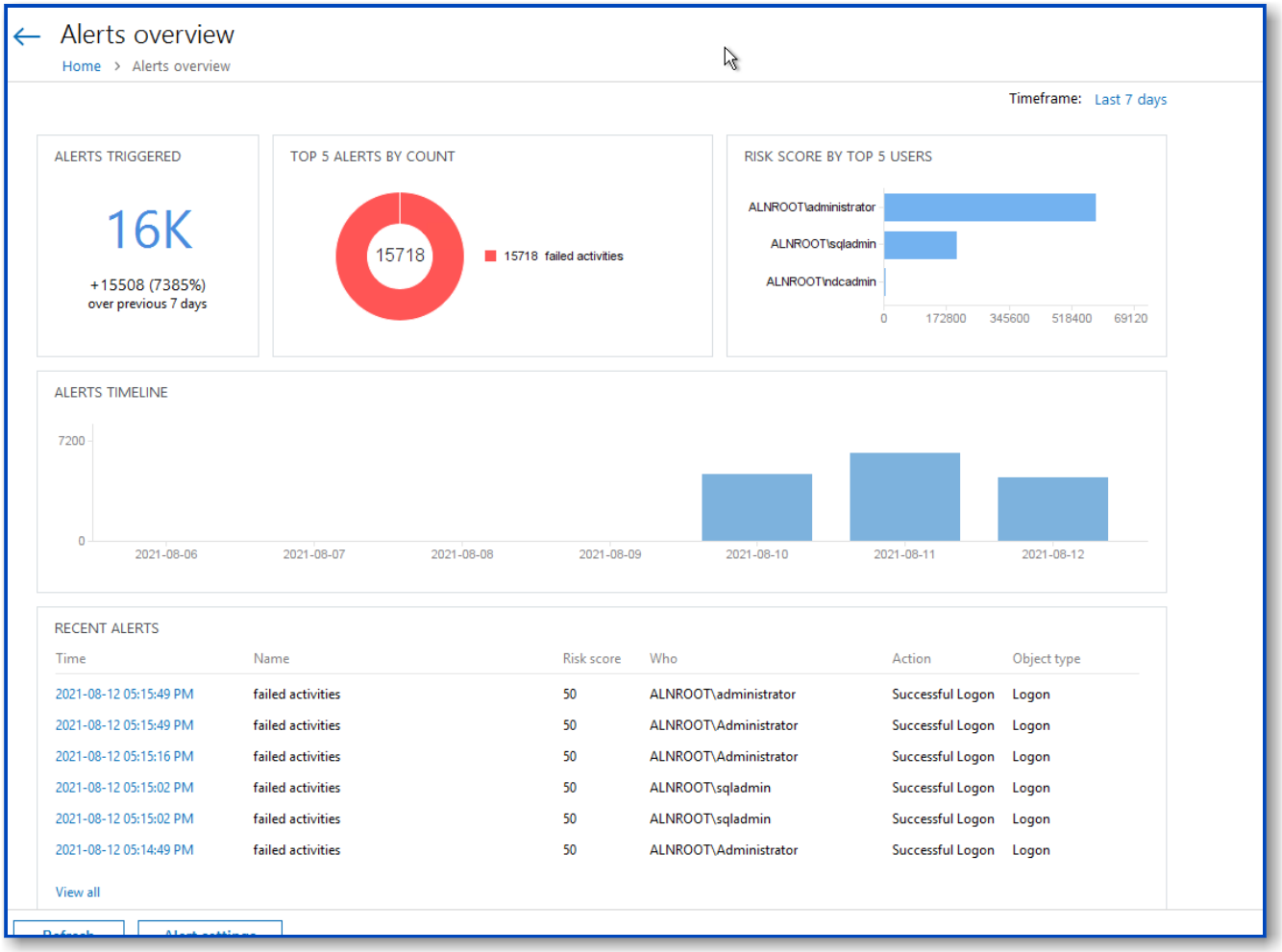
Aggregated statistics on the alerts is provided in the Alerts overview widget. It displays currently triggered alerts with detailed information.

To view the dashboard, on the main Auditor page, click the Alerts tile.

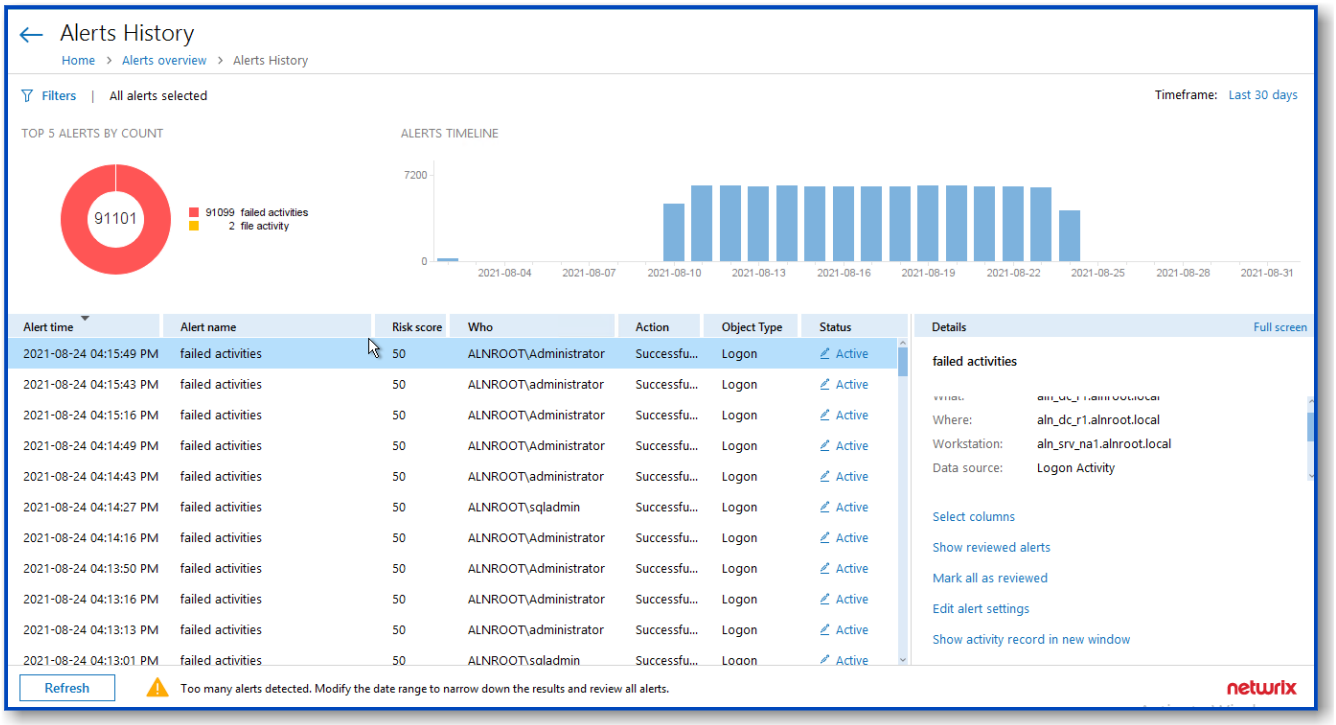
The dashboard includes the following widgets:

- Alerts triggered – Shows amount of alerts triggered for the last 7 days (by default). Use this tile to inspect the trend.

- Top 5 alerts by count – Shows most recently triggered alerts for the selected time period (7 days by default).
- Risk score by top 5 users – Shows potentially harmful users for the selected time period (7 days by default). Clicking the tile opens the Behavior Anomalies dashboard. See the Behavior Anomalies topic for additional information.
- Alerts timeline – Shows the number of alerts triggered at the specific day.
- Recent alerts – Shows all the triggered alerts in chronological order.



Clicking any tile except for Risk score by top 5 users drills down to the Alert history dashboard that provides users with the detailed information about the latest alerts triggered in their IT infrastructure enriched with the actionable chart and timeline.



Review detailed information about the triggered alerts and change anomaly status. See the Review User Profiles and Process Anomalies topic for additional information.

On the Details pane, you can review alert details and manage your alerts:

- Select columns – Select colums to be displayed.
- Show reviewed alerts – Click to view all alerts you have already reviewed.
- Mark all as reviewed – Click to mard all alerts in the list as reviewed. Netwrix recommends doing this only if you are completely sure that there are no critical alerts in your infrastructure.
- Edit alerts settings – Click to modify settings of the selected alert. See the Create Alerts topic for additional information.
- Show activity record in new window – Click to view more information about the activity record that triggered an alert. See the Activity Records Statistics topic for additional information.

You can also refresh the alerts information by clicking the Refresh button at the bottom or go to the general alerts settings page clicking the Alert settings. See the Manage Alerts topic for additional information.

Create Alerts

To create new alerts and modify existing alerts, the account used to connect to Auditor Server must be assigned the *Global administrator* or *Global reviewer* role in the product.

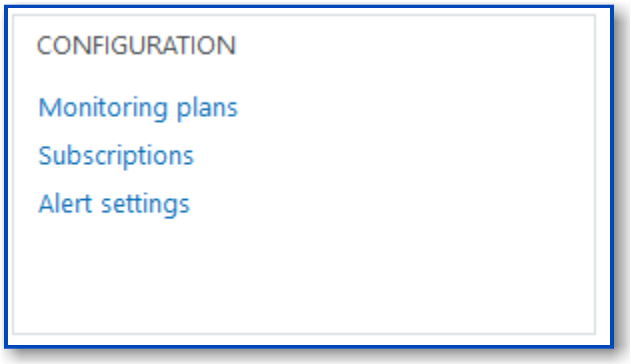
To set up a response action, this account must also be a member of the local *Administrators* group on Auditor Server.

See the Role-Based Access and Delegation topic for additional information.

Create a Custom Alert

Follow the steps to create a custom alert.

Step 1 – On the main Auditor page, click the Alert settings link under the Configuration section on the left:



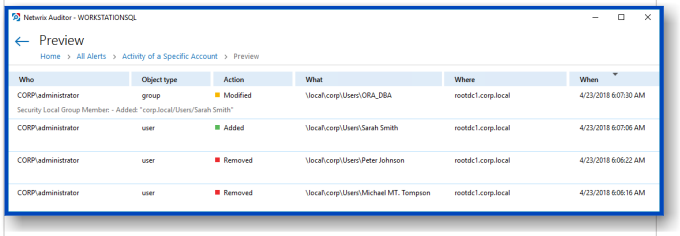
See the Navigation topic for additional information.

You can also create new alert directly from the interactive search results. Navigate to Tools and select Create alert to add a new alert with the same set of filters as your search.

Step 2 – In the All Alerts window, click Add. Configure the following:

Option	Description
General	• Specify a name and enter the description for the new alert.

Option	Description
	NOTE: Make sure that the Send alert when the action occurs option is enabled. Otherwise, the new alert will be disabled. • Email subject — Specify the subject of the email. It is possible to insert variables into the subject line. You can choose between "*Who*", "*What*" and"*Where*" variables. Consider the following: ◦ Only one variable of each type can be added ◦ You need to cut off the full path from the object names in "*What*" alert and leave only the actual name. For example, "*\com\Corp\Users\Departments\IT\Username*" should be just "*Username*". If you want to get back to the default Email subject line, click the **Restore Default** button. • Apply tags — Create a set of tags to more efficiently identify and sort your alerts. Select Edit under Apply tags to associate tags with your alert. Later, you can quickly find an alert of interest using Filter by tags in the upper part of the All Alerts window. To see a full list of alerts ever created in the product, navigate to Settings > Tags.
Recipients	Select alert recipients. Click Add Recipient and select alert delivery type: • Email — Specify the email address where notifications will be delivered. You can add as many recipients as necessary. ***RECOMMENDED:*** click **Send Test Email**. The system will send a test message to the specified

Option	Description
	email address and inform you if any problems are detected. • SMS-enabled email — Netwrix uses the sms gateway technology to deliver notifications to a phone number assigned to a dedicated email address. Specify email address to receive SMS notifications. Make sure that your carrier supports sms to email gateway technology.
Filters	Apply a set of filters to narrow events that trigger a new alert. Alerts use the same interface and logic as search. • Filter — Select general type of filter (e.g., "Who", "Data Source", "Monitoring plan", etc.) • Operator — Configure match types for selected filter (e.g., "Equals", "Does not contain", etc.) • Value — Specify filter value. See the View and Search Collected Data topic for additional information on how to create and modify filters. The Filters section contains required fields highlighted with red. Once you completed all filters, click Preview on the right pane to see search-based list of events that will trigger your alert. 

Option	Description
Thresholds	If necessary, enable threshold to trigger the new alert. In this case, a single alert will be sent instead of many alerts. This can be helpful when Auditor detects many activity records matching the filters you specified. Slide the switch under the Send alert when the threshold is exceeded option and configure the following: • Limit alerting to activity records with the same... — Select a filter in the drop-down list (e.g., who). Note that, Auditor will search for activity records with the same value in the filter you selected. Only alerts grouped by the Who parameter can be included in the Behavior Anomalies list. Mind that in this case, the product does not summarize risk scores and shows the value you associated with this alert. This may significantly reduce risk score accuracy. • Send alert for <...> activity records within <...> seconds — Select a number of changes that occurred in a given period (in seconds). For example, you want to receive an alert on suspicious activity. You select "*Action*" in the Limit alerting to activity records with the same list and specify a number of actions to be considered an unexpected behavior: *1000* changes in *60* seconds. When the selected threshold exceeded, an alert will be delivered to the specified recipients: one for every 1000 removals in 60 seconds, one for every 1000 failed removals in 60 seconds. So you can easily discover what is going on in your IT infrastructure.
Risk Score	• Slide the switch to On under Include this alert in Behavior Anomalies assessment. See the Behavior Anomalies topic for additional information.

Option	Description
	• Associate a risk score with the alert — Assign a risk score based on the type of anomaly and the severity of the deviation from the normal behavior. An action's risk score is a numerical value from 1 (Low) to 100 (High) that designates the level of risk with 100 being the riskiest and 1 the least risky. These are general guidelines you can adopt when setting a risk score: ◦ High score — Assign to an action that requires your immediate response (e.g., adding account to a privileged group). Configure a non-threshold alert with email recipients. ◦ Above medium score — Assign to a repetitive action occurring during a short period of time. While a standalone action is not suspicious, multiple actions merit your attention (e.g., mass deletions from a SharePoint site). Configure a threshold-based alert with email recipients. ◦ Low score — Assign to an infrequent action. While a single action is safe, multiple occurrences aggregated over a long period of time may indicate a potential in-house bad actor (e.g., creation of potentially harmful files on a file share). Configure a non-threshold alert, email recipients are optional but make sure to regularly review the Behavior Anomalies dashboard. ◦ Low score — Assign to a repetitive action that does not occur too often (e.g., rapid logons). Multiple occurrences of action sets may indicate a potential in-house bad actor or account compromise. Configure a threshold-based alert, email recipients are optional but make sure to regularly review the Behavior Anomalies dashboard.

Option	Description
Response Action	You can instruct Auditor to perform a response action when the alert occurs — for example, start an executable file (command, batch file, or other) that will remediate the issue, or open a ticket with the help desk, and so on. For that, you will need an executable file stored locally on the Auditor server. Slide the switch to turn the feature **ON**, and see the Configure a Response Action for Alert topic for additional information.

Create Alerts for Event Log

Alerts are configurable notifications triggered by certain events and sent to the specified recipients. You can enable or disable, and modify existing alerts, and create new alerts. To do it, click Configure next to Alerts.

Follow the steps to create new alert.

Step 1 – In the Alerts window, click Add to start new alert.

Step 2 – On the Alert Properties step, specify the alert name and enter alert description (optional). Specify the number alerts per email. Grouped alerts for different computers will be delivered in separate email messages. This value is set to 1 by default, which means that each alert will be delivered as a separate email message.

Step 3 – On the Notifications step, configure email notifications and customize the notification template, if needed. Click Edit next to Customize notifications template. Edit the template by deleting or inserting information fields.

The %ManagedObjectName% variable will be replaced with your monitoring plan name.

Step 4 – On the Event filters step, specify an event that will trigger the alert.

Step 5 – Complete the Event Filters wizard. Complete the following fields:

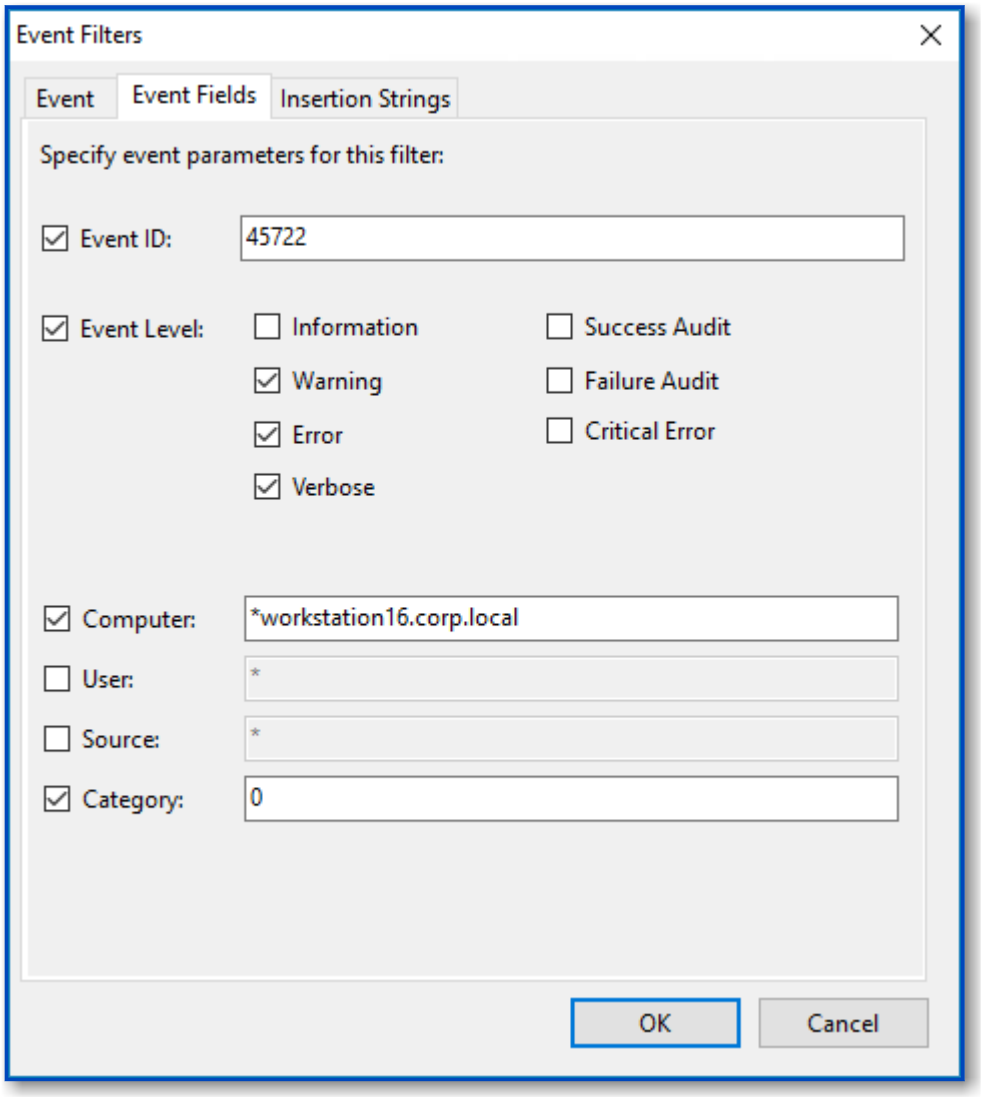
- In the Event tab:

Option	Description
Name	Specify the filter name.
Description	Enter the description for this filter (optional).
Event Log	Select an event log from the drop-down list. You will be alerted on events from this event log. You can also input a different event log. To find out a log's name, navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Event Viewer** > **Applications and Services Logs** > Microsoft > Windows and expand the required Log_Name node, right-click the file under it and select Properties. Find the event log's name in the Full Name field. Auditor does not collect the Analytic and Debug logs, so you cannot configure alerts for these logs. You can use a wildcard (*). In this case you will be alerted on events from all Windows logs except for the ones mentioned above.

- In the Event Fields tab:

Option	Description
Event ID	Enter the identifier of a specific event that you want to be alerted on. You can add several IDs separated by comma.
Event Level	Select the event types that you want to be alerted on. If the Event Level checkbox is cleared, you will be alerted on all event types of the specified log.
Computer	Specify a computer. You will only be alerted on events from this computer.

Option	Description
	If you want to specify several computers, you can define a mask for this parameter. Below is an example of a mask: ◦ * - any machine ◦ computer – a machine named 'computer' ◦ *computer* - machines with names like 'xXxcomputerxXx' or 'newcomputer' ◦ computer? – machines with names like 'computer1' or 'computerV' ◦ co?puter - machines with names like 'computer' or 'coXputer' ◦ ????? – any machine with a 5-character name ◦ ???* - any machine with a 3-character name or longer
User	Enter a user's name. You will be alerted only on the events generated under this account. If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Source	Specify this parameter if you want to be alerted on the events from a specific source. If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Category	Specify this parameter if you want to be alerted on a specific event category.



- In the Insertion Strings tab:

Option	Description
Consider the following event Insertion Strings	Specify this parameter if you want to receive alerts on events containing a specific string in the EventData. You can use a wildcard (*). Click Add and specify Insertion String.

Step 6 – Click OK to save the changes and close the Event Filters dialog.

Create Alerts for Non-Owner Mailbox Access Events

If you have a monitoring plan configured to audit Exchange, you can configure alerts to be triggered by non-owner mailbox access events (e.g., opening a message folder, opening/modifying/deleting a message) using the event log alerts. To enable monitoring of non-owner mailbox access events, you need to create a monitoring plan for auditing event logs.

Create Alerts for Non-Owner Mailbox Access Events

The procedure below describes the basic steps, required for creation of a monitoring plan that will be used to collect data on non-owner mailbox access events. See Event Log Manager topic for additional information.

Follow the steps to create alert for non-owner mailbox access events.

Step 1 – Create a monitoring plan in Netwrix Auditor Event Log Manager.

Step 2 – Make sure that the Enable event log collection checkbox is selected. Specify the name for the new plan, for example, "*Non-owner mailbox access auditing*".

Step 3 – Navigate to the Monitored computers list and add a server where your Exchange organization resides.

Step 4 – On the General tab, click Configure next to Alerts. Make sure the predefined alerts are disabled. Click Add to create an alert for non-owner mailbox access event.

Step 5 – In the Alert Properties wizard, specify the alert name and enter alert description (optional). Specify the number alerts per email. Grouped alerts for different computers will be delivered in separate email messages. This value is set to 1 by default, which means that each alert will be delivered as a separate email message.

Step 6 – Specify alert recipient if you want the alert to be delivered to a non-default email.

Step 7 – Navigate to Event Filters and click Add to specify an event that will trigger the alert.

Step 8 – Complete the Event Filter dialog.

- In the Event tab, specify the filter name and description. In the Event Log field enter *"Netwrix Non-Owner Mailbox Access Agent"*.
    - In the Event Fields tab, complete the following fields:

- Event ID—Enter the identifier of a specific event that you want to be alerted on. You can add several IDs separated by comma. Review the event IDs available in the Netwrix **Non-Owner Mailbox Access Agent** event log:

ID	Description	Access Type (as displayed in XML view of event details)
1	A folder was opened	actFolderOpen
2	A message was opened	actMessageOpened
3	A message was sent	actMessageSubmit
4	A message was changed and saved	actChangedMessageSaved
5	A message was deleted	actMessageDeleted
6	A folder was deleted	actFolderDeleted
7	The entire contents of a folder was deleted	actAllFolderContentsDeleted
8	A message was created and saved	actMessageCreatedAndSaved
9	A message was moved or/and copied	actMessageMoveCopy
10	A folder was moved or/and copied	actFolderMoveCopy
14	A folder was created	actFolderCreated

- Source—Enter *"Netwrix Non-Owner Mailbox Access Agent"*.

- In the Insertion Strings tab, select Consider the following event Insertion Strings to receive alerts on events containing a specific string in the EventData. Click Add and specify the Insertion String.

Step 9 – Click OK to save the changes and close the Event Filters dialog.

Step 10 – In the Netwrix Auditor Event Log Manager wizard, navigate to Notifications and specify the email address where notifications will be delivered.

RECOMMENDED: click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

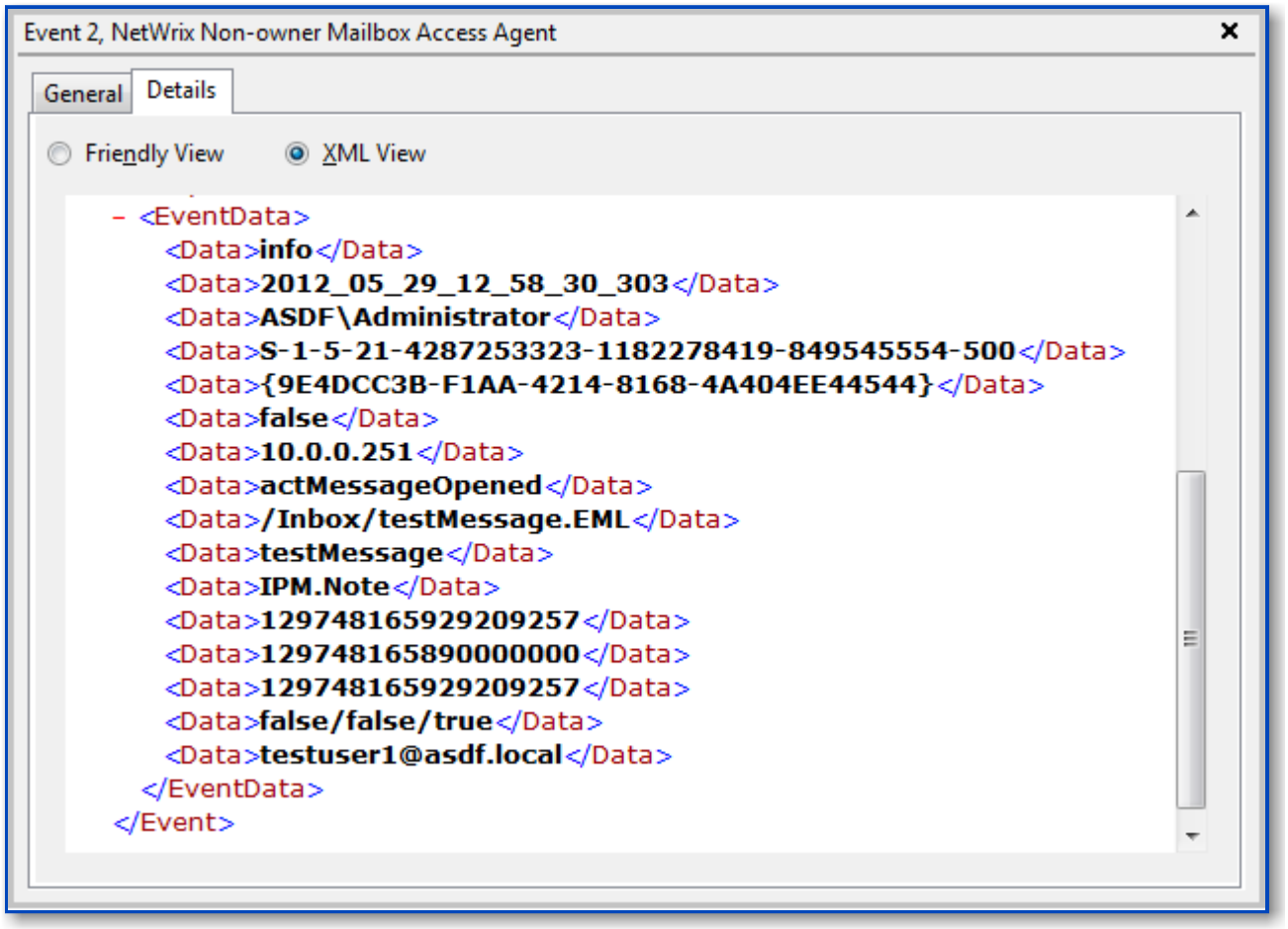
Step 11 – Click Edit next to Audit Archiving Filters step, in the Inclusive Filters section clear the filters you do not need, click Add and specify the following information:

- The filter name and description (e.g., Non-owner mailbox access event)
- In Event Log, enter *"Netwrix Non-Owner Mailbox Access Agent"*.
- In Write to, select Long-Term Archive. The events will be saved into the local repository.

Step 12 – Click Save. If an event occurs that triggers an alert, an email notification will be sent immediately to the specified recipients.

Review Event Description

Review the example of the MessageOpened event in the XML view:



Depending on the event, the strings in the description may vary. The first eight strings are common for all events:

String	Description
String1	The event type: info or warning
String2	The event date and time in the following format: YYYY_MM_DD_hh_mm_ss_000
String3	The name of the user accessing mailbox
String4	The SID of the user accessing mailbox

String	Description
String5	The GUID of the mailbox being accessed
String6	Shows whether the user accessing mailbox is the owner: it is always *false*
String7	The IP of the computer accessing the mailbox
String8	The access type

The following strings depend on the non-owner access type, represented by different Event IDs:

Event ID	Access type (String 8)	Strings	Description
1	actFolderOpen	String9	The internal folder URL
2	actMessageOpened	String9	The internal message URL
		String10	The message subject
		String11	The message type: IPM.Note—Email, IPM.Contact – contact, etc.
3	actMessageSubmit	String9	The internal message URL
		String10	The message subject
		String11	Email addresses of the message recipients, separated by a semicolon
		String12	The message type: IPM.Note—Email, IPM.Contact – contact, etc.

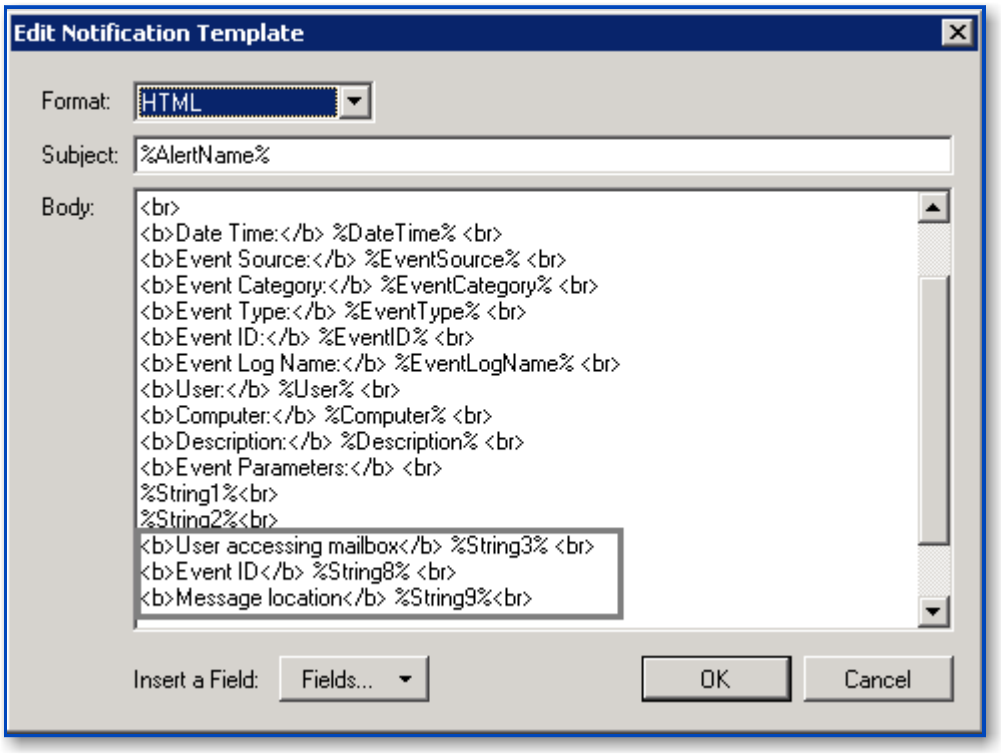
Event ID	Access type (String 8)	Strings	Description
4	actChangedMessageSaved	String9	The internal message URL
		String10	The message subject
		String11	The message type: IPM.Note – Email, IPM.Contact – contact, etc.
5	actMessageDeleted	String9	The internal message URL
		String10	The message subject
		String11	The message type: IPM.Note—Email, IPM.Contact – contact, etc.
6	actFolderDeleted	String9	The internal folder URL
7	actAllFolderContentsDeleted	String9	The internal folder URL
8	actMessageCreatedAndSaved	String9	The internal message URL
9	actMessageMoveCopy	String9	The message being moved/copied—the final part of the message URL, e.g., /Inbox/testMessage.EML
		String10	The action – copy or move
		String11	The folder URL the message is copied/moved from
		String12	The destination folder URL
		String13	The message type: IPM.Note—Email, IPM.Contact – contact, etc.
10	actFolderMoveCopy	Strings 9 -13	The string descriptions for the folder are similar to those for messages.
14	actFolderCreated	String9	The new folder URL

With different Exchange versions and/or different email clients, the same non-owner action (e.g., copying a message) may generate different events: e.g., actMessageMoveCopy with one server/client or actMessageCreatedAndSaved with another.

You can add the required strings contained in % symbols for your own custom alert separated by a `<br>` tag in `<b>Event Parameters:<b>`. Event parameter descriptions can also be added.

In the example below, the following information has been added:

- The description for String 3—User accessing mailbox
- String 8 with the description
- String 9 with the description



Create Alerts on Health Status

You can configure alerts to be triggered by important events in the Netwrix AuditorSystem Health log.

To create alerts to be notified on Auditor Health Status.

Follow the basic steps, required for creation of the monitoring plan that will be used to collect data on Auditor health status events. See the topic for additional information.

Step 1 – Start Netwrix Auditor Event Log Manager and create the new monitoring plan.

Step 2 – Make sure that the Enable event log collection checkbox is selected. Specify the name for the new plan, for example, "Netwrix Auditor *Health Status*".

Step 3 – Navigate to the Monitored computers list and add a server where the Auditor server resides.

Step 4 – On the General tab, click Configure next to Alerts. Make sure the predefined alerts are disabled. Click Add to create anew alert.

Step 5 – In the Alert Properties wizard, specify the alert name and enter alert description (optional). Specify the number alerts per email. Grouped alerts for different computers will be

delivered in separate email messages. This value is set to 1 by default, which means that each alert will be delivered as a separate email message.

Step 6 – Specify alert recipient if you want the alert to be delivered to a non-default email.

Step 7 – Navigate to Event Filters and click Add to specify an event that will trigger the alert.

Step 8 – Complete the Event Filter dialog.

- In the Event tab, specify the filter name and description. In the Event Log field select the Netwrix Auditor System Health log.
- In the Event Fields tab, select event levels that will trigger the alert.

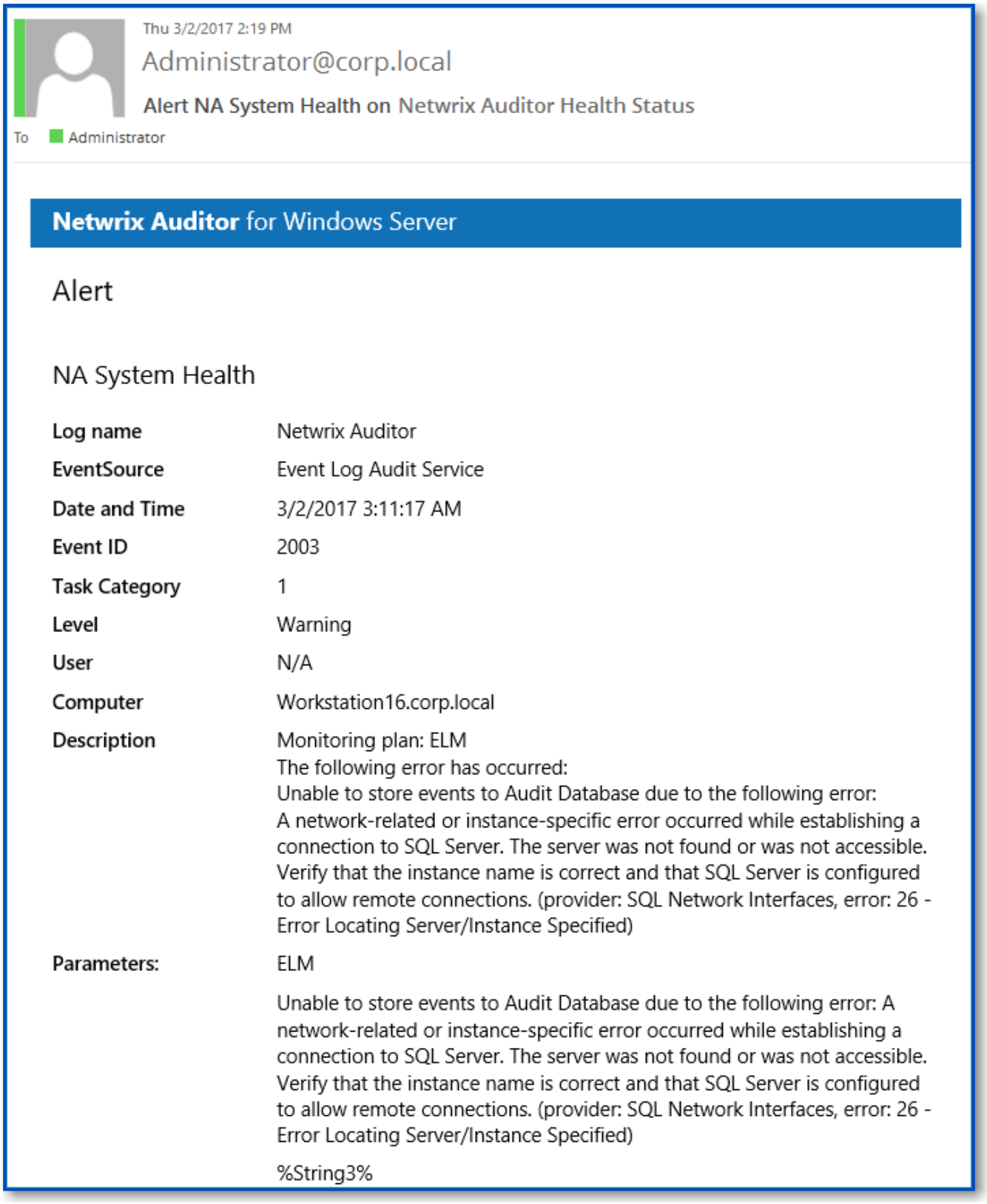
Step 9 – Click OK to save the changes and close the Event Filters dialog.

Step 10 – In the Netwrix Auditor Event Log Manager wizard, navigate to the Notifications section and specify the email address where notifications will be delivered.

RECOMMENDED: click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

Step 11 – In the Audit Archiving filters, select the Netwrix Auditor System Health as the inclusive filter.

Step 12 – Click Save to save your changes.



Thu 3/2/2017 2:19 PM

Administrator@corp.local

Alert NA System Health on Netwrix Auditor Health Status

To Administrator

Netwrix Auditor for Windows Server

Alert

NA System Health

Log name	Netwrix Auditor
EventSource	Event Log Audit Service
Date and Time	3/2/2017 3:11:17 AM
Event ID	2003
Task Category	1
Level	Warning
User	N/A
Computer	Workstation16.corp.local
Description	Monitoring plan: ELM The following error has occurred: Unable to store events to Audit Database due to the following error: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error: 26 - Error Locating Server/Instance Specified)
Parameters:	ELM Unable to store events to Audit Database due to the following error: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error: 26 - Error Locating Server/Instance Specified) %String3%

If an event occurs that triggers an alert, an email notification will be sent immediately to the specified recipients.

Manage Alerts

For your convenience, Netwrix provides you with a set of predefined alerts that are commonly used for IT infrastructure monitoring. The out-of-the-box alerts include those that help you detect suspicious activity and inform you on critical changes to your environment. The alerts contain pre-configured filters and in most cases you only need to enable an alert and select who will receive notifications.

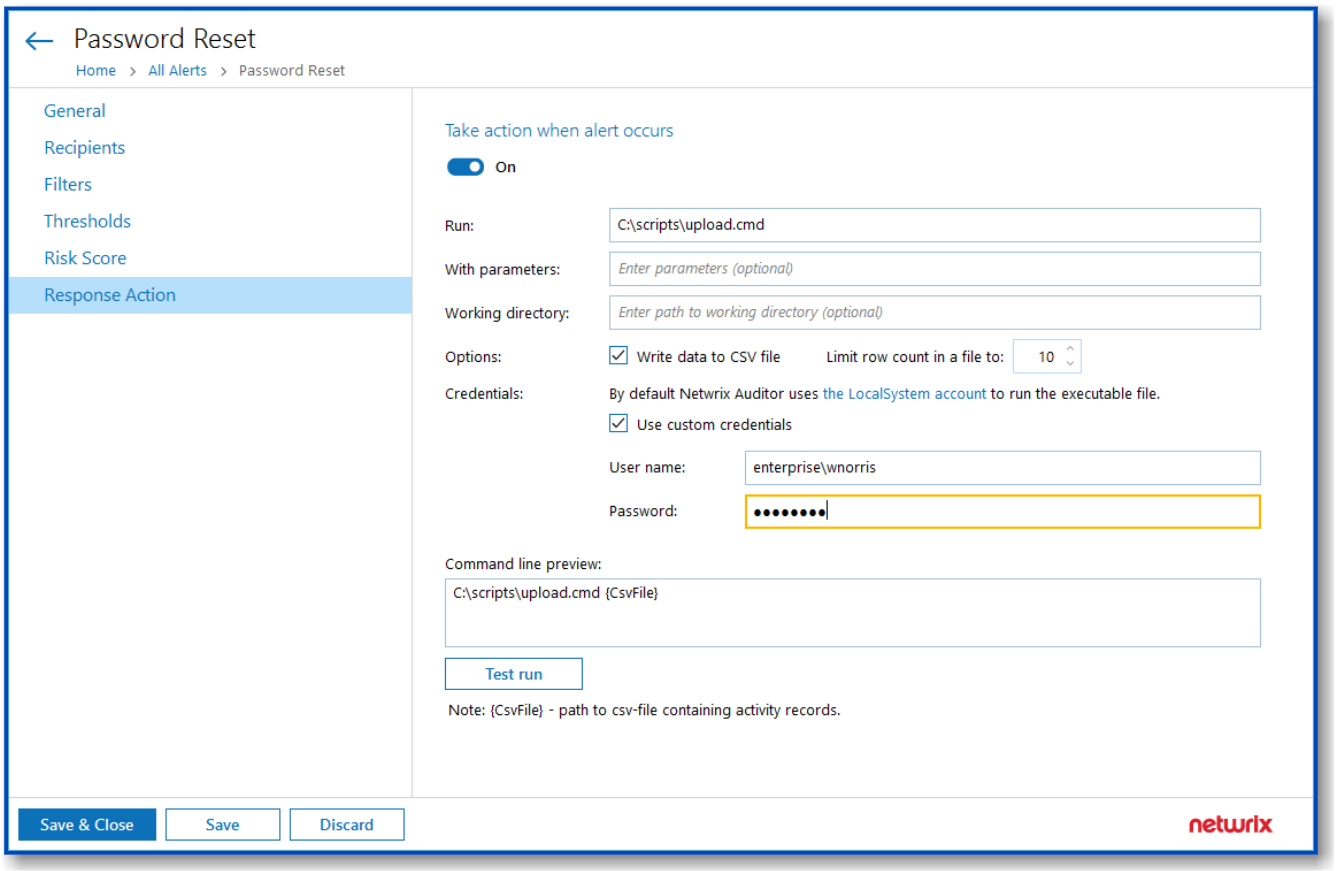
You can add any elements (a dashboard, report, alert, risk, etc.) to the Auditor Home screen to access them instantly. See the Navigation and Customize Home Screen topics for additional information.

To...	Follow the steps...
Enable / disable an existing alert	**Step 1 –** Select an alert from the list and enable it using the slider in the Mode column. **Step 2 –** Double-click the selected alert and specify alert recipients or set a risk score want to include an alert in Behavior Anomalies assessment. You can go on with a score suggested by Netwrix industry experts or fine-tune it to fit your organization's priorities. See the Risk Score topic for additional information on how to configure scoring settings. **Step 3 –** Review and update filters. For some alerts you should provide filter values, such as group name or user.
Modify an existing alert	Select an alert from the list and click Edit.
Create a new alert from existing	Select an alert from the list and click Duplicate at the bottom of the window.
Remove an alert	Select an alert from the list and click  in the right pane.

To...	Follow the steps...
Find an alert	Use the Filter by tags option to find an alert by tags associated with this alert. *OR* Use a search bar in the upper part of All Alerts window to find an alert by its name or tag.

Configure a Response Action for Alert

Upon the alert triggering, you can instruct Auditor to perform several actions such as run a command, a script or other executable file that will perform a remediation action, open a ticket with the organization help desk, etc.



Response Action settings contain the following configuration options:

- Take action when alert occurs - Toggle this setting to **On** to enable alert responses
- Run – Indicates the location of the script file you want to run as your response action
- With parameters – If your script contains parameters, specify them here
- Working directory – If you need to specify a working directory for your script to perform the operation, insert the path here
- Write data to CSV file – If this checkbox is selected, Netwrix Auditor will save activity records in a CSV file. You can use it to pass information into your response action to receive a more targeted response.
- Limit row count in a file to – Select the desired number of rows you want for the file
- Use custom credentials – Enter the username and password if you want the script to be run as an account different from LocalSystem
- Command line preview – Showing a preview of the command line script. Click **Test run** button to test its performance.

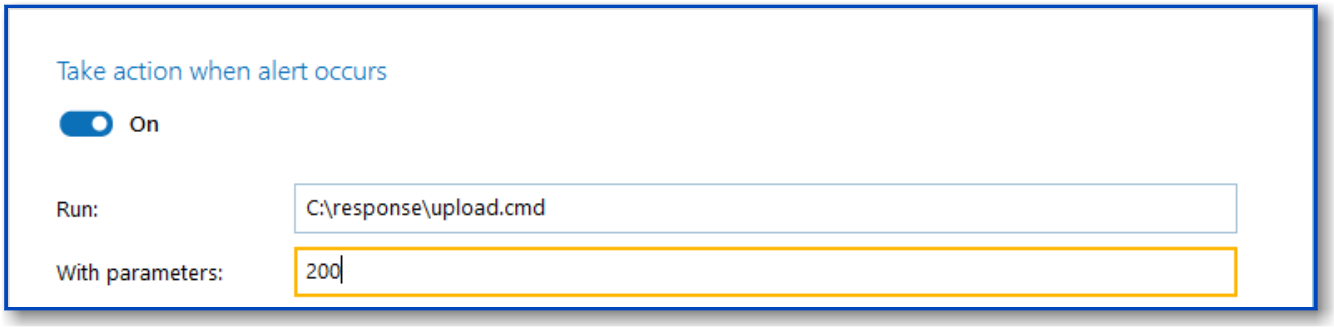
Follow the steps to configure the required settings in the Response Action tab of the alert properties.

Step 1 – Turn the switch to On if you want a response action to be taken when the alert occurs.

Step 2 – In the Run field, specify the path to the executable file (*.exe*, *.cmd*, *.bat*; for *.ps1* files see step 3 below). The file must be located on the machine where Netwrix Auditor server runs.

Step 3 – In the With parameters field, enter the parameters to be used by the executable file. Use space character as a separator.

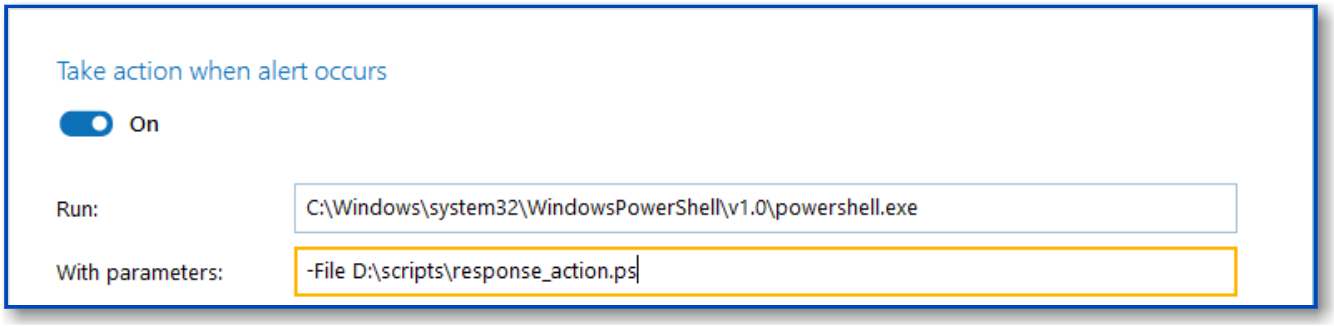
Step 4 – To run *.exe*, *.cmd* and *.bat* files, you can enter the path to your command-line or batch file directly in the Run field, for example:



To run the *.ps1* files, you will need to enter the path to *powershell.exe* and path to your script. For example:

- In the Run field, enter *C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe*

- In the With parameters field, enter `-File <path_to_your_ps_script>`



Unless you select to Write data to CSV file, Auditor will also pass the following parameters to the command line:

- *AlertID* — alert ID
- *RecordID* — ID of the activity record that triggered the alert

Selecting Write data to CSV file will change this behavior, as described in the Configure a Response Action for Alert section below.

Step 5 – In the Working directory field, specify path to the working directory of the executable file on NAuditor server.

Step 6 – In the Working directory field, specify path to the working directory of the executable file on NAuditor server.

If you leave this field empty, then the path to the file specified in the Run field will be used as a working directory. As shown in the example with the *.ps* file, this may be the system directory. So, to avoid system directory cluttering, it is recommended not to leave the Working directory field empty but to explicitly specify the directory where your executable file is located, or a dedicated directory for that purpose. In the latter case, make sure the directory exists on Auditor server.

Step 7 – Write data to CSV file — select this option if you want Auditor to locate the activity records associated with the alert, and write the record fields and their values in a structured way to a *.csv* file. For each new alert being created, this option is selected by default, as well as for the predefined alerts installed with Auditor.

After the upgrade, all alerts with previously configured response action will have this option cleared.

Step 8 – Limit row count in a file to <N> — limit the number of rows (activity records) to be written to a single *.csv* file. Enter a value from *1* to *1000*.

Learn more about how these options work in the Configure a Response Action for Alert section.

By default, the executable file will be launched under the *LocalSystem* account. If you want to use another account, select the Use custom credentials checkbox and specify user name and password. Make sure this account has **Log on as batch job** privilege.

The resulting command line including executable file name and execution parameters will appear in the Command line preview.

If you selected to **Write data to CSV file**, the command line will include *{CsvFile}*, i.e. the file path. Alternatively, the command line will include *{AlertID}* and *{RecordID}*, i.e. related IDs

Step 9 – Test run — if you click this button, the executable file will be run with the specified parameters on Netwrix Auditor server. This can be helpful, for example, if you want to ensure script operability before the related alert is triggered.

As there is no actual alert triggering in this case, sample alert ID and sample activity record ID will be passed to the executable file. If you selected to write data to CSV file, a sample file will be created and populated with these sample IDs.

To be able to perform the test run, current user account (logged on to Auditor client) must have local Administrator privileges on Auditor server where the executable file is located.

After the test run, you will get a notification message with the exit code. Typical values are as follows:

- **0** — the response action completed successfully
- Any other value — the response action was not a success

RECOMMENDED: Apply similar logic if you plan to use custom exit codes in your response action script.

Same exit codes will be returned by response action regular runs.

If the action is not a success (exit code is not 0), the program will try to perform response action again (up to 200 times) with increasing time interval.

Write Data to a CSV File

To pass certain activity record fields to the executable file, you can instruct the program to write the fields and their values in a structured way to a CSV file.

Here is an example of a CSV file structure:

Alert ID	"Record ID"	"Alert name"	"Alert description"	"Action"	"Object type"	"Data source"	"What"	"Where"	"Who"	"When"	"Monitoring plan"	"Item"	"Workstation"	"MAC"	"Details"
"2442f87a-f74d-4f86-b1b1-9cc9726f18c0"	"20190312133449522724508ECC4C84250A62601EA4BBA74F5"	"My alert"	""	"Added"	"alert test"	"Netwrix API"	"what"	"Where"	"Me"	"131968712840000000"	""Monitoring plan 8 API"	"Item (integration)"	""	""	"Property changed from "15" to "80""

The number of activity records retrieved per every response action launch will be only limited by user (see below for details). If the number of records associated with the alert exceeds this limit, the program will create multiple CSV files, storing data in chunks.

For example, if there are 50 records associated with the alert (e.g., "*Scanning threat is detected on network device*" alert), and the number of records for one CSV is set to 10, the program will create 5 CSV files, with 10 records in each chunk. Also notice that the response action will be launched once for every such chunk (5 times in this example), and will retrieve multiple activity records per launch (not more than the specified limit, i.e. 10 records in this example).

A CSV file is named using the timestamp and GUID and stored in the subfolder of Netwrix Auditor working folder (by default, *%ProgramData%\Netwrix Auditor\AuditCore\AuditArchive\AlertsToolLauncher\Csv*). Note that a CSV file will exist only while the executable file is running – after the execution is completed, the CSV file will be deleted. So if you plan, for example, to obtain some data from that file for further processing, you may need to copy it to a permanent location in a timely manner, e.g., using a script.

Behavior Anomalies

Netwrix Auditor enables you to detect behavior anomalies in your IT environment, such as activity surges or mass deletions of archived data. As you investigate suspicious activity and review incidents, you can identify intruders or in-house bad actors who keep violating your company's security policies.

The behavior anomalies assessment extends the alerting functionality and provides both a high-level visualization and a detailed history of malicious user activity. While alerts notify you on a single or repetitive action almost immediately, the Behavior Anomalies dashboard accumulates this data over time and thus gives you the bird's eye view of activity patterns. With Behavior Anomalies, you can step beyond individual actions and investigate more complicated user behavior scenarios that might otherwise stay concealed for a long time.

On a high level, your behavior anomalies assessment workflow can be described as follows:

1. You create alerts on threat patterns specific to your company. You include these alerts in Behavior Anomalies assessment and associate a risk score with each alert. The score, that is between 1 and 100 points, reflects how critical the action is for your organization. Risk Scorehow to set a risk score for an alert.

   Although Netwrix industry experts suggest risk scores for alerts that are provided out-of-the-box, you can easily tailor these scores to your organization needs and priorities. You

can always adjust risk scores over time as you become more aware of behavior patterns and anomalous actions in your environment.

2. Each action that provokes an alert is treated as anomaly. Once the anomaly is detected, it appears on a dashboard's timeline and its risk score is added to the user's total score.
3. Every now and then, you review the Behavior Anomalies dashboard—the risk score timeline with anomaly surges, and the most active users. The general rule of thumb is: the more risk score points the user has the more he or she merits your attention. Review Behavior Anomalies Dashboard
4. To learn more about user activity, you can drill-down to a user profile to review all alerts provoked by this user. As you review anomalies and mitigate risks, the user's total score reduces. Review User Profiles and Process Anomalies

The purpose of the dashboard is to keep risks low and help you spot and address issues as they occur. The risk score assigned to a user does not qualify him or her as a bad actor but rather brings your attention to behavior patterns. Depending on the role in your organization, users might have different safe levels while you should make your priority to review the anomalies on time, stay focused, and proactively mitigate risks.

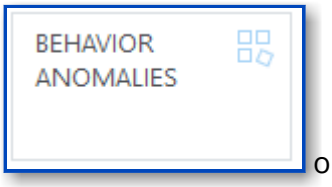
Using Behavior Anomaly Discovery page on Netwrix website.

Review Behavior Anomalies Dashboard

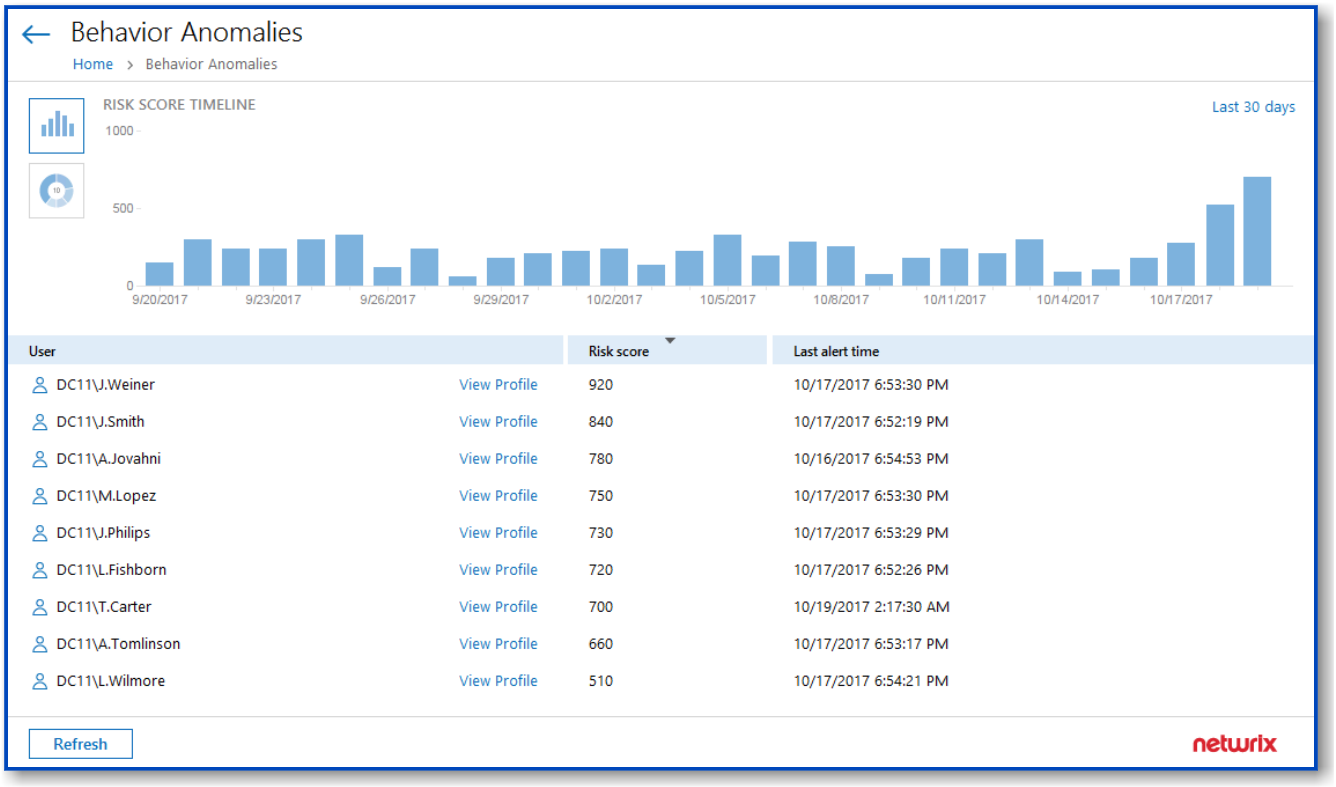
To review the Behavior Anomalies dashboard, process and filter anomalies in user profiles, you must be assigned the Global administrator or Global reviewer role in the product. See the Role-Based Access and Delegation topic for additional information.

You can add any elements (a dashboard, report, alert, risk, etc.) to the Auditor Home screen to access them instantly. See the Navigation and Customize Home Screen topics for additional information.

To review the Behavior Anomalies dashboard:

On the main Auditor page, click 

on the left.



The dashboards includes the following sections:

- The Risk score timeline that helps you review anomaly surges over time.
- The Risk score by top five users chart that helps you identify the most active users. To see the chart, click the pie chart icon in the upper left corner of the page.
- The user list with all users who provoked alerts and their total risk scores.

Once you reviewed the general anomaly trend and identified users that merit your special attention, review their profiles and process anomalies. Click View Profile next to a user name to dive into user activity and investigate each action in details. Review User Profiles and Process Anomalies

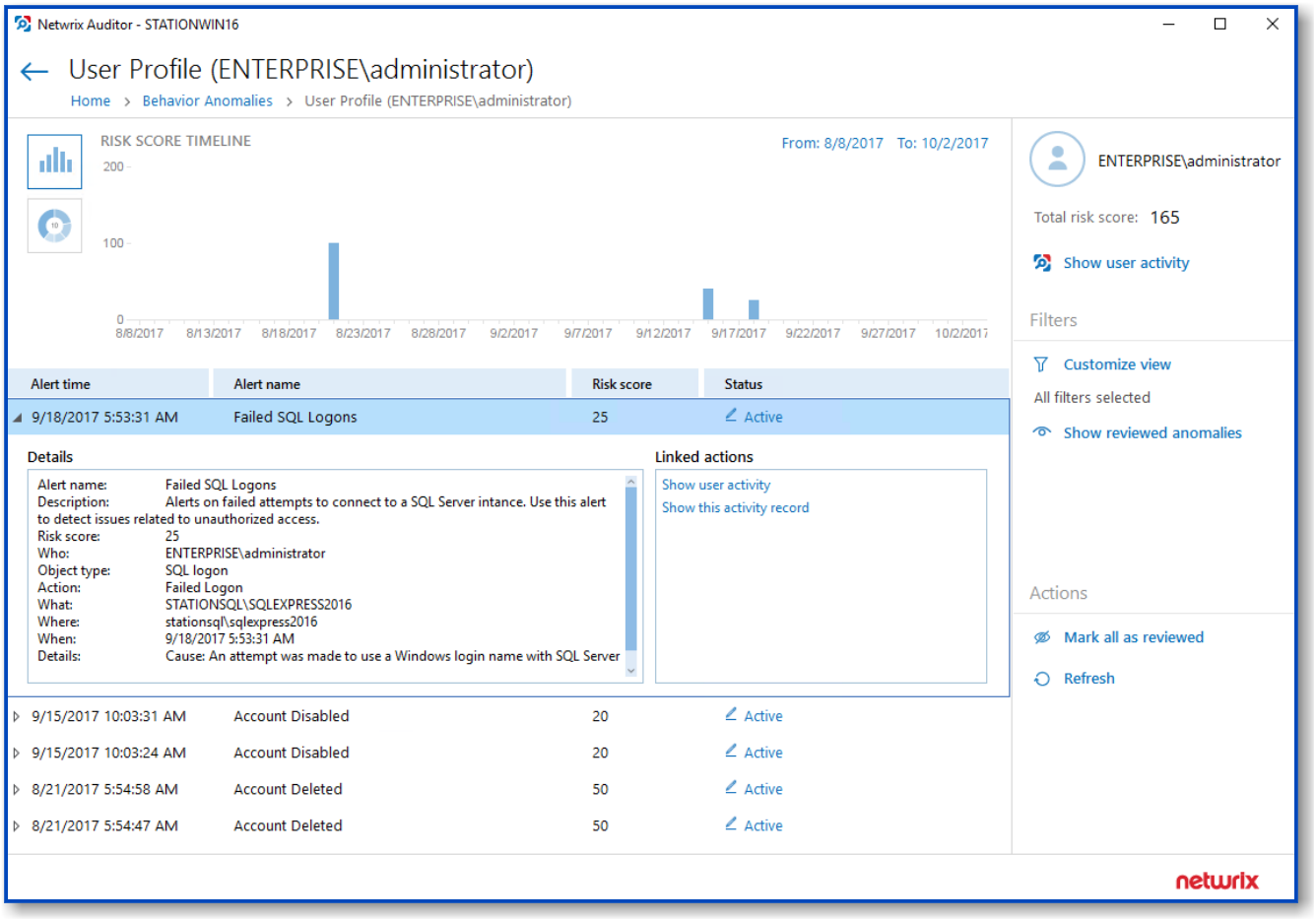
Review User Profiles and Process Anomalies

Review User Profiles and Process Anomalies

The user profile enables you to investigate user behavior and take a closer look at anomalies.

To view a user profile

- On the Behavior Anomalies assessment dashboard, locate a user and click View Profile next to his or her name.



The user profile page contains the following sections:

- User data with the name and the total risk score. Click Show user activity below the total risk score, to launch the Interactive Search in a new window. Use it to see all user actions, including those that were not treated as anomalies.
- The Risk score timeline that demonstrates anomalous activity surges. Modify the timeframe to narrow down the results.
- The Risk score by top five alerts chart that outlines the most frequent anomalies provoked by user. To see the chart, click the pie chart icon in the upper left corner of the page.

- The anomalies list displays details for each anomaly: the alert that was triggered, the date and time, the risk score and anomaly status.

  Double-click an entry to see more details: who did what, when and where the action was made, etc. Navigate to Linked actions and click Show user activity or Show this activity record to invoke Interactive Search and see all user actions or a specific action correspondingly.

Netwrix Auditor shows only the top 2,000 anomalies. Modify the timeframe or hide reviewed anomalies, and then click Refresh to see more anomalies.

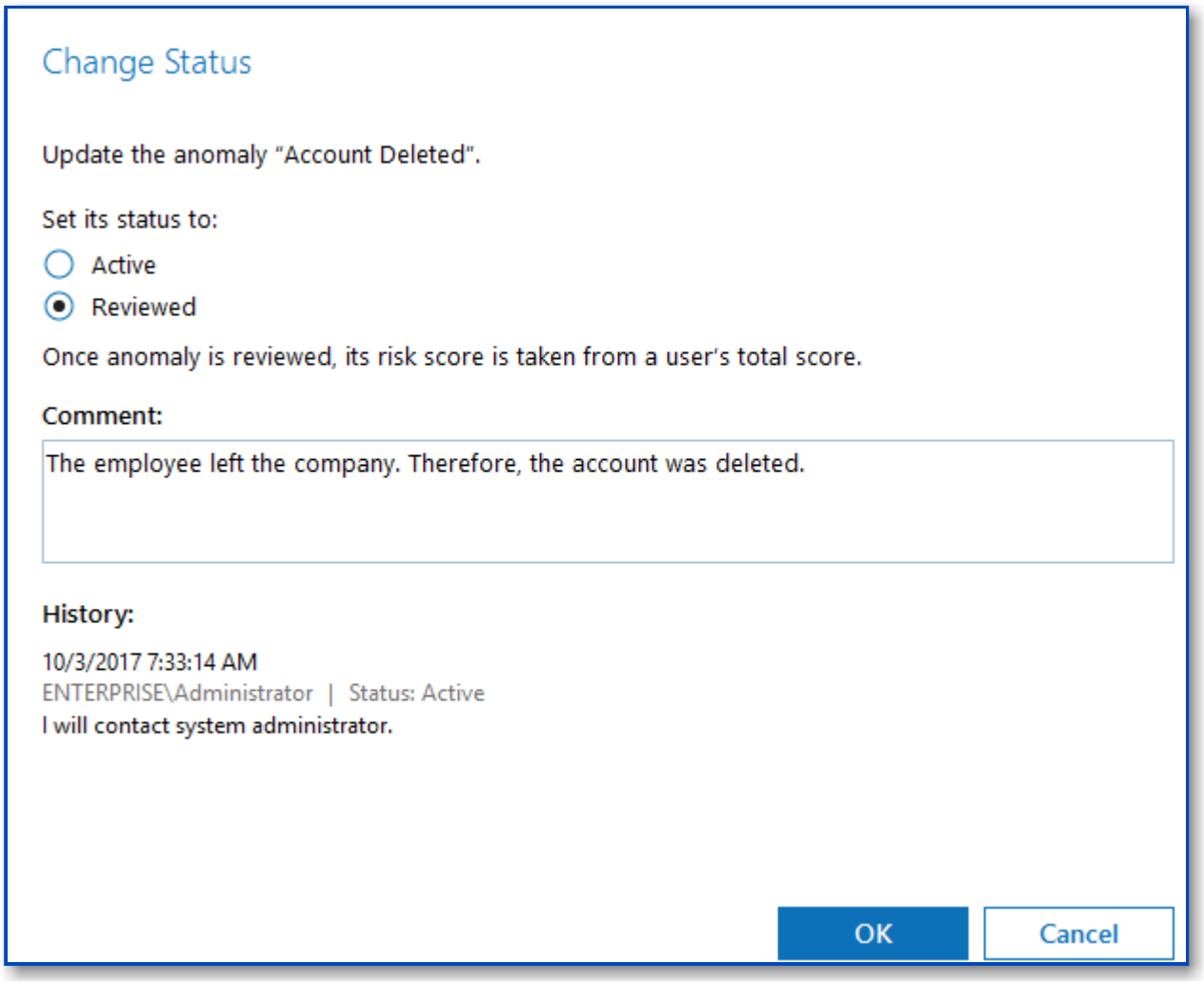
Process Anomalies and Reduce Risk Score

By default, the anomaly status is active and it indicates that the incident still requires some examination or is kept for further investigation. As you inspect anomalies and respond to threats, update statuses and add comments.

To change an anomaly status

1. Specify an anomaly from the list and click the Active link in the Status column.
2. In the Change Status dialog, set the status to *"reviewed"* and provide a justification.

   You can add comments without changing a status. This might be helpful if the anomaly remains active for a long period of time and you need even more time to examine it closely.



Once the anomaly is reviewed, it disappears from the timeline and chart, and its associated risk score is taken from user's total score. The reviewed anomalies supplement the status with the reviewer name and date (e.g., *Reviewed by CORP\Administrator (10/02/2017 10:12:03 AM)*).

You can always revert changes and assign the Active status back.

To process all anomalies

- In the Actions section, select Mark all as reviewed.

In this case, all anomalies that are currently in view will be set to *"reviewed"*. Perform this operation only with a proper justification. Since Netwrix Auditor shows only the top 2,000 anomalies, make sure to click Refresh to check if there are more anomalies to be reviewed.

The anomalies that are excluded from view by filters are not affected by the Mark all as reviewed action.

Customize Anomalies List

By default, all anomalies are in view. The Filters section helps you show or hide anomalies.

Click Customize view and clear the checkboxes next to alert names, if you do not want to see anomalies associated with them.

When you hide an alert from view, its associated anomalies will no longer be displayed on a timeline, chart, or in the list but the user total score will remain unchanged. Note that hidden anomalies cannot be reviewed in bulk with the Mark all as reviewed action.

Hide reviewed anomalies enables you to modify the anomalies list so that you can focus on active anomalies only. To see reviewed anomalies, click Show reviewed anomalies.

Behavior Anomalies Assessment Tips and Tricks

This topic contains various frequently asked questions as well as tips and tricks you might find helpful when configuring scoring settings and reviewing behavior anomalies.

- The user has a high score and keeps provoking same alerts almost every day.

  Drill-down to the user profile and then click Show user activity. Review user actions and compare them to his or her job responsibilities. Does the user seem trustworthy? Are there any rights elevation or suspicious access attempts?

Try to review user tasks—you may find out that the anomaly the user keeps provoking is a genuine part of his or her daily routine. For example, the office staff should not reset passwords for other accounts while this is a basic task for a system administrator. In this case, review your alert settings and exclude the user from the alert filters.

- Everyone in organization has a huge score

  Probably, you have configured too many alerts that turn behavior anomalies assessment into mess. It takes some time to learn what matters most to your organization and get accustomed to setting proper risk scores. Try to review your scoring settings regularly and adjust them when necessary.

- Is anyone who is charge of "Failed..." anomaly a bad actor?

  Anyone can forget a password or accidentally try to access some data in a wrong folder. Such users are not subject to immediate prosecution unless they do not provoke repetitive alerts. The best practice is to review user profile after some time and check if there are any threat patterns in user behavior.

IT Risk Assessment Overview

To help you identify configuration gaps in your environment and understand their impact on overall security, Netwrix Auditor offers a dashboard with a number of metrics and drill-down reports on IT risk assessment. They pinpoint the weak points in your IT infrastructure such as overly broad assignment of access rights, loose password policies, and stale accounts. This information will help you to take corrective measures in the required area, ensuring the IT risks stay in the safe zone.

Risk assessment dashboard can be accessed by clicking the Risk assessment tile in the main window of Netwrix Auditor. For details about using the dashboard, see IT Risk Assessment Dashboard.

For details about metrics calculation, see How Risk Levels Are Estimated .

Providing Data for Risk Assessment

To provide data for metrics and reports that belong to different categories, you will need to configure monitoring plans that will process related data sources. These monitoring plans should have at least one item added. See the following table for the certain reports:

Category	Report name	Collect data from
Users and Computers	User accounts with "Password never expires"	AD domain
	User accounts with "Password not required"	AD domain
	Disabled computer accounts	AD domain
	Inactive user accounts	AD domain
	Inactive computer accounts	AD domain
	Servers with Guest account enabled	Windows Server
	Servers that have local user accounts with "Password never expires"	Windows Server
Permissions	User accounts with administrative permissions	AD domain
	Administrative groups	AD domain
	Administrative group membership sprawl	Windows Server
	Empty security group	AD domain
	Site collections with the "Get a link" feature enabled	SharePoint farm

Category	Report name	Collect data from
	Sites with the "Anonymous access" feature enabled	SharePoint farm
	Site collections with broken inheritance	SharePoint farm
	Sites with broken inheritance	SharePoint farm
Data	Files and folders accessible by Everyone	Windows File Server
	Sensitive data shared with Everyone *	Windows File Server
	File and folder names containing sensitive data	Windows File Server
	Potentially harmful files on file shares	Windows File Server
	Direct permissions on files and folders	Windows File Server
	Direct permissions to sensitive files *	Windows File Server
	Documents and list items accessible by Everyone and Authenticated Users	SharePoint farm
	Files shared with external users	Windows File Server
	Files shared with anonymous users	Windows File Server
	Documents and list items accessible by Everyone	Windows File Server
	Files that can be modified by external users or anonymous users	Windows File Server
Infrastructure	Servers with inappropriate operating systems	Windows Server

Category	Report name	Collect data from
	Servers with under-governed Windows Update configurations	Windows Server
	Servers with unauthorized antivirus software	Windows Server

NOTE: Risks marked with (*) require both pre-configured NDC SQL database connection and NDC API connection. To check configuration status, go to Settings > Sensitive Data Discovery. See Sensitive Data Discovery for more information.

NOTE: Right after setting up the integration the drill down reports might be empty, while the risk indicator is already completed. Please wait until Auditor gets all the information from Netwrix Data Classification it needs.

Required Monitoring Plan Settings

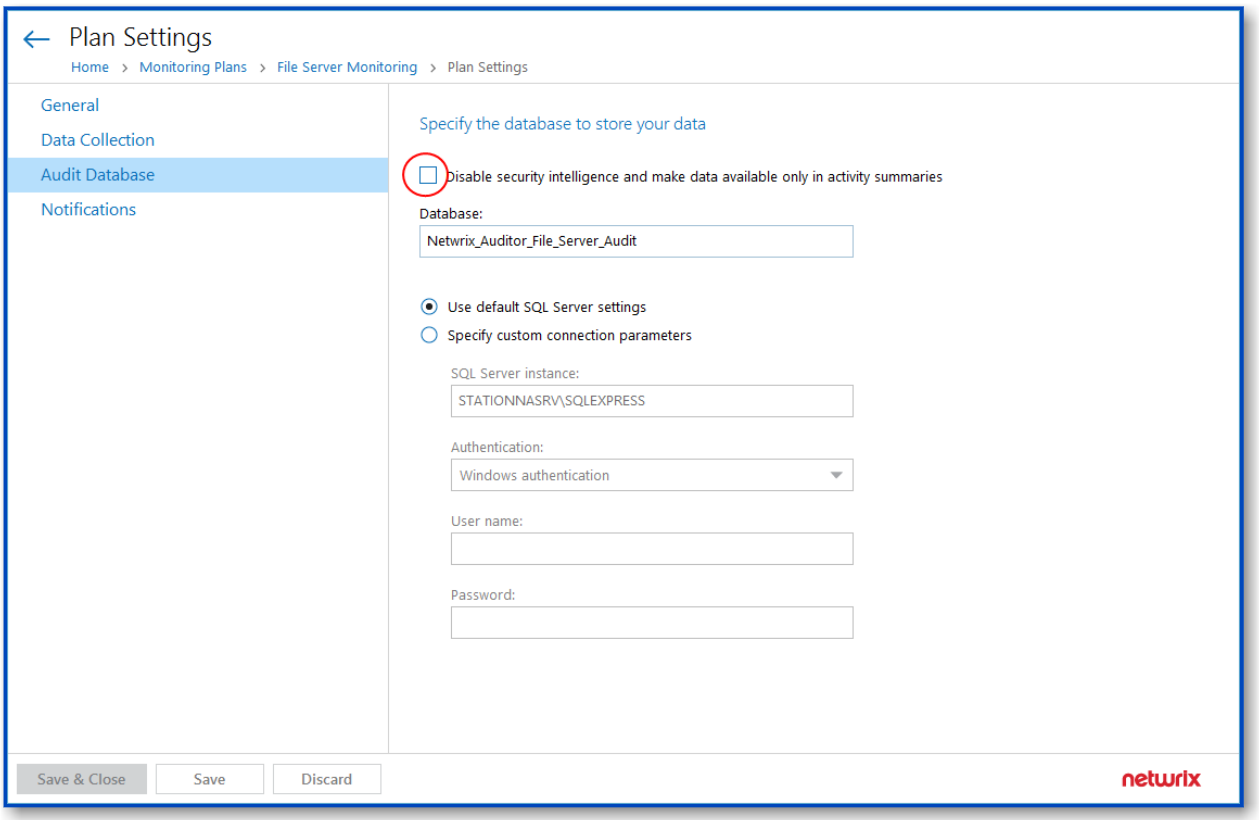
To provide data needed for risk assessment, the related monitoring plan must be set up to store data to the audit database.

Also, consider that all risk metrics and related reports require state-in-time data to be collected. You can select the relevant option when creating a new monitoring plan, as described in the Create a New Monitoring Plan section. For the exising plan, refer to the procedure below.

To verify the necessary settings of the existing plan

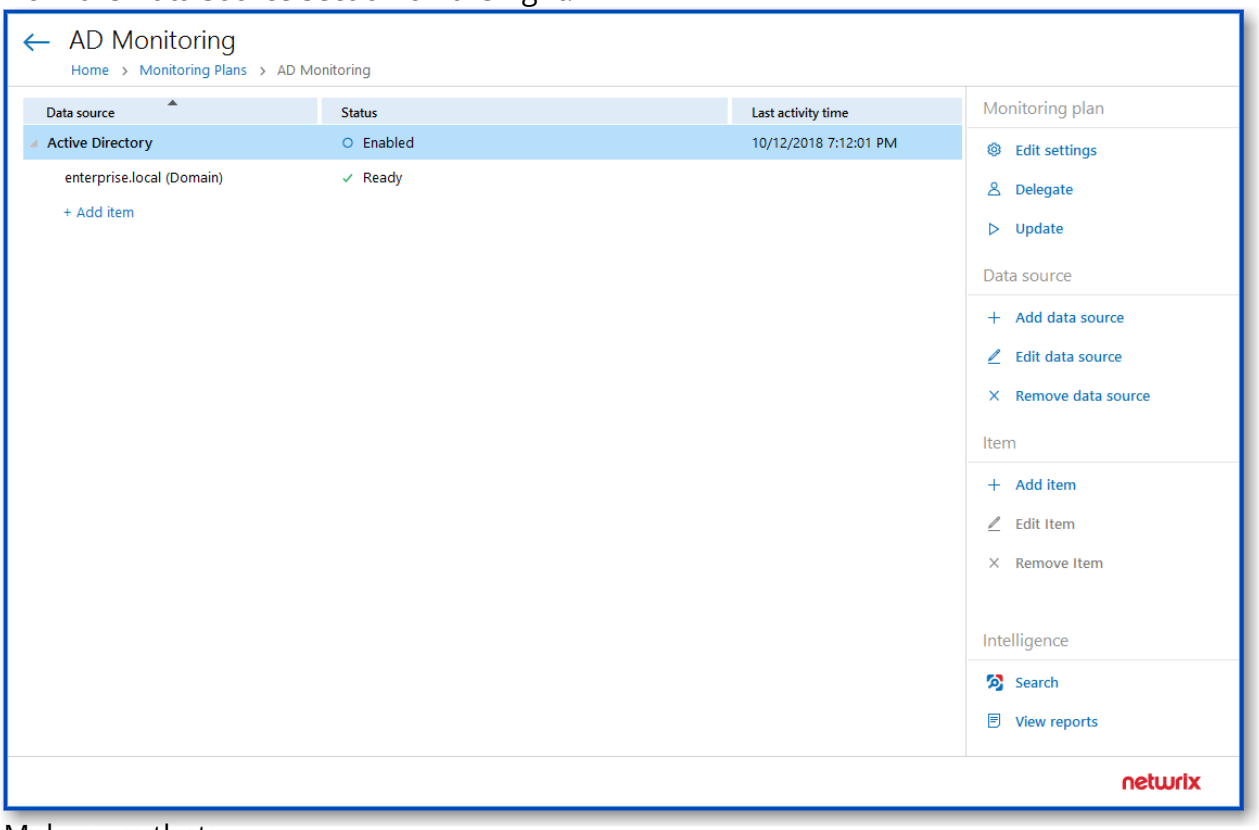
1. Select the monitoring plan you need and click the **Edit** button.
2. In the right pane of the dialog displayed, select Edit settings from the Monitoring plan section.
3. Go to the Audit Database section and make sure that Disable security intelligence ... checkbox is cleared. This will instruct Netwrix Auditor to store data to both Long-Term

Archive and audit database:

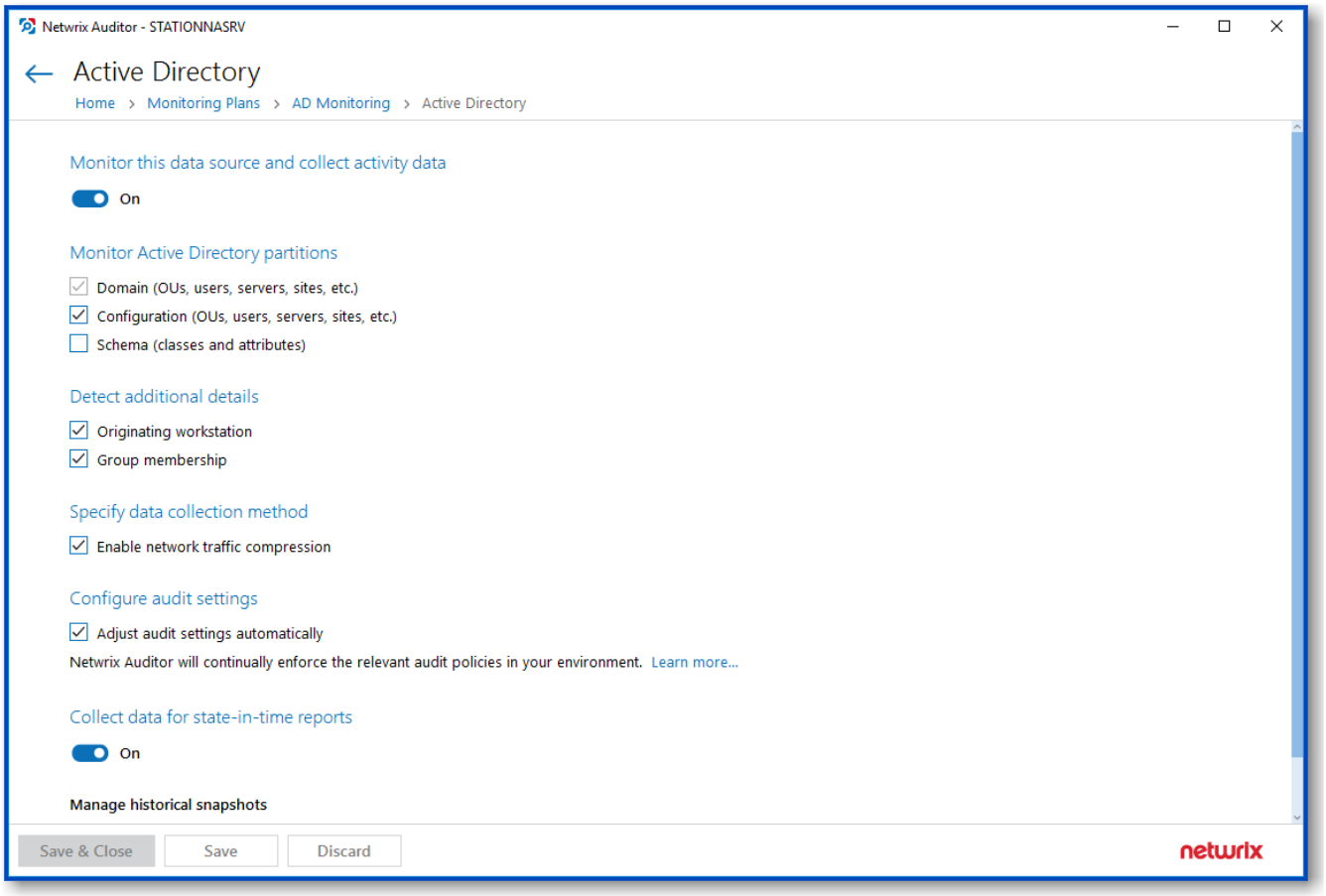


4. Save the settings and return to the window with the monitoring plan details. Make sure you have at least one monitored item in the plan. If necessary, add an item.

5. Select the data source you need (for example, Active Directory) and click Edit data source from the Data source section on the right.



6. Make sure that:
    1. Monitor this data source and collect activity data is switched ON.
    2. Collect data for state-in-time reports is switched ON.
7. Save the settings and close the dialog.



IT Risk Assessment Dashboard

To access the Risk Assessment dashboard, click the corresponding tile in the main window.

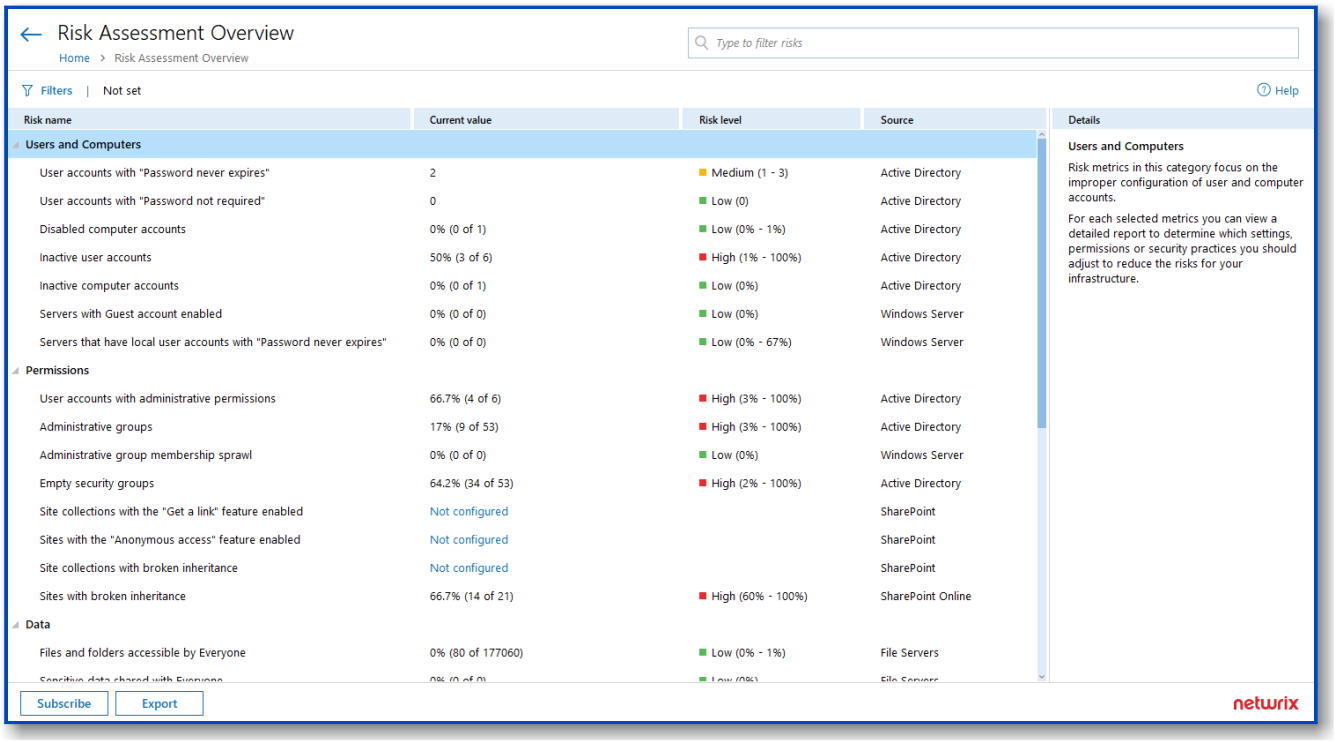
You can add any elements (a dashboard, report, alert, risk, etc.) to the Auditor Home screen to access them instantly. See the Navigation and Customize Home Screen topics for additional information.

The IT risks are grouped into the following categories:

- Users and Computers
- Permissions
- Data
- Infrastructure

Within each category there are several key metrics identified by Netwrix industry experts who also suggested formulas for calculating metrics values. Risks are assessed against these metrics and displayed with the color indicators in accordance with the level:

- High — red
- Medium — yellow
- Low — green



After reviewing general risks assessment results in each category, you can drill-down to details covered in the underlying report. To do so, double-click the selected metric or use the View Report button.

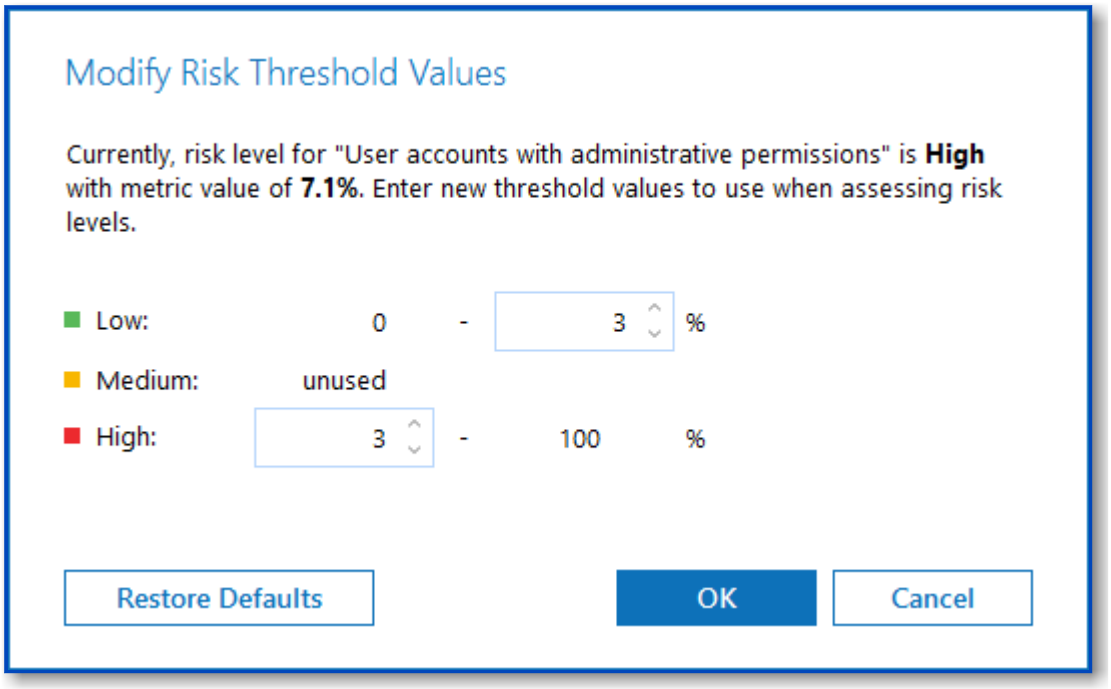
Customizing Metrics for Your Organization

Default threshold values for risk levels are set in accordance with recommendations of Netwrixindustry experts, as described in the How Risk Levels Are Estimated topic. They can be, however, easily customized to reflect your organization's internal security policies and standards. Follow the steps to customize the metrics.

Step 1 – In the dashboard pane, select the metric you need and in the **Actions** section on the right click Modify thresholds.

Step 2 – In the displayed dialog, specify new threshold values for risk levels.

Step 3 – Click OK to save the settings and close the dialog.



Also, for several metrics the Customize risk indicators command is available.

For metric...	Use Customize risk indicators command to...
File and folder names containing sensitive data	Edit the list of words you consider to be indicators of sensitive content if detected in the file or folder name.
Potentially harmful files on file shares	Edit the list of extensions you consider to be indicators of potentially harmful files detected in the file share.
Servers with inappropriate operating systems	Edit the whitelist of permitted OS versions. Any other OS version will be considered a risk factor.
Servers with unauthorized antivirus software	Edit the whitelist of permitted antivirus tools. Any other antivirus will be considered a risk factor.

For metric...	Use Customize risk indicators command to...
Administrative group membership sprawl	Edit the whitelist of permitted accounts that can be the members of local administrative groups. Any other account will be considered a risk factor.

New settings will be applied/risk level thresholds will be refreshed after the next data collection session.

Delivering Assessment Results as a File

You can create a subscription to periodically receive IT risk assessment results by email or using a file share. For that, in the dashboard window click Subscribe and configure the necessary settings. See the Create Subscriptions topic for additional information.

You can also save current results to a PDF file by using the Export button in the dashboard window.

How Risk Levels Are Estimated

As mentioned, dashboard and built-in reports give you a bird's eye view of the following high-risk areas:

- User and computer accounts
- Permissions
- Data
- Infrastructure

Within each area, Netwrix Auditor industry experts identified risk categories and suggested guidelines for them. For example, if the number of administrative accounts in your organization is less than 2%, the risk should be considered insufficient. If the value is between 2% and 3%, the risk is moderate, while any value that exceeds 3% should be considered a high risk. These guidelines are based on security best practices and analytical data.

The product compares your environment configuration against these metrics and assigns a risk level to each category. The risk levels in each category determine the overall risk level for the area you review. The following risk levels are used:

Risk level	Color	Comments
Low	Green	Keep monitoring your environment on a regular basic.
Medium	Yellow	Proactively mitigate risks and adjust your workflows before a breach occurs.
High	Red	Respond to the threat as soon as possible.

Calculation formulas for each metric are provided in the table below.

The following signs are used to define risk level intervals and threshold values:

- > —More than, exclusive
- ≥ —This value or more, inclusive
- = —Equals
- < —Less than, exclusive
- ≤ —This value or less, inclusive
- [ ] —Inclusive interval
- ( ) —Exclusive interval
- [ ) or ( ] —Half-closed interval, where 1 value is inclusive and the other is exclusive or vice versa.

Risk	Assessment formula	Default risk level thresholds
Users and computers		
User accounts with "Password never expires"	Number of enabled user accounts with **Password never expires** property set	• 0 — Low • [1 – 5] — Medium • > 5 — High

Risk	Assessment formula	Default risk level thresholds
User accounts with "Password not required"	Number of enabled user accounts with Password not required property set Interdomain trust accounts are excluded from total count.	• 0 — Low • [1 – 2] — Medium • > 2 — High
Disabled computer accounts	Number of disabled computer accounts / Overall number of computer accounts (%)	• ≤ 1% — Low • (1% – 3%) — Medium • ≥ 3% — High
Inactive user accounts	Number of inactive but enabled users / Overall number of enabled user accounts (%)	• 0% — Low • (0% – 1%) — Medium • ≥ 1% — High
Inactive computer accounts	Number of inactive but enabled computer accounts / Overall number of enabled computer accounts (%)	• 0% — Low • (0% – 3%) — Medium • ≥ 3% — High
Servers with Guest account enabled*	Number of servers with enabled Guest account / Overall number of servers (%)	• 0%— Low • (0% - 1%] — Medium • >1% — High
Servers that have local user accounts with Password never expires*	Servers that have local user accounts with Password never expires / Overall number of servers (%)	• 0% — Low • >0% — High
Permissions		
User accounts with administrative permissions	Number of administrative accounts / Overall number of accounts (%)	• ≤ 2%— Low • (2% – 3%) — Medium • ≥ 3% — High

Risk	Assessment formula	Default risk level thresholds
Administrative groups	Number of administrative groups / Overall number of groups (%)	• ≤ 2% — Low • (2% – 3%) — Medium • ≥ 3% — High
Administrative group membership sprawl*	Number of Windows servers whose Local Administrators Group members differ from those specified in the whitelist / Overall number of servers (%)	• 0% — Low • >0% — High
Empty security groups	Number of security groups without members / Overall number of security groups (%)	• ≤ 1% — Low • (1% – 2%) — Medium • ≥ 2% — High
Site collections with the Get a link feature enabled	Number of site collections with the Get a link feature enabled / Total number of site collections (%)	• ≤30% — Low • (30% - 60%) — Medium • ≥60% — High
Sites with the Anonymous access feature enabled	Number of sites with the Anonymous access feature enabled / Total number of sites (%)	• ≤30% — Low • (30% - 60%) — Medium • ≥60% — High
Site collections with broken inheritance	Number of site collections with broken inheritance / Total number of site collections (%)	• ≤30% — Low • (30% - 60%) — Medium • ≥60% — High
Sites with broken inheritance	Number of sites with broken inheritance / Total number of sites (%).	• ≤30% — Low • (30% - 60%) — Medium • ≥60% — High

Risk	Assessment formula	Default risk level thresholds
Data		
Files and folders accessible by Everyone	Files and folders shared with *Everyone* security group /Overall number of shared folders (%)	• ≤ 1% — Low • (1% – 5%) — Medium • ≥ 5% — High
Sensitive data shared with Everyone	Number of sensitive files shared with the security groups "Everyone" and "Authenticated" / Total number of sensitive files (%).	• 0% — Low • (1% – 2%) — Medium • ≥ 2% — High
Sensitive files shared with external users	Number of sensitive files shared with external users / Total number of sensitive files (%). Sharing sensitive data with external users (authenticated users who are not members of your Office 365 organization) may lead to data leaks. To reduce the risk of data leaks and non-compliance, control data sharing to external users.	• ≤ 5% — Low • (5% – 10%) — Medium • ≥ 10% — High
Sensitive files shared with anonymous users	Number of sensitive files shared with anonymous users / Total number of sensitive files (%). Files may be shared with any users outside the Office 365 organization, so that any user with the link can access the file. This may lead to your sensitive content being highly exposed. To reduce the risk of data leaks,	• 0% — Low • (0% – 2%) — Medium • ≥ 2% — High

Risk	Assessment formula	Default risk level thresholds
	control data sharing to anonymous users.	
Sensitive documents accessible by Everyone	Number of sensitive documents accessible by Everyone or similar groups / Total number of sensitive documents (%). Only designated personnel should have access to your sensitive data. Thus, only public data should be accessible by the following predefined Office 365 groups: • Everyone • Everyone Except External Users • All Authenticated Users • All Forms Users • All Users	• 0% — Low • (0% – 5%) — Medium • ≥ 5% — High
File and folder names containing sensitive data	Number of files and folders with names that suggest they contain sensitive data	• 0 — Low • 1 — Medium • > 1 — High
Potentially harmful files on file shares	Number of detected harmful files	• 0 — Low • 1 — Medium • > 1 — High
Direct permissions on files and folders	Number of shared objects with at least one direct permission / Overall number of shared objects (%)	• 0% — Low • (0% – 5%) — Medium • ≥ 5% — High

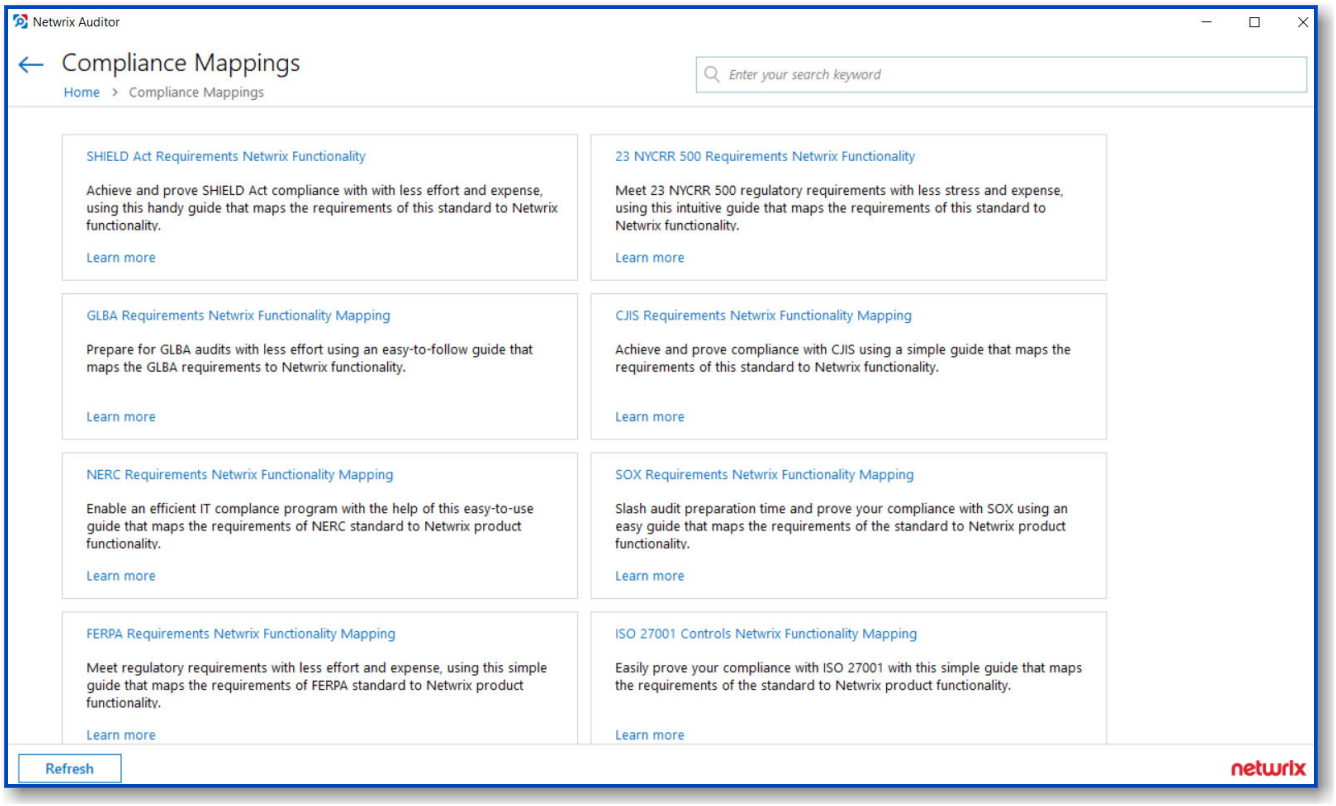
Risk	Assessment formula	Default risk level thresholds
Direct permissions to sensitive files	Number of sensitive files shared with users through direct permissions / Total number of shared files (%).	• 0% — Low • (0% - 3%) — Medium • ≥ 3% — High
Documents and list items accessible by Everyone and Authenticated Users	Number of documents and list items shared with the *Everyone* and *Authenticated Users* groups / Total number of documents and list items (%)	• ≤25% — Low • (25% - 50%) — Medium • ≥50% — High
Files shared with external users	Number of files that have been shared with external users / Total number of files (%).	• ≤ 10% — Low • (10% –25%) — Medium • ≥ 25% — High
Files shared with anonymous users	Number of files that have been shared with anonymous users / Total number of files (%).	• ≤ 5% — Low • (5% – 10%) — Medium • ≥ 10% — High
Documents and list items accessible by Everyone	Number of documents and list items accessible by Everyone or similar groups / Total number of documents and list items (%).	• ≤25% — Low • (25% - 50%) — Medium • ≥50% — High
Files that can be modified by external users or anonymous users	Number of files for which external users or anonymous users have "Edit" permissions / Total number of files (%).	• ≤ 5% — Low • (5% – 10%) — Medium • ≥ 10% — High
Infrastructure		

Risk	Assessment formula	Default risk level thresholds
Servers with inappropriate operating systems*	Number of Windows servers with OS not included in the whitelist / Overall number of servers (%)	• 0% — Low • >0% — High
Servers with under-governed Windows Update configurations*	Number of servers with Windows Update configuration source set to Local Settings AND/OR with auto-update set to Not configured or Disabled / Overall number of servers (%)	• 0% — Low • >0% — Medium
Servers with unauthorized antivirus software*	Number of Windows servers with antivirus tools not included in the whitelist / Overall number of servers (%)	• 0% — Low • >0% — High

* -here the *Overall number of servers* means the number of Windows servers for which data collection was a success. That said, this count may vary across the risks. In such a case, it is recommended to examine Netwrix Auditor health log and omit lists.

Compliance Mappings

This tile contains links to the practical guides on how to comply with different standards using Netwrix Auditor. The guides were prepared by Netwrix industry experts and contain full information about most popular compliance standards. Clicking the 'Learn more...' link under a desired standard opens the page on the Netwrix website. Here you can review a brief description of each compliance standard supported by the product and download E book containing detailed requirements for the standards.



Netwrix Auditor Operations and Health

This topic describes how you can monitor Auditor operations, health and resource usage. See the following topics for additional information:

- Health Status Dashboard
- Self-Audit
- Health Summary Email
- Netwrix Auditor Health Log

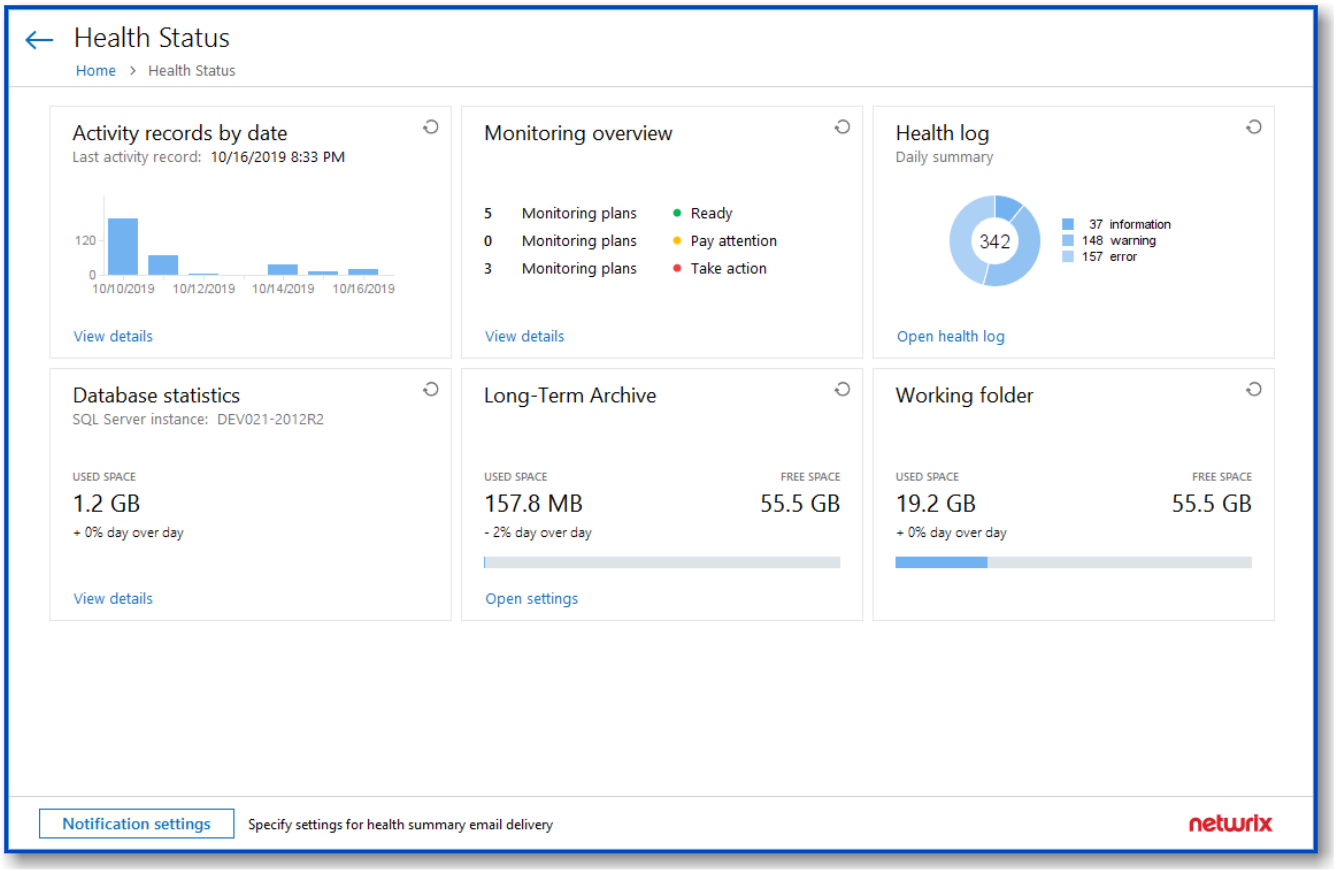
Health Status Dashboard

New Health Status dashboard facilitates Auditor maintenance and troubleshooting tasks, providing IT specialists with at-a-glance view on the most critical factors: data collection performance, product health and storage capacity. The dashboard comprises a set of widgets that display the status of these aspects using aggregated statistics and charts. Nearly each widget allows you to drill down to the detailed information on the aspect you are interested in.

To view the dashboard, on the main Auditor page, click the Health status tile located in the Configuration section.

The dashboard includes the following widgets:

- The Activity records by date chart—Shows the number of activity records produced by your data sources, collected and saved by Netwrix Auditor during the last 7 days. See the Activity Records Statistics topic for additional information.
- The Monitoring overview widget—Shows aggregated statistics on the statuses of all monitoring plans configured in Netwrix Auditor at the moment. See the Monitoring Overview topic for additional information.
- The Health log chart—Shows the statistics on the events written in the Netwrix Auditor health log in the last 24 hours. Click the link in this widget to view the log. See the Netwrix Auditor Health Log topic for additional information.
- The Database statistics widget—Helps you to estimate database capacity on the default SQL Server instance that hosts the product databases. See the Database Statistics topic for additional information.
- The Long-Term Archive widget—Helps you to estimate the capacity of the Long-Term Archive file-based storage. To modify its settings, including location and retention, click the link in this widget. See the System Health topic for additional information.
- The Working Folder widget—Helps you to estimate the capacity of the Auditor working folder used to keep operational information (configuration files of the product components, log files, and other data) on the Auditor Server. See the System Health topic for additional information.

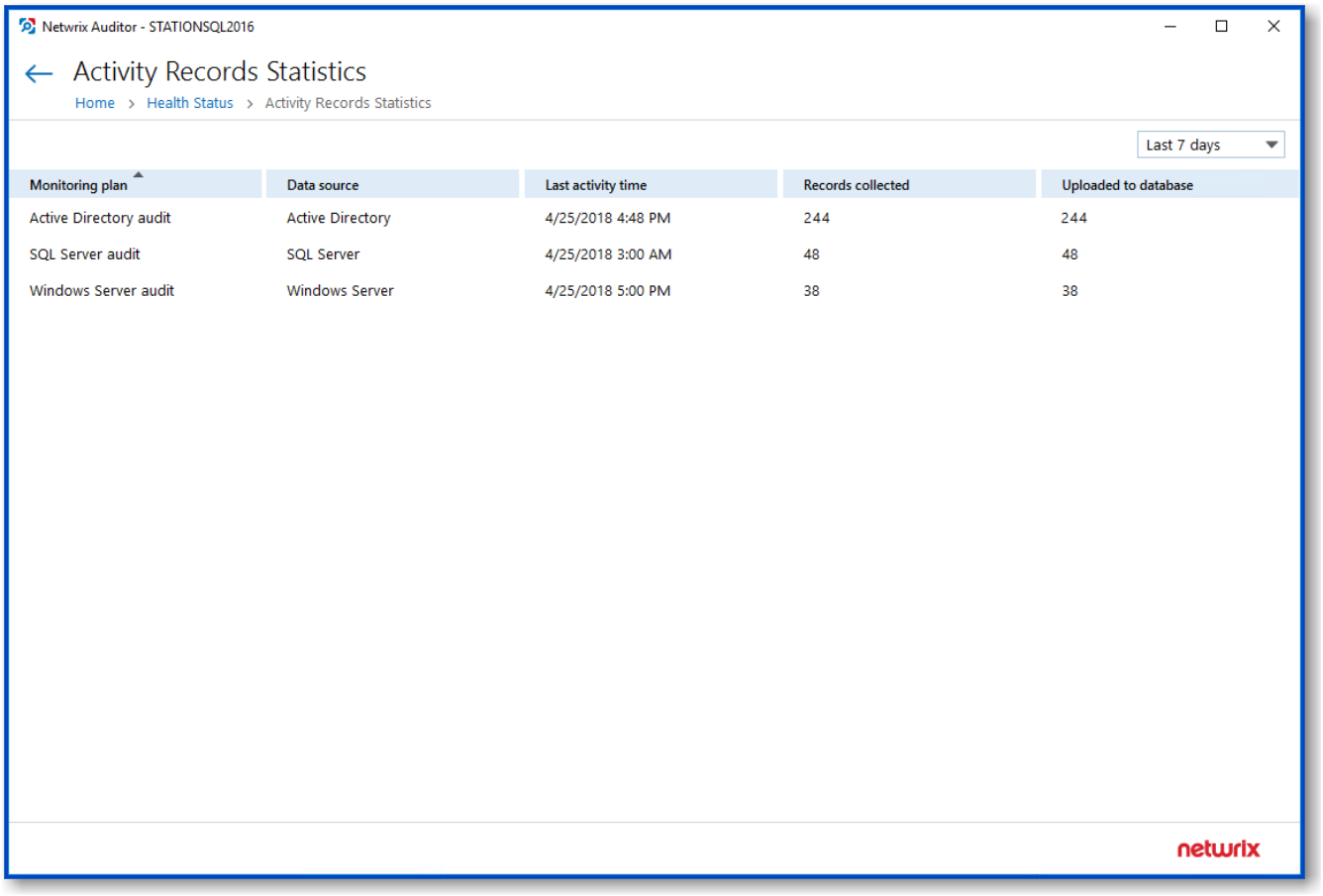


You can also instruct Netwrix Auditor to forward similar statistics as a health summary email to personnel in charge. For that, click Notification settings, then follow the steps described in the Notifications topic.

Activity Records Statistics

Aggregated statistics on the activity records is provided in the Activity records by date widget. The chart shows the number of activity records produced by your data sources, collected and saved by Netwrix Auditor during the last 7 days. This data can help you to assess the activity records generation intensity in your IT infrastructure, and product load.

After you click View details, the Activity Records Statistics window will be displayed.



By default, statistics on activity records processing is grouped by Monitoring plan and presented for the Last 7 days. To modify the timeframe, use the drop-down list in the upper right corner.

Other fields provide the following information: data source that produces activity records, with date and time of the last collected record, and the overall number of records collected and uploaded to the corresponding Audit database during the specified timeframe.

If the data sources processed by a monitoring plan did not produce any activity records during the specified timeframe, this monitoring plan will not appear in the list.

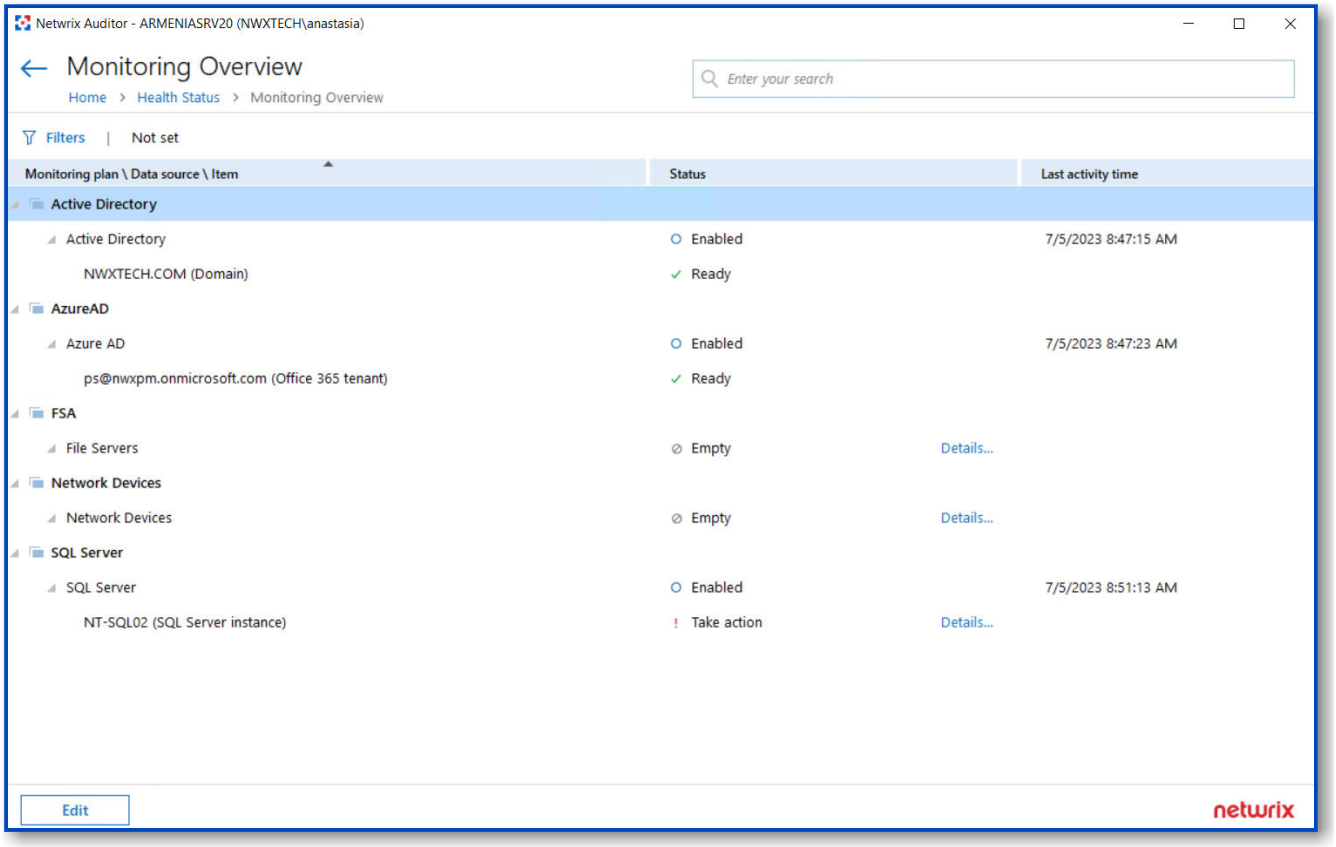
Monitoring Overview

Aggregated statistics on the monitoring plans is provided in the Monitoring overview widget. It displays current statuses of all monitoring plans:

- Ready (green indicator)—The monitoring plans (one or several) successfully processed the data sources with all their items and are ready for the next run.

- Pay attention (yellow indicator)—The monitoring plans (one or several) require your attention, as some items were not processed completely but only partially. This status applies to the monitoring plans targeted at Logon Activity and Windows File Server. See the table below for details.
- Take action (red indicator)—Any data source or item in the monitoring plan (one or several) was processed with errors.

After you click View details, the Monitoring Overview window will be displayed.



It provides the hierarchical list of monitoring plans, processed data sources and corresponding items with their current status and date/time of the last data processing session. For data sources and items their current status is depicted as follows:

Entity	Status	Description
Data source	Disabled	A data source can be disabled manually via its settings (by switching Monitor this data source and collect activity data to OFF), or automatically, if the license is not valid any more (for example, the

Entity	Status	Description
		count of licensed objects was exceeded, or the trial period has expired).
	Empty	No items have been added to this data source yet.
	Enabled	Monitor this data source and collect activity data is set to ON in the data source settings.
	Not available	The monitoring plan is corrupted and cannot process its data sources, so it is recommended to remove it and create anew.
	Not responding	Data collector for this data source is not responding. The underlying items will not be displayed for such data source.
	Working	The data source is being processed at the moment.
	(not displayed)	The data source status is unknown.
Item	Pay attention	The item was processed with some issues (non-critical). This status applies to the monitoring plans targeted at Logon Activity and

Entity	Status	Description
		Windows File Server. It means that data collection from at least one entity completed with errors. For example, a MyFileServer item included in the File Server monitoring plan contains all CIFS shares hosted on the MyFileServer computer. If any of these shares was processed with errors while others were processed successfully, the processing of the whole MyFileServer item will be considered partially completed, and the monitoring plan will have a yellow indicator, requiring your attention. Click the Details link to examine the product log.
	Ready	The item was processed successfully and is ready for the next run of data collection.
	Take action	Critical error(s) occurred while processing this item. Click the Details link to examine the product log.
	Working	The item is being processed at the moment.

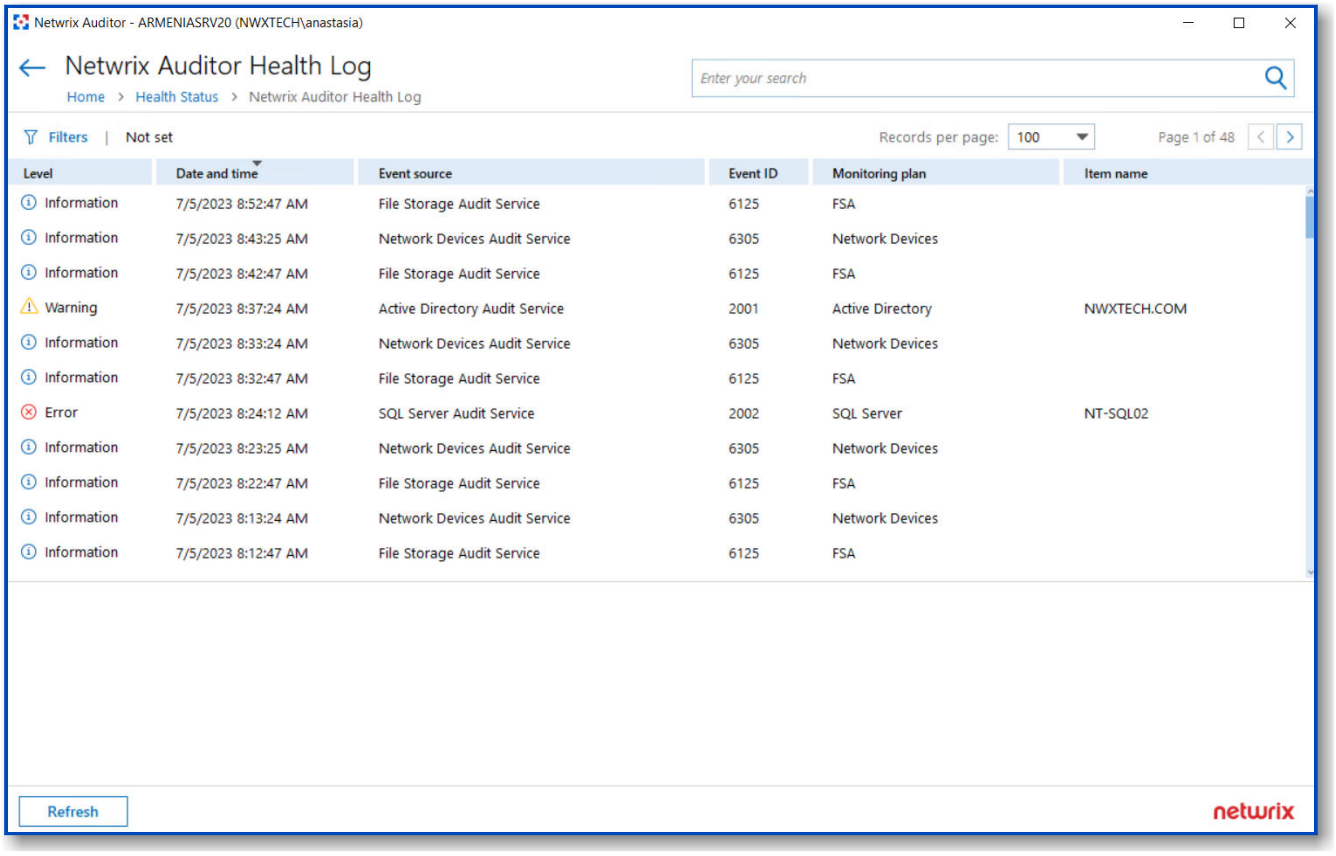
You can use the Search field, or apply a filter to display the information you need. For example, in the Apply Filters dialog you can select the Show only plans with issues to display only the monitoring plans that require attention and corrective actions.

This information will help you to troubleshoot the product operation, detect and eliminate the root cause of the monitoring errors, providing for auditing continuity and compliance.

Netwrix Auditor Health Log

Daily summary of the Netwrix Auditor health log is displayed in the Health log widget. The chart shows how many events with different severity levels were written to the product health log in the last 24 hours. To open the health log, click the **Open Health Log** link in the Health Status dashboard. See the topic for additional information.

If you want to clear Netwrix Auditor Health Log, son the computer where Auditor Server is installed, navigate to **EventViewer** -> **Application and Services Logs** and locate the **Netwrix Auditor System Health log**. Then, follow the instructions provided by Microsoft. See the Microsoft article for additional information on How to Clear Event Logs.



Netwrix Auditor System Health Log

When an error occurs, a system administrator or support engineer must determine what caused this error and prevent it from recurring. For your convenience, Auditor records important events in the proprietary Netwrix Auditor **System Health** event log.

You can review events directly in the product:

- When issues encountered during data collection, click Details... in the Status column and select View Health Log.

  OR

- In the main screen, in the Configuration section click the Health status tile, then in the Health log dashboard widget click Open health log.

You can also inspect the log in the Event Viewer.

There are three types of events that can be logged:

Event Type	Description
Information	An event that describes the successful operation beginning or completion. For example, the product successfully completed data collection for a monitoring plan.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, the product failed to process a domain controller.
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, the product failed to retrieve settings for your data source.

Review the following:

- Inspect Events in Health Log

If you want to monitor Auditor health status in more depth, you can do the following:

- Create a monitoring plan for this log using Event Log Manager too to collect activity data. See the Monitoring Overview topic for additional information.
- Configure alerts triggered by specific events in the product's health log. Create Alerts on Health Status

Inspect Events in Health Log

Follow the steps o inspect events in Netwrix Auditor health log

Step 1 – On the main Auditor page, select the Health status tile, then in the Health log dashboard widget click Open health log.

Step 2 – Select an entry to review it in details. You can also copy event details. Select the event in the list and click Copy details at the bottom of the window.

For your convenience, Auditor provides you with filters so that you can narrow down the number of events on the screen and focus on those that matter most. For example, warnings on failed data collection or events of an important monitoring plan.

Filter Events

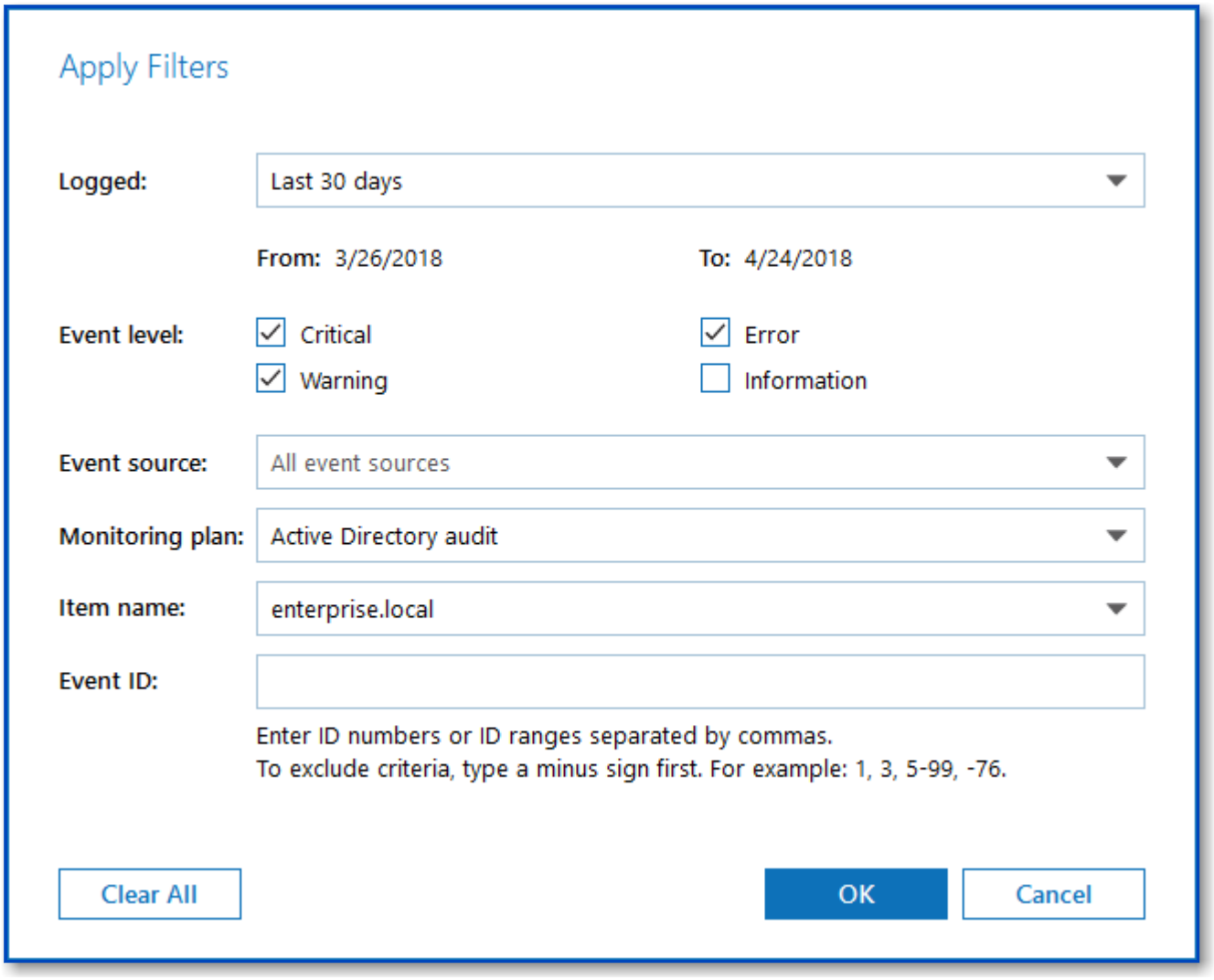
Follow the steps to filter events.

Step 1 – Select Filters in the upper part of the Netwrix Auditor Health Log window.

Step 2 – Complete the following fields:

Option	Description
Logged	Specify event logging time period (date range, yesterday, etc.).
Event level	Select level of the events that you want to be displayed.

Option	Description
Event source	Select services and applications whose events you want to view.
Monitoring plan	Select to display events from one or several monitoring plans.
Item name	Select to display events from the certain item(s) you need.
Event ID	Enter event ID number or range of event IDs separated by commas. For example, 1, 3, 5-99. You can also exclude unwanted event IDs from being displayed. Type the minus sign before selected event ID. For example, -76.



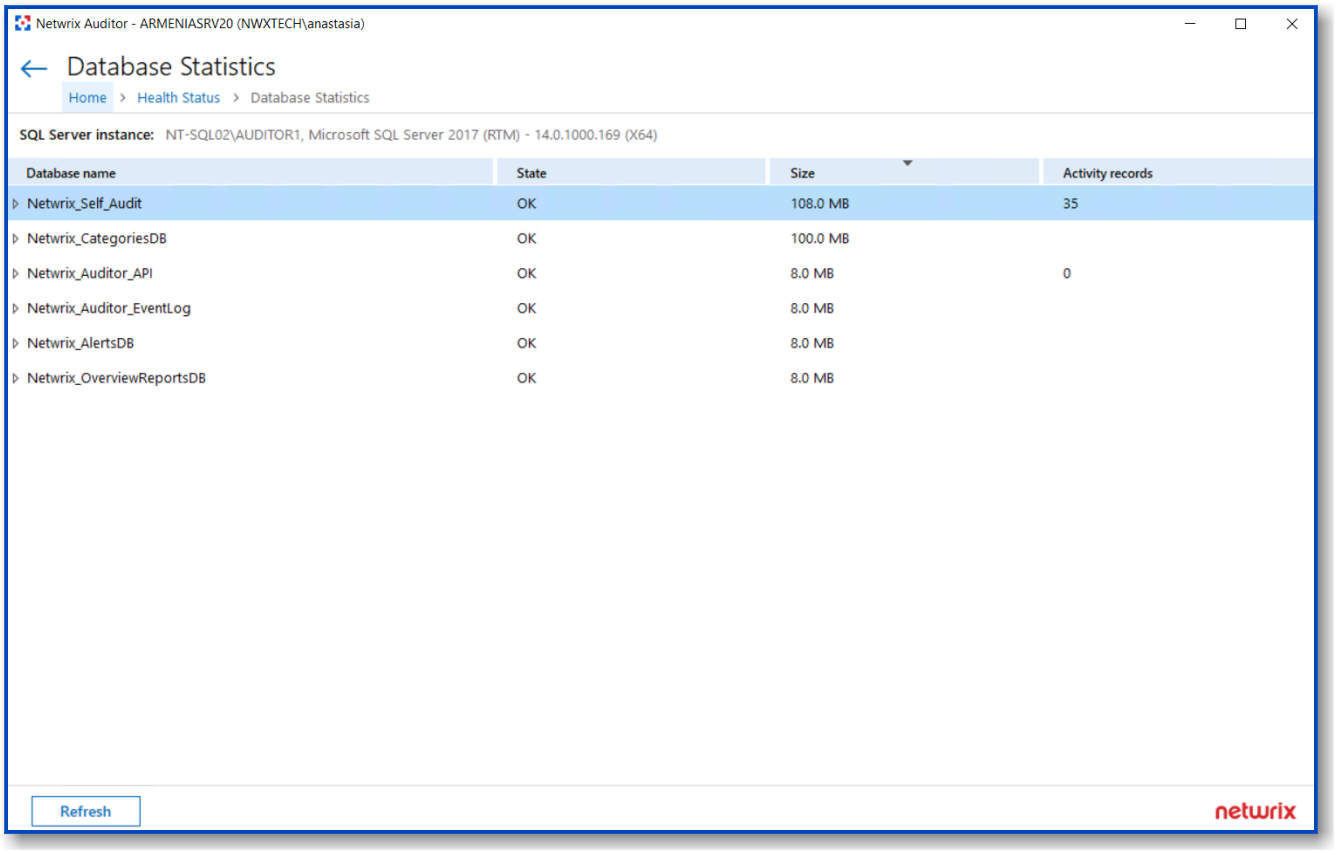
The applied filters will be listed on the top of the screen under the window title.

Database Statistics

Databases may tend to run out of free space due to poor capacity provisioning or to retention settings not configured properly. Use the Database statistics widget to examine database size and adjust retention accordingly. The widget displays the name of default SQL Server instance hosting all Netwrix Auditor databases, the overall database capacity at the moment and its change over the last day (24 hours).

Transaction logs size is not included in the calculations.

After you click View details, the following information will be displayed for the specified SQL Server instance:



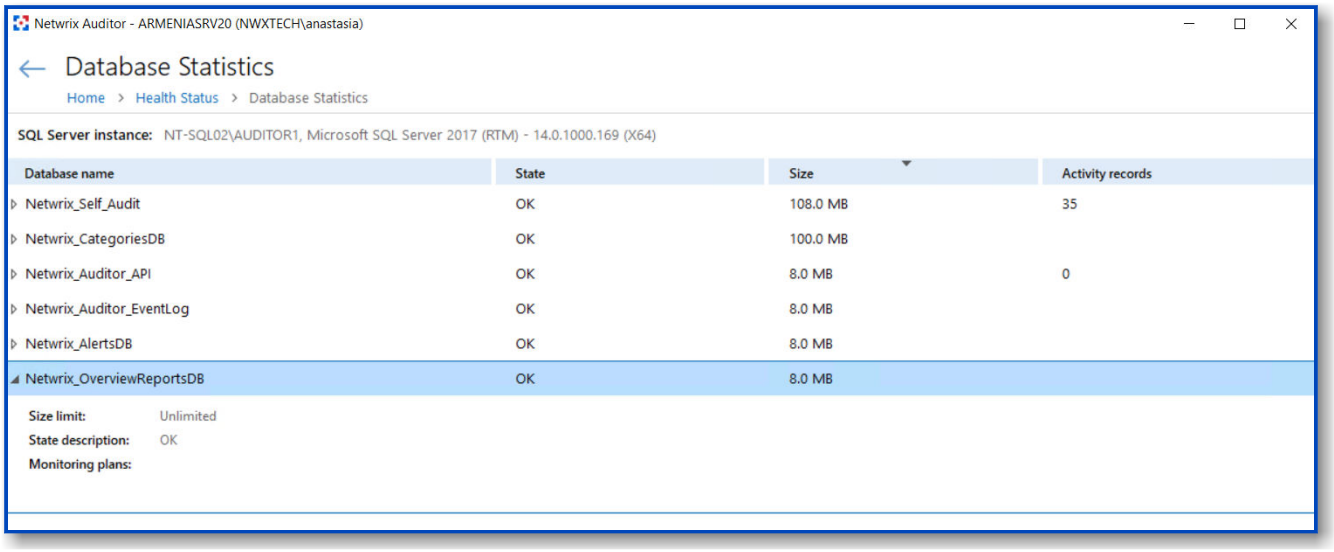
The Database name column contains the list of Netwrix Auditor databases hosted by the specified instance of the SQL Server:

- Special databases are created automatically on the default SQL Server instance to store:
  - alerts—*Netwrix_AlertsDB* database
  - activity records collected using Integration API—*Netwrix_Auditor_API* database
  - internal event records—*Netwrix_Auditor_EventLog* database
  - data collected by Netwrix Auditor self-audit—*Netwrix_Self_Audit* database
  - data needed for overview reports generation—*Netwrix_OverviewReportsDB*
- To store data from the data sources included in the monitoring plan, dedicated Audit databases are created and named by user (default name format is *Netwrix_Auditor_<monitoring_plan_name>*)

The following capacity metrics are displayed for each database:

- **State**—database state summary
- **Size**—current database size (logs are not included)
- **Activity records**—number of the activity records stored in the database at the moment

After you expand the database node, the detailed database properties will be shown:



These properties are as follows:

Property	Possible Values	Description
Size limit	*<size_limit>*	For SQL Server Express Edition– shows database size limitations
	Unlimited	
State description	OK	Database is operating properly.
	Capacity error	Database is running low on disk space. -OR- Size limit for SQL Server Express Edition will be reached soon (threshold is 500 MB, i.e. 5% of 10 GB limit remaining).

Property	Possible Values	Description
	Failed to store data	Failed to store data to the database due to some issues.
	Unavailable	Failed to connect to the database.
	Upgrade in progress	Database is being upgraded.
Monitoring plans	*<monitoring_plan>*	All monitoring plans for which this database is a target. Usually it is recommended to configure a dedicated database for each plan.

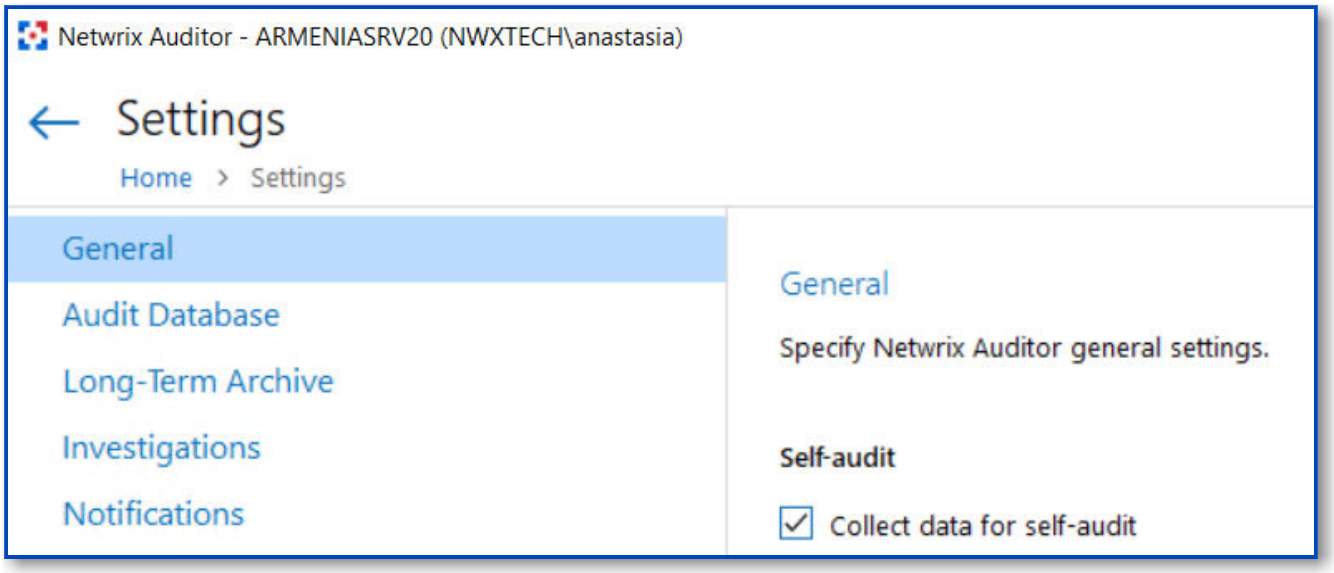
You can use the Search field, or apply a filter to display the information you need. For example, in the Apply Filters dialog you can select the Show only plans with issues to display only the monitoring plans that require attention and corrective actions.

This information will help you to troubleshoot the product operation, detect and eliminate the root cause of the monitoring errors, providing for auditing continuity and compliance.

Self-Audit

Built-in Netwrix Auditor self-audit allows you to track changes to the product configuration, including monitoring plans, data sources, audit scope and details about it (before-after values). This helps you to ensure that monitoring scope is complete and changed only in line with the workflows adopted by our organization.

The corresponding option is available on the General tab of Netwrix AuditorSettings. By default, the **Collect data for self-audit checkbox** is selected (enabled).



Search for Self-audit Results

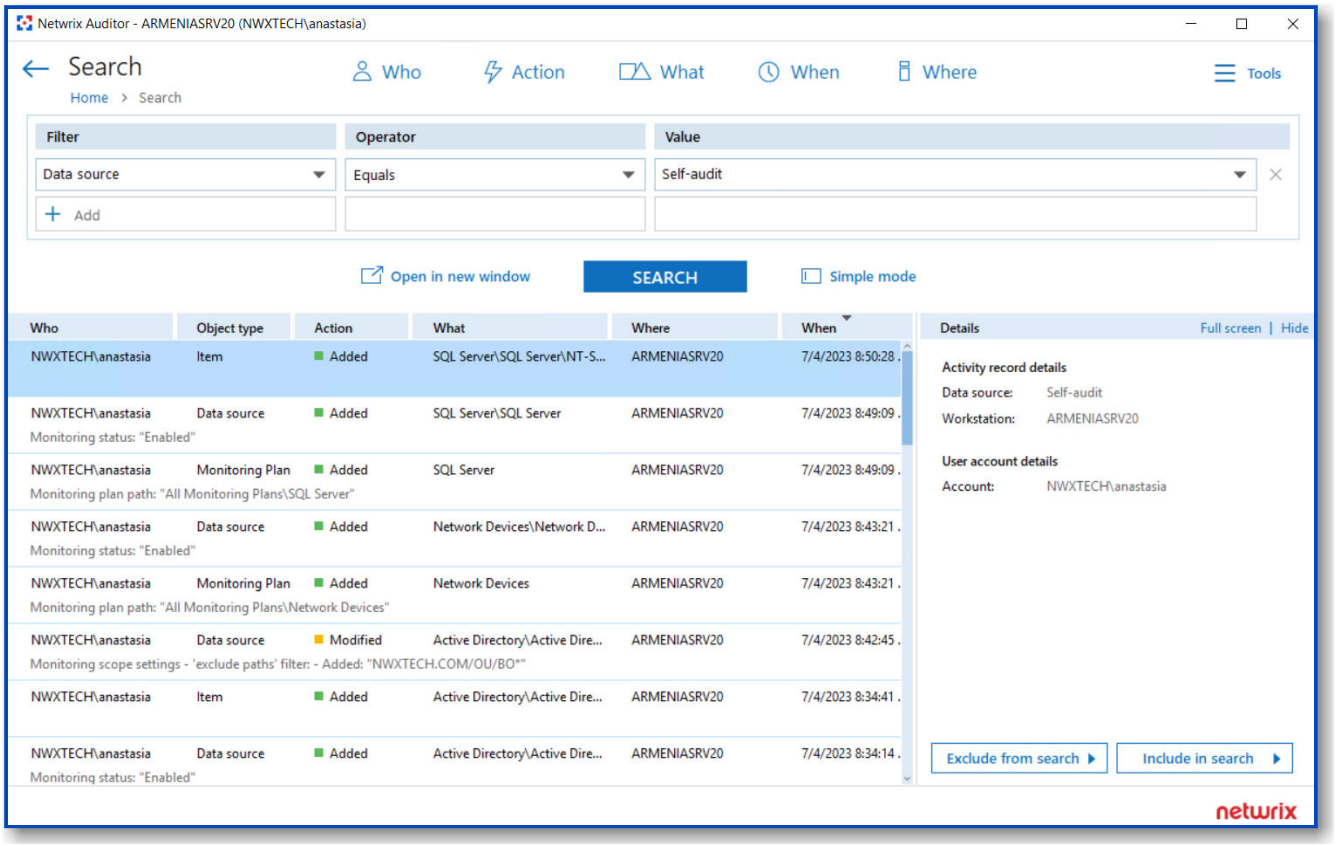
All Auditor self-audit Activity Records can be found quickly using AuditIntelligence Search.

Follow the steps to search for self-audit results.

Step 1 – In Auditor, navigate to Search.

Step 2 – Set the Data source filter to **Self-audit**.

Step 3 – Click Search to review results:



NOTE: After reviewing your search results, apply filters to narrow your data. See the View Reports topic for additional information.

Step 4 – After browsing your data, navigate to Tools to use the search results as intended. See the View and Search Collected Data topic for additional information.

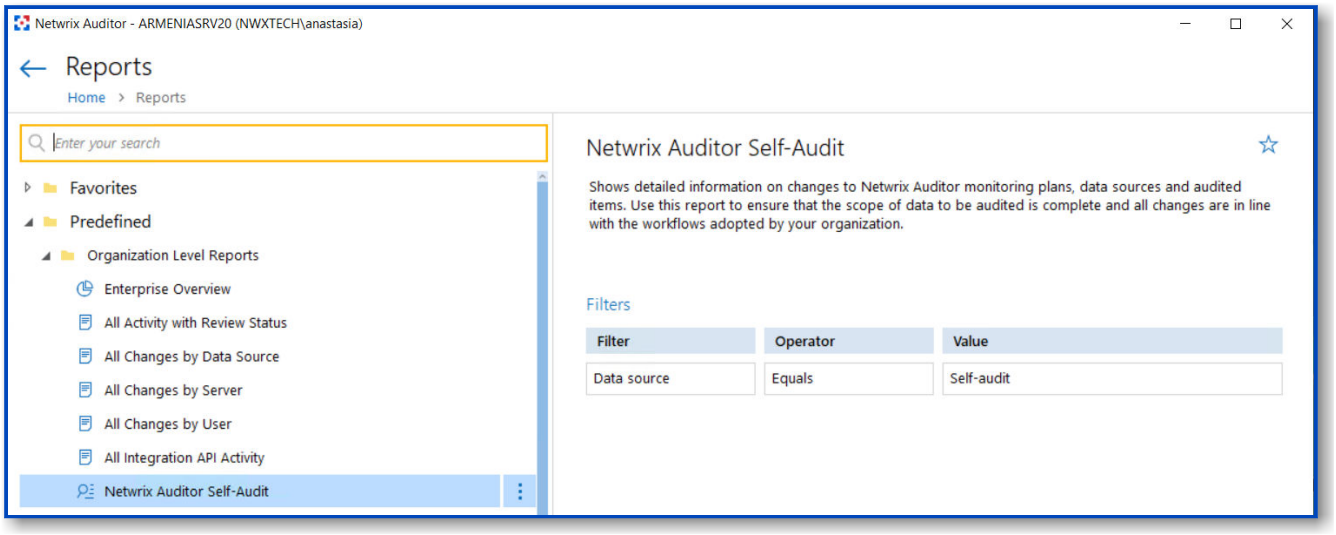
Review Auditor Self-Audit Report

Also, there is a new Netwrix Auditor Self-Audit report available under Organization Level Reports in the predefined set of reports. This report shows detailed information on changes to Auditor monitoring plans, data sources and audited items.

Follow the steps to review the Self-audit report.

Step 1 – In Auditor, navigate to Reports > Organization Level Reports.

Step 2 – Select the Netwrix Auditor Self-Audit report and click View.



Netwrix Auditor Self-Audit Scope

Review the full list of components and settings captured within Netwrix Auditor self-audit scope.

Object type	Action	What	Details
Local logon	• Successful Logon • Logoff	• Netwrix Auditor server name	-
Remote logon	• Successful Logon • Logoff	• Netwrix Auditor server name	-
Netwrix Auditor global settings	• Modified	• Self-audit settings • Usage statistics collection settings • Tags • Audit database settings • Long-term archive settings • Data import for investigations • Notification settings • Integration API settings	• Self audit (enabled / disabled) • Settings changed

Object type	Action	What	Details
		• License settings • Check for update settings	
Monitoring plan	• Added • Modified • Removed	• Monitoring plan name	• Monitoring plan path changed • Role assignments (added / removed) • Activity Summary recipients (added / removed) • Settings changed
Data source	• Added • Modified • Removed	• Monitoring plan name \ Data source name	• Monitoring status (enabled / disabled) • Settings changed
Item	• Added • Modified • Removed	• Monitoring plan name \ Data source name \ Item name	• Item name changed • Settings changed
Alert	• Added • Modified • Removed	• Alert name	• Name changed • Mode (enabled / disabled) • Alert recipients (added / removed) • Settings changed
Monitoring plans folder	• Added • Modified • Removed	• All Monitoring Plans \ Folder name	• Name changed • Role assignments (added / removed)

Object type	Action	What	Details
Monitoring plans root folder	• Modified	• All Monitoring Plans	• Role assignment (added / removed)
Custom search-based report	• Added • Modified • Removed	• Report name	• Name changed • Settings changed
• **Subscription to custom search-based report** • **Subscription to overview reports** • **Subscription to SSRS-based report** • **Subscription to risk assessment overview**	• Added • Modified • Removed	• Subscription name	• Name changed • Mode (enabled / disabled) • Subscription recipients (added / removed) • Settings changed
Configuration integrity	• Added • Modified	• Configuration data • Configuration integrity state	• Alerts, saved searches, subscriptions, etc.

Health Summary Email

Auditor Health Summary email includes all statistics on the product operations and health for the last 24 hours; it also notifies you about license status. By default, this email is generated daily at 7:00 AM and delivered to the recipient specified in the Notifications settings. Email content is very similar to data presented in the Health Status Dashboard.

For greater usability, to depict overall product health state, the email includes a color indicator in the topmost section: green means Auditor had no issues while auditing your IT infrastructure, and red means there were some problems that require your attention.

The email looks like shown below:

Netwrix Auditor Health Summary

Generated on 4/20/2018 7:00 AM UTC+03:00 to notify you about audit status for the last 24 hours.

Current State

This is a trial version expiring in 11 days

Several items need your attention.

- **1** monitoring plan needs your attention
- **6** errors reported in Netwrix Auditor health log

See the sections below for details.

Activity Records

Statistics on activity records produced by your data sources, collected and saved by Netwrix Auditor in the last 24 hours.

Last activity record collected on 4/18/2018 2:23:49 PM

Collected:	2186
Uploaded to database:	2186

Monitoring Overview

Latest status of the monitoring plans processing your data sources.

1	Monitoring plan	• Ready
0	Monitoring plans	• Pay attention
1	Monitoring plan	• Take action

Monitoring plans with issues

Monitoring plan\Data source\Item	Status	Last activity time
File Server Monitoring		
File Servers		4/20/2018 6:53:03 AM
StationWin10.enterprise.local (Computer)	! Take action	

Health Log

Events written in the last 24 hours:

- **56** Information
- **2** Warning
- **6** Error

Capacity

Examine database statistics and storage capacity.

The Monitoring Overview section of the email provides detail information only for the monitoring plans with issues. Successfully completed monitoring plans are not included.

Network Traffic Compression

To reduce network traffic in distributed deployments, multi-site networks and other environments with remote locations that have limited bandwidth, it is recommended to use network traffic compression. For that purpose, special Netwrix utilities should be installed in the audited environment. These utilities will run on the target computers (depending on your monitoring plan), collect, pre-filter data and send it to Auditor Server in a highly compressed format.

With network traffic compression, data from the target machines is collected simultaneously, providing for network load balance and minimizing data collection time. (Unlike that, without network traffic compression the target machines will be processed sequentially, i.e. one at a time.) So, network traffic compression helps to increase scalability and optimize network traffic.

Its key capabilities are as follows:

- Allows Auditor to collect detailed metrics for the servers, log files, hardware and individual processes
- Collects audit data with no recognizable load on the server
- Communicates with Netwrix Auditor Server at predefined intervals, relaying data back to a central repository for storage

Network traffic compression is available for the following data sources:

- Active Directory
- Exchange
- File Servers
- Dell
- NetApp
- Windows Server
- Event Logs
- Group Policy
- Logon Activity
- SharePoint
- User Activity

To learn how to enable this feature, refer to the Create a New Monitoring Plan topic for additional information.

Troubleshooting

This section provides instructions on how to troubleshoot issues that you may encounter while using Netwrix Auditor.

If your issue is not listed in the table below, try searching Netwrix Knowledge Base.

If you need assistance from the Technical Support team, you can open a ticket using the Customer portal as described in the Creating a ticket with Customer portal section.

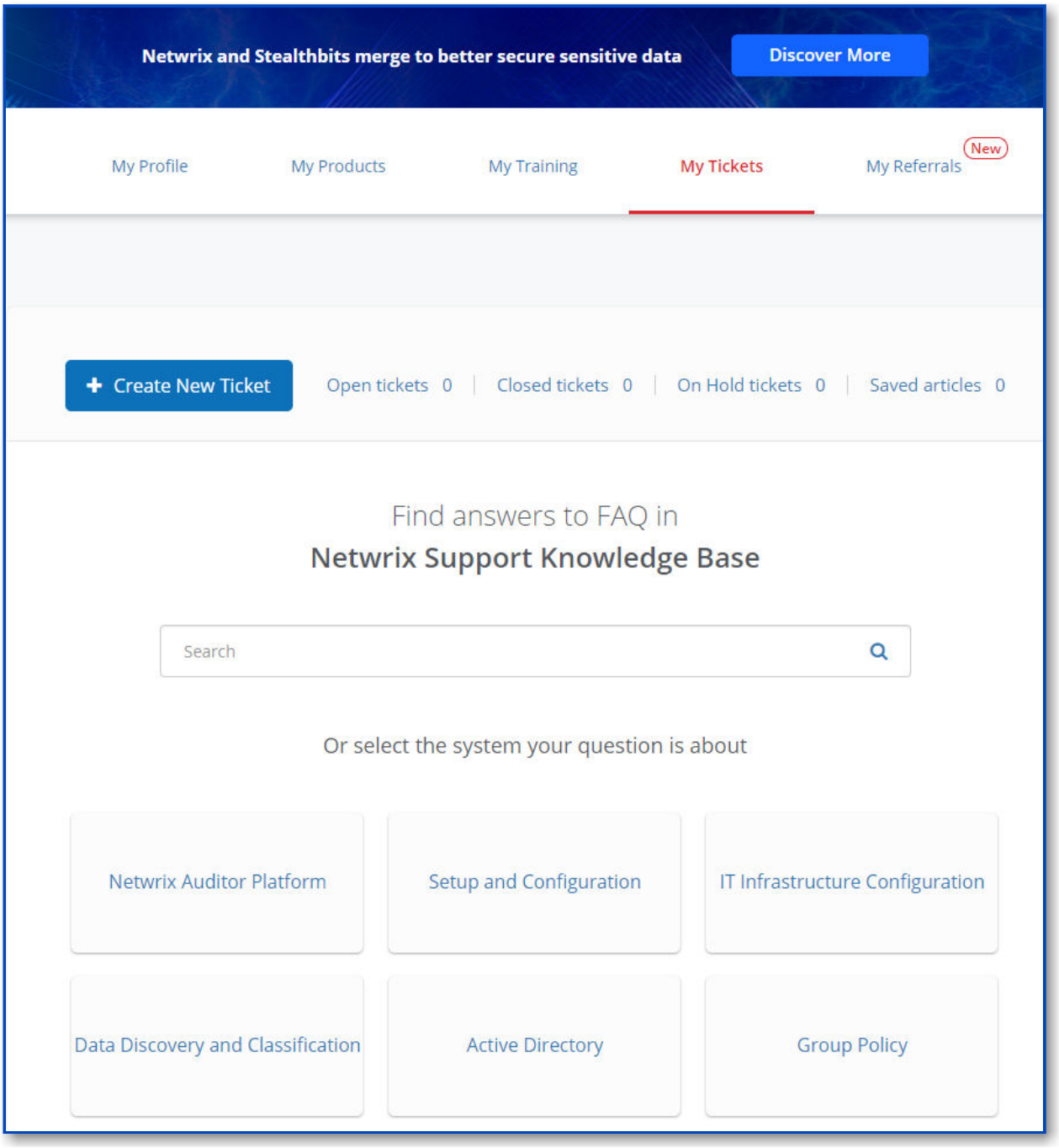
Issue	Reason and solution
I cannot connect/logon to Auditor.	1. You may have insufficient permissions. Contact your Auditor Global administrator to make sure that your account is delegated control of the product. 2. You are trying to connect to a remote Auditor specified by its IP address while the NTLM authentication is disabled. Try specifying a server by its name (e.g., EnterpriseWKS).
I do not receive any results while searching audit data or generating reports, or I am sure that some data is missing.	1. No changes were detected. 2. You do not have sufficient permissions to review intelligence data. Contact your Global administrator. 3. Review your filter settings and make sure that your filters are properly configured. Try modifying your search. 4. You are looking for changes that occurred more than 180 days ago. These changes are no longer available for reporting and running searches. Ask your Auditor Global administrator to import audit data for a required date range from the Long-Term Archive. 5. Data collection for this monitoring plan might not have been launched two times yet or there was no data collection after this change; therefore, audit data has not been written to the Audit Database yet. 6. Some settings in Auditor are configured incorrectly. Contact your Auditor administrator to make sure that:

Issue	Reason and solution
	• The monitoring plan you want to audit is properly configured, and the monitoring is enabled for each data source individually. • Audit Database settings are properly configured for each data source individually and Disable security intelligence and make data available only in activity summaries is cleared. Netwrix recommends to store all audit data on the same default SQL Server instance.
"No plans found" text in the Monitoring plan field.	Contact your Auditor Global administrator or Configurator to make sure that the monitoring plans exist and are properly configured.
I see a blank window instead of a report.	Contact your Auditor Global administrator to make sure that you are granted sufficient permissions on the Report Server. To view reports in a web browser • Open a web browser and type the Report Manager URL (found under Settings>**Audit Database**). In the page that opens, navigate to the report you want to generate and click the report name. You can modify the report filters and click View Report to apply them.
I configured report subscription to be uploaded to a file server, but cannot find it / cannot access it.	Subscriptions can be uploaded either to a file share (e.g., *filestorage**reports*) or to a folder on the computer where Auditor Server is installed. To access these reports, you must be granted the Read permission.
When trying to collect event data from Active Directory domain, an error message like this appears in Netwrix Health Log:	This may happen due to Secondary Logon Service disabled state. To collect event data from the domain, this service must be up and running. Open its properties and start the service.

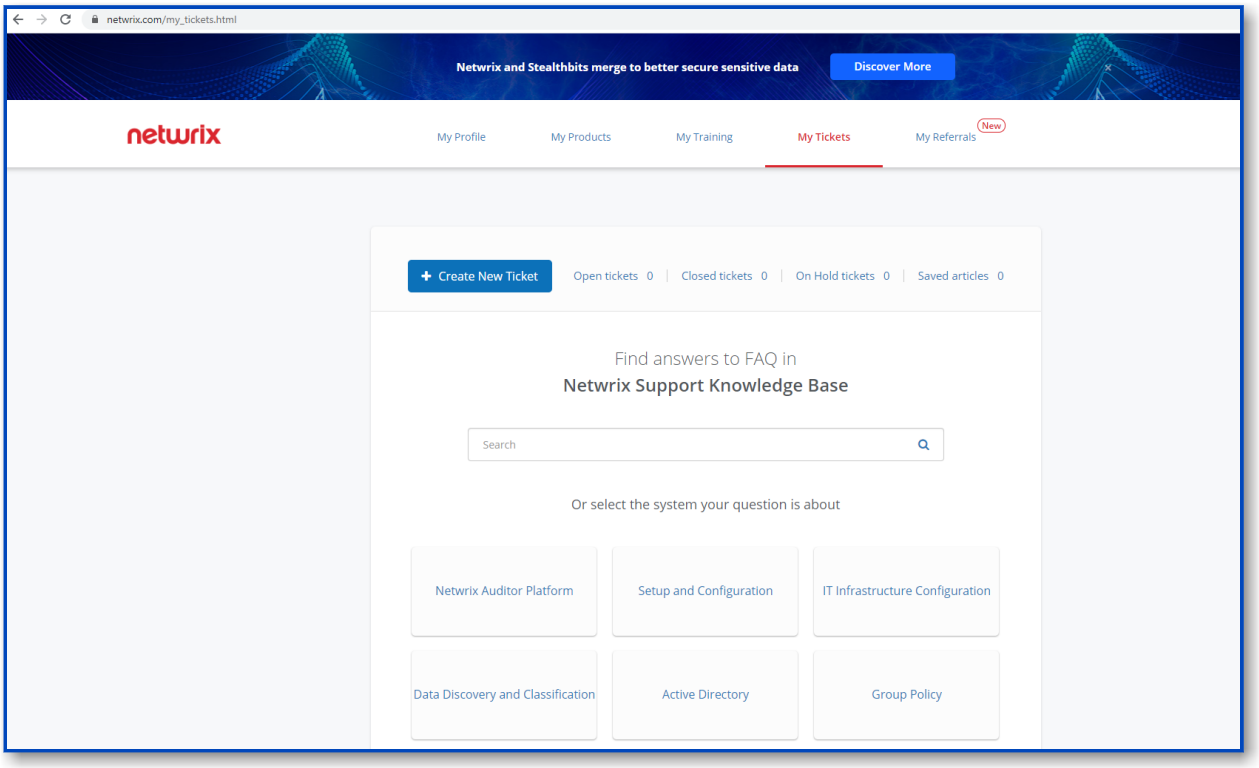
Issue	Reason and solution
Monitoring Plan: <Monitoring_Plan_Name> The following error has occurred while processing '<Item_Name>': Error collecting the security log of the domain <Domain_Name>. Failed to process the domain controller <Domain_Controller_Name> due to the following error: The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.	
The 'Workstation' field in search, reports, and Activity Summary is reported as 'unknown'	For the full list of possible reasons, please refer to the following Netwrix Knowledge Base article: Why is the "Workstation" field reported as "unknown"?

Creating a ticket with Customer portal

1. Sign in at https://www.netwrix.com/my_tickets.html.
2. You can search or browse through the Knowledge Base articles here, or click **Create New Ticket**:



3. Fill in the form, describing the issue, and click **Open a ticket**.
4. After that, you will be able to attach the files you need (screenshots, emails, reports, etc.).



Tools

There are several tools available with Netwrix Auditor:

- Audit Configuration Assistant
- Event Log Manager
- Inactive User Tracker
- Object Restore for Active Directory
- Password Expiration Notifier

Audit Configuration Assistant

Auditor Audit Configuration Assistant utility helps you to assess your environment readiness to being monitored with the product and automatically adjust the audit settings with the requirements.

It checks current settings of your Active Directory and Group Policies against those required for monitoring of selected data sources: Group Policy settings, auditing entries for directory partitions, and admin audit log settings of Exchange server. Assessment results are reported on the screen and can be downloaded as a PDF file.

You can instruct the utility to automatically apply the required settings.

For that, you should ensure that the account you plan to use for accessing the target domain has the necessary rights.

Audit Configuration Assistant is a part of Netwrix Auditor product setup. It is installed together with the Auditor client and can be launched from the **Start menu > Netwrix Auditor > Netwrix Auditor Audit Configuration Assistant**. Alternatively, you can launch this utility from the monitoring plan wizard for Active Directory data source. See the Launch Audit Configuration Assistant section for additional information.

Currently, the utility supports Active Directory and Logon Activity data sources.

Prerequisites

When working with the utility, you will need to provide an account with the rights required to access the AD audit entries and other settings. Thus, the account should be a member of the following groups:

- *Domain Admins* — to access audit policies and audit entries on the domain controllers
- *Enterprise Admins* — to configure audit entries for AD partitions
- *Organization Management* or *Records Management* (in Exchange organization) — to configure admin audit log settings

You can create a dedicated account for the assessment purposes, include it in these groups for the assessment period, and after finishing, remove it from these privileged groups.

Usage

To assess and adjust the audit settings with Audit Configuration Assistant, take the following steps:

1. Launch Audit Configuration Assistant
2. Start Assessment
3. View Results
4. Complete the process

Launch Audit Configuration Assistant

Audit Configuration Assistant is a part of Netwrix Auditor product setup. It is installed together with Netwrix Auditor client and can be launched from the **Start** menu.

Select **Netwrix Auditor→Netwrix Auditor Audit Configuration Assistant**.

- If the utility is installed on the same machine as Netwrix Auditor server, you will be taken to the **Welcome** step.
- If the utility is installed on the remote machine together with Netwrix Auditor client, the initial window will allow you to enter the settings to connect to Netwrix Auditor Server. Specify the following:

Setting	Description
Host	Enter the name or IP address of Netwrix Auditor Server to connect to.
Use specified credentials	If not selected, then your current Windows credentials will be used to access Netwrix Auditor Server. Select this option if you want to use other credentials
User	Enter user account in the *domain**name* format.
Password	Enter account password.

After you click **Connect**, the connection with Netwrix Auditor Server will be established, and you will be taken to the **Welcome** step.

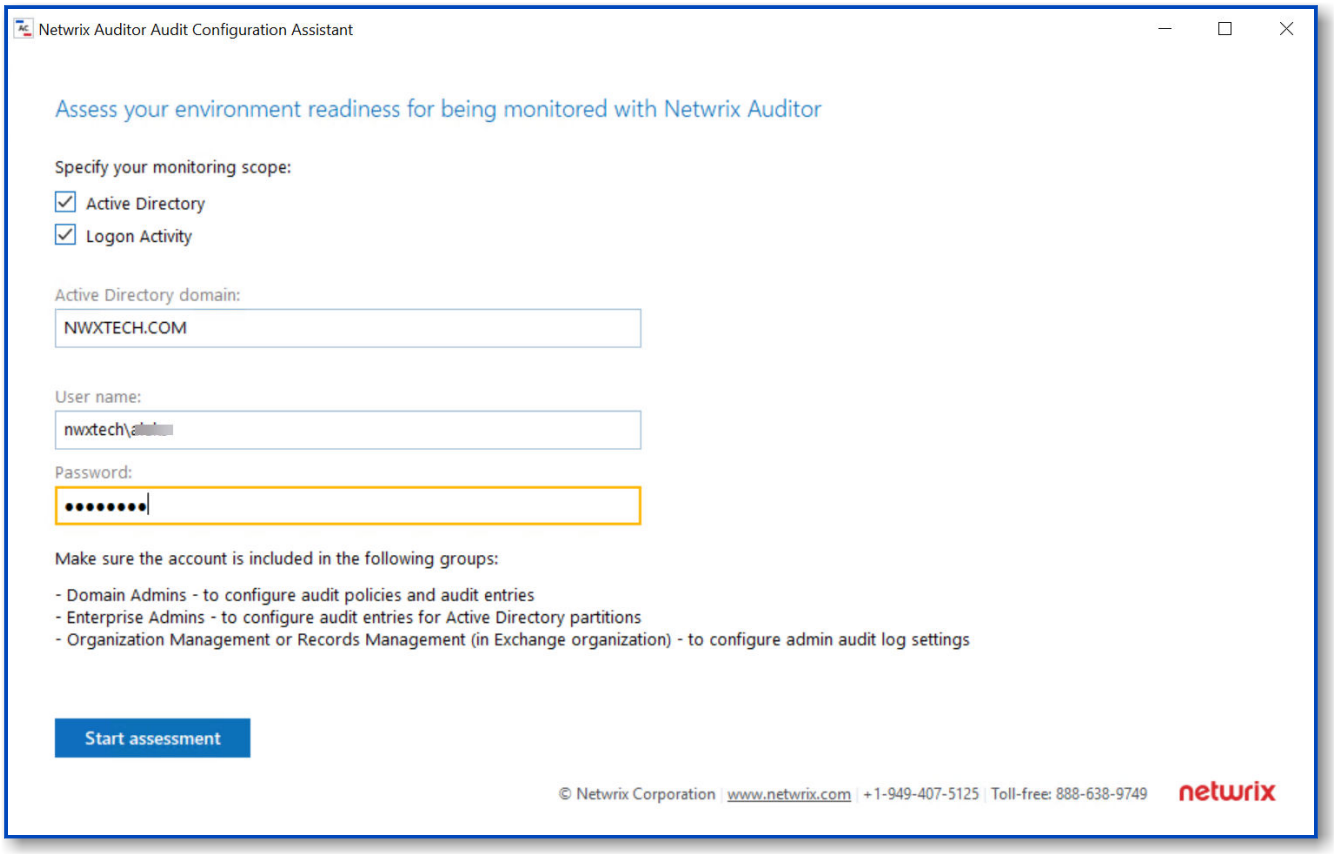
Alternatively, you can launch this utility by clicking the corresponding link:

- From Create a New Monitoring Plan for Active Directory data source.
- From the Active Directory within the plan.
- From the Logon Activity source properties.

Start Assessment

Follow the steps to start assessment.

Step 1 – Specify the monitoring scope —select what you plan to monitor with Netwrix Auditor. You can select both **Active Directory** and **Logon Activity**, or any of them.



Step 2 – If you launched **Audit Configuration Assistant** from the **Start** menu (not from the monitoring plan settings), enter the name of Active Directory domain you want to assess.

Step 3 – Enter credentials that will be used to access the audit setting of that domain. This account must be included in the following groups:

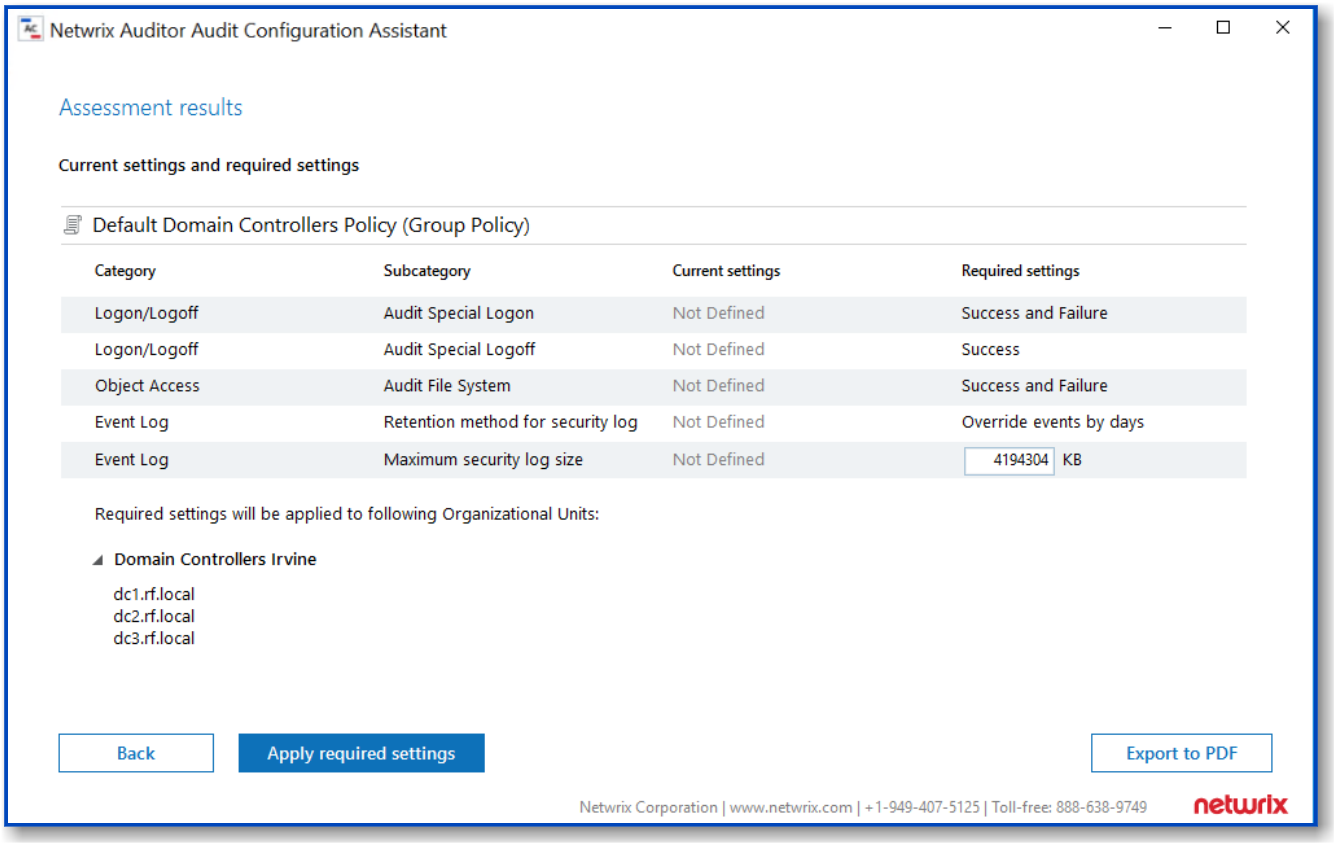
- *Domain Admins* — to access audit policies and audit entries on the domain controllers
- *Enterprise Admins* — to configure audit entries for AD partitions
- *Organization Management* or *Records Management* (in Exchange organization) — to configure admin audit log settings

Step 4 – Click **Start assessment**.

View Results

At this step, you will be presented the results of the environment readiness assessment, including:

- the list of current and required settings for each entity
- the list of issues (if any) that occurred during the assessment



Follow the steps to view results.

Step 1 – Examine the report.

Step 2 – If some issues occurred due to the lack of access rights during the assessment, you can click **Back** and modify the settings provided at the previous step.

Step 3 – If you need to save this report (for example, to get your manager's approval), click **Export to PDF**.

Step 4 – When ready, you can automatically adjust audit settings with the requirements — for that, click **Apply required settings**.

Complete the process

After you click **Apply required settings**, the utility will proceed with modifying your current audit settings. Operation progress will be reported in the bottom of the window.

Step 1 – Wait for the process to complete.

Step 2 – Review the results. Successfully applied settings will be reported with a green tick; those that did not manage to apply will be with the yellow warning sign and explanatory text.

Step 3 – You can click **Start over** to get to the Start Assessment, fix the issues and perform the procedure again, or click **Finish**.

Event Log Manager

Netwrix Auditor Event Log Manager standalone tool consolidates and archives event log data, and allows setting up alerts on critical events including unauthorized access to mailbox in your Exchange organization and events generated by Auditor.

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 Auditor console computer. 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.

CAUTION: Folder associated with NETWRIX AUDITOR must be excluded from antivirus scanning. See the Antivirus Exclusions for Netwrix Auditor knowledge base article for additional information.

You can configure your IT Infrastructure for monitoring in one of the following ways:

- Automatically through a monitoring plan – This is a recommended method. 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 – Native audit settings must be adjusted manually to ensure collecting comprehensive and reliable audit data. You can enable Auditor to continually enforce the relevant audit policies or configure them manually:
    - 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.

Review the following for additional information:

- Create Monitoring Plans for Event Logs
- Configure Audit Archiving Filters for Event Log
- Create Monitoring Plan for System Health Log
- Review Past Event Log Entries

- Import Audit Data with the Database Importer
- Create Alerts for Event Log
- Create Alerts for Non-Owner Mailbox Access Events

Create Monitoring Plans for Event Logs

Follow the steps to configure monitoring plan for event logs.

Step 1 – Navigate to **Start >** Netwrix Auditor **>** Netwrix Auditor **Event Log Manager.**

Step 2 – On the main page, you will be prompted to select a monitoring plan. Click Add to add new plan.

Step 3 – Configure basic parameters as follows:

- Enable event log collection — Select the checkbox to start monitoring event logs.
- Monitoring plan — Enter a name for a new list of monitored computers.
- Notification recipients — Specify one or several email addresses for users to receive daily Event Log collection status notifications. Use semicolon to separate several addresses.

- Monitored computers — Select items that you want to audit. You can add several items to your monitoring plan. Click **Add** and complete the following:

Option	Description
Computer name	Allows specifying a single computer by entering its FQDN, NETBIOS or IP address. You can click Browse to select a computer from the list of computers in your network.
Active Directory container	Allows specifying a whole AD container. Click **Browse** to select from the list of containers in your network. You can also: ◦ Select a particular computer type to be monitored within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**.

Option	Description
	◦ Click **Exclude** to specify domains, OUs, and containers you do not want to audit. The list of containers does not include child domains of trusted domains. Use other options (**Computer name, IP address range**, or **Import computer names from a file**) to specify the target computers.
IP address range / Computers within an IP range	Allows specifying an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP range you want to exclude, and click **Add**.

Step 4 – You can specify multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). Click Import and select a .txt file. You can choose whether to import the list once, or to update it on every data collection.

Step 5 – Navigate to the General tab and configure the following:

Option	Description
User name **Password**	Enter the account that will be used by Netwrix Auditor Event Log Manager for data collection. For a full list of the rights and permissions required for the account, and instructions on how to configure them, refer to the Permissions for Event Log Auditing section.
Audit archiving filters	Define what events will be saved to the Long-Term Archive or the Audit Database. Refer to for detailed instructions on how to configure audit archiving filters.
Alerts	Configure alerts that will be triggered by specific events. Refer to Create Alerts for Event Log for

Option	Description
	detailed instructions on how to configure Netwrix Auditor Event Log Manager alerts.

Step 6 – Navigate to the Notifications tab and complete the following fields:

Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the From field. *RECOMMENDED:* click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.

Option	Description
Use implicit SSL	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission. The option is not available for auditing User Activity as well Netwrix Auditor tools.

Step 7 – Navigate to the Audit Database tab to configure Audit Database and review SQL Server settings. Netwrix Auditor Event Log Manager synchronizes Audit Database and reports settings with the default Audit Database configuration from Netwrix Auditor Server. If this option is disabled, contact your Netwrix Auditor Global administrator and make sure that these settings are properly configured in Netwrix Auditor Server. Refer to Audit Database for detailed instructions on how to configure the Audit Database settings.

Step 8 – Complete the following fields:

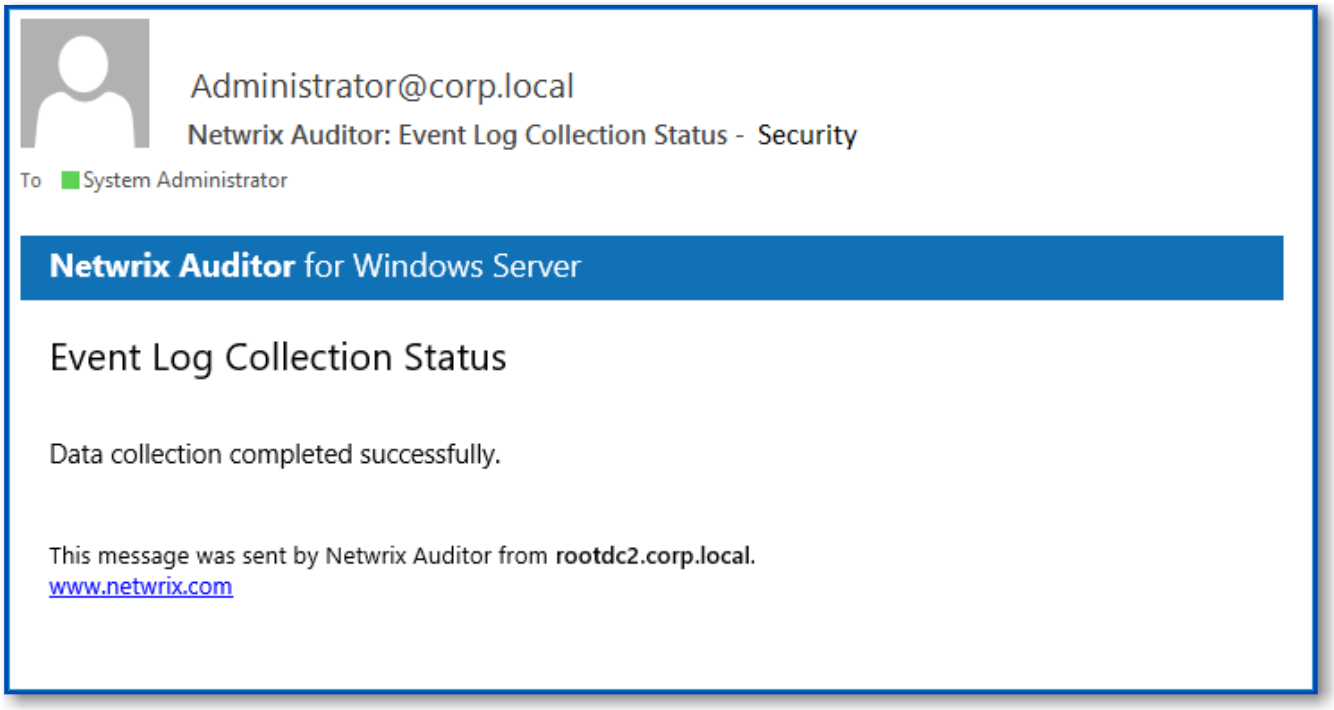
Option	Description
Write data to Audit Database and enable reports	Select if you want to generate reports. Even if you do not select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database.
Write event descriptions to Audit Database	Select if you want to see the exact error or warning text.
Store events for... days	Specify the Audit Database retention period. This setting affects all monitoring plans. The minimum value specified across the plans will be applied. When configuring, mind that your data will be deleted automatically when its retention period is over.

NOTE: You cannot edit SQL Server settings for Netwrix Auditor Event Log Manager.

Step 9 – Navigate to the Advanced tab and configure the following:

Option	Description
Enable network traffic compression	If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Specify notification delivery time	Modify the Event Log collection status email delivery schedule.

If you want to review the Event Log Collection Status email, the Event Log Collection Status email shows whether data collection for your monitoring plan completed successfully or with warnings and errors.



Configure Audit Archiving Filters for Event Log

Audit archiving filters define what events will be saved to the Long-Term Archive or the Audit Database, and provide more granular reporting. For example, if you are going to audit Internet Information Services (IIS) or track health status of the product, enable the Internet Information Services Events or Netwrix Auditor System Health filter respectively. You can also skip certain events with exclusive filters (e.g., computer logons). You can enable or disable, and modify existing filters, and create new filters. To do it, click Configure next to Audit archiving filters.

The product allows creating inclusive and exclusive audit archiving filters.

Follow the steps to configure audit archiving filters.

Step 1 – To create or modify an audit archiving filter, see Create Monitoring Plans for Event Logs.

Step 2 – To collect events required to generate a specific report, you must select a filter which name coincides with this report's name. Click Enable and select Filters for Reports. All filters required to store events for all available reports will be selected automatically.

Follow the steps to create or edit an audit archiving filter.

Step 1 – On the Audit archiving filters page, click Add or select a filter and click Edit.

Step 2 – Complete the fields. Review the following for additional information:

Option	Description
The Event tab	
Name	Specify the filter name.
Description	Enter the description for this filter (optional).
Event Log	Select an event log from the drop-down list. You will be alerted on events from this event log. You can also input a different event log.

Option	Description
	To find out a log's name, navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)**→ Event Viewer → Applications and Services Logs → Microsoft → Windows and expand the required <Log_Name> node, right-click the file under it and select Properties. Find the event log's name in the Full Name field. Netwrix Auditor Event Log Manager does not collect the Analytic and Debug logs, so you cannot configure alerts for these logs. You can use a wildcard (*). For inclusive filters: all Windows logs except for the ones mentioned above will be saved. For exclusive: all Windows logs events will be excluded.
Write to/Don't write to	Select the location to write/not to write events to, depending on the filter type (inclusive or exclusive). It is recommended to write events both to the Long-Term Archive and to the Audit Database, because if your database is corrupted, you will be able to import the necessary data from the Long-Term Archive using the DB Importer tool. See Import Audit Data with the Database Importer for more information.
The Event Fields tab	
Event ID	Enter the identifier of a specific event that you want to be save. You can add several IDs separated by comma.
Event Level	Select the event types that you want to be save. If the Event Level check box is cleared, all event types will be saved.

Option	Description
	If you want to select the inclusive Success Audit/ Failure Audit filters, note that on these platforms these events belong to the “Information” level, so they will not be collected if you select the Information checkbox in the Exclusive Filters.
Computer	Specify a computer (as it is displayed in the Computer field in the event properties). Only events from this computer will be saved. If you want to specify several computers, you can define a case-sensitive mask for this parameter. Below is an example of a mask: • * - any machine • computer – a machine named ‘computer’ • *computer* - machines with names like ‘xXxcomputerxXx’ or ‘newcomputer’ • computer? – machines with names like ‘computer1’ or ‘computerV’ • co?puter - machines with names like ‘computer’ or ‘coXputer’ • ????? – any machine with a 5-character name • ???* - any machine with a 3-character name or longer
User	Enter a user’s name. Only events created by this user will be saved. If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Source	Specify this parameter if you want to save events from a specific source. Input the event source as it is displayed in the Source field in the event properties.

Option	Description
	If you need to specify several sources, you can define a mask for this parameter in the same way as described above.
Category	Specify this parameter if you want to save a specific events category.
The Insertion Strings tab	
Consider the following event Insertion Strings	Specify this parameter if you want to store events containing a specific string in the EventData. You can use a wildcard (*). Click Add and specify Insertion String.

Create Monitoring Plan for System Health Log

If you want to generate reports on health state and to be alerted on important Netwrix Auditor health events, you need to create a dedicated monitoring plan for this log with Netwrix Auditor Event Log Manager standalone tool.

You can also review and filter Netwrix Auditor health events right in the product. See Netwrix Auditor Health Log for addditional information

Follow the steps to configure the Netwrix Auditor System Health log monitoring.

Step 1 – Start Netwrix Auditor Event Log Manager and create the new monitoring plan.

Step 2 – Make sure that the Enable event log collection checkbox is selected. Specify the name for the new monitoring plan, for example, "Netwrix Auditor *Health Status*".

Step 3 – Navigate to the Monitored computers list and add a server where the Netwrix Auditor Server resides.

Step 4 – Navigate to the Audit Database tab and select Write event descriptions to Audit Database if you want to see the exact error or warning text. Make sure that Audit Database settings are configured properly, follow the Audit Database

Step 5 – Click Configure next to Audit archiving filters and select the Netwrix Auditor System Health Log filter in the Inclusive Filters list.

This procedure describes the basic steps, required for creation of the monitoring plan that will be used to collect data on Netwrix Auditor health status events.

Review Past Event Log Entries

Netwrix Auditor Event Log Manager collects event log entries and stores them to the Audit Archive. Follow the steps to review past events.

Step 1 – On the main Netwrix Auditor Event Log Manager page, click View next to View collected events.

Step 2 – In the Netwrix Auditor Event Viewer window, complete the following to narrow results:

Option	Description
Monitoring plan	Select the monitoring plan that audits desired event log entries.
Computer	If you have several items in the monitoring plan, adjust a computer.
Event log	Select event log that contains desired entries.
From... To...	Specify the time range for which you want to retrieve past audit data.

Import Audit Data with the Database Importer

Follow the steps to Import Audit Data with the Database Importer.

Step 1 – On the main Netwrix Auditor Event Log Manager page, click Import Data.

Step 2 – Select a monitoring plan and the time range for which you want to import data.

Step 3 – Click Import.

Permissions 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:

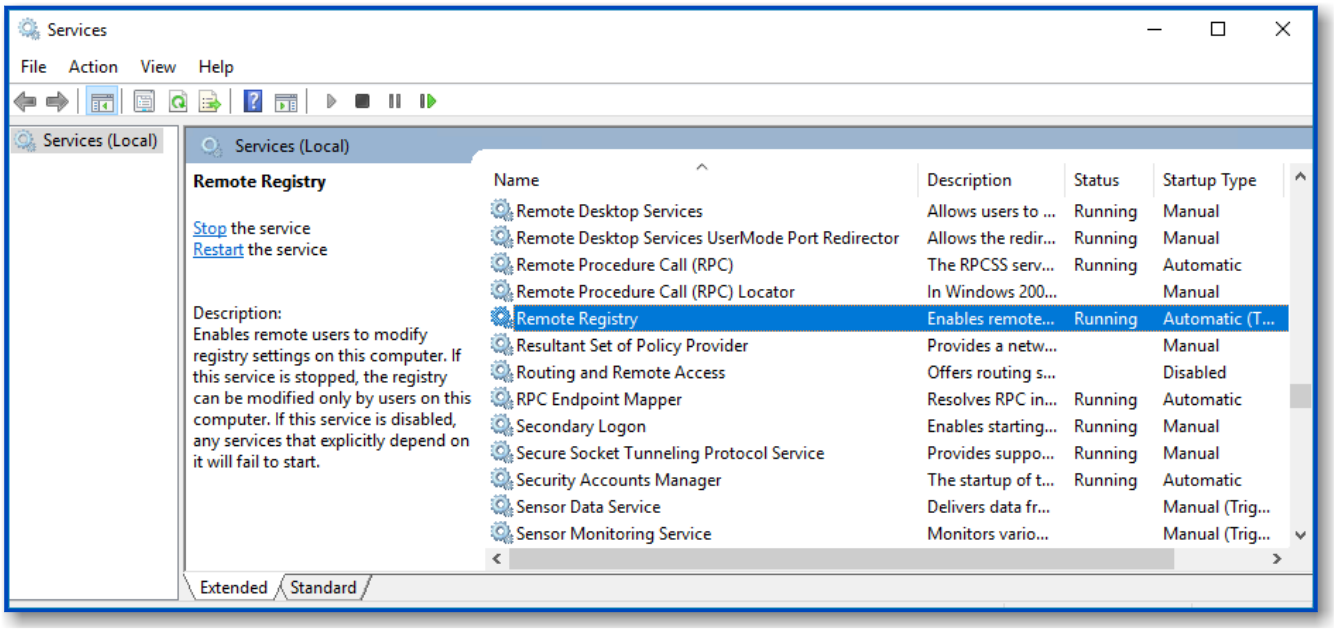
The account must have be a member of the local Administrators group.

Windows Event Logs

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

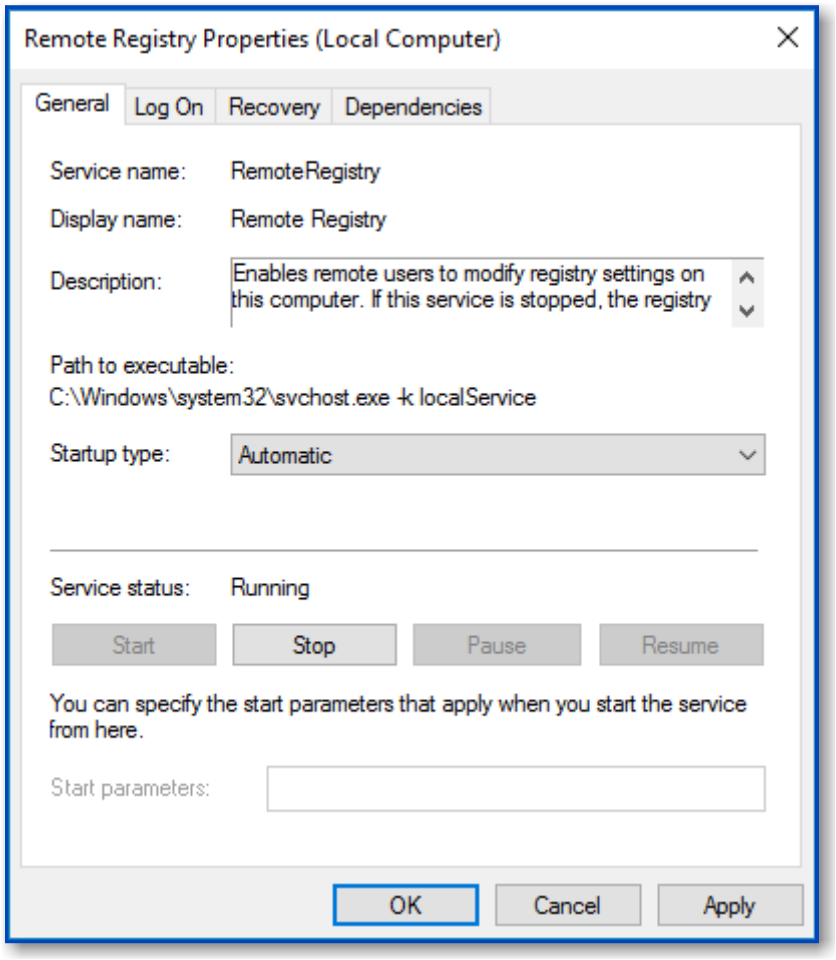
Follow the steps to enable the Remote Registry service.

Step 1 – Navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > **Services**.



Step 2 – In the **Services** dialog, locate the **Remote Registry** service, right-click it and select **Properties**.

Step 3 – In the **Remote Registry Properties** dialog, make sure that the **Startup type** parameter is set to *"Automatic"* and click **Start**.



Step 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.

NOTE: The Remote Registry should be enabled on the target server.

Event Log

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Event Log monitoring scope.

Follow the steps to exclude data from the Event Log monitoring scope:

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Event Log Management* folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.

- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
OmitErrorsList.txt	Contains a list of data collection errors and warnings to be excluded from the Netwrix Auditor System Health event log.	`Error text`

omitServerList.txt	Contains a list of server names or servers IP addresses to be excluded from processing.	`ip address` or `server name`
		For example:
		`192.168.3.*`

Inactive User Tracker

Auditor Inactive User Tracker standalone tool discovers inactive user and computer accounts. It performs the following tasks:

- Checks the managed domain or specific organizational units by inquiring all domain controllers, and sends reports to managers and system administrators listing all accounts that have been inactive for the specified number of days.
- Automatically deactivates inactive accounts by settings a random password, disabling, deleting or moving them to a specified organizational unit.

  NOTE: The password that is generated will contain uppercase and lowercase letters, numbers and special characters. The default value for the password length is 15 characters. You can modify this password any time by configuring registry keys. See the Registry Keys topic for additional information.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

- Windows Server 2012

Create Monitoring Plan to Audit Inactive Users

Follow the steps to create a monitoring plan to audit inactive users.

Step 1 – Navigate to Start > Netwrix Auditor > Netwrix Auditor Inactive Users Tracker.

Step 2 – On the main page, you will be prompted to select a monitoring plan. Click Add to add a new monitoring plan.

Step 3 – Configure basic parameters as follows:

Option	Description
Enable inactive user tracking	Select the checkbox to discover inactive users in your Active Directory domain.
Audited domain	Specify domain name in the FQDN format.
Send report to administrators	Enable this option and specify one or several email addresses for administrators to receive daily reports with a list of inactive users. Use semicolon to separate several addresses.

Step 4 – Navigate to the General tab and complete the following fields:

Option	Description
Specify account which will be used to collect data: • **User name** • **Password**	Enter the account which will be used for data collection.

Option	Description
	See theData Collecting Account topic for additional information about the full list of the rights and permissions for the account.
Consider user inactive after	Specify account inactivity period, after which a user is considered to be inactive.
Customize the report template	Click Edit to edit the notification template, for example, modify the text of the message. You can use HTML tags when editing a template.
Attach report as a CSV files	Select this option to receive reports attached to emails as CSV files.

Step 5 – Navigate to the Actions tab and complete the following fields:

Option	Description
Notify manager after	Specify account inactivity period, after which the account owner's manager must be notified.
Set random password after	Specify account inactivity period, after which a random password will be set for this account.
Disable accounts after	Specify account inactivity period, after which the account will be disabled.

Option	Description
Move to a specific OU after	• Specify account inactivity period, after which the account will be moved to a specified organizational unit. • OU name—Specify OU name or select an AD container using  button.
Delete accounts after	Specify account inactivity period, after which the account will be removed.
Delete account with all its subnodes	Select this checkbox to delete an account that is a container for objects.
Notify managers only once	If this checkbox is selected, managers receive one notification on account inactivity and one on every action on accounts. Managers will receive a notification in the day when the account inactivity time will be the same as specified in the inactivity period settings. By default, managers receive notifications every day after the time interval of inactivity specified in the Notify managers after entry field.

Step 6 – Navigate to the Advanced tab and complete the following fields:

Option	Description
Filter by account name	Specify one or several user account names (e.g., *John*). Use semicolon to separate several names. Only user accounts that contain selected name will be notified and included in the administrators and managers reports.

Option	Description
Filter by organizational unit	To audit inactive users that belong to certain organizational units within your Active Directory domain, select this option and click Select OUs. In the dialog that opens, specify the OUs that you want to audit. Only users belonging to these OUs will be notified and included in the administrators and managers reports.
Process user accounts	Select this checkbox to audit user accounts.
Process computer accounts	Select this checkbox to audit computer accounts.

Step 7 – Navigate to the Notifications tab and complete the following fields:

Option	Description
Use Netwrix Auditor notification settings	Select this option if you want to use modern authentication. Please note that modern authentication must already be configured in the monitoring plan you are going to use. If you select this option, the fields below are not needed.
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the From field.

Option	Description
	RECOMMENDED: click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission. The option is not available for auditing User Activity as well Netwrix Auditor tools.
Display the following From address in email notifications	Enter the address that will appear in the "*From*" field in email notifications. This option does not affect notifications sent to users' managers and administrators. Before configuring the

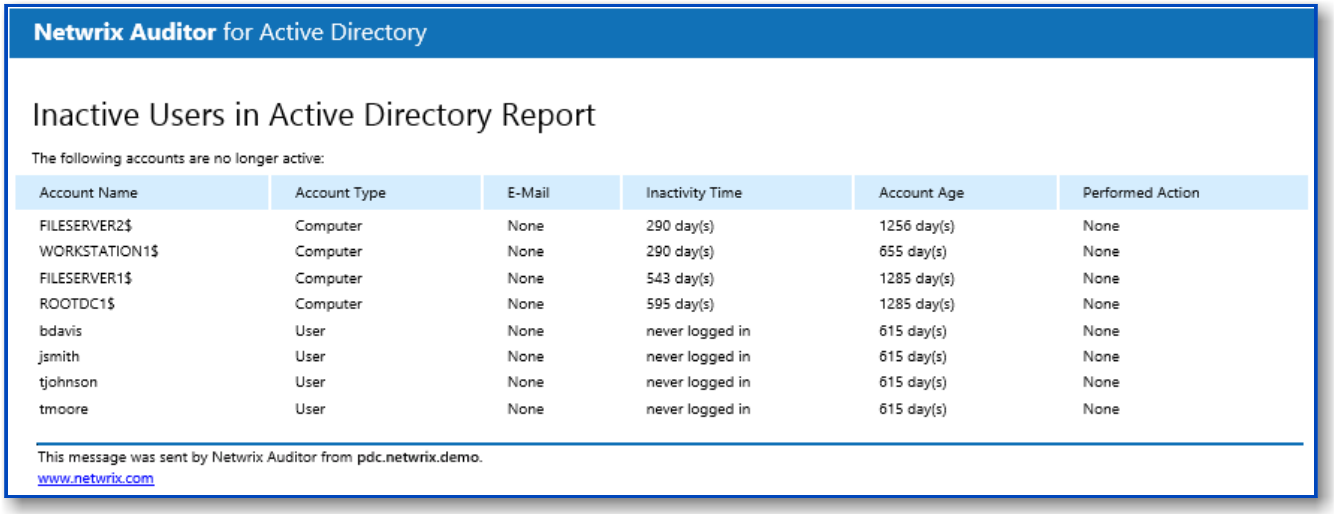
Option	Description
	"*From*" field for user email notifications, make sure that your Exchange supports this option.

Review your configuration and click Save.

Review Report on Inactive Users

Follow the steps to review report on inactive users.

Step 1 – Click Generate next to Generate report on inactive users to view report immediately.



Netwrix Auditor for Active Directory

Inactive Users in Active Directory Report

The following accounts are no longer active:

Account Name	Account Type	E-Mail	Inactivity Time	Account Age	Performed Action
FILESERVER2$	Computer	None	290 day(s)	1256 day(s)	None
WORKSTATION1$	Computer	None	290 day(s)	655 day(s)	None
FILESERVER1$	Computer	None	543 day(s)	1285 day(s)	None
ROOTDC1$	Computer	None	595 day(s)	1285 day(s)	None
bdavis	User	None	never logged in	615 day(s)	None
jsmith	User	None	never logged in	615 day(s)	None
tjohnson	User	None	never logged in	615 day(s)	None
tmoore	User	None	never logged in	615 day(s)	None

This message was sent by Netwrix Auditor from pdc.netwrix.demo.
www.netwrix.com

Registry Keys

Review the basic registry keys that you may need to configure for monitoring inactive users within your Active Directory domain with Netwrix Auditor. Navigate to Start > Run and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Inactive Users Tracker	
HideEmailAdditionalInfo	Defines whether to show or hide the header and footer in emails sent to managers (emails sent to administrators always have default header and footer): • 0—Show • Any other number—Hide
RandomPasswordLength	Defines the length of a random password to be set for inactive user.
WriteEventLog	Defines whether to write events to the Application Log: • 0—No • 1—Yes

Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Inactive User monitoring scope.

Follow the steps to exclude data from the Inactive Users monitoring scope:

Step 1 – Navigate to the `%PROGRAMDATA%\Netwrix Auditor\Inactive Users Tracker` folder.

NOTE: This is default location. However, it may be changed because users can move this folder.

Step 2 – Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
filter.txt	Contains a list of accounts to be excluded from processing.	`Username`
omitdclist.txt	Contains a list of domain controllers to be excluded from processing. Auditor skips all automated deactivation actions for inactive accounts (disable, move, delete) even if one domain controller is unavailable during scheduled task execution. Add the unavailable domain controllers to this file to ensure Auditor functions properly.	`Full DNS name` or `NetBIOS name` IP addresses are not supported.

omitoulist.txt	Contains a list of organizational units to be excluded from processing.	`Path`
		
		`*OU=OUNAME*`
		
		For example:
		
		If the OU is
		
		"sampledomain.sample/sampling", the syntax should be:
		
		`*OU=sampling*`

Object Restore for Active Directory

With Netwrix Auditor you can quickly restore deleted and modified objects using the Netwrix Auditor Object Restore for Active Directory tool shipped with the product. This tool enables AD

object restore without rebooting a domain controller and affecting the rest of the AD structure, and goes beyond the standard tombstone capabilities.

The following Windows Server versions are supported:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Perform the following procedures:

- Modify Schema Container Settings
- Roll Back Unwanted Changes

Modify Schema Container Settings

By default, when a user or computer account is deleted from Active Directory, its password is discarded as well as a domain membership. When you restore deleted accounts with the Netwrix Auditor Object Restore for Active Directory tool, it rolls back a membership in domain and sets random passwords which then have to be changed manually. If you want to be able to restore AD objects with their passwords preserved, you must modify the Schema container settings so that account passwords are retained when accounts are being deleted.

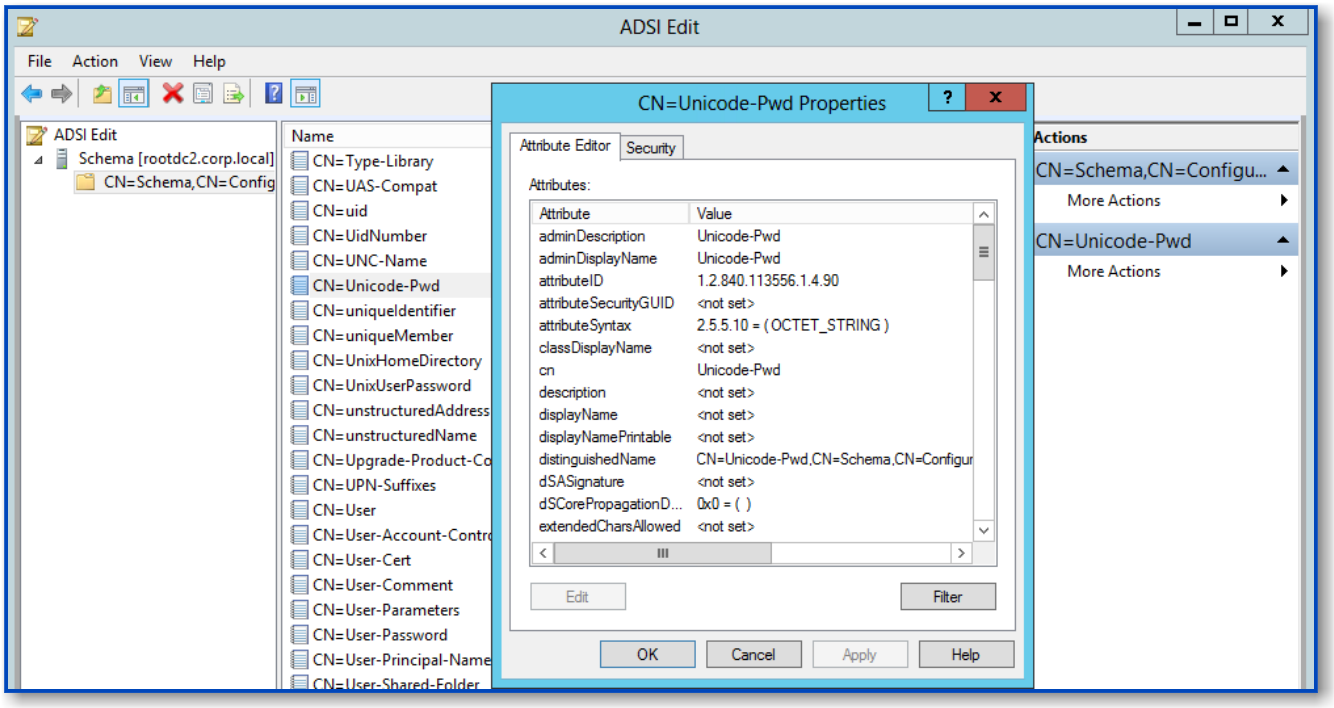
To perform this procedure, you will need the ADSI Edit utility.utility.

Follow the steps to modify schema container settings.

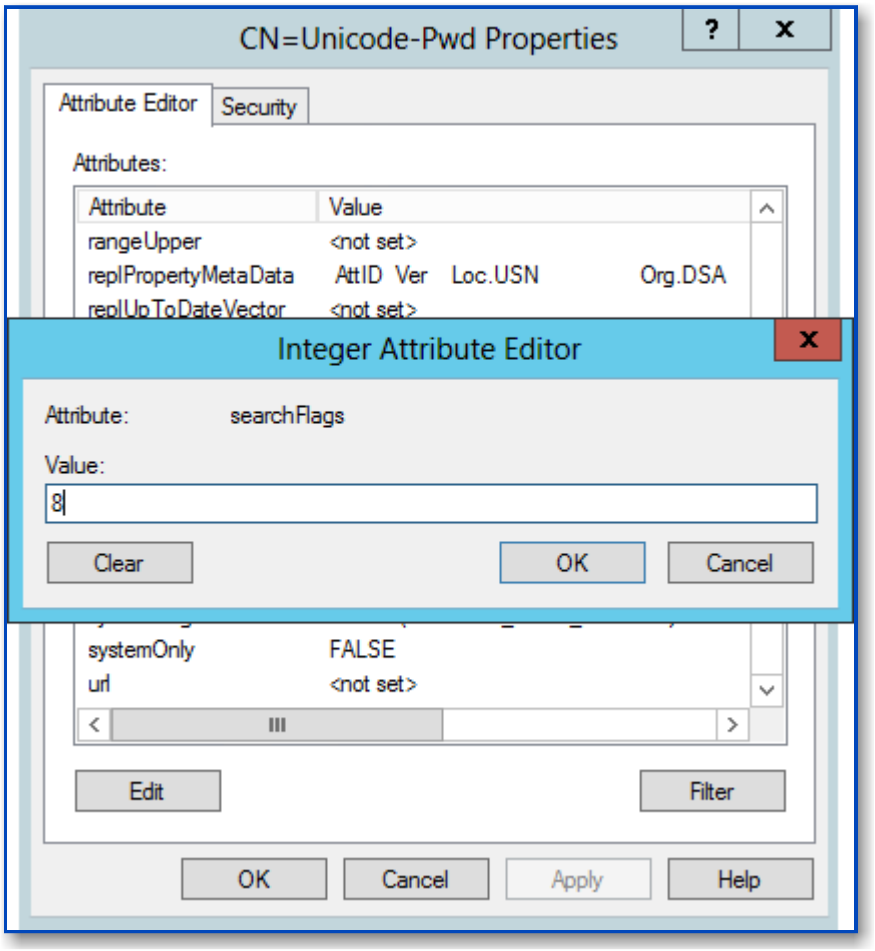
Step 1 – Navigate to **Start** > **Windows Administrative Tools (Windows Server 2016 and higher) or** Administrative Tools **(Windows 2012)** > ADSI Edit.

Step 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 **Schema** from the drop-down list.

Step 3 – Expand the Schema your_Root_Domain_name node. Right-click the CN=Unicode-Pwd attribute and select Properties.



Step 4 – Double-click the searchFlags attribute and set its value to *"8"*.



Now you will be able to restore deleted accounts with their passwords preserved.

Roll Back Unwanted Changes

Follow the steps to roll back unwanted changes.

Step 1 – Navigate to Start > Netwrix Auditor > Netwrix Auditor Object Restore for Active Directory.

Step 2 – On the Select Rollback Period step, specify the period of time when the changes that you want to revert occurred. You can either select a period between a specified date and the present date, or between two specified dates.

Step 3 – On the Select Rollback Source step, specify the rollback source. The following restore options are available:

- State-in-time snapshots — This option allows restoring objects from configuration snapshots made by Netwrix Auditor. This option is more preferable since it allows to restore AD objects with all their attributes.

  Complete the following fields:

Option	Description
Audited domain	Select a domain where changes that you want to rollback occurred.
Select a state-in-time snapshot	Select if you want to revert to a specific snapshot. Otherwise, the program will automatically search for the most recent snapshot that will cover the selected time period.

- Active Directory tombstones — This option is recommended when no snapshot is available. This is a last resort measure as the tombstone holds only the basic object attributes.

Step 4 – On the Analyzing Changes step, the product analyzes the changes made during the specified time period. When reverting to a snapshot, the tool reviews the changes that occurred between the specified snapshots. When restoring from a tombstone, the tool reviews all AD objects put in the tombstone during the specified period of time.

Step 5 – On the Rollback Results step, the analysis results are displayed. Select a change to see its rollback details in the bottom of the window. Select an attribute and click Details to see what changes will be applied if this attribute is selected for rollback. Check the changes you want to roll back to their previous state.

Wait until the tool has finished restoring the selected objects. On the last step, review the results and click Finish to exit the wizard.

Password Expiration Notifier

Netwrix Auditor Password Expiration Notifier standalone tool checks which domain accounts or passwords are about to expire in the specified number of days and sends notifications to users. It also generates summary reports that can be delivered to system administrators and/or users'

managers. Besides, Netwrix Auditor Password Expiration Notifier allows checking the effects of a password policy change before applying it to the managed domain.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

Review the following for additional information:

- Configure Password Expiration Alerting
- Registry Key Configuration
- Password Expiration Notifier Ports
- Password Expiration Monitoring Scope

Configure Password Expiration Alerting

Follow the steps to configure password expiration alerting.

Step 1 – Navigate to **Start** > **Netwrix Auditor** > **Password Expiration Notifier**.

Step 2 – On the main page, you will be prompted to select a monitoring plan. Click Add to add a new monitoring plan.

Step 3 – Configure basic parameters as follows:

Option	Description
Enable password expiration alerting or inactive user tracking	Select the checkbox to discover expiring passwords or inactive users in your Active Directory domain.
Audited domain	Specify domain name in the FQDN format.

Option	Description
Send report to administrators	Enable this option and specify one or several email addresses for administrators to receive daily reports with a list of inactive users whose accounts/passwords are going to expire in the specified number of days. Use semicolon to separate several addresses.

Step 4 – Navigate to the General tab and complete the following fields:

Option	Description
Specify account which will be used to collect data: • **User name** • **Password**	Enter the account which will be used for data collection. For a full list of the rights and permissions this account, and instructions on how to configure them, refer to Monitoring Plans.
Filter users by organizational unit	To audit users for expiring accounts/passwords that belong to certain organizational units within your Active Directory domain, select this option and click Select OUs. In the dialog that opens, specify the OUs that you want to audit. Only users belonging to these OUs will be notified and included in the administrators and managers reports.
Filter users by group	To audit users for expiring accounts/passwords that belong to certain groups within your Active Directory domain, select this option and click Select Groups. In the dialog that opens, specify the groups that you want to audit. Only users belonging to these groups will be notified and included in the administrators and managers reports.

Option	Description
Filter by account name	Specify one or several user account names (e.g., *John*). Use semicolon to separate several names. Only user accounts that contain selected name will be notified and included in the administrators and managers reports.

Step 5 – Navigate to the Actions tab and complete the following fields:

Option	Description
Send report to the users' managers	Enable this option to deliver reports to the user's managers. To review and edit the user's managers 1. Start Active Directory Users and Computers. 2. Navigate to each group where the user belongs to, right-click it and select Properties. 3. In the <user account> Properties dialog, select the Managed By tab and review a manager. Update it if necessary. To edit a report template, click **Customize**. You can use HTML tags when editing a template.
List users whose accounts or passwords expire in <> days or less	Specify the expiration period for accounts and/or passwords to be included in the administrators and managers reports.

Option	Description
Only report on users with expiring accounts	Select this option to deliver reports on users with expiring accounts only and ignore users whose passwords will be valid for a rather long time.
Notify users	Select this option to notify users that their passwords and/or accounts are about to expire.
Every day if password expires in <> days or less	Select this option for users to be notified daily that their passwords are going to expire, and specify the number of days before the expiration date. To edit a report template, click **Customize**. You can use HTML tags when editing a template. In order to send a test email, click Test and select an account. Make sure this account has a password that expires within the period you specifed next to this option.
First/Second/Last time when password expires in <> days	Select this option for users to be notified three times, and specify the number of days before the expiration date for each of three notifications. To edit a report template, click **Customize**. You can use HTML tags when editing a template. In order to send a test email, click Test and select an account. Make sure this account has a password that expires within the period you specifed next to this option.
Notify users by email every day if their accounts expire in <> days	Select this option for users to be notified daily that their account is going to expire, and specify the number of days before the expiration date.

Option	Description
Notify users by text messages	Select this option for users to receive text messages if their passwords are about to expire. To edit SMS Notifications template, click Customize. • Every day if password expires in <> days or less—Select this option for users to be notified daily that their passwords are going to expire, and specify the number of days before the expiration date. • First/Second/Last time when password expires in <> days—Select this option for users to be notified three times, and specify the number of days before the expiration date for each of three notifications. • Provider name—Specify provider name. • Property name—Specify the name of the Active Directory User Property where the recipient's phone number is stored. Pager is the default property. If the Pager property of an AD User contains a full email address, Provider Name will be ignored. In order to send a test email, click Test and select an account. Make sure this account has a password that expires within the period you specifed next to this option.

Step 6 – Navigate to the Notifications tab and complete the following fields:

Option	Description
Use Netwrix Auditor notification settings	Select this option if you want to use modern authentication. Please note that modern authentication must already be configured in the

Option	Description
	monitoring plan you are going to use. If you select this option, the fields below are not needed.
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the From field. ***RECOMMENDED:*** click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.

Option	Description
Use implicit SSL	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission. The option is not available for auditing User Activity as well Netwrix Auditor tools.
Display the following From address in email notifications	Enter the address that will appear in the "*From*" field in email notifications. This option does not affect notifications sent to users' managers and administrators. Before configuring the "*From*" field for user email notifications, make sure that your Exchange supports this option.

Step 7 – Navigate to the Advanced tab and complete the following fields:

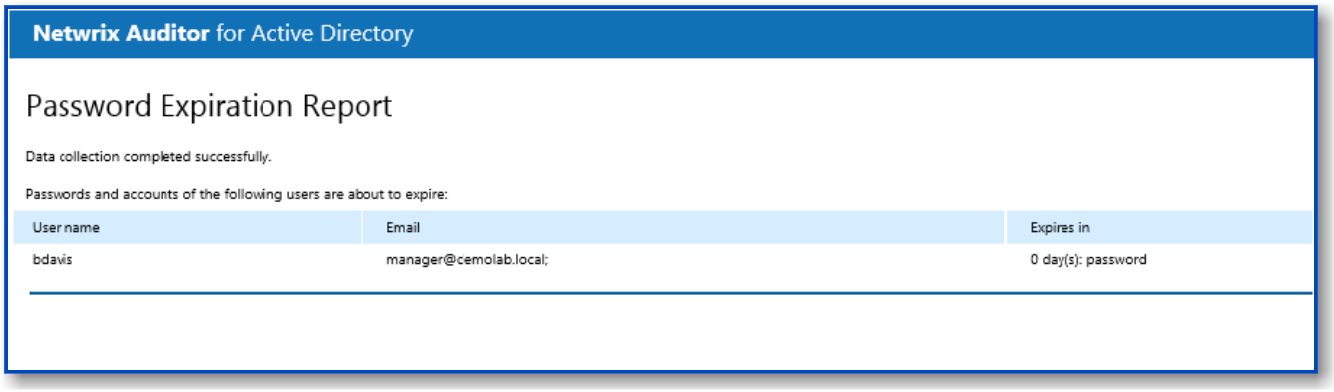
Option	Description
Modify scheduled task start time	The default start time of the scheduled task is 3.00 AM every day. Click Modify to configure custom schedule.
Customize the report template	Click Customize to edit the notification template, for example, modify the text of the message. You can use HTML tags when editing a template.

Option	Description
Attach reports as a CSV files	Select this option to receive reports attached to emails as CSV files.
Ignore users who must change password at next logon	Select this option to exclude users who must change password at next logon from reports.
Ignore users with the "*Password never expires*" option enabled	Select this option to exclude users with the "*Password never expires*" option enabled from reports.
Ignore users who do not have email accounts	Select this option to exclude users who do not have email accounts from reports.
Ignore users whose passwords have already expired	Select this option to exclude users whose passwords have already expired from reports.
Include data on expiring accounts	Select this option to include data on expiring domain accounts further to expiring passwords information.
Only report on users with fine-grained password policies applied	Select this option to include in reports only users who have fine-grained policies applied.

Step 8 – If you want to save your current configuration, click Save.

To review Password Expiration Report

Click Generate next to Generate report on users with expired account or passwords to view report on users passwords immediately. In the Maximum Password Age Setting dialog that opens, select domain policy settings or specify the maximum password age in days.



Registry Key Configuration

Review the basic registry keys that you may need to configure for monitoring expiring passwords within your Active Directory domain with Netwrix Auditor. Navigate to **Start > Run** and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Password Expiration Notifier	
HideEmailAdditionalInfo	Defines whether to show or hide the header and footer in emails sent to users and their managers (emails sent to administrators always have default header and footer): • 0—Show • Any other number—Hide

Password Expiration Notifier Ports

Review a protocol and port required for Netwrix Auditor Password Expiration Notifier.

NOTE: Tip for reading the table – On the compuer where the Netwrix Auditor server resides (source), allow outbound connections to remote 389 the TCP port. On domain controllers in your domain (target), allow inbound connections to the local 389 TCP port.

Port	Protocol	Source	Target	Purpose
Password Expiration Notifier				
389	TCP	Netwrix Auditor Server	Domain controllers	LDAP Common queries

Password Expiration Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from monitoring and alerting on password expiration.

Follow the steps to exclude data from the Active Directory monitoring scope.

Step 1 – Navigate to the *%Netwrix Auditor installation folder%\Password Expiration Alerting*folder.

Step 2 – Edit the omitoulist.txt file, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. You can use * for cmdlets and their parameters.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitoulist.txt	This file defines a list of OUs to exclude from being audited. To specify the OUs and their subOUs, type names each on a separate line.	Name For example: *OU=C,OU=B,OU=A*

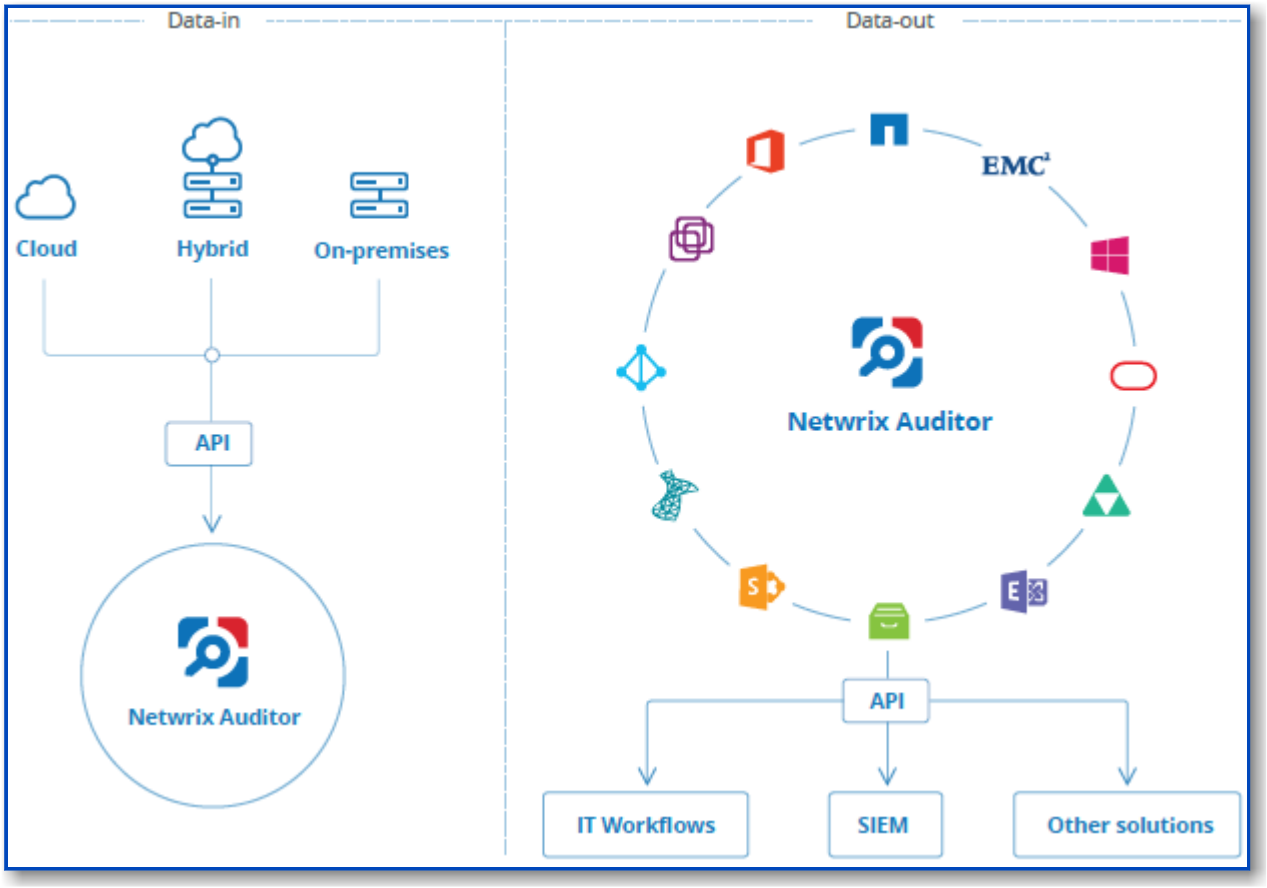
Integration API

Netwrix Auditor Netwrix Risk Insights leverages Netwrix Auditor Integration API. Although you can always use the add-on as is, but Netwrix encourages customers to create their own integration add-ons. The add-ons created based on Netwrix Auditor Integration API capabilities are easily tailored to your specific environment and business requirements.

Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

The Netwrix Auditor Integration API provides access to audit data collected by Netwrix Auditor through REST API endpoints. According to the RESTful model, each operation is associated with a URL. Integration API provides the following capabilities:

- Data in: Solidify security and meet regulatory compliance standards by enabling visibility into what is going on in any third-party application.
- Data out: Further automate your business processes, IT security and operations workflows by enriching third-party solutions with actionable audit data.



Netwrix Auditor Integration API operates with XML- and JSON-formatted Activity Records—minimal chunks of audit data containing information on *who* changed *what*, *when* and *where* this change was made. XML format is set as default.

With Integration API you can write Activity Records to the SQL Server-based Audit Database and access audit data from remote computers. Also, Netwrix prepares add-ons—sample scripts—to help you integrate your SIEM solutions with Netwrix Auditor.

Netwrix Auditor Integration API Service is responsible for processing API requests. This component is installed along with Netwrix Auditor Server and is enabled automatically. By default, Netwrix Auditor Integration API works over HTTPS protocol using an automatically generated certificate. Default communication port is 9699.

Netwrix does not limit you with applications that can be used with Integration API. You can write RESTful requests using any tool or application you prefer—cURL, Telerik Fiddler, various Google Chrome or Mozilla FireFox plug-ins, etc.

Integration Option

Integration is a custom item type that helps diversify activity records coming from custom sources and integrations (e.g., Amazon Web Services, Cisco devices) within Netwrix API data source. It is optional to add this item to your monitoring plan.

Complete the following fields:

Option	Description
Specify a name for your integration	Specify the add-on name or provide any other name that distinguishes this custom source from any other. This name will be listed in the Item filter in the interactive search.

Make sure Integration API is enabled. To check it, navigate to Settings → Integrations tab. See Integrations for more information.

Make sure to provide a monitoring plan name and item name in activity records before importing data.

Prerequisites

Configure Integration API Settings

By default, for communication Netwrix Auditor Integration API uses HTTPS with automatically generated certificate. Default communication port is 9699.

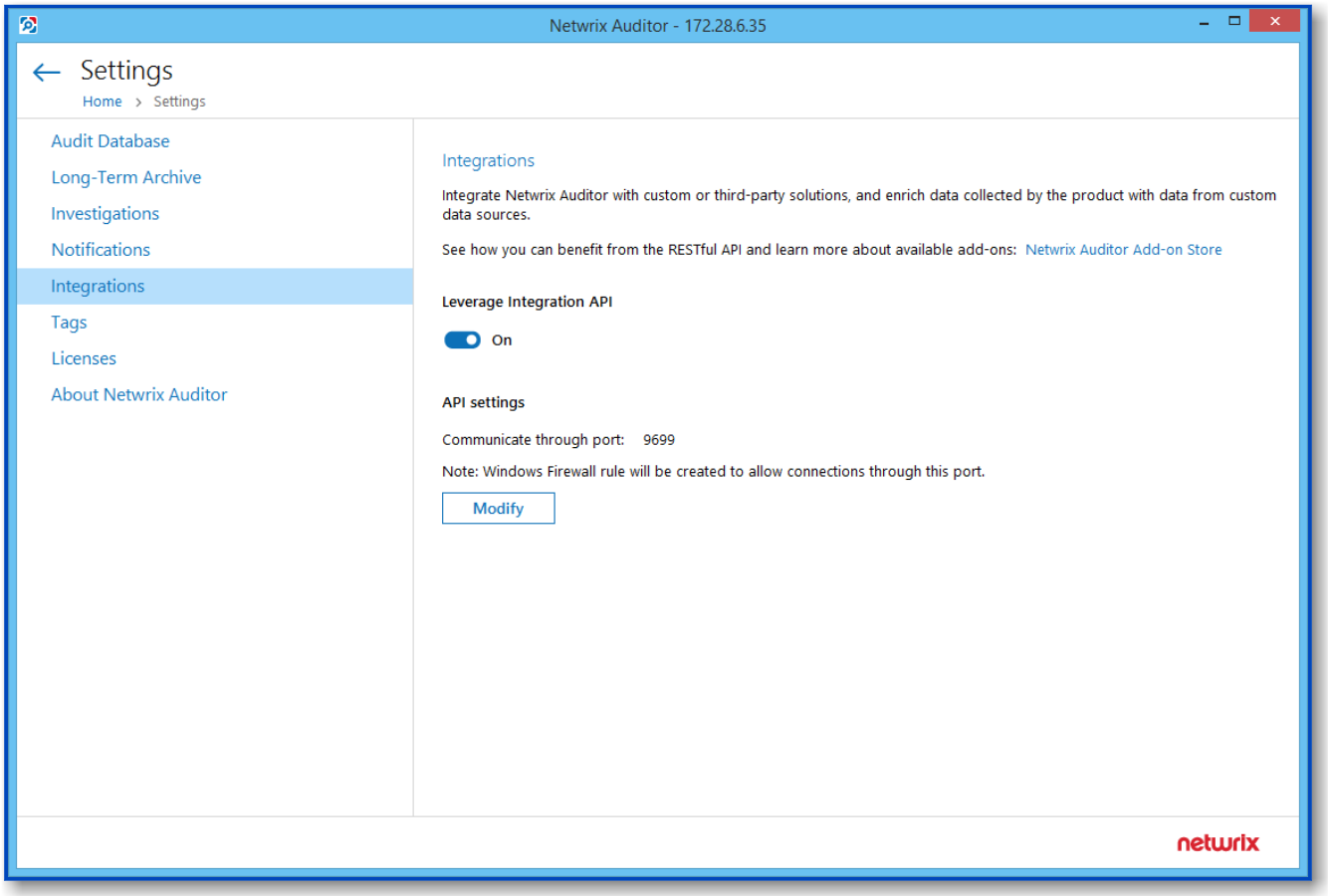
Securityhow to disable HTTPS and manage other API settings.

To change port

1. In the Netwrix Auditor main window, navigate to the Integration tile.
2. Make sure the Leverage Integration API option is set to *"On"*.

3. Click Modify under the API settings section and specify a port number. Windows firewall rule will be automatically created.

   If you use a third-party firewall, you must create a rule for inbound connections manually.



Configure Audit Database Settings

When you first configure the Audit Database settings in Netwrix Auditor, the product also creates several databases for special purposes, including Netwrix_Auditor_API. This database is designed to store data imported from the other sources using Netwrix Auditor Integration API.

Make sure the Audit Database settings are configured in Netwrix Auditor. To check or configure these settings, navigate to Settings → Audit Database.

You cannot use Netwrix Auditor Integration API without configuring the Audit Database.

Audit Database how to configure SQL Server settings.

API Endpoints

Method	Endpoint	POST Data	Description
GET	/netwrix/api/v1/activity_records/enum	—	Returns Activity Records. Retrieve Activity Records
POST	/netwrix/api/v1/activity_records/enum	Continuation Mark	Returns next 1,000 Activity Records. Continuation Mark
POST	/netwrix/api/v1/activity_records/search	Search Parameters	Returns Activity Records matching a criteria defined in search parameters. Search Activity Records
POST	/netwrix/api/v1/activity_records/	Activity Records	Writes data to the Audit Database. Write Activity Records

Authentication

Authentication is required for all endpoints. The following authentication methods are supported:

- NTLM—recommended

  If NTLM authentication is disabled through a group policy, you will not be able to address Netwrix Auditor Server by its IP address.

- Negotiate
- Digest
- Basic

Account Permissions

Netwrix Auditor restricts control to its configuration and data collected by the product. Role-based access system ensures that only relevant employees and services can access the exact amount of data they need. To be able to retrieve activity records or supply data to the Audit Database, an account must be assigned a role in the product. Role-Based Access and Delegation

To...	Required role
Retrieve all activity records and write data	The user must be assigned the Global administrator role in the product, or be a member of the Netwrix Auditor Administrators group on the computer that hosts Netwrix Auditor Server.
Retrieve all activity records	The user must be assigned the Global reviewer role in the product or be a member of the Netwrix Auditor Client Users group on the computer that hosts Netwrix Auditor Server.
Retrieve activity records within a limited scope	The user must be assigned the Reviewer role on a monitoring plan or folder with plans. In this case, Netwrix Auditor Server will retrieve only activity records the user is allowed to review according to the scope delegated (e.g., a scope can be limited to a single domain or file share).

To...	Required role
Write activity records	The user must be assigned the Contributor role in the product.

Review the example below to see how to authenticate in cURL:

- `curl https://172.28.6.15:9699/netwrix/api/v1/activity_records/enum -u Enterprise\NetwrixUser:NetwrixIsCool`

Reference for Creating Activity Records

The table below describes Activity Record elements.

Netwrix recommends limiting the input Activity Records file to 50MB and maximum 1,000 Activity Records.

Element	Mandatory	Datatype	Description
Activity Record main elements			
RID	No	string	RID is a unique key of the Activity Record. The identifier is created automatically when you write an Activity Record to the Audit Database. RID is included in output Activity Records only.
Who	Yes	nvarchar 255	A specific user who made the change (e.g., *Enterprise\ Administrator*, *Admin@enterprise.onmicrosoft.com*).
Action	Yes	—	Activity captured by Auditor (varies depending on the data source):

Element	Mandatory	Datatype	Description	
			• Added	• Add (Failed Attempt)
			• Removed	• Remove (Failed Attempt)
			• Modified	• Modify (Failed Attempt)
			• Read	• Read (Failed Attempt)
			• Moved	• Move (Failed Attempt)
			• Renamed	• Rename (Failed Attempt)
			• Checked in	• Checked out
			• Discard check out	• Successful Logon

Element	Mandatory	Datatype	Description
			• Failed Logon • Logoff • Copied • Sent • Session start • Session end • Activated
What	Yes	nvarchar max	A specific object that was changed (e.g., *NewPolicy*).
When	Yes	dateTime	The moment when the change occurred. When supports the following datetime formats: • YYYY-mm-ddTHH:MM:SSZ—Indicates UTC time (zero offset) • YYYY-mm-ddTHH:MM:SS+HH:MM—Indicates time zones ahead of UTC (positive offset) • YYYY-mm-ddTHH:MM:SS-HH:MM—Indicates time zones behind UTC (negative offset)

Element	Mandatory	Datatype	Description
Where	Yes	nvarchar 255	A resource where the change was made (e.g., *Enterprise-SQL*, *FileStorage.enterprise.local*). The resource name can be a FQDN or NETBIOS server name, Active Directory domain or container, SQL Server instance, SharePoint farm, VMware host, etc.
ObjectType	Yes	nvarchar 255	An type of affected object or its class (e.g., *user, mailbox*).
MonitoringPlan	No	nvarchar 255	The Auditor object that responsible for monitoring of a given data source and item. Sub-elements: Name and ID. If you provide a monitoring plan name for input Activity Records, make sure the plan is created in Auditor, the Netwrix API data source is added to the plan and enabled for monitoring. In this case, data will be written to the database associated with this plan.
DataSource	No	nvarchar max	IT infrastructure monitored with Auditor (e.g., *Active Directory*). For input Activity Records, the data source is

Element	Mandatory	Datatype	Description
			automatically set to Netwrix API.
Item	No	nvarchar max	The exact object that is monitored (e.g., a domain name, SharePoint farm name) or integration name. Sub-element: Name. The item type is added inside the name value in brackets (e.g., *enterprise.local (Domain)*). For input Activity Records, the type is automatically set to Integration, you do not need to provide it. The output Activity Records may contain the following item types depending on the monitoring plan configuration: • AD container • Computer • Domain • EMC Isilon • NetApp • Office 365 tenant • Oracle Database instance • SharePoint farm

Element	Mandatory	Datatype	Description
			• Dell VNX/ VNXe • SQL Server instance • Integration • VMware ESX/ ESXi/ vCenter • IP range • Windows file share If you provide an item name for input Activity Records, make sure this item is included in the monitoring plan within the Netwrix API data source. If you specify an item that does not exist, data will be written to the plan's database anyway but will not be available for search using the Item filter.
Workstation	No	nvarchar max	An originating workstation from which the change was made (e.g., *WKSwin12.enterprise.local*).
IsArchiveOnly	No	—	IsArchiveOnly allows to save Activity Record to the Long-Term Archive only. In this case, these Activity Records will not be

Element	Mandatory	Datatype	Description
			available for search in the Auditor client.
DetailList	No	—	Information specific to the data source, e.g., assigned permissions, before and after values, start and end dates. References details.
Detail sub-elements (provided that DetailList exists)			
PropertyName	Yes	nvarchar 255	The name of a modified property.
Message	No	string	Object-specific details about the change. Message is included in output Activity Records only.
Before	No	ntext	The previous value of the modified property.
After	No	ntext	The new value of the modified property.

Retrieve Activity Records

Endpoint

Use to export data from the Audit Database. By default, first 1,000 Activity Records are returned. To get the next Activity Records, send a POST request to the same endpoint containing a Continuation mark.

Method	Endpoint	POST Data
GET	`https://{host:port}/netwrix/api/v1/activity_records/enum{?format=json}{&count=Number}`	—
POST	`https://{host:port}/netwrix/api/v1/activity_records/enum{?format=json}{&count=Number}`	Continuation Mark

Request Parameters

Parameter	Mandatory	Description
`host:port`	Yes	Replace with the IP address or a name of your Netwrix Auditor Server host and port (e.g., *172.28.6.15:9699*, *stationwin12:9699*, *WKSWin2012.enterprise.local:9699*). With enabled HTTPS, provide the computer name as it appears in certificate properties.
`format=json`	No	Add this parameter to retrieve data in JSON format. Otherwise, XML-formatted Activity Records will be returned.
`count=Number`	No	Add this parameter to define the number of Activity Records to be

Parameter	Mandatory	Description
		exported. Replace `Number` with a number (e.g., `&count=1500`).

Optional parameters (format and count) can be provided in any order. The first parameter must start with ?, others are joined with &, no spaces required (e.g., `?format=json&count=1500`).

Response

Request Status	Response

Success	The HTTP status code in the response header is 200 OK. The response body contains Activity Records and Continuation Mark.
	`HTTP/1.1 200 OK`
	`Server: Microsoft-HTTPAPI/2.0`
	`Content-Length: 311896`
	`Content-Type: application/xml`
	`Date: Fri, 08 Apr 2017 13:56:22 GMT`

Error	The header status code is an error code. Depending on the error code, the response body may contain an error object. See Response Status Codes for more information.

Usage Example—Retrieve All Activity Records

This example describes how to retrieve all Activity Records from the Audit Database.

1. Send a GET request. For example:

Format	Request
XML	`curl https://WKSWin2012:9699/netwrix/api/v1/activity_records/enum -u Enterprise\NetwrixUser:NetwrixIsCool`
JSON	`curl https://WKSWin2012:9699/netwrix/api/v1/activity_records/enum?format=json -u Enterprise\NetwrixUser:NetwrixIsCool`

2. Receive the response. Activity Records are retrieved according to the account's delegated scope. Below is an example of a successful GET request. The status is 200 OK. For XML, a response body contains the `ActivityRecordList` root element with Activity Records and a Continuation mark inside. For JSON, a response body contains the `ActivityRecordList` array with Activity Records collected in braces {} and a Continuation mark.

XML

```
<?xml version="1.0" standalone="yes"?>
<ActivityRecordList xmlns="http://schemas.netwrix.com/api/v1/activity_records/
<ContinuationMark>PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A↙ContinuationMark>
                        <ActivityRecord>
                        <MonitoringPlan>
                    <Name>AD Monitoring↙Name>
            <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
                        ↙MonitoringPlan>
                <DataSource>Active Directory↙DataSource>
                        <Item>
                <Name>enterprise.local (Domain)↙Name>
                        ↙Item>
                    <ObjectType>user↙ObjectType>
        <RID>20160215110503420B9451771F5964A9EAC0A5F35307EA155↙RID>
              <What>\local\enterprise\Users\Jason Smith↙What>
                        <Action>Added↙Action>
                    <When>2017-02-14T15:42:34Z↙When>
                <Where>EnterpriseDC1.enterprise.local↙Where>
                    <Who>ENTERPRISE\Administrator↙Who>
            <Workstation>EnterpriseDC1.enterprise.local↙Workstation>
                        ↙ActivityRecord>
                    <ActivityRecord>...↙ActivityRecord>
```

```
<ActivityRecord>...↙ActivityRecord>
↙ActivityRecordList>
```

JSON

```
{
"ActivityRecordList": [
{
"Action": "Added",
"MonitoringPlan" : {
"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}",
"Name": "AD Monitoring"
},
"DataSource": "Active Directory",
"Item": {"Name": "enterprise.local (Domain)"},
"ObjectType": "user",
"RID": "20160215110503420B9451771F5964A9EAC0A5F35307EA155",
"What": "\\local\\enterprise\\Users\\Jason Smith",
"When": "2017-02-14T15:42:34Z",
"Where": "EnterpriseDC1.enterprise.local",
"Who": "ENTERPRISE\\Administrator",
"Workstation": "EnterpriseDC1.enterprise.local"
},
{...},
{...}
],
"ContinuationMark": "PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A"
}
```

3. Continue retrieving Activity Records. Send a POST request containing this Continuation mark to the same endpoint. Continuation Mark

XML

```
curl -H "Content-Type: application/xml; Charset=UTF-8" https://
WKSWin2012:9699/netwrix/api/v1/activity_records/enum -u
Enterprise\NetwrixUser:NetwrixIsCool --data-binary
@C:\APIdocs\ContMark.xml

<?xml version="1.0" standalone="yes"?>
<ContinuationMark xmlns="http://schemas.netwrix.com/api/v1/activity_records/">
PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A
↙ContinuationMark>
```

JSON

```
curl -H "Content-Type: application/json; Charset=UTF-8" https://
WKSWin2012:9699/netwrix/api/v1/activity_records/enum?format=json -u
```

```
Enterprise\NetwrixUser:NetwrixIsCool --data-binary
@C:\APIdocs\ContMark.json

"PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A"
```

Ensure to pass information about transferred data, including `Content-Type:application/xml` or `application/json` and encoding. The syntax greatly depends on the tool you use.

4. Receive the next response. On success, the status is 200 OK. For XML, a response body contains the `ActivityRecordList` root element with next Activity Records and a new Continuation mark inside. For JSON, a response body contains the `ActivityRecordsearch` array with next Activity Records collected in braces {} and a new Continuation mark.

5. Continue retrieving Activity Records. Send POST requests containing new Continuation marks until you receive a 200 OK response with no Activity Records inside the `ActivityRecordList`. It means you reached the end of the Audit Database.

Search Activity Records

The search functionality in the Netwrix Auditor Integration API reproduces interactive search available in the Netwrix Auditor client. See View and Search Collected Data for detailed instruction on how to search and filter audit data.

As the interactive search in the Netwrix Auditor client, this REST API endpoint allows you to retrieve Activity Records matching a certain criteria. You can create your own set of filters in the Search parameters file. Search Parameters Activity Records are retrieved according to the account's delegated scope.

Endpoint

To retrieve Activity Records matching a certain criteria, send a POST request containing search parameters (also may include a Continuation mark). Search Parameters

Method	Endpoint	POST Data
POST	`https://{host:port}/netwrix/api/v1/activity_records/`	Search Parameters

Method	Endpoint	POST Data
	`search{?format=json}{&count=Number}`	

Request Parameters

Parameter	Mandatory	Description
`host:port`	Yes	Replace with the IP address or a name of your Netwrix Auditor Server host and port (e.g., *172.28.6.15:9699*, *stationwin12:9699*, *WKSWin2012.enterprise.local:9699*). With enabled HTTPS, provide the computer name as it appears in certificate properties.
`format=json`	No	Add this parameter to retrieve data in JSON format. Otherwise, XML-formatted Activity Records will be returned.
`count=Number`	No	Add this parameter to define the number of Activity Records to be exported. Replace `Number` with a number (e.g., `?count=1500`).

Optional parameters (format and count) can be provided in any order. The first parameter must start with ?, others are joined with &, no spaces required (e.g., `?format=json&count=1500`).

Response

Request Status	Response
Success	The HTTP status code in the response header is 200 OK. The response body contains Activity Records and Continuation Mark. HTTP/1.1 200 OK Server: Microsoft-HTTPAPI/2.0 Content-Length: 311896 Content-Type: application/xml Date: Fri, 08 Apr 2017 13:56:22 GMT
Error	The header status code is an error code. Depending on the error code, the response body may contain an error object. See Response Status Codes for more information.

Usage Example—Retrieve All Activity Records Matching Search Criteria

This example describes how to retrieve all Activity Records matching search criteria.

1. Send a POST request containing search parameters. Search Parameters

   For example, this request retrieves Activity Records where administrator added new objects to the Active Directory domain. Groups and group policies are not taken into account. Changes could only occur between September 16, 2016 and March 16, 2017.

XML

```
curl -H "Content-Type:application/xml; Charset=UTF-8" https://
  WKSWin2012:9699/netwrix/api/v1/activity_records/search -u
     Enterprise\NetwrixUser:NetwrixIsCool --data-binary
                  @C:\APIdocs\Search.xml

            <?xml version="1.0" standalone="yes"?>
<ActivityRecordSearch xmlns="http://schemas.netwrix.com/api/v1/activity_record
                         <FilterList>
```

```
<Who>Administrator↙Who>
<DataSource>Active Directory↙DataSource>
<Action>Added↙Action>
<ObjectType Operator="DoesNotContain">Group↙ObjectType>
<When>
<From>2016-09-16T16:30:00+11:00↙From>
<To>2017-03-16T00:00:00Z↙To>
↙When>
↙FilterList>
↙ActivityRecordSearch>
```

JSON

```
curl -H "Content-Type:application/json; Charset=UTF-8" https://
WKSWin2012:9699/netwrix/api/v1/activity_records/ search?format=json
-u Enterprise\NetwrixUser:NetwrixIsCool --data-binary
@C:\APIdocs\Search.json

{
"FilterList": {
"Who": "Administrator",
"DataSource": "Active Directory",
"Action": "Added",
"ObjectType": { "DoesNotContain": "Group"},
"When": {
"From": "2016-09-16T16:30:00+11:00",
"To": "2017-03-16T00:00:00Z"
}
}
}
```

Ensure to pass information about transferred data, including `Content-Type:application/xml` or `application/json` and encoding. The syntax greatly depends on the tool you use.

2. Receive the response. Activity Records are retrieved according to the account's delegated scope. Below is an example of a successful search request. The status is 200 OK. For XML, a response body contains the `ActivityRecordList` root element with Activity Records matching filter criteria and a Continuation mark inside. For JSON, a response body contains the `ActivityRecordList` array with Activity Records matching filter criteria and collected in braces {}, and a Continuation mark.

XML

```
<?xml version="1.0" standalone="yes"?>
<ActivityRecordList xmlns="http://schemas.netwrix.com/api/v1/activity_records/
<ContinuationMark>PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A↙ContinuationMark>
<ActivityRecord>
<MonitoringPlan>
```

```
                    <Name>AD Monitoring↙Name>
                <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
                                ↙MonitoringPlan>
                    <DataSource>Active Directory↙DataSource>
                                <Item>
                     <Name>enterprise.local (Domain)↙Name>
                                ↙Item>
                            <ObjectType>user↙ObjectType>
<RID>20160215110503420B9451771F5964A9EAC0A5F35307EA155↙RID>
                <What>\local\enterprise\Users\Jason Smith↙What>
                            <Action>Added↙Action>
                        <When>2017-02-14T15:42:34Z↙When>
                    <Where>EnterpriseDC1.enterprise.local↙Where>
                        <Who>ENTERPRISE\Administrator↙Who>
                <Workstation>EnterpriseDC1.enterprise.local↙Workstation>
                                ↙ActivityRecord>
                            <ActivityRecord>...↙ActivityRecord>
                            <ActivityRecord>...↙ActivityRecord>
                                ↙ActivityRecordList>
```

JSON

```
                                {
                        "ActivityRecordList": [
                                {
                            "Action": "Added",
                         "MonitoringPlan" : {
                "ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}",
                            "Name": "AD Monitoring"
                                },
                        "DataSource": "Active Directory",
                "Item": {"Name": "enterprise.local (Domain)"},
                            "ObjectType": "user",
"RID": "20160215110503420B9451771F5964A9EAC0A5F35307EA155",
            "What": "\\local\\enterprise\\Users\\Jason Smith",
                            "When": "2017-02-14T15:42:34Z",
                    "Where": "EnterpriseDC1.enterprise.local",
                        "Who": "ENTERPRISE\\Administrator",
                "Workstation": "EnterpriseDC1.enterprise.local"
                                },
                                {...},
                                {...}
                                ],
"ContinuationMark": "PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A"
                                }
```

3. Continue retrieving Activity Records. Send a POST request containing your search parameters and this Continuation mark to the same endpoint. Continuation Mark

XML

```
curl -H "Content-Type:application/xml; Charset=UTF-8" https://
  WKSWin2012:9699/netwrix/api/v1/activity_records/search -u
     Enterprise\NetwrixUser:NetwrixIsCool --data-binary
                  @C:\APIdocs\Search.xml

             <?xml version="1.0" standalone="yes"?>
<ActivityRecordSearch xmlns="http://schemas.netwrix.com/api/v1/activity_record
<ContinuationMark>PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A↙Continua
                          <FilterList>
                       <Who>Administrator↙Who>
                <DataSource>Active Directory↙DataSource>
                       <Action>Added↙Action>
     <ObjectType Operator="DoesNotContain">Group↙ObjectType>
                          <When>
              <From>2016-09-16T16:30:00+11:00↙From>
                  <To>2017-03-16T00:00:00Z↙To>
                          ↙When>
                       ↙FilterList>
                    ↙ActivityRecordSearch>
```

JSON

```
  curl -H "Content-Type:application/json; Charset=UTF-8" https://
 WKSWin2012:9699/netwrix/api/v1/activity_records/search?format=json
       -u Enterprise\NetwrixUser:NetwrixIsCool --data-binary
                  @C:\APIdocs\Search.json

                                {
"ContinuationMark": "PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A",
                          "FilterList": {
                       "Who": "Administrator",
                 "DataSource": "Active Directory",
                         "Action": "Added",
            "ObjectType": { "DoesNotContain": "Group"},
                          "When": {
               "From": "2016-09-16T16:30:00+11:00",
                   "To": "2017-03-16T00:00:00Z"
                                }
                                }
                                }
```

Ensure to pass information about transferred data, including `Content-Type:application/xml` or `application/json` and encoding. The syntax greatly depends on the tool you use.

4. Receive the next response. On success, the status is 200 OK. For XML, a response body contains the `ActivityRecordList` root element with next Activity Records and a new Continuation mark inside. For JSON, a response body contains the `ActivityRecordsearch` array with next Activity Records collected in braces {} and a new Continuation mark.

5. Continue retrieving Activity Records. Send POST requests containing your search parameters with new Continuation marks until you receive a 200 OK response with no Activity Records inside the `ActivityRecordList`. It means you retrieved all Activity Records matching your search criteria.

Write Activity Records

Endpoint

Write data to the Audit Database and to the Long-Term Archive. By default, all imported data is written to a special Netwrix_Auditor_API database and recognized as the Netwrix API data source. This data is not associated with any monitoring plan in the product. You can associate Activity Records with a plan, in this case data will be written to a database linked to this plan. Make sure the plan you specify is already created in Netwrix Auditor, the Netwrix API data source is added to the plan and enabled for monitoring.

To feed data, send a POST request containing Activity Records. The user sending a request must be assigned the Contributor role in Netwrix Auditor. After feeding data to the Audit Database it will become available for search in the Netwrix Auditor client and through /netwrix/api/v1/activity_records/search and /netwrix/api/v1/activity_records/enum endpoints.

Method	Endpoint	POST Data
POST	`https://{host:port}/netwrix/api/v1/activity_records/{?format=json}`	Activity Records

Netwrix recommends limiting the input Activity Records file to 50MB and maximum 1,000 Activity Records.

Request Parameters

Parameter	Mandatory	Description
`host:port`	Yes	Replace with the IP address or a name of your Netwrix Auditor Server host and port (e.g., *172.28.6.15:9699*, *stationwin12:9699*, *WKSWin2012.enterprise.local:9699*). With enabled HTTPS, provide the computer name as it appears in certificate properties.
`?format=json`	No	Add this parameter to write data in JSON format. Otherwise, Netwrix Auditor Server will expect XML-formatted Activity Records and will consider JSON invalid.

Response

Request Status	Response

Success	The HTTP status code in the response header is 200 OK and the body is empty.
	
	 `HTTP/1.1 200 OK`
	`Server: Microsoft-HTTPAPI/2.0`
	`Content-Length: 0`
	`Content-Type: text/plain`
	`Date: Fri, 08 Apr 2017 13:56:22 GMT`

Error	The header status code is an error code. Depending on the error code, the response body may contain an error object. See Response Status Codes for more information.

Usage Example—Write Data

This example describes how to feed Activity Records to the Audit Database.

1. Send a POST request containing Activity Records. Activity Records For example:

XML

```
curl -H "Content-Type:application/xml; Charset=UTF-8" https://
WKSWin2012:9699/netwrix/api/v1/activity_records/ -u
Enterprise\NetwrixUser:NetwrixIsCool --data-binary
@C:\APIdocs\Input.xml
<?xml version="1.0" encoding="utf-8"?>
<ActivityRecordList xmlns="http://schemas.netwrix.com/api/v1/activity_records/
<ActivityRecord>
<Who>Admin↙Who>
<ObjectType>Stored Procedure↙ObjectType>
<Action>Added↙Action>
<What>Databases\ReportServer\Stored Procedures\dbo.sp_New↙What>
<MonitoringPlan>
<Name>Integrations and custom sources↙Name>
↙MonitoringPlan>
<Where>WKSWin12SQL↙Where>
<When>2017-02-19T03:43:49-11:00↙When>
↙ActivityRecord>
<ActivityRecord>
<Action>Modified↙Action>
<ObjectType>Mailbox↙ObjectType>
<What>Shared Mailbox↙What>
<When>2017-02-10T14:46:00Z↙When>
<Where>BLUPR05MB1940↙Where>
<Who>admin@enterprise.onmicrosoft.com↙Who>
<DetailList>
<Detail>
<PropertyName>Custom_Attribute↙PropertyName>
<Before>1↙Before>
<After>2↙After>
↙Detail>
↙DetailList>
↙ActivityRecord>
↙ActivityRecordList>
```

JSON

```
curl -H "Content-Type:application/json; Charset=UTF-8" https://
WKSWin2012:9699/netwrix/api/v1/activity_records/?format=json -u
```

```
        Enterprise\NetwrixUser:NetwrixIsCool --data-binary
                    @C:\APIdocs\Input.json

                                    [
                                    {
                                "Who": "Admin",
                            "ObjectType": "Stored Procedure",
                                  "Action": "Added",
  "MonitoringPlan": {"Name": "Integrations and custom sources"},
 "What": "Databases\\ReportServer\\Stored Procedures\\dbo.sp_New",
                              "Where": "WKSWin12SQL",
                          "When": "2017-02-19T03:43:49-11:00"
                                    },
                                    {
                                 "Action": "Modified",
                               "ObjectType": "Mailbox",
                              "What": "Shared Mailbox",
                            "When": "2017-02-10T14:46:00Z",
                               "Where": "BLUPR05MB1940",
                     "Who": "admin@enterprise.onmicrosoft.com",
                                  "DetailList": [
                                          {
                        "PropertyName": "Custom_Attribute",
                                   "Before": "1",
                                    "After": "2"
                                          }
                                          ]
                                    }
                                    ]
```

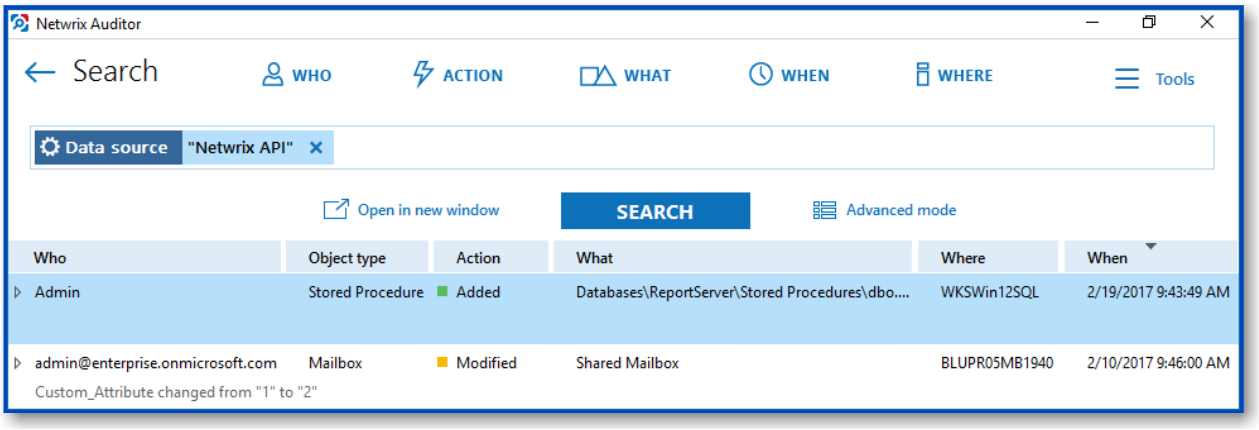
Ensure to pass information about transferred data, including `Content-Type:application/xml` or `application/json` and encoding. The syntax greatly depends on the tool you use.

2. Receive the response. Below is an example of a successful write request. The status is 200 OK and the body is empty.

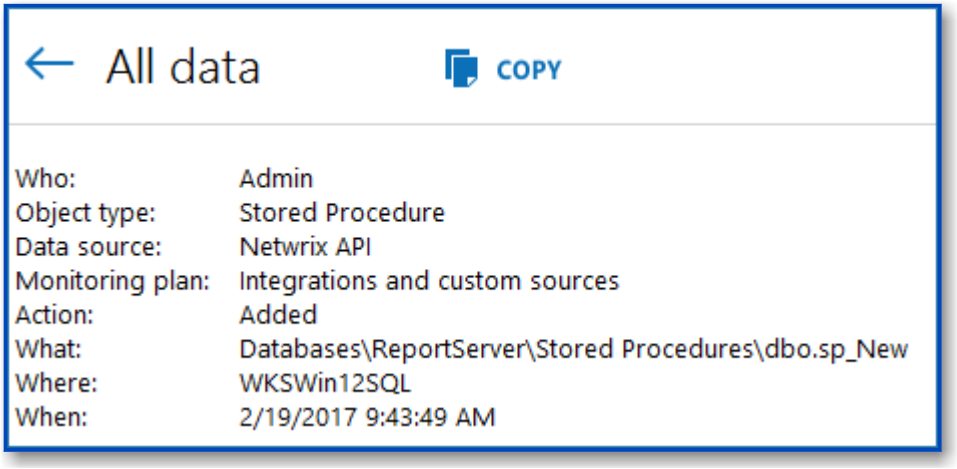
   ```
   HTTP/1.1 200 OK
   Server: Microsoft-HTTPAPI/2.0
   Content-Length: 0
   Content-Type: text/plain
   Date: Fri, 08 Apr 2017 13:56:22 GMT
   ```

3. Send more POST requests containing Activity Records if necessary.

4. Check that posted data is now available in the Audit Database. Run a search request to /netwrix/api/v1/activity_records/search endpoint or use interactive search in the Netwrix Auditor client. For example:



For input Activity Records, the data source in set to Netwrix API.



Reference for Creating Search Parameters File

Review this section to learn more about operators and how to apply them to Activity Record filters to create a unique search. You can:

- Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical AND.

Format	Example
XML	<Who Operator="Equals">Admin↙Who> <DataSource Operator="NotEqualTo">Active Di <What>User↙What>

Format	Example

JSON	<pre>"Who" : { "Equals" : "Admin" },
	"DataSource" : { "NotEqualTo" : "Active Dire
	"What" : "User"</pre>

- Specify several values for the same filter. To do this, add two entries one after another.

  Entries with Equals, Contains, StartsWith, EndsWith, and InGroup operators work as a logical OR (Activity Records with either of following values will be returned). Entries with DoesNotContain and NotEqualTo operators work as a logical AND (Activity Records with neither of the following values will be returned).

Format	Example

XML	<pre><Who>Admin↙Who>
	<Who>Analyst↙Who></pre>

JSON	<pre>"Who" : ["Admin" , "Analyst"]</pre> Use square brackets to add several values for the entry.

Review the following for additional information:

- Filters
- Operators

The table below shows filters and Activity Records matching them.

Filters	Matching Activity Records

• XML:
 	
<pre><Who>Administrator↙Who>
<DataSource>
SharePoint
↙DataSource>
<Action Operator="NotEqualTo">
Read
↙Action></pre>
• JSON:
 	
<pre>"Who" : "Admin",
"DataSource" : "SharePoint",</pre>
	Retrieves all activity records where administrator made any actions on SharePoint, except Read.
	
	• XML:
	
	<pre><ActivityRecord>
	<Action>Added↙Action>
	<MonitoringPlan>
	<ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
	<Name>Compliance↙Name>
	↙MonitoringPlan>
	<DataSource>SharePoint↙DataSource>
	<Item>
	<Name>http://demolabsp:8080 (SharePoint farm)↙</pre>

Filters	Matching Activity Records

"Action" : {
"NotEqualTo" : "Read"
}
	↙Item>
	<ObjectType>List↙ObjectType>
	<RID>20160217093959797091D091D2EAF4A89BF7A1CC
	<What>http://demolabsp/lists/Tasklist↙What>
	<When>2017-02-17T09:28:35Z↙When>
	<Where>http://demolabsp↙Where>
	<Who>Enterprise\Administrator↙Who>
	<Workstation>172.28.15.126↙Workstation>
	↙ActivityRecord>
	<ActivityRecord>
	<Action>Removed↙Action>
	<MonitoringPlan>
	<ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
	<Name>Compliance↙Name>
	↙MonitoringPlan>
	<DataSource>SharePoint↙DataSource>
	<Item>
	<Name>http://demolabsp:8080 (SharePoint farm)↙
	↙Item>
	<ObjectType>List↙ObjectType>
	<RID>20160217093959797091D091D2EAF4A89BF7A1CC
	<What>http://demolabsp/lists/Old/Tasklist↙Wh
	<When>2017-02-17T09:28:35Z↙When>
	<Where>http://demolabsp↙Where>
	<Who>Enterprise\Administrator↙Who>
	<Workstation>172.28.15.126↙Workstation>
	↙ActivityRecord>
	
	• JSON:
	
	{
	"Action": "Added",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}
	"Name": "Compliance"
	},
	"DataSource": "SharePoint",
	"Item": {"Name": "http://demolabsp:8080 (Share
	"ObjectType" : "List",
	"RID" : "20160217093959797091D091D2EAF4A89BF7A
	"What" : "http://demolabsp/lists/Tasklist",
	"When" : "2017-02-17T09:28:35Z",
	"Where" : "http://demolabsp",
	"Who" : "Enterprise\\Administrator",
	"Workstation" : "172.28.15.126"
	},

Filters	Matching Activity Records

	{
	"Action" : "Removed",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}
	"Name": "Compliance"
	},
	"DataSource": "SharePoint",
	"Item": {"Name": "http://demolabsp:8080 (Share
	"ObjectType" : "List",
	"RID": "20160217093959797091D091D2EAF4A89BF7A1
	"What" : "http://demolabsp/lists/Old/Taskslist
	"When" : "2017-02-17T09:28:35Z",
	"Where" : "http://demolabsp",
	"Who" : "Enterprise\\Administrator",
	"Workstation" : "172.28.15.126"
	}

• XML: <Who>Administrator↙Who> <Action>Added↙Action> • JSON: "Who" : "Administrator", "Action" : "Added"	Retrieves all activity records where administrator added an object within any data source. • XML: <ActivityRecord> <Action>Added↙Action> <MonitoringPlan> <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID> <Name>Compliance↙Name> ↙MonitoringPlan> <DataSource>SharePoint↙DataSource> <Item> <Name>http://demolabsp:8080 (SharePoint farm)↙ ↙Item> <ObjectType>List↙ObjectType> <RID>20160217093959797091D091D2EAF4A89BF7A1CC0 <What>http://demolabsp/lists/Taskslist↙What> <When>2017-02-17T09:28:35Z↙When> <Where>http://demolabsp↙Where> <Who>Enterprise\Administrator↙Who> <Workstation>172.28.15.126↙Workstation> ↙ActivityRecord> <ActivityRecord> <Action>Added↙Action> <MonitoringPlan> <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID> <Name>Compliance↙Name> ↙MonitoringPlan>

Filters	Matching Activity Records

	<DataSource>Exchange↙DataSource>
	<Item>
	<Name>enterprise.local (Domain)↙Name>
	↙Item>
	<ObjectType>Mailbox↙ObjectType>
	<RID>20160211163547592O7E9DDCEEB674986AD30CD3
	<What>Shared Mailbox↙What>
	<When>2017-02-10T14:46:00Z↙When>
	<Where>eswks.enterprise.local↙Where>
	<Who>Enterprise\Administrator↙Who>
	↙ActivityRecord>
	
	• JSON:
	
	{
	"Action" : "Added",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}
	"Name": "Compliance"
	},
	"DataSource": "SharePoint",
	"Item": {"Name": "http://demolabsp:8080 (Share
	"ObjectType": "List",
	"RID": "20160217093959797091D091D2EAF4A89BF7A
	"What": "http://demolabsp/lists/Taskslist",
	"When": "2017-02-17T09:28:35Z",
	"Where": "http://demolabsp",
	"Who": "Enterprise\\Administrator",
	"Workstation": "172.28.15.126"
	},
	{
	"Action" : "Added",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}
	"Name": "Compliance"
	},
	"DataSource" : "Exchange",
	"Item": {"Name": "enterprise.local (Domain)"}
	"ObjectType" : "Mailbox",
	"RID": "20160211163547592O7E9DDCEEB674986AD30
	"What": "Shared Mailbox",
	"When": "2017-02-10T14:46:00Z",
	"Where": "eswks.enterprise.local",
	"Who": "Enterprise\\Administrator"
	}

Filters	Matching Activity Records
• XML: <Who>Admin↙Who> <Who>Analyst↙Who> • JSON: "Who" : ["Admin" , "Analyst"]	Retrieves all activity records where admin or analyst made any changes within any data source. • XML: <ActivityRecord> <Action>Added↙Action> <MonitoringPlan> <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID> <Name>Compliance↙Name> ↙MonitoringPlan> <DataSource>File Servers↙DataSource> <Item> <Name>wks.enterprise.local (Computer)↙Name> ↙Item> <ObjectType>Folder↙ObjectType> <RID>20160211163547592O7E9DDCEEB674986AD30CD3 <What>Annual_Reports↙What> <When>2017-02-10T14:46:00Z↙When> <Where>wks.enterprise.local↙Where> <Who>Enterprise\Admin↙Who> ↙ActivityRecord> <ActivityRecord> <Action>Removed↙Action> <MonitoringPlan> <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID> <Name>Compliance↙Name> ↙MonitoringPlan> <DataSource>Active Directory↙DataSource> <Item> <Name>enterprise.local (Domain)↙Name> ↙Item> <ObjectType>User↙ObjectType> <RID>20160211163547592O7E9DDCEEB674986AD30CD3 <What>Anna.Smith↙What> <When>2017-02-10T10:46:00Z↙When> <Where>dc1.enterprise.local↙Where> <Who>Enterprise\Analyst↙Who> <Workstation>172.28.6.15↙Workstation> ↙ActivityRecord> • JSON: { "Action": "Added",

Filters	Matching Activity Records

	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}"
	"Name": "Compliance"
	},
	"DataSource" : "File Servers",
	"Item": {"Name": "wks.enterprise.local (Compu
	"ObjectType": "Folder",
	"RID": "20160211163547592O7E9DDCEEB674986AD30
	"What": "Annual_Reports",
	"When": "2017-02-10T14:46:00Z",
	"Where": "wks.enterprise.local",
	"Who": "Enterprise\\Admin"
	},
	{
	"Action": "Removed",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}"
	"Name": "Compliance"
	},
	"DataSource": "Active Directory",
	"Item": {"Name": "enterprise.local (Domain)"}
	"ObjectType": "User",
	"RID": "20160211163547592O7E9DDCEEB674986AD30
	"What": "Anna.Smith",
	"When": "2017-02-10T10:46:00Z",
	"Where": "dc1.enterprise.local",
	"Who": "Enterprise\\Analyst",
	"Workstation": "172.28.6.15"
	}

• XML: <When> <LastSevenDays↗ ↙When> <When> <From> 2017-01-16T16:30:00Z ↙From> <To> 2017-02-01T00:00:00Z ↙To> ↙When> • JSON:	Retrieves all activity records for all data sources and users within a specified data range: • January 16, 2017 — February 1, 2017 • March 11, 2017 — March 17, 2017 (assume, today is March, 17). • XML: <ActivityRecord> <Action>Modified↙Action> <MonitoringPlna>My Cloud↙MonitoringPlan> <MonitoringPlan> <ID>{42F64379-163E-4A43-A9C5-4514C5A23701}↙ID>

Filters	Matching Activity Records

"When" : [
 	
{"LastSevenDays" : ""},
 	
{
 	
"From" : "2017-01-16T16:30:00Z",
 	
"To" : "2017-02-01T00:00:00Z"
 	
}
 	
]
	<Name>My Cloud↙Name>
	↙MonitoringPlan>
	<DataSource>Exchange Online↙DataSource>
	<Item>
	<Name>mail@corp.onmicrosoft.com (Office 365 te
	↙Item>
	<ObjectType>Mailbox↙ObjectType>
	<RID>20160217093959797097D56DDA034420B904424
	<What>Shared Mailbox↙What>
	<When>2017-03-17T09:37:11Z↙When>
	<Where>BLUPR05MB1940↙Where>
	<Who>admin@corp.onmicrosoft.com↙Who>
	↙ActivityRecord>
	<ActivityRecord>
	<Action>Successful Logon↙Action>
	<MonitoringPlan>
	<ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
	<Name>Compliance↙Name>
	↙MonitoringPlan>
	<DataSource>Logon Activity↙DataSource>
	<Item>
	<Name>enterprise.local (Domain)↙Name>
	↙Item>
	<ObjectType>Logon↙ObjectType>
	<RID>20160217093959797091D091D2EAF4A89BF7A1CC
	<What>stationexchange.enterprise.local↙What>
	<When>2017-02-17T09:28:35Z↙When>
	<Where>enterprisedc1.enterprise.local↙Where>
	<Who>ENTERPRISE\Administrator↙Who>
	<Workstation>stwin12R2.enterprise.local↙Works
	↙ActivityRecord>
	
	• JSON:
	
	{
	"Action" : "Modified",
	"MonitoringPlan" : "My Cloud",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23701}
	"Name": "My Cloud"
	},
	"DataSource": "Exchange Online",
	"Item": {
	"Name": "mail@corp.onmicrosoft.com (Office 365
	},
	"ObjectType" : "Mailbox",

Filters	Matching Activity Records

	"RID" : "20160217093959797097D56DDA034420B904
	"What" : "Shared Mailbox",
	"When" : "2017-03-17T09:37:11Z",
	"Where" : "BLUPR05MB1940",
	"Who" : "admin@corp.onmicrosoft.com"
	},
	{
	"Action" : "Successful Logon",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}"
	"Name": "Compliance"
	},
	"DataSource": "Logon Activity",
	"Item": {"Name": "enterprise.local (Domain)"}
	"ObjectType": "Logon",
	"RID" : "20160217093959797091D091D2EAF4A89BF7A
	"What" : "stationexchange.enterprise.local",
	"When" : "2017-02-17T09:28:35Z",
	"Where" : "enterprisedc1.enterprise.local",
	"Who" : "ENTERPRISE\\Administrator",
	"Workstation" : "stwin12R2.enterprise.local"
	}

• XML: <DataSource> Logon Activity ↙DataSource> • JSON: "DataSource" : "Logon Activity"	Retrieves all activity records for Logon Activity data source irrespective of who made logon attempt and when it was made. • XML: <ActivityRecord> <Action>Successful Logon↙Action> <MonitoringPlan> <ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID> <Name>Compliance↙Name> ↙MonitoringPlan> <DataSource>Logon Activity↙DataSource> <Item> <Name>enterprise.local (Domain)↙Name> ↙Item> <ObjectType>Logon↙ObjectType> <RID>20160217093959797091D091D2EAF4A89BF7A1CC <What>stationexchange.enterprise.local↙What> <When>2017-02-17T09:28:35Z↙When> <Where>enterprisedc1.enterprise.local↙Where> <Who>ENTERPRISE\Administrator↙Who> <Workstation>stwin12R2.enterprise.local↙Works

Filters	Matching Activity Records

	↙ActivityRecord>
	<ActivityRecord>
	<Action>Successful Logon↙Action>
	<MonitoringPlan>
	<ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
	<Name>Compliance↙Name>
	↙MonitoringPlan>
	<DataSource>Logon Activity↙DataSource>
	<Item>
	<Name>enterprise.local (Domain)↙Name>
	↙Item>
	<ObjectType>Logon↙ObjectType>
	<RID>20160217093959797097D56DDA034420B904424
	<What>stationwin12r2.enterprise.local↙What>
	<When>2017-02-17T09:37:11Z↙When>
	<Where>enterprisedc2.enterprise.local↙Where>
	<Who>ENTERPRISE\Analyst↙Who>
	<Workstation>stwin12R2.enterprise.local↙Works
	↙ActivityRecord>
	
	• JSON:
	
	{
	"Action" : "Successful Logon",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}
	"Name": "Compliance"
	},
	"DataSource": "Logon Activity",
	"Item": {"Name": "enterprise.local (Domain)"}
	"ObjectType" : "Logon",
	"RID" : "20160217093959797091D091D2EAF4A89BF7
	"What" : "stationexchange.enterprise.local",
	"When" : "2017-02-17T09:28:35Z",
	"Where" : "enterprisedc1.enterprise.local",
	"Who" : "ENTERPRISE\\Administrator",
	"Workstation" : "stwin12R2.enterprise.local"
	},
	{
	"Action" : "Successful Logon",
	"MonitoringPlan": {
	"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}
	"Name": "Compliance"
	},
	"DataSource": "Logon Activity",
	"Item": {"Name": "enterprise.local (Domain)"}

Filters	Matching Activity Records
	"ObjectType" : "Logon", "RID" : "20160217093959797097D56DDA034420B904 "What" : "stationwin12r2.enterprise.local", "When" : "2017-02-17T09:37:11Z", "Where" : "enterprisedc2.enterprise.local", "Who" : "ENTERPRISE\\Analyst", "Workstation" : "stwin12R2.enterprise.local" }

Filters

Review the table below to learn more about filters. The filters correspond to Activity Record fields.

Filter	Description	Supported Operators
RID	Activity Record ID. Limits your search to a unique key of the Activity Record. Max length: 49.	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith
Who	Limits your search to a specific user who made the change (e.g., *Enterprise\ Administrator*, *administrator@enterprise.onmicrosoft.com*).	• Contains (default) • DoesNotContain

Filter	Description	Supported Operators
	Max length: 255.	• Equals • NotEqualTo • StartsWith • EndsWith • InGroup • NotInGroup
Where	Limits your search to a resource where the change was made (e.g., *Enterprise-SQL*, *FileStorage.enterprise.local*). The resource name can be a FQDN or NETBIOS server name, Active Directory domain or container, SQL Server instance, SharePoint farm, VMware host, etc. Max length: 255.	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith
ObjectType	Limits your search to objects of a specific type only (e.g., *user*). Max length: 255.	• Contains (default) • DoesNotContain

Filter	Description	Supported Operators
		• Equals • NotEqualTo • StartsWith • EndsWith
What	Limits your search to a specific object that was changed (e.g., *NewPolicy*) . Max length: 1073741822.	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith
DataSource	Limits your search to the selected data source only (e.g., *Active Directory*). Max length: 1073741822.	• Contains (default) • DoesNotContain • Equals • NotEqualTo

Filter	Description	Supported Operators
		• StartsWith • EndsWith
MonitoringPlan	Limits your search to a specific monitoring plan —Netwrix Auditor object that governs data collection. Max length: 255.	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith
Item	Limits your search to a specific item —object of monitoring—and its type provided in brackets. The following item types are available: • AD container • Computer • NetApp • Office 365 tenant	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith

Filter	Description	Supported Operators
	• Domain • EMC Isilon • EMC VNX/ VNXe • Integration • IP range • Oracle Database instance • SharePoint farm • SQL Server instance • VMware ESX/ESXi/ vCenter • Windows file share Max length: 1073741822.	
Workstation	Limits your search to an originating workstation from which the change was made (e.g., *WKSwin12.enterprise.local*). Max length: 1073741822.	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith

Filter	Description	Supported Operators
Detail	Limits your search results to entries that contain the specified information in Detail. Normally contains information specific to your data source, e.g., assigned permissions, before and after values, start and end dates. This filter can be helpful when you are looking for a unique entry. Max length: 1073741822.	• Contains (default) • Equals • NotEqualTo • StartsWith • EndsWith
Before	Limits your search results to entries that contain the specified before value in Detail. Max length: 536870911.	• Contains (default) • DoesNotContain • Equals • NotEqualTo • StartsWith • EndsWith
After	Limits your search results to entries that contain the specified after value in the Detail. Max length: 536870911.	• Contains (default) • DoesNotContain • Equals

Filter	Description		Supported Operators
			• NotEqualTo
			• StartsWith
			• EndsWith
Action	Limits your search results to certain actions:		• Equals (default) • NotEqualTo
	• Added	• Add (Failed Attempt)	
	• Removed	• Remove (Failed Attempt)	
	• Modified	• Modify (Failed Attempt)	
	• Read	• Read (Failed Attempt)	
	• Moved	• Move (Failed Attempt)	
	• Renamed	• Rename (Failed Attempt)	

Filter	Description	Supported Operators
	• Checked in • Checked out • Discard check out • Successful Logon • Failed Logon • Logoff • Copied • Sent • Session start • Session end • Activated	
When	Limits your search to a specified time range. Netwrix Auditor supports the following for the When filter: • Use Equals (default operator) or NotEqualTo operator • To specify time interval, use Within timeframe with one of the enumerated values (Today, Yesterday, etc.), and/or values in the To and From. To and From support the following date time formats: • YYYY-mm-ddTHH:MM:SSZ—Indicates UTC time (zero offset)	1. Equals (default) 2. NotEqualTo 3. Within timeframe: • Today • Yesterday • LastSevenDays • LastThirtyDays • Equals (default) • NotEqualTo

Filter	Description	Supported Operators
	• YYYY-mm-ddTHH:MM:SS+HH:MM—Indicates time zones ahead of UTC (positive offset) • YYYY-mm-ddTHH:MM:SS-HH:MM—Indicates time zones behind UTC (negative offset)	2. From..To interval
WorkingHours	Limits your search to the specified working hours. You can track activity outside the business hours applying the *NotEqualTo* operator. To and From support the following date time formats: • HH:MM:SSZ—Indicates UTC time (zero offset) • HH:MM:SS+HH:MM—Indicates time zones ahead of UTC (positive offset) • HH:MM:SS-HH:MM—Indicates time zones behind UTC (negative offset)	• "From..To" interval • Equals (default) • NotEqualTo

Operators

Review the table below to learn more about operators.

Operator	Description	Example
Contains	This operator shows all entries that contain a value specified in the filter.	If you set the Who filter to contains *John*, you will get the following results: *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*, *John@domain.com*.

Operator	Description	Example
Equals	This operator shows all entries with the exact value specified. Make sure to provide a full object name or path. To apply this operator when adding filters in the Simple mode, provide a value in quotation marks (e.g., *"Domain1\John"*).	Use this operator if you want to get precise results, e.g., *\\FS\Share\NewPolicy.docx*.
Not equal to	This operator shows all entries except those with the exact value specified. In the Search field in the Simple mode, this operator appears as not, e.g., Who not for the Who filter.	If you set the Who filter to not equal to *Domain1\John*, you will exclude the exact user specified and find all changes performed by other users, e.g., *Domain1\Johnson, Domain2\John*.
Starts with	This operator shows all entries that start with the specified value.	If you set the Who filter to starts with *Domain1\John*, you will find all changes performed by *Domain1\John*, *Domain1\Johnson*, and *Domain1\Johnny*.
Ends with	This operator shows all entries that end with the exact specified value.	If you set the Who filter to ends with *John*, you will find all changes performed by *Domain1\John*, *Domain2\Dr.John*, *Domain3\John*.
Does not contain	This operator shows all entries except those that contain the specified value. In the Search field in the Simple mode, this operator appears as not, e.g., Who not for the Who filter.	If you set the Who filter to does not contain *John*, you will exclude the following users: *Domain1\John*, *Domain2\Johnson*, and *Johnny@domain.com*.
In group	This operator relates to the Who filter. It instructs Netwrix Auditor to	If you set the In group condition for Who filter to *Domain\Administrators*, only the

Operator	Description	Example
	show only data for the accounts included in the specified group.	data for the accounts included in that group will be displayed.
Not in group	This operator relates to the Who filter. It instructs Netwrix Auditor to show only data for the accounts not included in the specified group.	If you set the Not in group condition for Who filter to *Domain\Administrators*, only the data for the accounts not included in that group will be displayed.

Post Data

While running requests to Netwrix Auditor Integration API endpoints, you will need to post data, e.g., a Continuation mark in order to continue retrieving Activity Records, Search parameters to find Activity Records matching your search, or Activity Records you want to feed to the Audit Database. Data is sent in the request body and must be formatted according to XML convention and compatible with Netwrix-provided XSD schemas.

In Netwrix Auditor 9.0, Netwrix has updated API schemas. Make sure to check and update your custom scripts and add-ons. Compatibility Notice

The file must be formatted in accordance with XML standard. The following symbols must be replaced with corresponding XML entities: & (ampersand), " (double quotes), ' (single quotes), < (less than), and > (greater than) symbols.

Symbol	XML entity
& e.g., Ally & Sons	& e.g., Ally & Sons
" e.g., Domain1\Users\"Stars"	" e.g., Domain1\Users\"Stars"
' e.g., Domain1\Users\O'Hara	' e.g., Domain1\Users\O'Hara

Symbol	XML entity
< e.g., CompanyDC<100	< e.g., CompanyDC<100
> e.g., ID>500	> e.g., ID>500

Also, Netwrix allows transferring data in JSON format (organized as name and value pairs). JSON file must be formatted in accordance with JSON specification. Special characters in JSON strings must be preceded with the \ character: " (double quotes), / (slash), \ (backslash). E.g., "\\local\ \enterprise\\Users\\Jason Smith". Trailing comma is not supported.

Review the following for additional information:

- Continuation Mark
- Search Parameters
- Activity Records

Continuation Mark

When exporting data from the Audit Database, a successful response includes:

- For XML—A `<ContinuationMark>` inside the `<ActivityRecordsList>` root element.
- For JSON—An object with the "ContinuationMark" field.

Continuation mark is a checkpoint, use it to retrieve data starting with the next Activity Record.

Send a POST request containing Continuation mark to the following endpoints:

Method	Endpoint	Description
POST	/netwrix/api/v1/activity_records/enum	Returns next Activity Records.
POST	/netwrix/api/v1/activity_records/search	Returns next Activity Records matching a filter criteria.

Ensure to pass information about transferred data, including `Content-Type:application/xml` or `application/json` and encoding. The syntax greatly depends on the tool you use.

You can send as many POST requests as you want. A new response returns next Activity Records and a new Continuation mark. Once all the Activity Records are retrieved, you will receive a 200 OK response with no Activity Records inside the `ActivityRecordList` root element (XML) or array (JSON).

Schema

Copy the contents of `ContinuationMark` to a separate XML or JSON file (e.g., ContMark.xml).

Format	Schema description
XML	The file must be compatible with the XML schema. On the computer where Auditor Server resides, you can find XSD file under *Netwrix_Auditor_installation_folder\Audit Core\API Schemas*. The `ContinuationMark` root element contains a value previously returned by Netwrix Auditor Integration API.
JSON	JSON-formatted Continuation mark includes the field value in quotes.

If you want to retrieve next Activity Records for your search, include the Continuation mark to your Search parameters file. Search Parameters

Example

XML
Retrieve Activity Records

`<?xml version="1.0" standalone="yes"?>`
`<ContinuationMark xmlns="http://schemas.netwrix.com/api/v1/activity_records/">`
`PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A`
`↙ContinuationMark>`

Search Activity Records

```
<?xml version="1.0" standalone="yes"?>
<ActivityRecordSearch xmlns="http://schemas.netwrix.com/api/v1/activity_records/">
<ContinuationMark>PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A↙Continuation
<FilterList>
<Who>Administrator↙Who>
<DataSource>Active Directory↙DataSource>
<Action>Added↙Action>
<ObjectType Operator="DoesNotContain">Group↙ObjectType>
<When>
<From>2016-09-16T16:30:00+11:00↙From>
<To>2017-03-16T00:00:00Z↙To>
↙When>
↙FilterList>
↙ActivityRecordSearch>
```

JSON

Retrieve Activity Records

```
"PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A"
```

Search Activity Records

```
{
"ContinuationMark": "PG5yPjxuIG49IntFNzA...PjwvYT48L24+PC9ucj4A+PC9ucj4A",
"FilterList": {
"Who": "Administrator",
"DataSource": "Active Directory",
"Action": "Added",
"ObjectType": { "DoesNotContain": "Group"},
"When": {
"From": "2016-09-16T16:30:00+11:00",
"To": "2017-03-16T00:00:00Z"
}
}
}
```

Search Parameters

Send the search parameters in the POST request body to narrow down the search results returned by the /netwrix/api/v1/activity_records/search endpoint. The Search parameters file includes one or more filters with operators and values (e.g., to find entries where *data source* is *SharePoint*); it may also contain a Continuation Mark. Generally, the Search parameters file looks similar to the following:

XML

```
<?xml version="1.0" encoding="utf-8"?>
<ActivityRecordSearch xmlns="http//schemas.netwrix.com/api/v1/activity_records/">
```

```
<ContinuationMark>Continuation mark↙ContinuationMark>
                    <FilterList>
                  <Filter1>Value↙Filter1>
                  <Filter2>Value1↙Filter2>
                  <Filter2>Value2↙Filter2>
   <Filter3 Operator="MatchType1">Value1↙Filter3>
   <Filter3 Operator="MatchType2">Value2↙Filter3>
                  <Filter4>Value1↙Filter4>
    <Filter4 Operator="MacthType">Value2↙Filter4>
                    ↙FilterList>
                 ↙ActivityRecordSearch>
```

JSON

```
{
  "ContinuationMark": "Continuation Mark",
              "FilterList": {
            "Filter1": "Value",
     "Filter2": [ "Value1", "Value2" ],
              "Filter3": {
          "MatchType1": "Value1",
          "MatchType2": "Value2"
              },
 "Filter4": [ "Value1", { "MatchType": "Value2" } ]
              }
              }
```

Ensure to pass information about transferred data, including `Content-Type:application/xml` or `application/json` and encoding. The syntax greatly depends on the tool you use.

Schema

Format	Schema description
XML	The file must be compatible with the XML schema. On the computer where Auditor Server resides, you can find XSD file under *Netwrix_Auditor_installation_folder\Audit Core\API Schemas*. The `ActivityRecordSearch` root element includes the `FilterList` element with one or

Format	Schema description
	more `Filter` elements inside. The root element may contain a `ContinuationMark` element. Each `Filter` specified within the `FilterList` must have a value to search for. The element may also include a modifier—a match type operator. minOccurs="0" indicates that element is optional and may be absent in the Search parameters. 
JSON	The `FilterList` object includes with one or more `Filter` entries inside. JSON may contain a `ContinuationMark` object. Each `Filter` specified within the `FilterList` must have a value to search for. The entry may also include a modifier—a match type operator.

Review the following for additional information:

- Filters
- Operators

Example

XML

```
<?xml version="1.0" encoding="utf-8"?>
<ActivityRecordSearch xmlns="http://schemas.netwrix.com/api/v1/activity_records/">
<FilterList>
<Who Operator="NotEqualTo">Administrator</Who>
<MonitoringPlan>My Hybrid Cloud enterprise</MonitoringPlan>
<DataSource>Active Directory</DataSource>
<DataSource Operator="StartsWith">Exchange</DataSource>
<Action>Removed</Action>
<Action>Added</Action>
<ObjectType Operator="DoesNotContain">Group</ObjectType>
<When>
<From>2016-01-16T16:30:00+11:00</From>
<To>2017-01-01T00:00:00Z</To>
</When>
</FilterList>
</ActivityRecordSearch>
```

JSON

```
{
"FilterList": {
"Who": { "NotEqualTo": "Administrator" },
"MonitoringPlan": "My Hybrid Cloud enterprise",
"DataSource": [ "Active Directory", { "StartsWith": "Exchange" } ],
"Action": [ "Added", "Removed" ],
"ObjectType": { "DoesNotContain": "Group" },
"When": {
"From": "2016-01-16T16:30:00+11:00",
"To": "2017-01-01T00:00:00Z"
}
}
}
```

Activity Records

In Netwrix terms, one operable chunk of information is called the Activity Record. Netwrix Auditor Integration API processes both XML and JSON Activity Records. The Activity Records have the format similar to the following—the exact schema depends on operation (input or output).

Format	Example
XML	<?xml version="1.0" encoding="UTF-8" ?> <ActivityRecordList xmlns="http://schemas.netw <ActivityRecord> <Who>Who</Who>

Format	Example
	<ObjectType>Object Type↙ObjectType> <Action>Action↙Action> <What>What↙What> <When>When↙When> <Where>Where↙Where> <MonitoringPlan> <ID>Unique ID↙ID> <Name>Name↙Name> ↙MonitoringPlan> <DataSource>Data source↙DataSource> <Item> <Name>Item name (Item type)↙Name> ↙Item> <DetailList> <Detail> <Before>Before Value↙Before> <After>After Value↙After> <PropertyName>Property↙PropertyName> <Message>Text↙Message> ↙Detail> ↙DetailList> ↙ActivityRecord> <ActivityRecord>...↙ActivityRecord> ↙ActivityRecordList>

JSON	[
	{
	"Action": "Action",
	"MonitoringPlan": {
	"ID": "Unique ID",
	"Name": "Name"
	},
	"DataSource": "Data source",
	"Item": {"Name": "Item name (Item type)"},
	"DetailList": [
	{
	"Before": "Before Value",
	"After": "After Value",
	"PropertyName": "Property",
	"Message": "Text"
	}
	],
	"ObjectType": "Object Type",
	"What": "What",
	"When": "When",
	"Where": "Where",

Format	Example

	<pre>"Who": "Who"
	},
	{...}
	]</pre>

To feed data from a custom audit source to Netwrix Auditor, send a POST request containing Activity Records. Write Activity Records

Schema

The Activity Records you want to feed to Netwrix Auditor must be compatible with input schema. The output schema resembles the input schema and can be used to validate Activity Records returned by Netwrix Auditor before further data parsing.

Format	Schema description
XML	The file must be compatible with the XML schema. On the computer where Auditor Server resides, you can find XSD file under *Netwrix_Auditor_installation_folder\Audit Core\API Schemas*. The `ActivityRecordList` root element includes the `ActivityRecord` elements. Each `ActivityRecord` contains values in the `Who`, `When`, `Where`, etc. fields. The `MonitoringPlan` element contains sub-elements such as `Name` and `ID`, the `Item` element contains `Name`. Both `MonitoringPlan` and `Item` are optional for input Activity Records. The `DetailList` element is optional too, it may include one or more `Detail` entries. The `Detail` element may contain sub-elements with values (e.g., before and after values). For input Activity Records, the data source is automatically set to Netwrix API. minOccurs="0" indicates that element is optional and may be absent when writing data to the Audit Database.

Format	Schema description
JSON	Activity Records are sent as an array collected within square brackets [ ]. Each `ActivityRecord` object is collected in braces {} and contains values in the `Who`, `When`, `Where`, etc. fields. The `DetailList` field is not mandatory, it may include one or more detail. The `Detail` field may contain sub-fields with values (e.g., before and after values). For input Activity Records, the data source is automatically set to Netwrix API.

Example

The examples below show an output Activity Record.

XML

```
<?xml version="1.0" encoding="UTF-8" ?>
<ActivityRecordList xmlns="http://schemas.netwrix.com/api/v1/activity_records/">
<ActivityRecord>
<Action>Modified↙Action>
<MonitoringPlan>
<ID>{42F64379-163E-4A43-A9C5-4514C5A23798}↙ID>
<Name>Compliance↙Name>
↙MonitoringPlan>
<DataSource>Exchange Online↙DataSource>
<Item>
<Name>mail@enterprise.onmicrosoft.com (Office 365 tenant)↙Name>
↙Item>
<ObjectType>Mailbox↙ObjectType>
<What>Shared Mailbox↙What>
<When>2017-03-17T09:37:11Z↙When>
<Where>BLUPR05MB1940↙Where>
<Who>admin@enterprise.onmicrosoft.com↙Who>
<DetailList>
<Detail>
<Before>1↙Before>
<After>2↙After>
<PropertyName>Custom_attribute↙PropertyName>
↙Detail>
↙DetailList>
↙ActivityRecord>
```

↙ActivityRecordList>

JSON


```
[
{
"Action": "Modified",
"MonitoringPlan": {
"ID": "{42F64379-163E-4A43-A9C5-4514C5A23798}",
"Name": "Compliance"
},
"DataSource": "Exchange Online",
"Item": {"Name": "mail@enterprise.onmicrosoft.com (Office 365 tenant)"},
"ObjectType": "Mailbox",
"What": "Shared Mailbox",
"When": "2017-03-17T09:37:11Z",
"Where": "BLUPR05MB1940",
"Who": "admin@enterprise.onmicrosoft.com",
"DetailList": [
{
"PropertyName": "Custom_Attribute",
"Before": "1",
"After": "2"
}
]
}
]
```


Response Status Codes

Code	Status	Write Activity Records	Retrieve, search Activity Records
200 OK	Success	Success. The body is empty. Activity Records were written to the Audit Database and the Long-Term Archive.	Success. The body contains Activity Records. Activity Records were retrieved from the Audit Database.
400 Bad Request	Error	Error validating Activity Records.	Error validating request parameters or post data.

Code	Status	Write Activity Records	Retrieve, search Activity Records
		Make sure the Activity Records are compatible with the Schema.	Make sure the post data files (Continuation mark, Search parameters) are compatible with their schemas and the ? `count=` parameter is valid.
401 Unauthorized	Error	The request is unauthorized and the body is empty. See for API Endpoints more information.	
404 Not Found	Error	Error addressing the endpoint. The body is empty. The requested endpoint does not exist (e.g., / netwrix/api/v1/mynewendpoint/).	
405 Method Not Allowed	Error	Error addressing the endpoint. The body is empty. Wrong HTTP request was sent (any except POST).	Error addressing the endpoint. The body is empty. Wrong HTTP request was sent (any except GET or POST).
413 Request Entity Too Large	Error	Error transferring files. The body is empty. The posted file exceeds supported size.	
500 Internal Server Error	Error	Error writing Activity Records to the Audit Database or the Long-Term Archive: • One or more Activity Records were not processed. • Netwrix Auditor license has expired. • Internal error occurred.	Error retrieving Activity Records from the Audit Database: • Netwrix Auditorlicense has expired. • The Netwrix Auditor Archive Service is unreachable. Try restarting the service on the computer that hosts Netwrix Auditor Server.

Code	Status	Write Activity Records	Retrieve, search Activity Records
			• Internal error occurred.
503 Service Unavailable	Error	The Netwrix Auditor Archive Service is busy or unreachable. Try restarting the service on the computer that hosts Netwrix Auditor Server.	—

Most failed requests contain error in the response body (except those with empty body, e.g., 404, 405). Error Details

Error Details

On error, most requests contain an error description in the response body (except some requests with empty body, e.g., 404, 405). Response Status Codes

The error details include:

Block	Description
Category	Defines the type of error (XML formatting-related error, invalid input-related error, etc.)
Description	Provides details about this error.
Location	(optional) Provides a link to a corrupted text in request. XML is considered a default format for Netwrix Auditor Integration API. Error location is defined in XML format.

The error details have the format similar to the following:

Format	Example
XML	<?xml version="1.0" encoding="UTF-8" ?> <ErrorList xmlns="http://schemas.netwrix.com/ <Error> <Category>Category↙Category> <Description>Error Description↙Description> <Location>Error Location↙Location> ↙Error> ↙ErrorList>

JSON	{
	"ErrorList": [
	{
	"Category": "Category",
	"Description": "Error Description",
	"Location": "Error Location"
	}
	]
	}

Review examples below to see how error details correspond to invalid requests.

Request	Error details returned
Invalid request: XML: curl -H "Content-Type: application/xml; Charset=UTF-8" https://WKSWin12R2:9699/ netwrix/api/v1/activity_records/search -u Enterprise\NetwrixUser:NetwrixIsCool --data-binary @C:\APIdocs\Search.xml <?xml version="1.0" encoding="utf-8"?> <ActivityRecordSearch xmlns="http://schemas.netwrix.com/api/v1/activity_records/"> <FilterList> <Who>Administrator↙Who> <DataSource>Active Directory <Action>Modified↙Action> ↙FilterList> ↙ActivityRecordSearch>	400 Bad Request • XML: <?xml version="1.0" encoding="UTF-8" ?> <ErrorList xmlns="http://schemas.netwrix.com/ <Error> <Category>XMLError↙Category> <Description>0xC00CE56D End tag 'FilterList' does not match the start tag 'DataSource' ↙Description> ↙Error> ↙ErrorList> • JSON: If JSON is corrupted, server returns 500 Internal Server Error with empty body.

Request	Error details returned

• JSON:
 	
curl -H "Content-Type: application/json; Charset=UTF-8" https://WKSWin12R2:9699/ netwrix/api/v1/activity_records/search?format=json -u Enterprise\NetwrixUser: NetwrixIsCool --data-binary @C:\APIdocs\Search.json
 	
{
"FilterList": {
"Who": "Administrator",
"DataSource": "Active Directory
"Action": "Added"
}
}	

Invalid request:
 	
• XML:
 	
curl https://WKSWin12R2:9699/ netwrix/api/v1/activity_records/enum?count=FIVE -u Enterprise\NetwrixUser:NetwrixIsCool
 	
• JSON:
 	
curl https://WKSWin12R2:9699/ netwrix/api/v1/activity_records/enum?format=json&count=FIVE -u Enterprise\NetwrixUser:NetwrixIsCool
	400 Bad Request
	
	• XML:
	
	<?xml version="1.0" encoding="UTF-8" ?>
	<ErrorList xmlns="http://schemas.netwrix.com/
	<Error>
	<Category>InputError↙Category>
	<Description>Invalid count parameter specified
	Error details: 0x80040204 Cannot convert the attribute data type
	↙Description>
	↙Error>
	↙ErrorList>
	
	• JSON:
	
	{
	"ErrorList": [
	{
	"Category": "InputError",
	"Description": "Invalid count parameter specif
	Error details: 0x80040204 Cannot convert the attribute data type"
	}
	]
	}

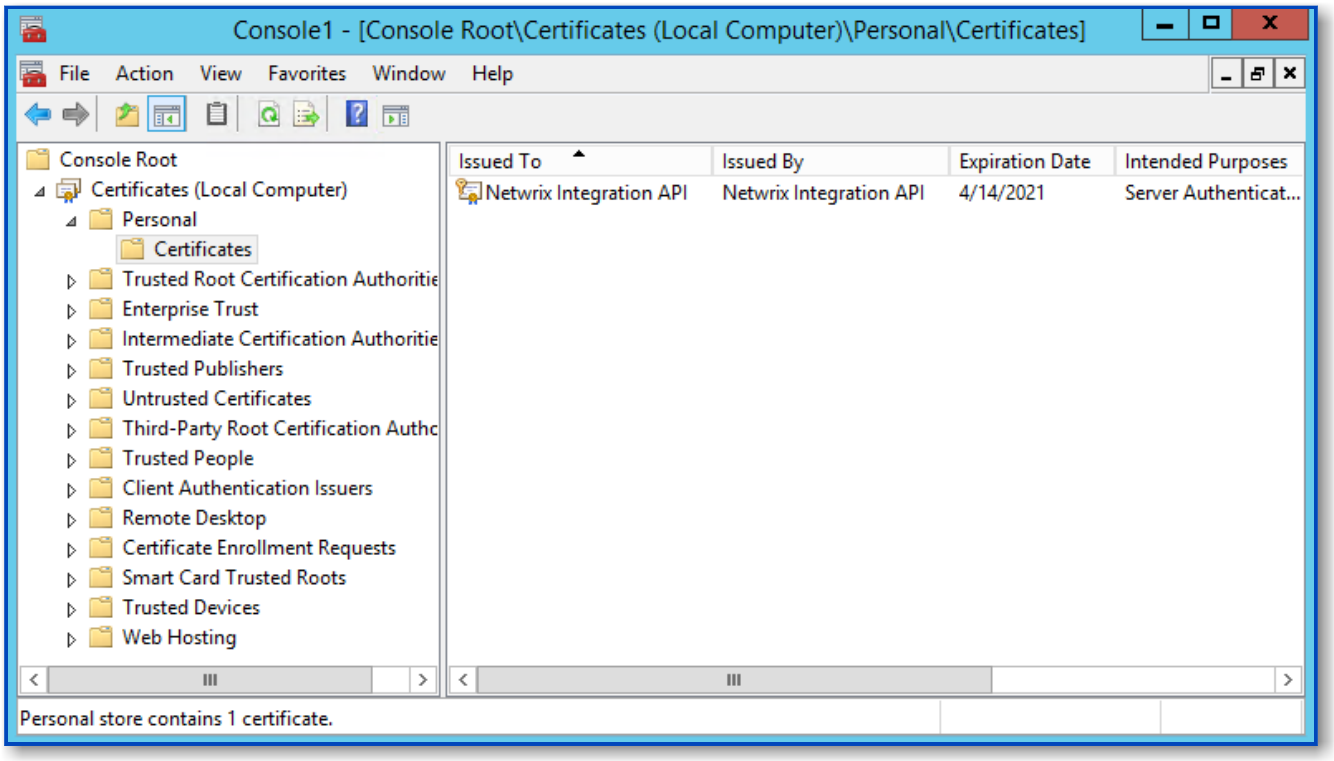
Request	Error details returned

Valid request, but the Audit Database is unreachable:
 	
• XML:
 	
curl https://WKSWin12R2:9699/netwrix/api/v1/activity_records/enum -u Enterprise\NetwrixUser:NetwrixIsCool
 	
• JSON:
 	
curl https://WKSWin12R2:9699/netwrix/api/v1/activity_records/enum?format=json -u Enterprise\NetwrixUser:NetwrixIsCool
	500 Internal Server Error
	
	• XML:
	
	<?xml version="1.0" encoding="UTF-8" ?>
	<ErrorList xmlns="http://schemas.netwrix.com/
	<Error>
	<Category>ServerError↙Category>
	<Description>0x80040C0A SQL Server cannot be contacted, connection is lost (0x80040C0A SQL Server cannot be contacted, connection is lost (0x80004005 [DBNETLIB][ConnectionOpen (Connec]SQL Server does not exist or access denied.)[0x00007FFDCC06BBC8,0x00007FFDB99EF4BA;0x00007FFDB99BEEEF,0x00007FFDB99EF4DC]
	↙Description>
	↙Error>
	↙ErrorList>
	
	• JSON:
	
	{
	"ErrorList": [
	{
	"Category": "ServerError",
	"Description": "0x80040C0A SQL Server cannot b contacted, connection is lost (0x80040C0A SQL Server cannot be contacted, connection is lost (0x80004005 [DBNETLIB][ConnectionOpen (Connec]SQL Server does not exist or access denied.)[0x00007FFDCC06BBC8,0x00007FFDB99EF4BA;0x00007FFDB99BEEEF,0x00007FFDB99EF4DC]"
	}
	]
	}

Security

By default, Netwrix Auditor API uses HTTPS for sending requests to its endpoints. Netwrix encrypts data with a self-signed automatically generated SSL certificate and strongly recommends you to replace it with a new secured certificate acquired from any reliable source.

The automatically generated Netwrix API certificate is located in the Personal store. To enable trust on remote computers, install this certificate in the Trusted Root Certification Authorities store.



To manage API security settings with APIAdminTool.exe

Netwrix provides a command-line tool for managing Integration API. The tool allows switching between HTTP and HTTPS, assigning new certificates, etc.

1. On the computer where Auditor Server resides, start the Command Prompt and run the tool. The tool is located in the *Netwrix Auditor installation folder*, inside the *Audit Core* folder. For example:

   ```
   C:↘cd C:\Program Files (x86)\Netwrix Auditor\Audit Core

   C:\Program Files (x86)\Netwrix Auditor\Audit Core>APIAdminTool.exe
   ```

2. Execute one of the following commands depending on your task. Review the tips for running the tool:

   - Some commands require parameters. Provide parameters with values (parameter=value) if you want to use non-default. E.g., `APIAdminTool.exe api http port=4431`.
   - Append `help` to any command to see available parameters and sub-commands. E.g., `APIAdminTool.exe api help`.

To...	Execute...
Disable API	`APIAdminTool.exe api disable` This command duplicates the checkbox on the Integrations page in Netwrix Auditor.
Switch to HTTP	`APIAdminTool.exe api http` Netwrix recommends switching to HTTP only in safe intranet environments. To use a non-default port (9699), append a parameter port with value to the command above (e.g., `port=4431`).
Switch to HTTPS	`APIAdminTool.exe api https` Run this command if you want to continue using Netwrix-generated certificate. To use a non-default port (9699), append a parameter port with value to the command above (e.g., `port=4431`).
Assign a new SSL certificate	`APIAdminTool.exe api https certificate` Run this command if you want to apply a new certificate and use it instead default. You must add a certificate to the store before running this command. Provide parameters to specify a certificate: • For a certificate exported to a file: ◦ path—Mandatory, defines certificate location. ◦ store—Optional, defines the store name where certificate is located. By default, Personal. For example: `APIAdminTool.exe api https certificate path=`

To...	Execute...
	`C:\SecureCertificate.cef store= Personal` • For a self-signed certificate: ◦ subject—Mandatory, defines certificate name. ◦ validFrom—Optional, defines a certificate start date. By default, today. ◦ validTo—Optional, defines a certificate expiration date. By default, 5 years after a validFrom date. For example: `APIAdminTool.exe api https certificate subject= New validTo= 01/01/2024` If you want to create a new self-signed certificate for a default period of 5 years from the current date: `APIAdminTool.exe api https certificate subject= "Netwrix Integration API"` • For a certificate specified using thumbprint: ◦ store—Optional, defines the store name where certificate is located. By default, Personal. ◦ thumbprint—Mandatory, defines a thumbprint identifier for a certificate. For example: `APIAdminTool.exe api https certificate thumbprint= 3478cda8586675e420511dc0fdf59078093eeeda`

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Property in 8.0 – 8.5	New property in 9.0 and above
• XML: <AuditedSystem>↙AuditedSystem> • JSON: "AuditedSystem"	• XML: <DataSource>↙DataSource> • JSON: "DataSource"

• XML:
<ManagedObject>↙ManagedObject>
• JSON:
"ManagedObject"
	• XML:
	<MonitoringPlan>
	<Name>Name↙Name>
	<ID>Unique ID↙ID>
	↙MonitoringPlan>
	• JSON:
	"MonitoringPlan" : {
	"ID": "{Unique ID}",
	"Name": "Name"
	}
	Now the MonitoringPlan contains two sub-entries: ID and Name. The ID property is optional and is assigned automatically by the product.

—	• XML: <Item> <Name>Item name↙Name> ↙Item> • JSON: "Item": {"Name": "Item name"}

To learn more about input and output Activity Record structure, refer to Activity Records.

Add-Ons

The Netwrix Auditor Add-on Store contains free add-ons developed by Netwrix Corp. and your peers in the community. The add-ons help you leverage integration between your on-premises or cloud applications and Netwrix Auditor.

The list of available add-ons keeps growing because with the new RESTful API, the integration capabilities of Netwrix Auditor are unlimited. Netwrix encourages users to develop add-ons, upload them to Netwrix website, and share with community.

Benefits:

- Centralize auditing and reporting of your IT environment—Netwrix Auditor unifies auditing of all IT systems across your on-premises, cloud or hybrid environment, and enables centralized reporting for security and compliance.
- Get the most from your SIEM investment—To maximize SIEM value, Netwrix Auditor increases the signal-to-noise ratio and feeds your HP ArcSight, Splunk, IBM QRadar or any other SIEM solution with much more granular audit data.
- Automate your IT workflows—Automate and improve your change management, service desk and other critical IT workflows by feeding them audit data from Netwrix Auditor.

Review the following for additional information:

- Available Add-Ons
- Use Add-Ons

Available Add-Ons

At the time of Netwrix Auditor10.5 release, the following add-ons were verified and posted in Add-ons Store.

Name	Technology	Data in/out	Description
Add-on for Amazon Web Services	PowerShell	In	Exports user activity data from your Amazon Web Services using CloudTrail and feeds events to the Audit Database. Use this

Name	Technology	Data in/out	Description
			script if you want to get more out of native Amazon auditing.
CEF Export Add-on	PowerShell	Out	Exports Activity Records from the Audit Database to a CEF file. Use this script to integrate data collected by Netwrix Auditor with SIEM solutions that use CEF files as input data.
Event Log Export Add-on	PowerShell	Out	Exports Activity Records from the Audit Database to a custom Windows event log—Netwrix_Auditor_Integration. Use this script to integrate data collected by Netwrix Auditor with SIEM solutions that use events as input data. Starting with Netwrix Auditor 9.8, this add-on is generic and provides a universal solution for integration with the following SIEM systems either out of the box or with minimal customizations, including the following: 1. Splunk 2. IBM QRadar 3. AlienVault USM 4. Solarwinds Log & Event Manager 5. Intel Security 6. LogRhythm

Name	Technology	Data in/out	Description
Add-on for ArcSight	PowerShell	Out	Exports Activity Records from the Audit Database to ArcSight in its native CEF format. Use this script to integrate Netwrix Auditor with ArcSight and extend auditing possibilities.
Add-on for RADIUS server	PowerShell	In	Exports RADIUS logon events from the Security event log and feeds them to the Audit Database. Use this script to track logon activity on servers with RADIUS protocol enabled. The add-on works in collaboration with Netwrix Auditor for Active Directory, collecting additional data that augments the data collected by Netwrix Auditor. Aggregating data into a single audit trail simplifies logon activity analysis and helps you keep tabs on your IT infrastructure.
Add-on for Generic Linux Syslog	C#	In	Implemented as a service, the add-on listens to UDP port and feeds events from Syslog-based devices to the Audit Database. The add-on comes with processing rules for rsyslog messages. Use this add-on if you want to include Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42,

Name	Technology	Data in/out	Description
			and Ubuntu 16, etc., activity in your audit trail.
Add-on for Privileged User Monitoring on Linux and Unix	C#	In	Implemented as a service, the add-on listens to UDP port and feeds events from Syslog-based devices to the Audit Database. The add-on comes with processing rules for rsyslog messages. Use this add-on if you want to detect SUDO commands and remote access (SSH) on Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu 16, etc.
Add-on for ServiceNow Incident Management	C#	Out	Implemented as a service, the add-on facilitates data transition from Netwrix Auditor and automates ticket creation in ServiceNow (versions *Istanbul, Helsinki, Kingston, London*)
Add-on for ConnectWise Manage	C#	Out	Implemented as a service, the add-on forwards data collected by Netwrix Auditor to the ConnectWize Manage ticketing system, supporting automated incident management.
Add-on for CyberArk PAS	C#	In	Implemented as a service, the add-on operates as a syslog listener for the CyberArk system, providing visibility into the password-related activities.

Name	Technology	Data in/out	Description
Add-on for Microsoft System Center Virtual Machine Manager	C#	In	Implemented as a service, the add-on supplies data about operations on your SCVMM server to Netwrix database, supporting detailed SCVMM monitoring and effective response to changes.

Netwrix Auditor Integration API uses HTTPS with an automatically generated certificate for running requests to its endpoints. By default, add-ons are configured to accept all certificates that is appropriate for evaluation purposes and allows running the script without adjusting.

Refer to Security for detailed instructions on how to assign a new certificate and enable trust on remote computers.

Use Add-Ons

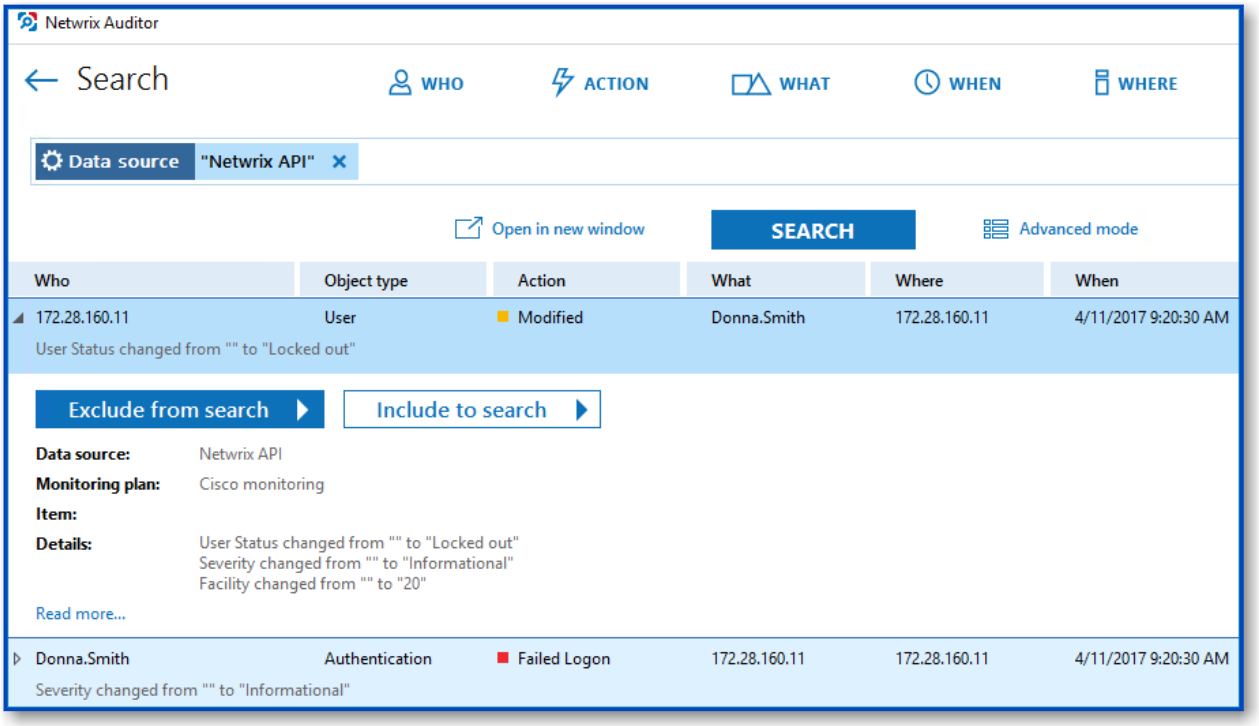
Before your start working with the add-on, go through its quick-start guide at Netwrix Documentation page. Each guide contains detailed instructions for deploying and running the add-on, as well as prerequisites and configuration settings. Generic steps are described below.

To use the add-on

1. Check prerequisites. Since the add-ons work only in combination with Netwrix Auditor, make sure that Netwrix Auidtor and its Audit Database are configured, and roles are assigned properly.
2. Specify parameters required for add-on operation. Before running or scheduling the add-on, you should define configuration details like Netwrix Auditor Server host, user credentials, etc.
3. Choose appropriate deployment scenario, then install and start the add-on. For example, if the add-on is implemented as a service, you will need to run the installation file that will deploy and start that service automatically.

4. If you are using a PowerShell-based add-on, run it from a command line: start Windows PowerShell and provide parameters. First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters—the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

5. Review the add-on operation results. For example, if you are using the add-on that imports data to Netwrix Auditor, you can search Activity Records in the Netwrix Auditor client.



6. (optional) For PowerShell based add-ons, you can schedule a daily task to ensure your audit data is always up-to-date.

AlienVault USM

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the AlienVault USM SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this

On...	Ensure that...
	case, this user will have the most extended permissions in the product.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values

unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting the Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN**username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials.

Parameter	Default value	Description
		Provide a different password if necessary.

In-Script Parameters

You may also need to modify the parameters that define how EventIDs should be generated for exported events, though their default values address most popular usage scenarios. In-script parameters are listed in the table below. To modify them, open the script for edit and enter the values you need.

Once set, these parameter values must stay unchanged until the last run of the script — otherwise dynamically calculated EventIDs will be modified and applied incorrectly.

Parameter	Default value	Description
EventID generation		
GenerateEventId	True	Defines whether to generated unique EventIDs. Possible parameter values: • True — generate unique EventIDs using Activity Record fields • False — do not generate a unique ID, set EventID=0 for all cases EventID is generated through CRC32 calculation that involves the following Activity Record field values: • ObjectType • Action • DataSource (optional, see below for details)

Parameter	Default value	Description
		Only the lowest 16 bits of the calculation result are used. See the Activity Records topic for additional information.
IncludeDataSourceToMakeEventId*	True	Defines whether the DataSource field of Activity Record should be used in the EventID calculation. This parameter is applied only if GenerateEventId is set to *TRUE*.
SetDataSourceAsEventCategory	True	Defines whether to fill in Event Category event field with a numeric value derived from the DataSource field of Activity Record. Possible parameter values: • True — generate a numeric value for Event Category using Activity Record field • False — do not generate a numeric value, set Event Category=1 for all cases The Event Category field value is generated through CRC32 calculation that involves the DataSource field of Activity Record. Only the lowest 9 bits of the calculation result are used.
SetDataSourceAsEventSource	False	Defines whether to fill in the Event Source event field with the value from the DataSource field of Activity Record. Possible parameter values:

Parameter	Default value	Description
		• True — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by $EventSourcePrefix. Default prefix is *NA*, for example:*NA Windows Server* • False — set Event Source to *Netwrix_Auditor_Integration_API* for all cases If the script cannot fill in the Event Source for some DataSource, the default value *Netwrix_Auditor_Integration_API* will be used. If the event source for particular DataSource does not exist in the Netwrix_Auditor_Integration event log, elevated privileges are required for add-on execution.

* When configuring the **IncludeDataSourceToMakeEventId** parameter, consider that the *Object Type - Action* pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding DataSource from calculation may lead to the same EventID (duplicates). See the Run the Add-On with PowerShell topic for additional information about duplicates.

Choose Appropriate Execution Scenario

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ AlienVault_USM.ps1`
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ AlienVault_USM.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ AlienVault_USM.ps1-NetwrixAuditorHost 172.28.6.15`
The add-on exports Activity Records from a remote Auditor Server using explicitly defined credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ AlienVault_USM.ps1-NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_AlienVault_USM.ps1" -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-
on_for_AlienVault_USM.ps1 - NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor Integration event log will be created and filled with events.

By default, the Netwrix Auditor Integration event log size is set to 1GB, and retention is set to "*Overwrite events as needed*". See the Appendix. Netwrix Auditor Integration Event Log Fields topic for additional information.

NOTE: Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt** file. It defines mapping between the Activity Records and related Event IDs . You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt** file.

Similarly, the add-on also creates the **Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt** file that defines mapping between the Data Source and related Category ID.

Applying Filters

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

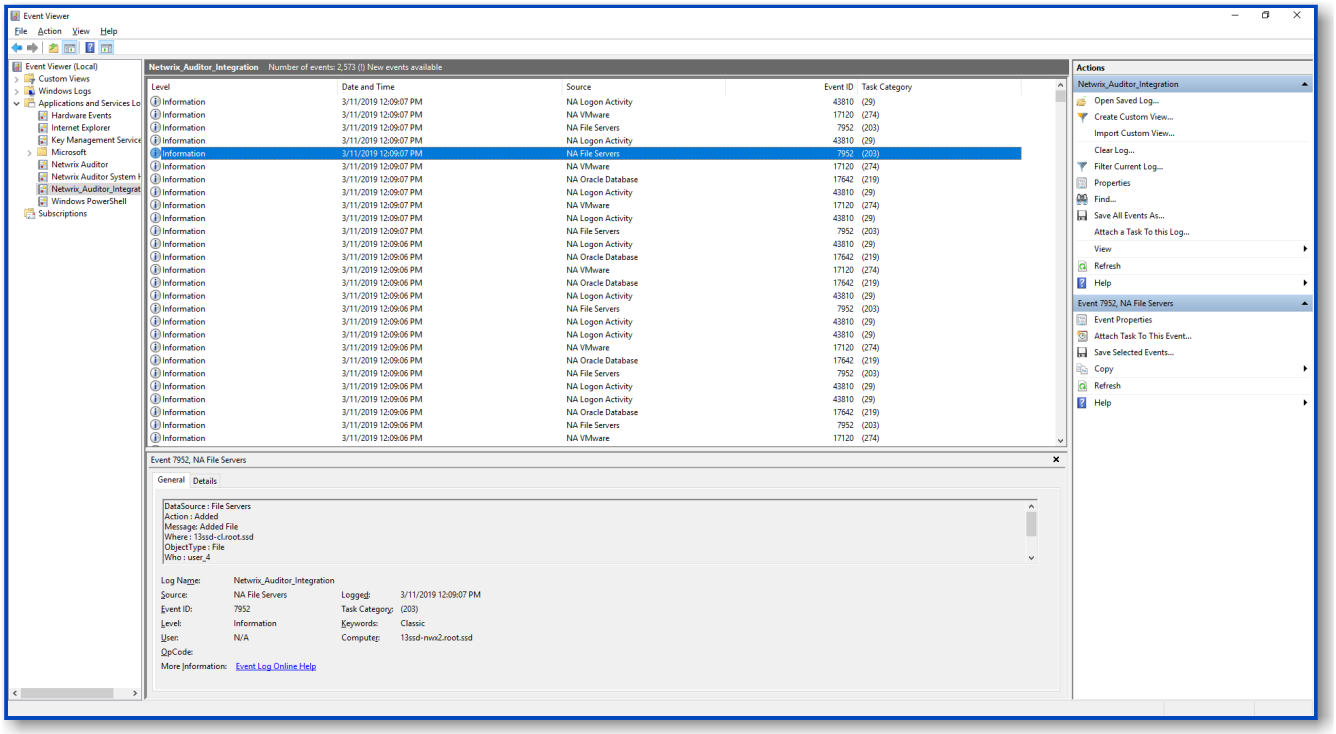
- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.
- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

Work with Collected Data

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the Event Viewer dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** >Netwrix Auditor Integration log.

Step 3 – Review events.



Now you can augment Windows event log with data collected by the Auditor.

Integration Event Log Fields

This section describes how the add-on fills in the Netwrix Auditor **Integration** event log fields with data retrieved from Activity Records.

The Activity Record structure is described in the Reference for Creating Activity Recordstopic.

Event log field name	Filled in with value	Details
Source	**NA{Data Source Name}** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter.
EventID	**{Calculated by add-on}** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*).
Task Category	**{DataSource ID}** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter.

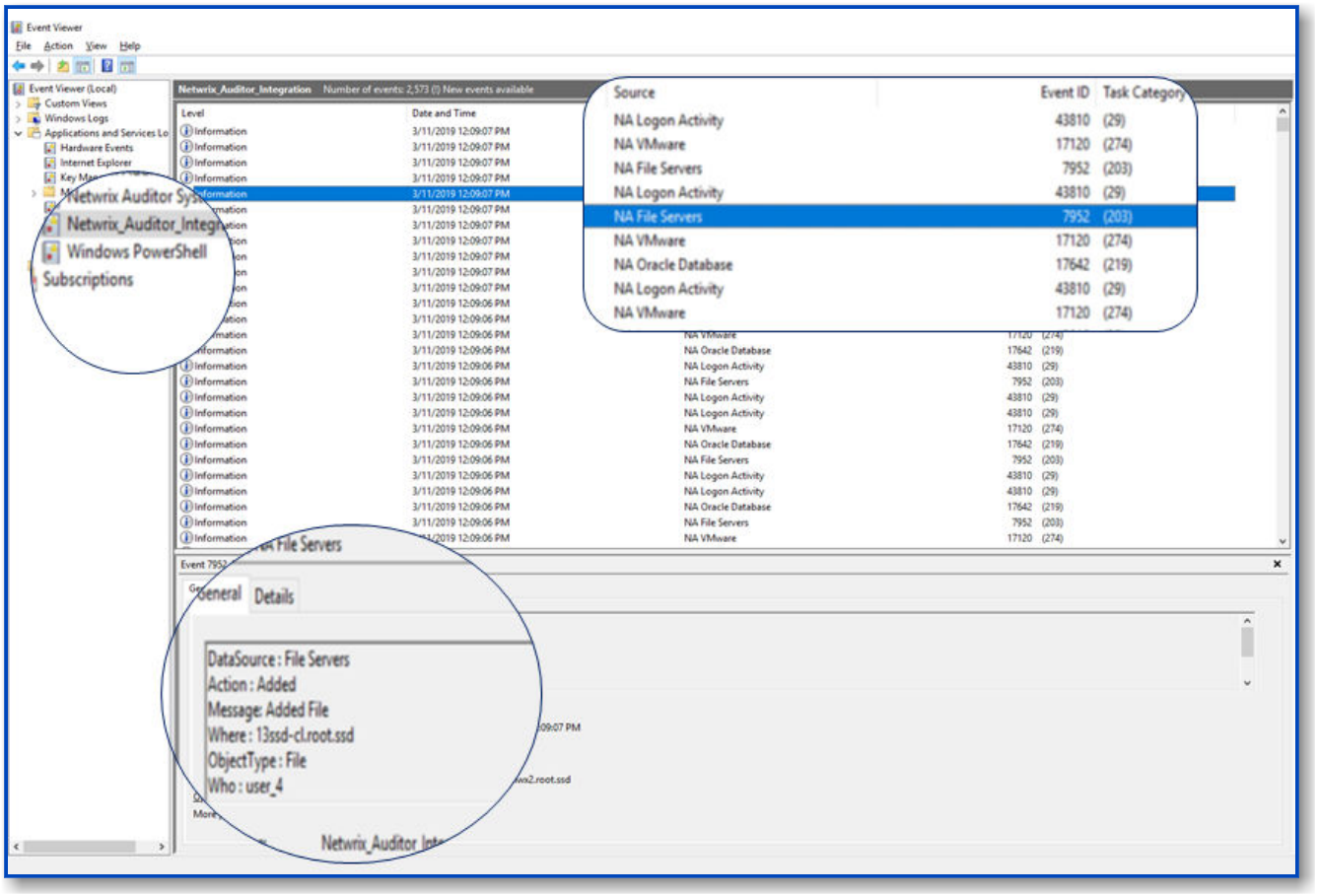
See the Define Parameters topic for additional information.

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}
Action	{Action}

Entry in EventData	Activity Record field
Message	{Action ObjectType}
Where	{Where}
ObjectType	{ObjectType}
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

Details are filled in only if this Activity Record field is not empty.



Amazon Web Services

Amazon Web Services (AWS) provides a wide range of cloud-based services, including solutions and management tools for virtualization, data storage and hosting, private networking, relational and NoSQL databases, and many more. AWS CloudTrail is an internal tracking service that records AWS API calls. Companies leverage this information for analyzing user activity patterns and detecting potential threats. Unfortunately, collected audit data cannot be used for future reference: AWS CloudTrail stores events for 7 days allowing administrators and security analysts to review data for only short time periods.

Netwrix Auditor helps you gain complete visibility into Amazon Web Services user and service activity. The Add-on for Amazon Web Services extends native AWS CloudTrail auditing and reporting possibilities. Aggregating data into a single audit trail simplifies activity analysis and helps you keep tabs on your hybrid cloud IT infrastructure. With Netwrix Auditor, AWS audit data is kept for much longer periods of time and always ready for review in easy-to-use search interface.

Implemented as a PowerShell script, this add-on automates the acquisition of Amazon Web Services CloudTrail logs and their transition to Netwrix Auditor. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

- The add-on makes an AWS API call and collects activity events from AWS CloudTrail.
- The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.

  Currently, Netwrix Auditor processes details for the following AWS events (other events can be imported without details):

CreateGroup	CreateUser	CreateLoginProfile	CreateAccessKey
DeleteGroup	DeleteUser	DeleteLoginProfile	DeleteAccessKey
AddUserToGroup	RemoveUserFromGroup	UpdateLoginProfile	UpdateAccessKey

- Using the Integration API, the add-on sends the activity events to the Auditor Server, which writes them to the **Long-Term Archive** and the **Audit Database**.

See the Integration API topic for additional information.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging the Integration API. Download the latest add-on version in the Add-on Store.

See the Integration API topic for additional information about schema updates.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Parameter or switch	Default value	Description
AWSSDKInstallPath	'C:\Program Files (x86)\AWS SDK for .NET'	Assumes that AWS SDK for .NET is installed by its default path. To specify another location, provide a path in single quotes (e.g., '*C:\Program Files (x86)\My SDKs\AWS SDK for .NET*').
ImportAllEvents	—	By deafult, only events with processed details will be imported. To import all events, set the switch during the add-on execution. **NOTE:** Importing all events makes audit data less human-readable.
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**. If you want to run the add- on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15, EnterpriseNAServer,WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor

Parameter or switch	Default value	Description
		Server, specify the account name in the *DOMAIN\username* format. **NOTE:** The account must be assigned the **Contributor** role in Auditor.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.
NetwrixAuditorPlan	—	Unless specified, data is written to the **Netwrix_ Auditor_API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add-on, make sure a dedicated plan is created in Auditor, the **Netwrix API** data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the **Audit Database**.

Update In-Script Parameters

Step 1 – Right-click a script and select **Edit**. **Windows PowerShell ISE** will start.

Step 2 – Navigate to the following lines:

```
$RegionEndpoint = "your AWS region endpoint"

$AccessKeyID = "your AWS access key ID"

$SecretAccessKey = "your AWS secret access key"
```

Step 3 – Update the following parameters:

Parameter	Description
RegionEndpoint	Provide an endpoint for your region, e.g., us-east-1 (N. Virginia). **NOTE:** If you use more than one region in your environment, run the script several times with different region endpoints. See the AWS service endpoints article for additional information.
AccessKeyID	Provide an AWS access key ID for your account. Access key is used to run requests to AWS SDK, CLIs, and API.
SecretAccessKey	Provide an AWS secret access key that works with your access key ID.

Step 4 – Save the script.

Choose Appropriate Execution Scenario

The Add-on runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Amazon Web Services topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ Amazon_Web_Services.ps1`
The add-on runs on the Auditor Server with the explicitly specified user credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ Amazon_Web_Services.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on runs on a remote computer. Data is written to a remote Auditor repository with the current user credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ Amazon_Web_Services.ps1 -NetwrixAuditorHost 172.28.6.15`
The add-on runs on a remote computer. Data is written to a remote Auditor repository with the explicitly specified user credentials and monitoring plan name.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ Amazon_Web_Services.ps1 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool -NetwrixAuditorPlan Integrations`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-
on_for_Amazon_Web_Services.ps1 - NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., `C:\Netwrix Add-ons\`), embrace it in double quotes and insert the ampersand (&) symbol in front (e.g., & "`C:\Netwrix Add-ons\`").

Step 4 – Hit **Enter**.

Depending on the number of events logged by CloudTrail it may take a while. Ensure the script execution completed successfully. Every time you run a script, Auditor makes a checkpoint with the last imported event. The next time you run the script, it will start retrieving new events.

NOTE: By default, CloudTrail keeps events for **7** days.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_ Services.ps1" -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

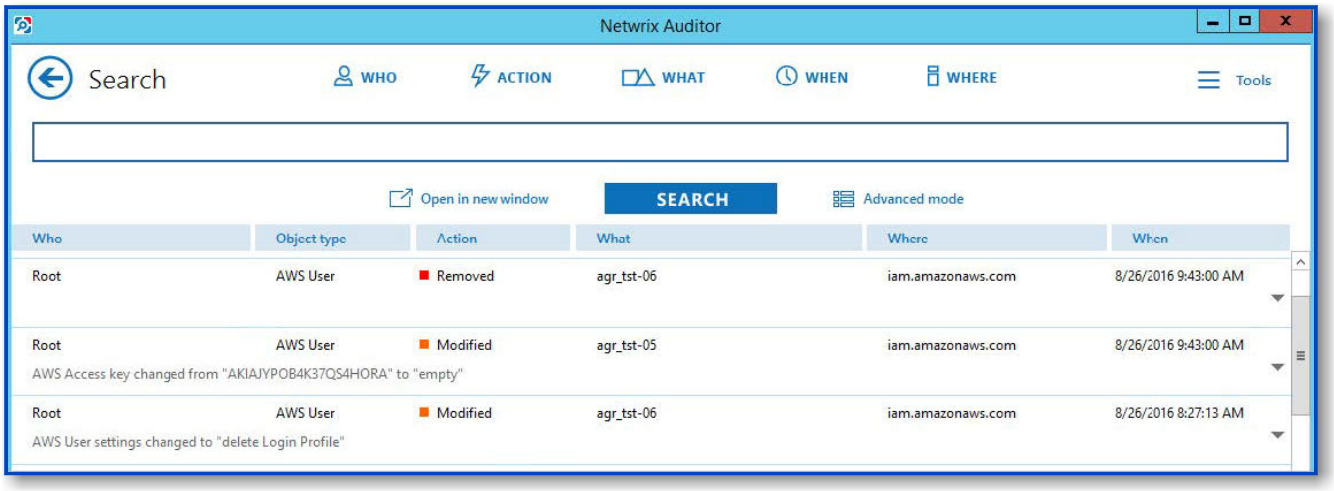
After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

Work with Collected Data

Follow the steps to work with collected data.

Step 1 – Start the Auditor client and navigate to **Search**.

Step 2 – Click **Search**.



You might want to apply a filter to narrow down your search results to the NetwrixAPI data source only.

ArcSight

Netwrix Auditor helps you extend auditing possibilities and get most from your ArcSight investment. The Netwrix Auditor Add-on for ArcSight works in collaboration with Auditor, supplying additional data that augments the data collected by ArcSight.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to ArcSight. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor Server and retrieves audit data using the Integration API.

2. The add-on processes Auditor-compatible data (Activity Records) into native ArcSight CEF format. Each exported event contains the user account, action, time, and other details.

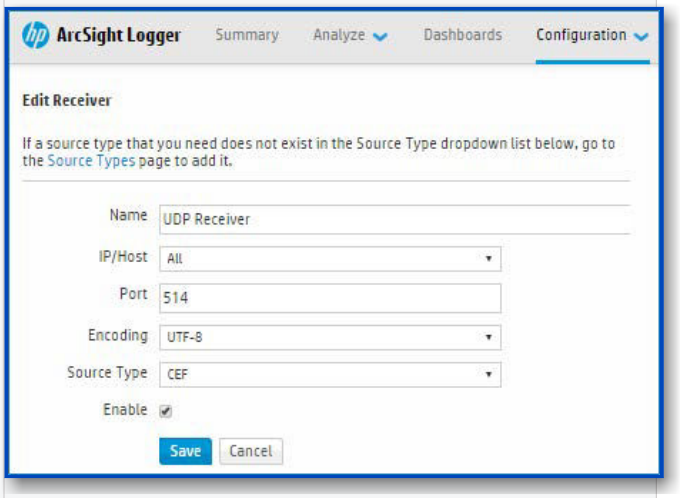
3. The add-on uploads audit trails to ArcSight Logger making it immediately ready for review and analysis. ArcSight SmartConnector configured as Syslog Daemon is supported as well.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

on...	Ensure that...
The Auditor Server side	• The Audit Database settings are configured in the Auditor. See the Audit Database topic for additional information. • The TCP 9699 port (default Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the **Global reviewer** role in Auditor or is a member of the **Netwrix Auditor Client Users** group. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.
On the ArcSight side	• The UDP Receiver is enabled and is configured to receive CEF as source and use the default port **514**. • To check receiver settings or add a new receiver, start the ArcSight Logger web interface and navigate to **Configuration** > **Receivers**.

on...	Ensure that...
	 **NOTE:** You can configure TCP Receiver and switch to TCP protocol and port **515**. • The user running the script must have sufficient permissions to supply data to ArcSight.
The computer where the script will be executed	• Execution policy for powershell scripts is set to "*Unrestricted*". Run **Windows PowerShell** as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the **write** permission on the script folder—the add-on creates a special .bin file with the last exported event.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging the Integration API. Download the latest add-on version in the Add-on Store. See the Integration APItopic for additional information.

The add-on was renamed due to HPE acquisition by Micro Focus. The former add-on name was Netwrix Auditor Add-on for HPE ArcSight. This name may still be present in the add-on files and documentation. ArcSight trademarks and registered trademarks are property of their respective owners.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See theChoose Appropriate Execution Scenario topic for additional information.

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Parameter or switch	Default value	Description
TCP	–	By default, UDP protocol is used. Specify the switch during the add-on execution if you want to use TCP protocol for transferring data. Via UDP, events will be sent one by one, via TCP— in a batch.
ArcSightHost	–	Provide a name of the computer where ArcSight resides (e.g., 172.28.6.18, ArcSightSRV, ArcSightSRV.enterprise.local). **NOTE:** This is a mandatory parameter. Unless specified, the add- on assumes that the default port 514 is used for UDP and 515 for TCP. To specify a non-default port, provide a server name followed by

Parameter or switch	Default value	Description
		the port number (e.g., *ArcSightSRV.enterprise.local:9998*).
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Auditor Server and uses default port 9699. If you want to run the add- on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN\username* format. **NOTE:** The account must be assigned the **Global reviewer** role in Netwrix Auditor or be a member of the **Netwrix Auditor Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials.

Parameter or switch	Default value	Description
		Provide a different password if necessary.

Choose Appropriate Execution Scenario

The Add-on runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Data is written a remote ArcSight through UDP protocol.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ ArcSight.ps1 -ArcSightHost 172.28.6.18`
The add-on runs on the Auditor Server with the current user credentials. Data is written a remote ArcSight through TCP protocol.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ ArcSight.ps1 -TCP -ArcSightHost 172.28.6.18`
The add-on runs on the Auditor Server with the explicitly specified user credentials. Data is written a remote ArcSight with a non-default UDP port.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ ArcSight.ps1 -ArcSightHost 172.28.6.18:9999 -NetwrixAuditorUserName enterprise\NAuser - NetwrixAuditorPassword NetwrixIsCool`
The add-on runs on a remote computer with the current user credentials. Data is retrieved from a remote Auditor repository and written to a remote ArcSight.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ ArcSight.ps1 -ArcSightHost 172.28.6.24 - NetwrixAuditorHost 172.28.6.15`

Scenario	Example
The add-on runs on a remote computer. Data is retrieved from a remote Auditor repository with the explicitly specified user credentials and written to a remote ArcSight.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ ArcSight.ps1 -ArcSightHost 172.28.6.24 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ArcSight.ps1 - ArcSightHost 172.28.6.24 -NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in the Audit Database execution may take a while. Ensure the script execution completed successfully. As a result, data will be exported to ArcSight. Note that events exceeding 4000 symbols are trimmed.

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records.

Automate Add-On Execution

To ensure you feed the most recent data to ArcSight, Netwrix recommends scheduling a daily task for running the add-on.

To create a scheduled task

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – Select **Create Task**.

Step 3 – On the **General** tab, specify a task name, e.g., Netwrix Auditor Add-on for ArcSight. Make sure the account that runs the task has all necessary rights and permissions.

Step 4 – On the **Triggers** tab, **click** New and define the schedule. This option controls how often audit data is exported from Auditor and transferred to ArcSight Logger. Netwrix recommends scheduling a daily task.

Step 5 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information.

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_HPE_ArcSight.ps1" -ArcSightHost 172.28.6.24 - NetwrixAuditorHost 172.28.6.15`

Step 6 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

Work with Collected Data

Follow the steps to see collected data.

Step 1 – Log on to your ArcSight Logger web interface.

Step 2 – On the **Summary** page, select the **Event Summary by Receiver** diagram and click the **UDP Receiver** segment (Activity Records are imported through UDP Receiver). Select **TCP Receiver** if you specified TCP protocol for transferring data.

Step 3 – On the **Analyze** page that opens, review the search field. Ensure your computer is listed as Receiver (e.g., "*172.28.156.131 [UDP Receiver]*"). If you imported Activity Records from more than one Netwrix Auditor Server, add all of them in the search field.

NOTE: You might want to modify time range and the fields shown.

	Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceEventClassId
1	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon
2	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon
3	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon
4	2017/02/09 09:29:14 EST	172.28.156.131 [UDP Receiver]	Local	Netwrix	Logon Activity	Successful Logon

Step 4 – Review imported Activity Records.

Azure Files

Azure Files is a Microsoft service that offers file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol, Network File System (NFS) protocol, and Azure Files REST API. Azure file shares can be mounted concurrently by cloud or on-premises deployments. SMB Azure file shares are accessible from Windows, Linux, and macOS clients. To learn more about Azure Files, refer to the corresponding Microsoft article.

The Netwrix Auditor Add-On for Azure Files works in collaboration with Netwrix Auditor, supplying data about SMB changes on your Azure Files shares, such as document reads, modifications and deletions.

To get the add-on up and running, please read the following topics:

- Deployment Procedure
- Work with Collected Data

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

- The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information.
- The TCP 9699 port (default Integration API port) is open for inbound connections.
- The user writing data to the Audit Database is granted the Contributor role in Auditor. See the Role-Based Access and Delegation topic for additional information.
- Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
- Azure Files environment is configured for auditing. The connection of Azure file share to Windows should be configured with authentication through Active Directory or Entra ID (as opposed to the account key). See the Deployment Proceduretopic for more information.
- Active Directory Domain Services or Microsoft Entra Kerberos is used as an Identity source. See the Deployment Procedure topic for additional information.

How It Works

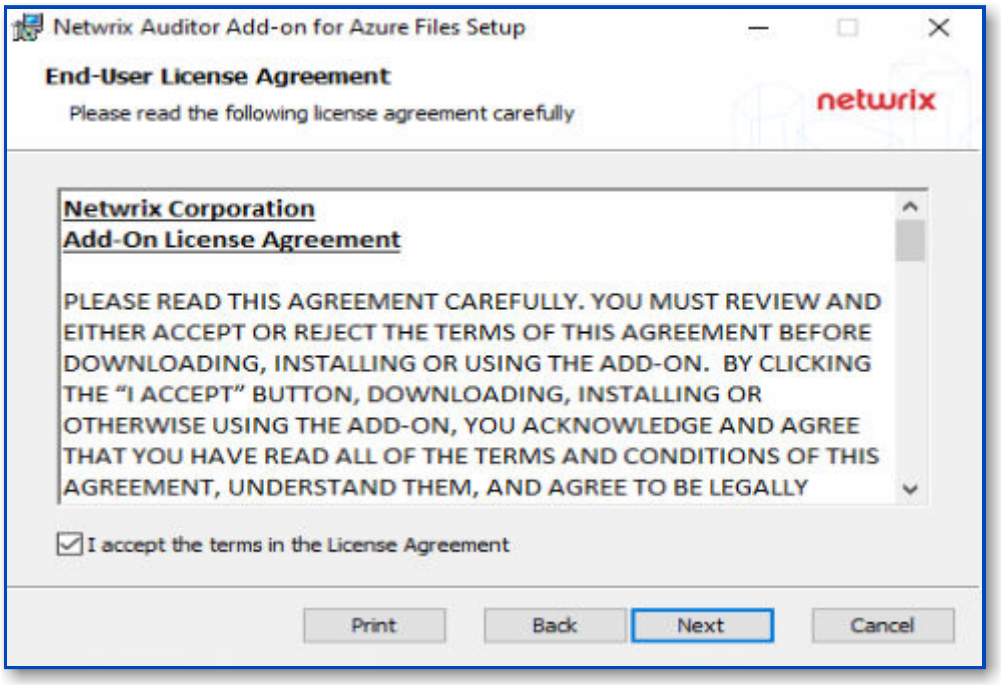
On a high level, the add-on works as follows:

- The add-on collects logs from the specified Azure storage account. The add-on supports activity auditing of shares with identity-based access via saved logs collected from storage account and using Graph API for SIDs resolving.
- The add-on processes these events into Netwrix Auditor compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.
- Using the Integration API, the add-on sends the activity records to the Netwrix Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

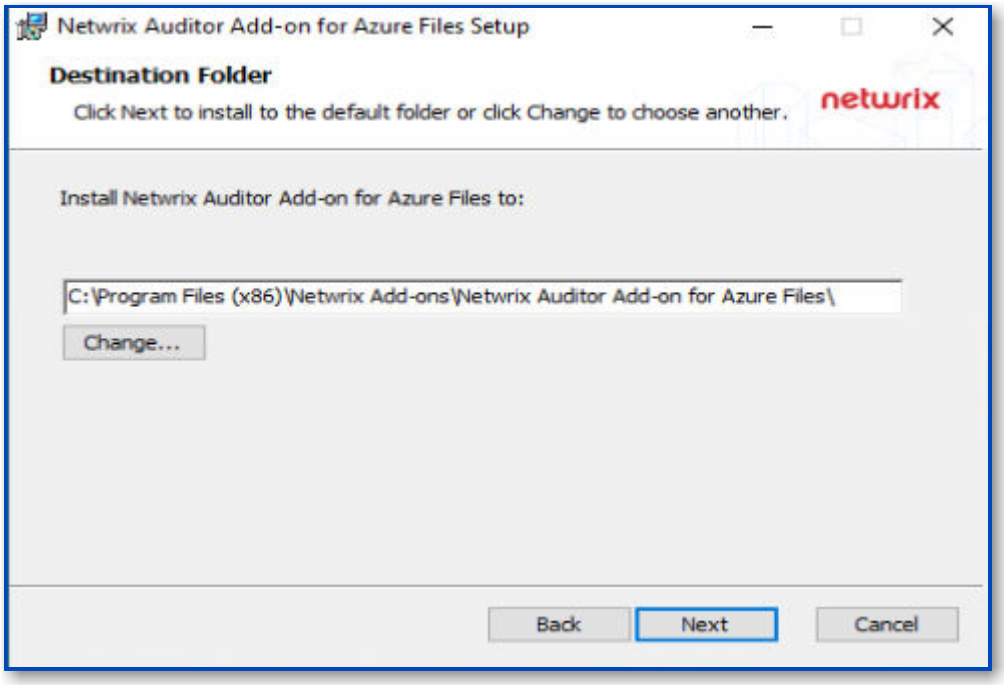
Deployment Procedure

Follow the steps to install Azure Files add-on.

Step 1 – Accept EULA.



Step 2 – Select the installation folder and click **Next**.



Step 3 – Click **Install**. The wizard will start and ask the additional parameters.

Configure Azure Files for Monitoring

Follow the steps to configure Azure files for monitoring.

Step 1 – Make sure you have a storage account to store logs. To reduce the volume of the stored logs and the corresponding cost, it is recommended to create a rule in Life Cycle Management for this storage. Netwrix Auditor doesn't need historic logs, after the add-on has written them into the database. Refer to the corresponding Microsoft article for additional information.

Step 2 – Enable audit in the Azure Files settings. Go to the Diagnostic settings, and make sure that the following options are selected:

- "Audit" under the **Logs**
- "Archive to a storage account" under the **Destination details**
- Correct Storage account in the drop-down menu

Step 3 – Go to the storage account that has been created before and copy Connection String. This parameter will be used in the add-on configuration.

Step 4 – If Microsoft Entra Kerberos or Active Directory Domain Services is used as an Identity source, Graph API will be used to resolve the user names. It is necessary to register an Azure App and grant it the following permissions:

- Type - Application
- Microsoft.Graph - User.Read.All

After that, save the Tenant ID, Application ID, and secret.

Configure the add-on

Follow the steps to configure the add-on.

Step 1 – After the installation, the add-on configuration wizard will start. If it didn't start automatically - open it from the installation folder.

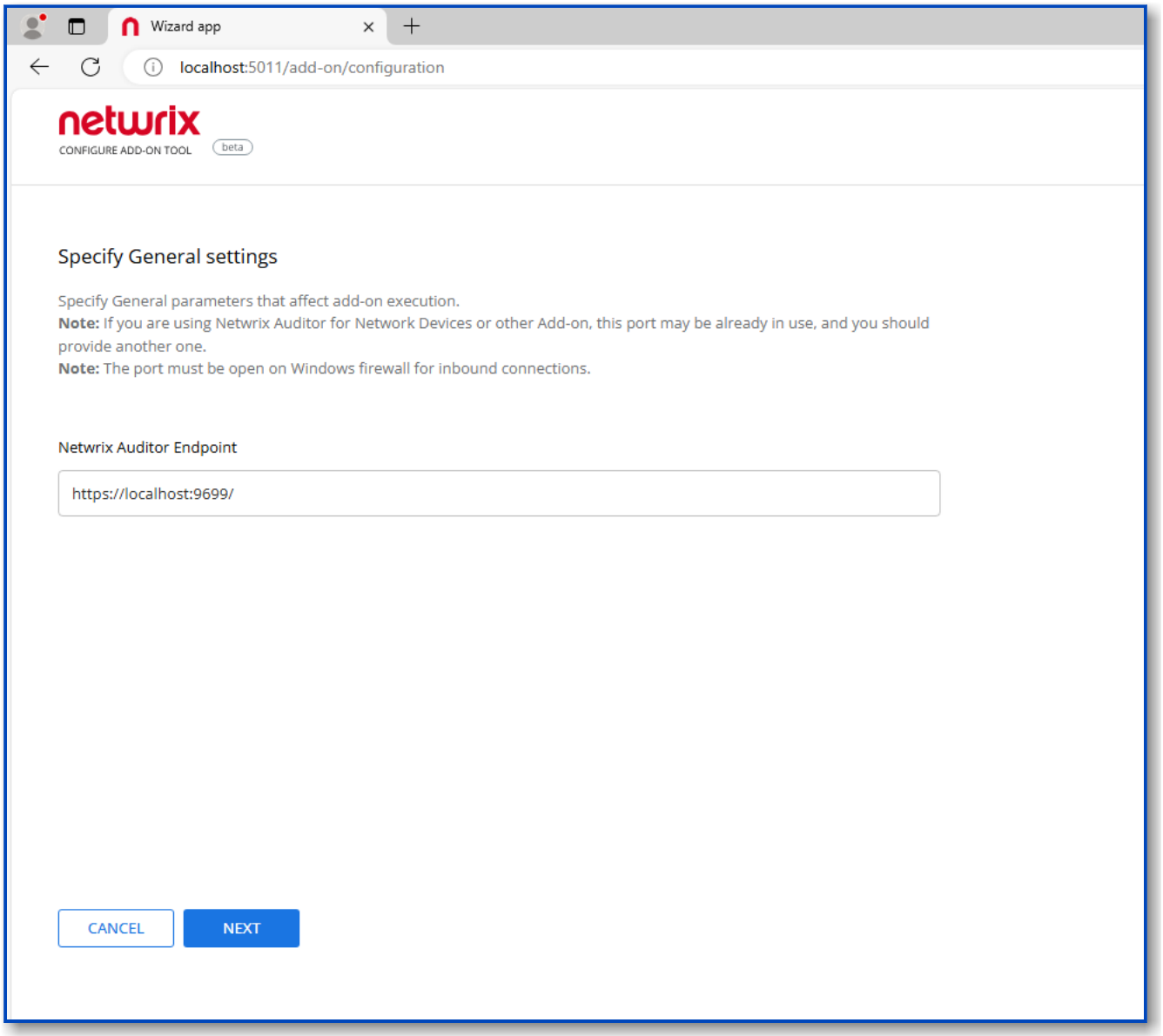
Step 2 – Select **Proceed**.

Step 3 – Provide Auditor Server IP address and port number followed by endpoint for posting Activity Records. See the API Endpoints topic for more information.

This assumes that the add-on runs on the computer hosting Auditor Server and uses default port 9699.

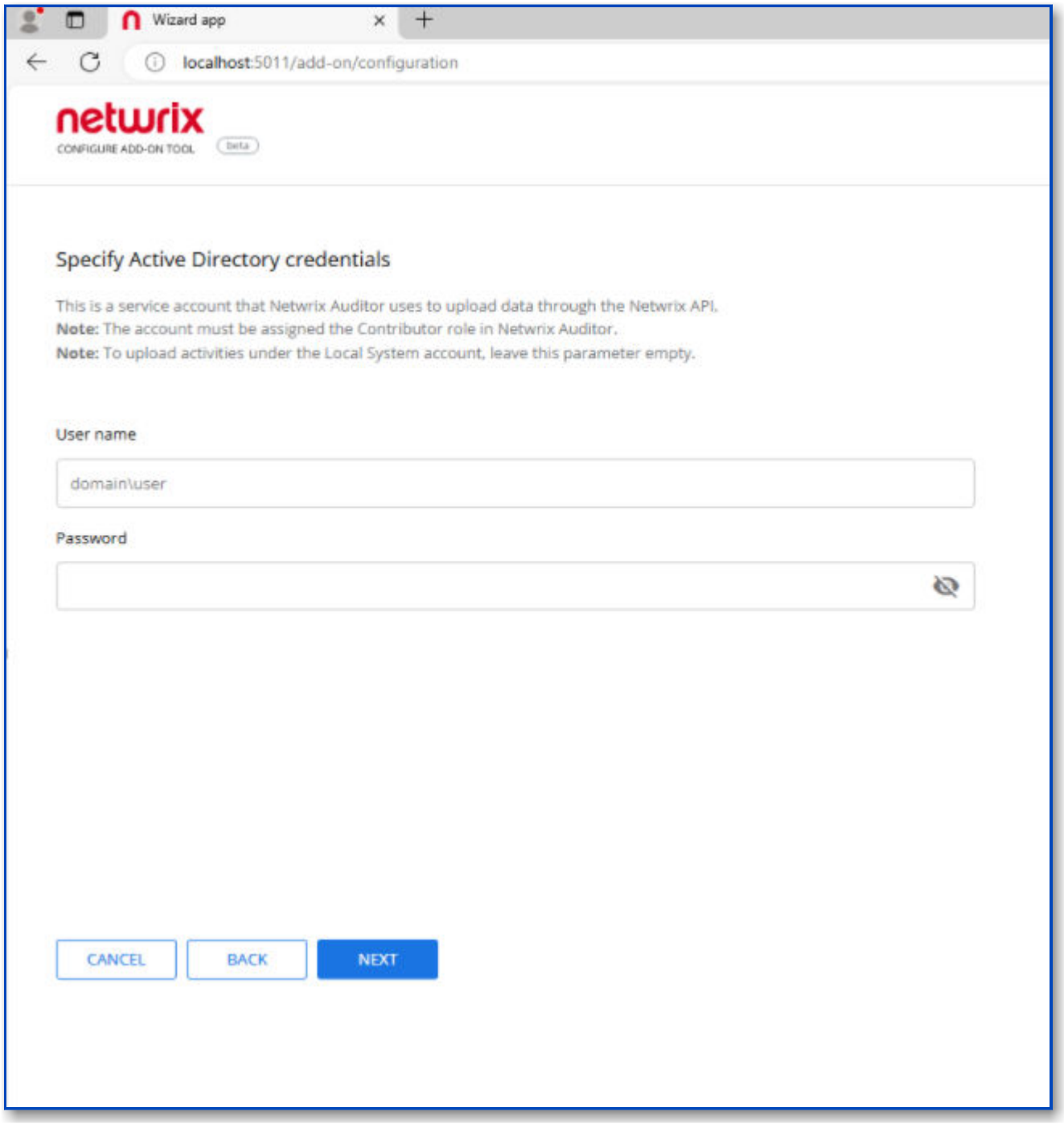
If you want to run the add-on on another machine, you need to provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15*, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.ent erprise.local:9999).

CAUTION: Do not modify the endpoint part (*/netwrix/api*).

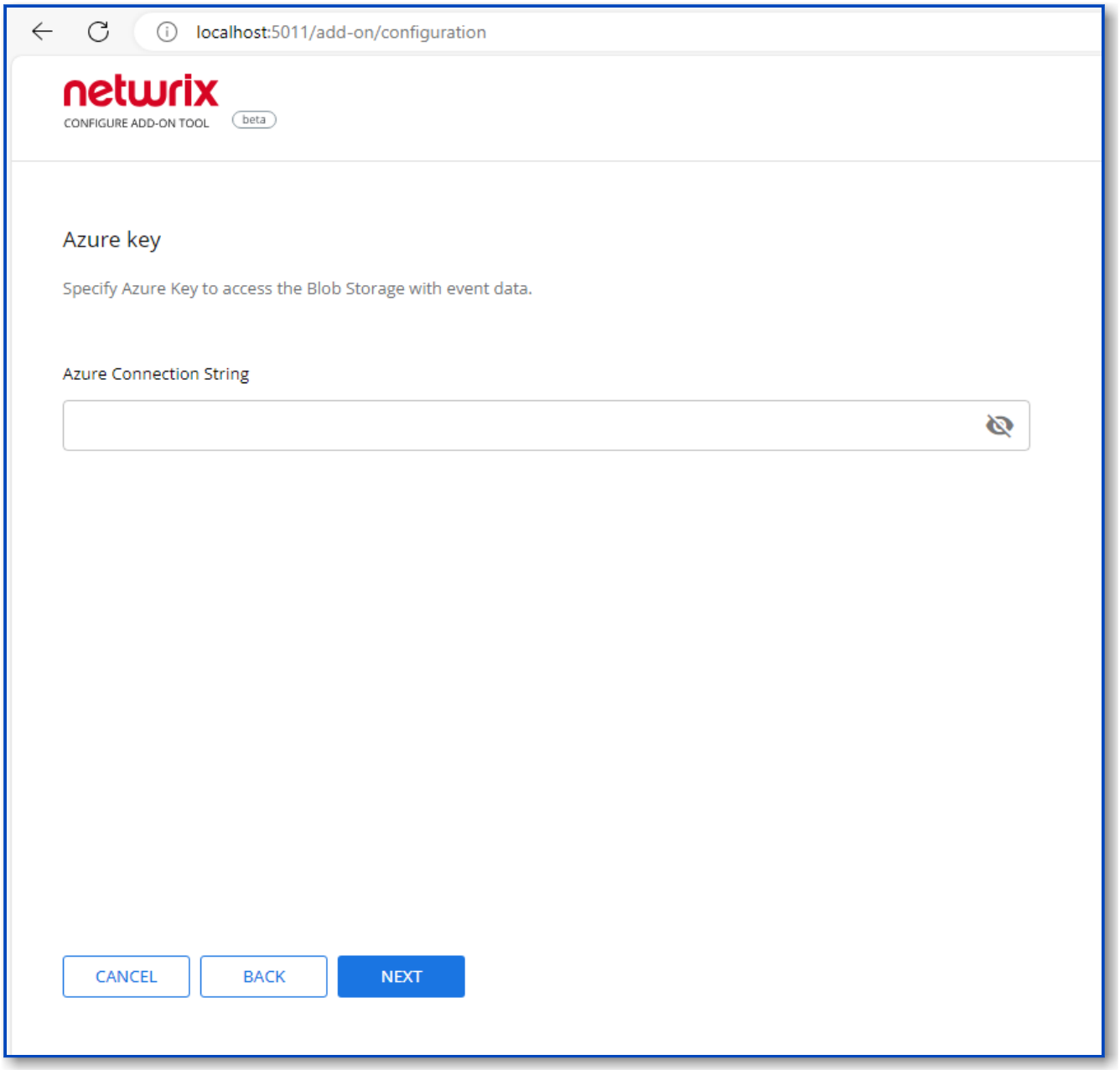


Step 4 – Specify Active Directory credentials:

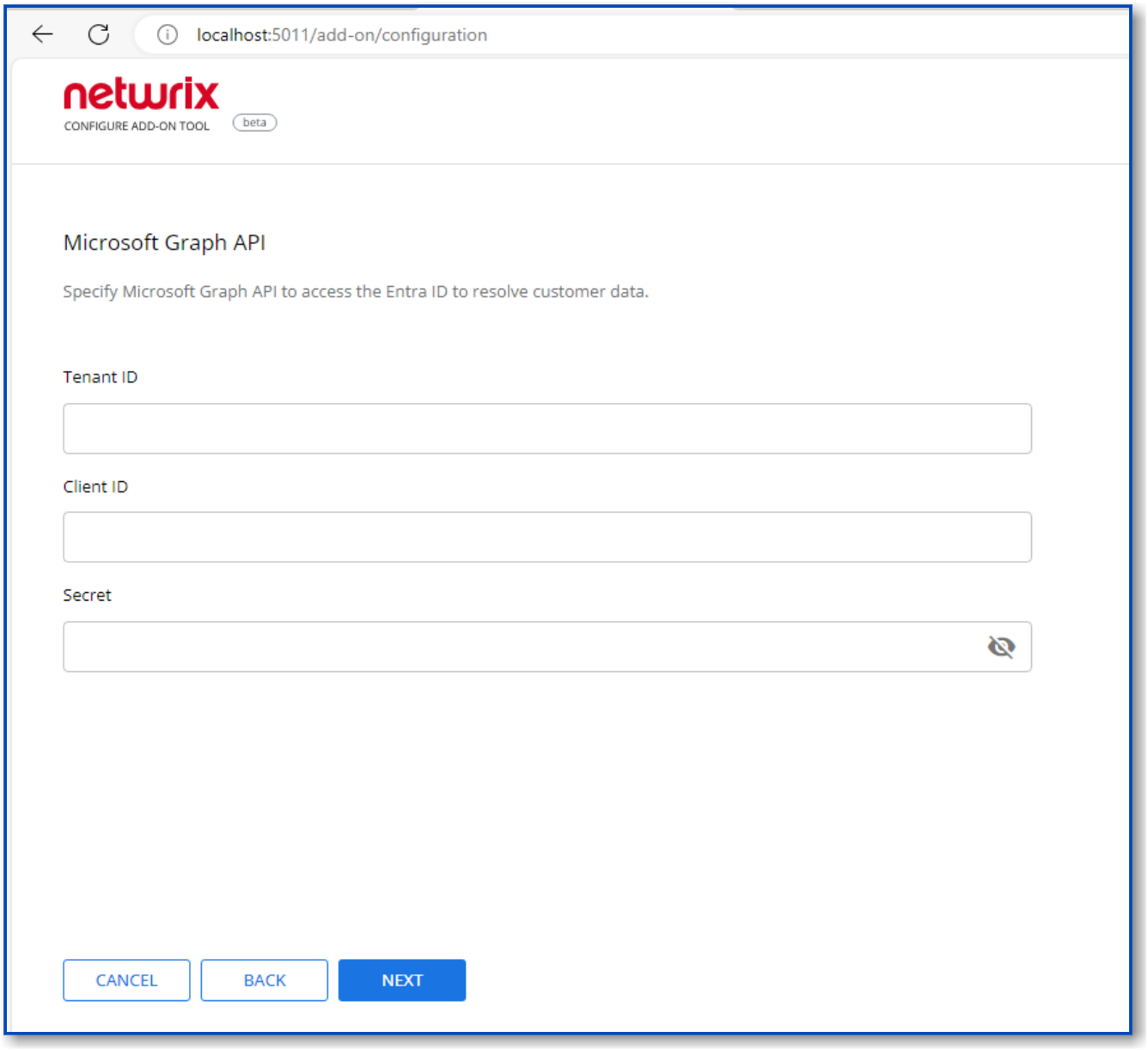
- Username – Provide the name of the account under which the service runs. Unless specified, the service runs under the account currently logged on.
- Password – Provide the password for the selected account.



Step 5 – Paste Azure Connection String in the corresponded field and click **Next**.



Step 6 – Enter Tenant ID, App ID and App Secret of the Azure App you registered for the add-on. Click **Next**.



Step 7 – Click **Run** and close the window. The service should start the data collection now.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You might want to apply a filter to narrow down your search results to the Netwrix**API** data source only.

- You can also click **Tools** in the upper-right corner and select the command you need. For example:
  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See the following topics for additional information:

- Alerts
- View and Search Collected Data
- Subscriptions

ConnectWise Manage

Managed Service Providers (MSP) need to effectively utilize and standardize IT service management tools. Those who use for that purpose the ConnectWise Manage solution usually have similar processes in place:

- When an incident or a problem occurs in the IT environment, managed client sends (usually by email) a request to the MSP's service desk. A service ticket is then created manually or automatically in ConnectWise Manage.
- Each ticket is assigned to authorized personnel for investigation and resolution in accordance with the existing workflow.
- To control ticket handling and report on statistics, ConnectWise service boards are used.

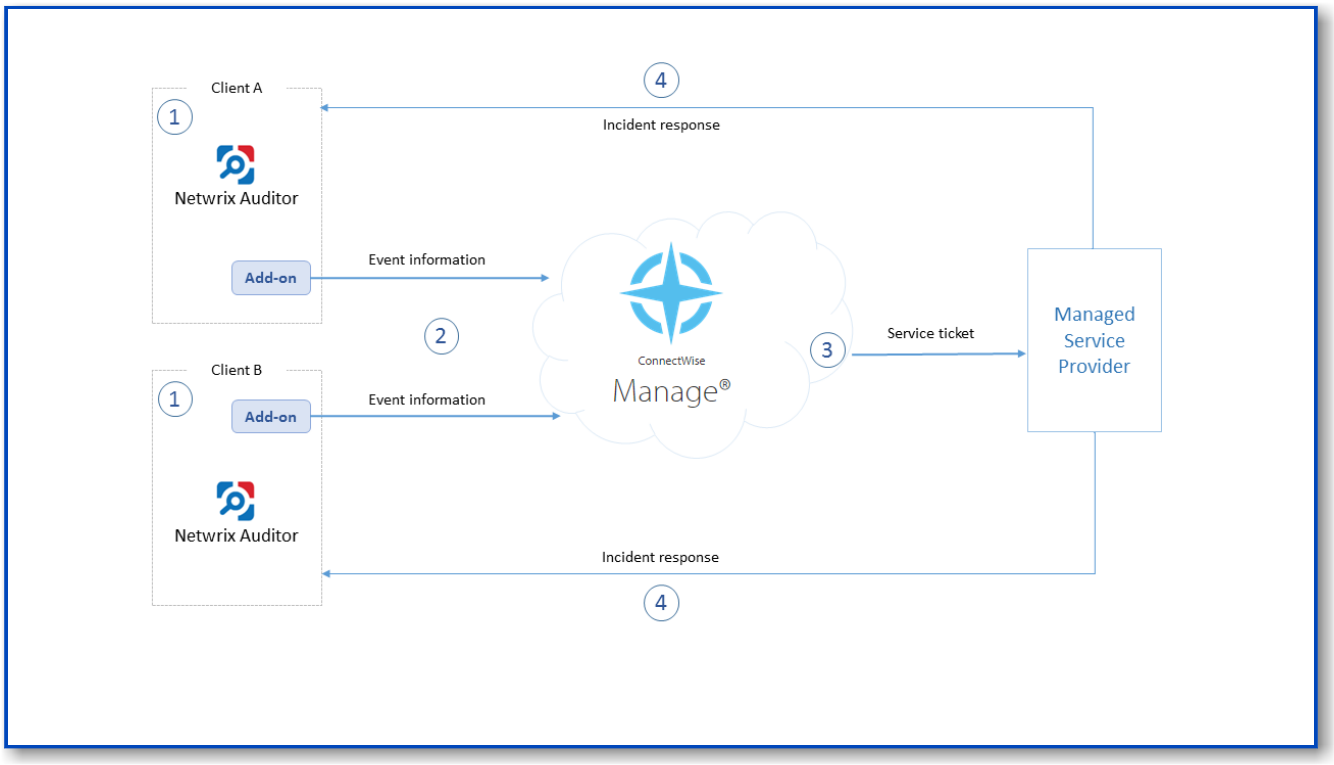
Netwrix has built a ready-to-use add-on that automates incident management, automatically creating service tickets for security alerts triggered by Netwrix Auditor This integration brings in the following benefits:

- Seamless integration with the existing MSP service process
- Speeding up the process of restoring secure, normal business service
- Minimizing the gap between incident detection and the start of a resolution process
- Automating ticket handling and reducing human errors that could impact its quality
- Meeting or exceeding service level agreements (SLAs) while saving time and effort

To implement the solution, Managed Service Provider does the following on the client side:

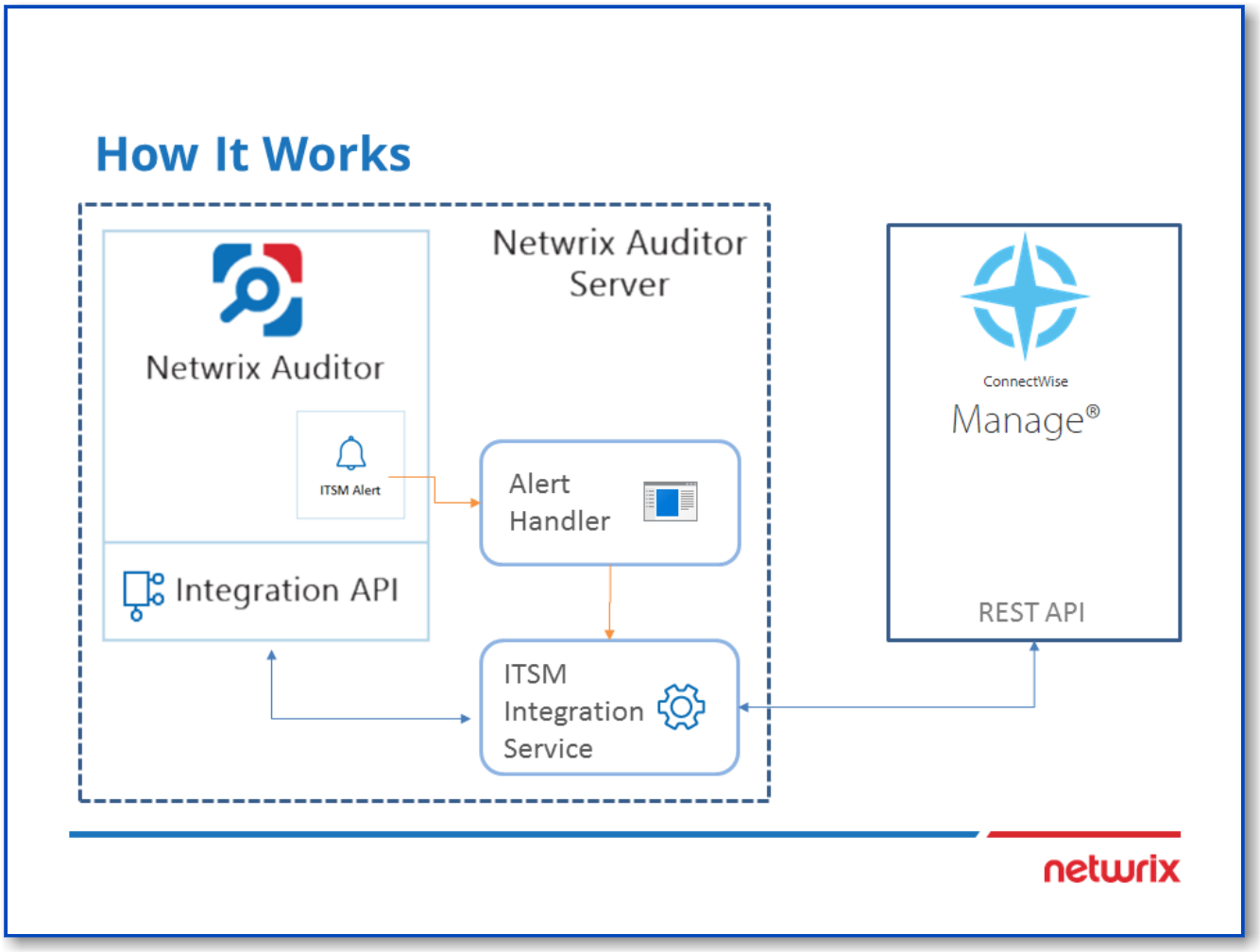
1. Deploys and maintains Netwrix Auditor that monitors users' activity and configuration changes
2. Installs and configures integration solution (add-on) on Netwrix Auditor Server
3. Controls ticket resolution and corrective measures

On a high level, the workflow is as follows:



1. Managed Service Provider installs and configures the add-on on AuditorServer. MSP also enables the necessary alerts in Netwrix Auditor, specifying add-on launch as the response action in the alert settings.
2. Whenever the alert is triggered, the add-on uses the Integration API to retrieve activity record for the original event from the audit store. An activity record contains the user account, action, time, and other details. The add-on creates a service ticket in ConnectWise Manage, populates it with data from the activity record, and assigns Impact, Priority and SLA status to the ticket.
3. The designated service team performs data analysis and root cause detection to resolve the ticket; MSP is notified of the results and possible response actions to take on the client side.
4. MSP performs actions for incident response.

Solution architecture and key components are shown in the figure below:



- **Alert Handler (Netwrix.ITSM.AlertResponseAction.exe)** — the executable that is specified in the Auditor alerts as the response action. Alert Handler:
  - Receives the IDs of the alert and associated activity record.
  - Forwards them to the Netwrix AuditorConnectWise Manage Integration Service over RPC, putting the alert into the service queue.

For details on the alert response action, see the Configure a Response Action for Alert topic for additional information.

- **Netwrix Auditor ConnectWise Manage Integration Service (Netwrix.ITSM.IntegrationServiceCW.exe)** — the main component of the solution, implemented as Windows service. It does the following:
  - Interacts with Auditor via its Integration API to retrieve the activity records from the Audit Database by record ID.
  - Forwards activity record data to ConnectWise Manage via its REST API, creates a new service ticket and populates its properties, as specified by user in the add-on configuration.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

Location	Prerequisites
Auditor Server	• The add-on supports Auditor version 9.96. • The add-on will run on the computer where Auditor Server works, so the add-on package should be copied to that machine. • For add-on operation, **NET 4.5** framework is required on Auditor Server. • Starting with add-on build 1.0.12.0, **TLS 1.2** protocol is supported. By default, this capability is disabled. For detailed information on enabling it, see the Deploy the Add-On topic for additional information. **Auditor settings** • The Audit Database settings should be configured in Auditor Server. • Monitoring plans should be configured to store data to the Audit Database. • The **TCP 9699** port (default Integration API port) should be open for inbound connections. **Required permissions** • Unless specified, the **Netwrix.ITSM.IntegrationServiceCW.exe** Windows service (main add-on co mponent) will run under the **LocalSystem** account. • The account that will be used by Netwrix.ITSM.IntegrationServiceCW.exe component to access Auditor Server must be granted the Global administrator role in Auditor. -OR- be a member of the Netwrix Auditor **Administrators** group.

Location	Prerequisites
ConnectWise Manage	• By default, the add-on connects to the latest version of the ConnectWise Manage application (v4_6_release). **Required permissions** • To connect to ConnectWise Manage via its REST API, you will require an API Member account — it is needed to log in to ConnectWise Manage. See this article for details. • It is recommended to assign the **API Member** account to a limited security role with the following permissions: ◦ **System** – **Table Setup** – **Inquire Level** = **All** ◦ **Companies** – **Company Maintenance** – **Add(all)**, **Inquire(all)** ◦ **Companies** – **Manage Attachments** – **Add(all)**, **Inquire(all)** ◦ **Service Desk** – **Service Tickets** – **Add(all)**, **Inquire(all)**

Deploy the Add-On

Follow the steps to deploy the Add-On for ConnectWise.

Step 1 – Prepare Auditor for using the add-on:

1. In the Auditor settings, enable Integration API and specify connection port. See the Integrations topic for additional information.
2. Make sure your monitoring plans set up in Auditor are using Audit Databases to store collected data. See the Audit Database topic for additional information.

Step 2 – Download the add-on package and copy it to the computer where Auditor Server resides.

Step 3 – Unpack the ZIP archive to a folder of your choice; by default, it will be unpacked to the Netwrix Auditor Add-On for ConnectWise Manage folder.

Step 4 – Run the install.cmd file. It will deploy and enable the Netwrix Auditor **ConnectWise Manage Integration Service**.

Step 5 – Run the ConfigureConnection.exe and follow the steps of the wizard to configure connection and ticketing settings for ConectWise Manage. See the Configure ConnectWise topic for additional information.

Step 6 – (optional) To adjust the add-on operation and data flow settings, edit the ITSMSettings.xml file. See the Operational Settings topic for additional information.

Step 7 – In Auditor, go to Alerts, select the required alerts, click Edit, and in the Response Action section of the alert properties specify the full path to Netwrix.ITSM.AlertResponseAction.exe file (the add-on component responsible for alert handling), for example, *C:\Addon\ITSM_CW\Netwrix.ITSM.AlertResponseAction.exe*.

Enabling TLS 1.2 Usage

The add-on supports Transport Layer Security (TLS) 1.2 security protocol. By default, this capability is disabled. To enable it, in the **ConnectWiseSettings.xml**, locate the **<EnableTls12>** parameter and set its value to *TRUE*.

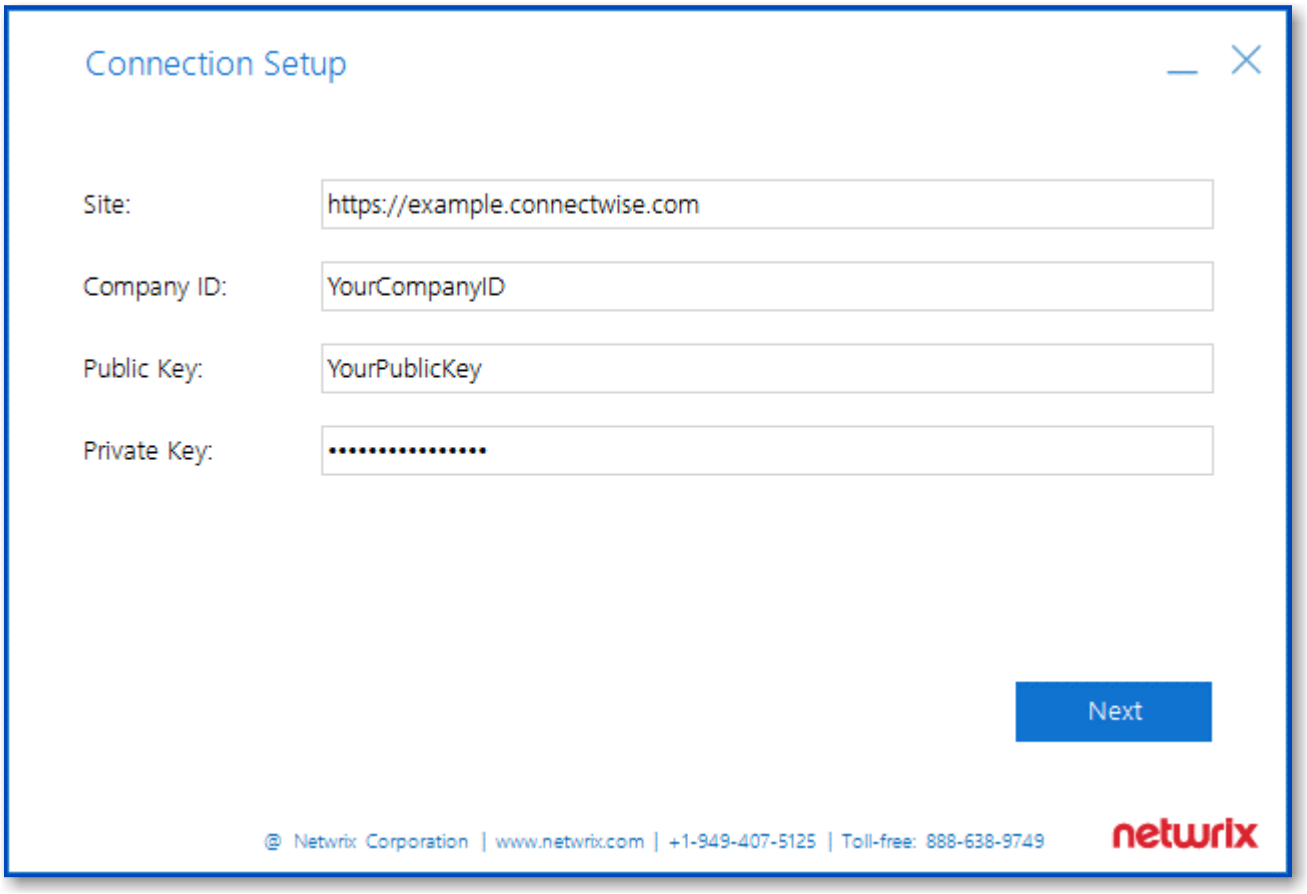
Configure ConnectWise

This section describes how to configure settings of the main add-on component, Netwrix Auditor **ConnectWise Manage Integration Service** that is required for connection to ConnectWise Manage and service ticket creation.

Follow the steps to configure ConnectWise.

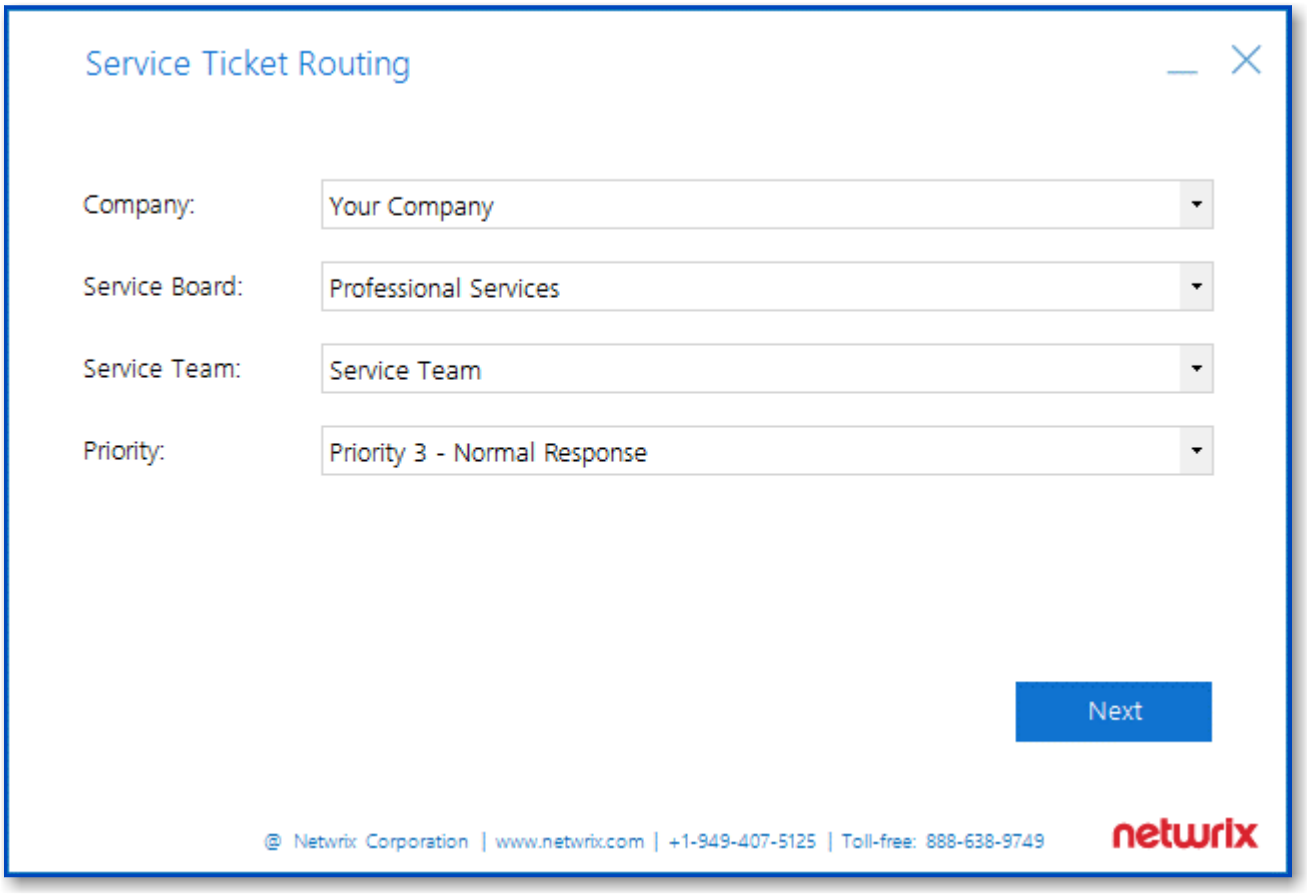
Step 1 – To connect to ConnectWise Manage REST API, the API keys will be required. To obtain them, you will need an API Member account. See this article for details.

Step 2 – Navigate to the add-on folder and run ConfigureConnection.exe. Follow the steps of the wizard to configure connection to ConnectWise Manage and ticketing options. At the Connection Setup step, specify the following:



Parameter	Description
Site	URL of ConnectWise Manage system.
Company ID	The ID of ConnectWise Manage subscriber (Managed Service Provider).
PublicKey	Public key you obtained for the API Member — it will be used to access ConnectWise REST API.
PrivateKey	Private key you obtained for the API Member — it will be used to access ConnectWise REST API.

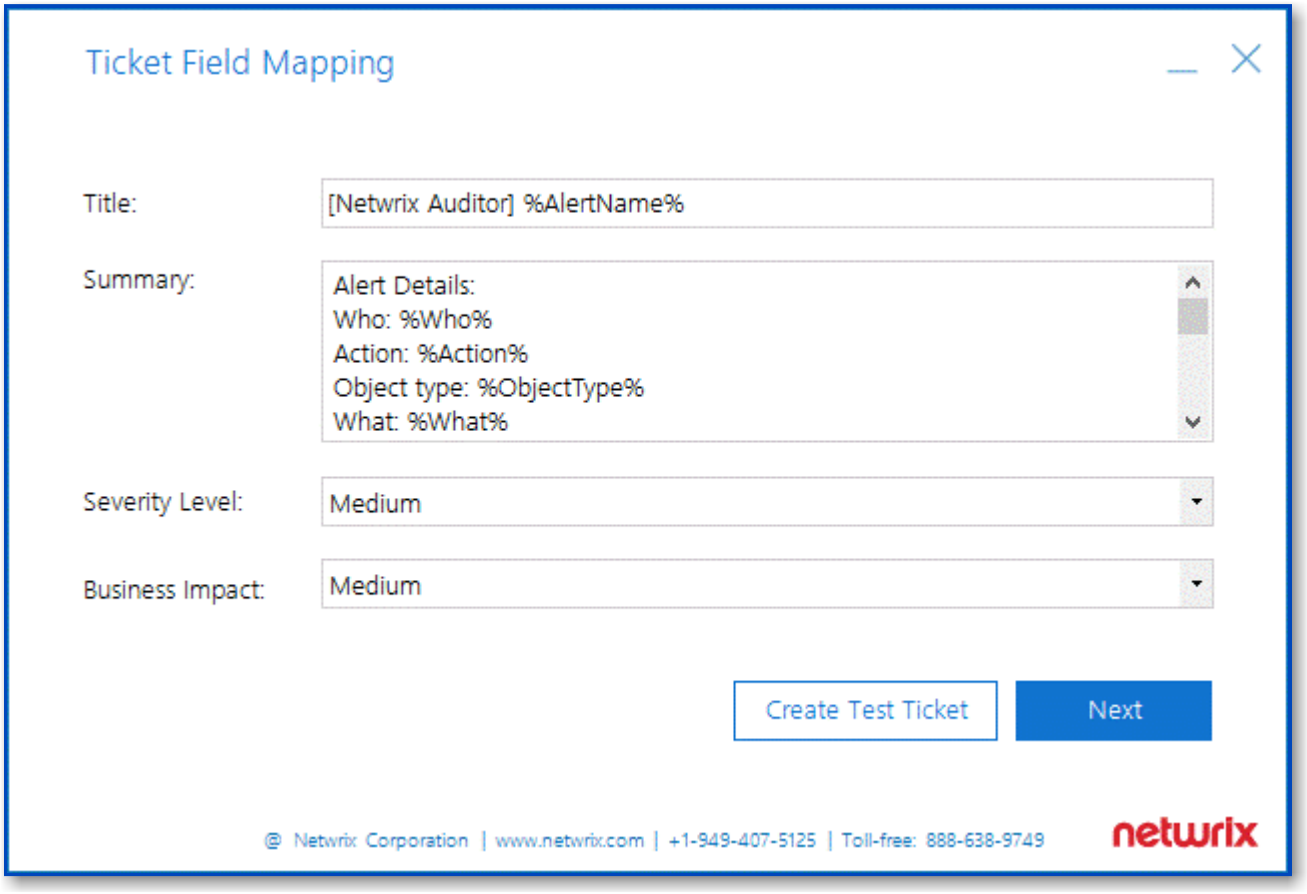
Step 3 – At the Service Ticket Routing step, specify the following:



Parameter	Description
Company	Organization that will be recorded as ticket originator — this can be a company or MSP's managed client.
Service Board	Service board where the tickets will be processed. Service tickets created by the add-on will be assigned the default ticket status for the selected service board.
Service Team	Service team that will be responsible for tickets handling.

Parameter	Description
Priority	Priority for ticket handling. Default is *Priority 3 — Normal Response*.

Step 4 – Configure how Auditor activity record fields will be mapped with **ConnectWise Manage** ticket fields.

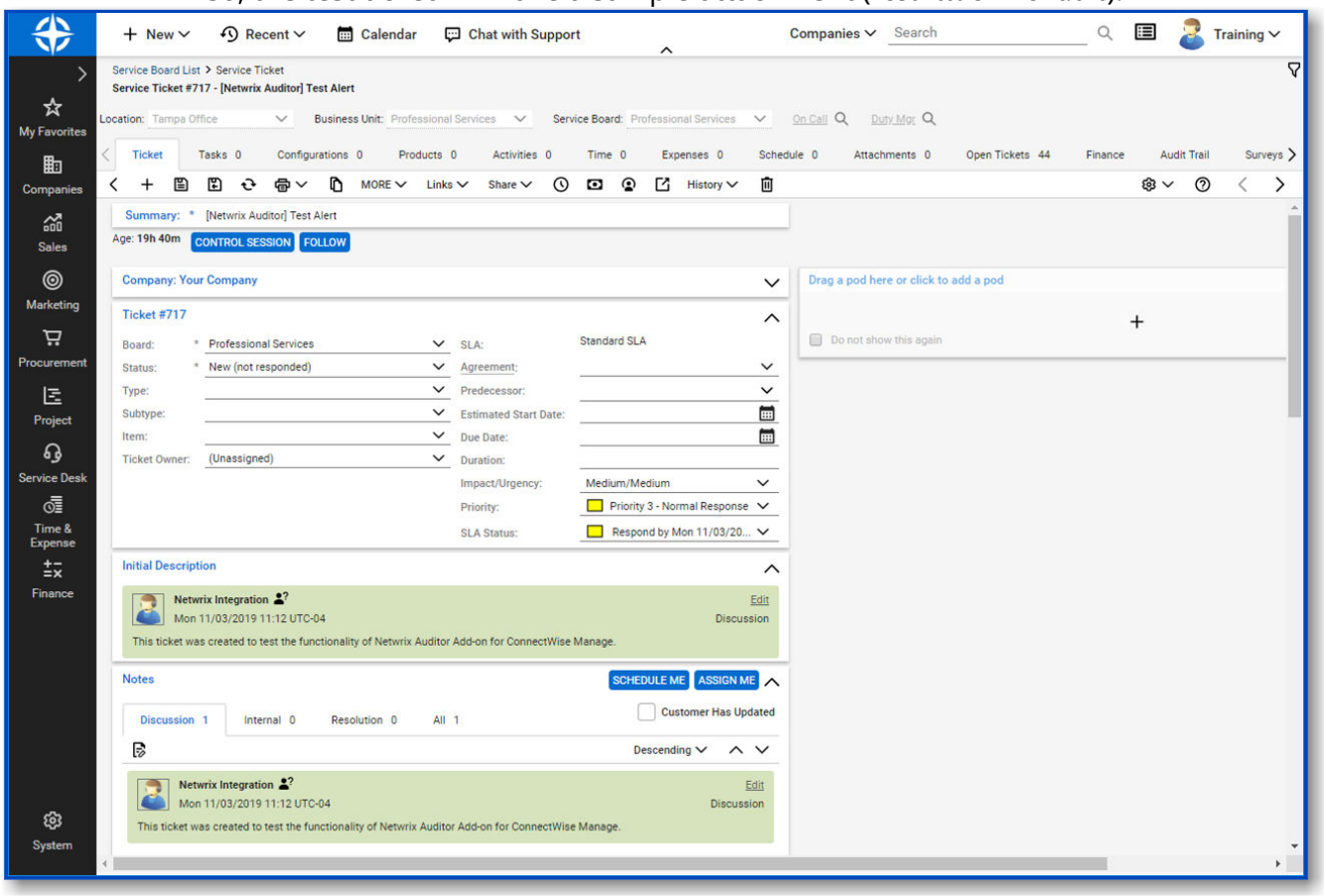


Parameter	Description
Title	Specify how the Title field of the service ticket will be filled in. Default: [Netwrix Auditor] %AlertName% That is, the Title field for tickets originating from Netwrix alerts will include the alert name with

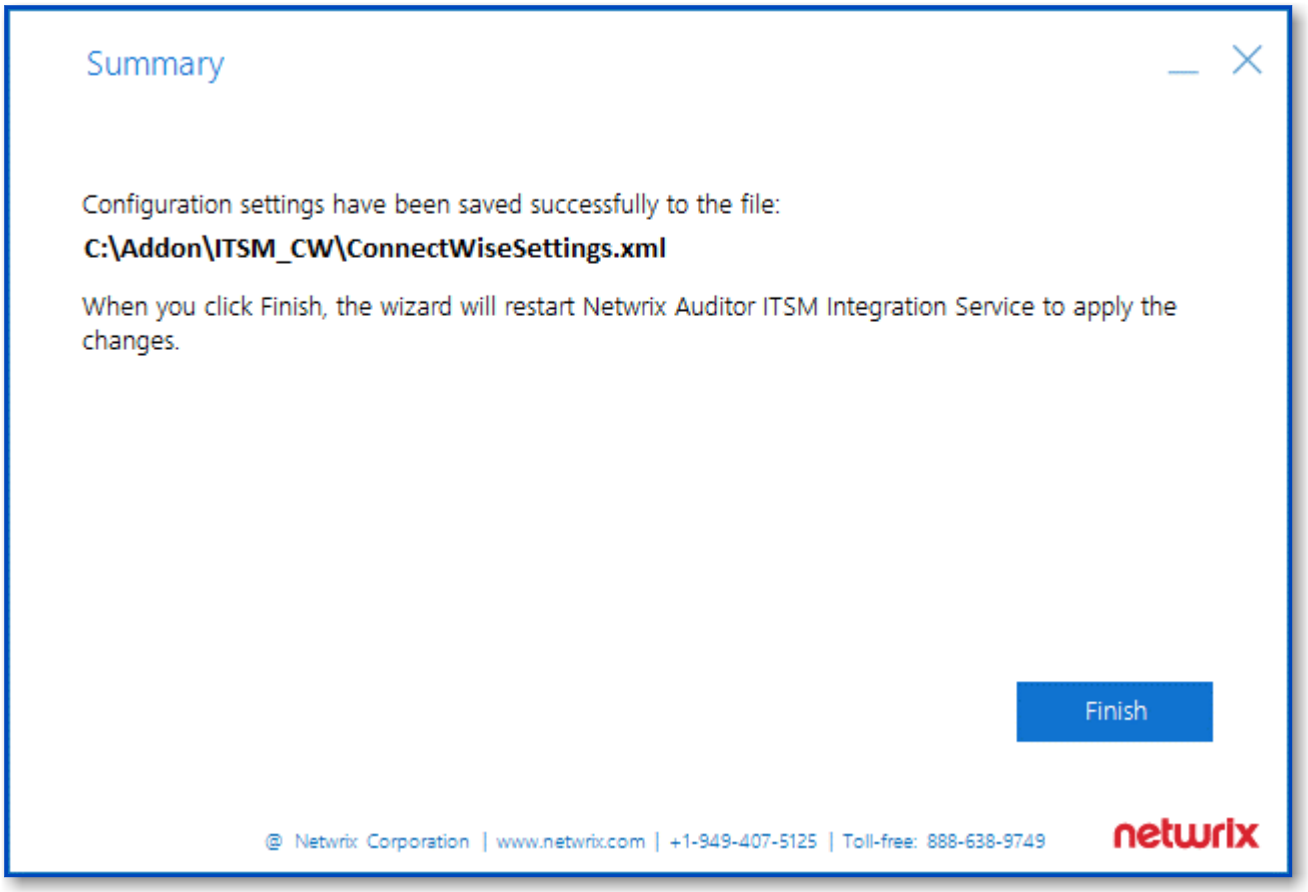
Parameter	Description
	[Netwrix Auditor] prefix (e.g., *[Netwrix Auditor] Password Reset)*.
Summary	Specify how the Summary field of the service ticket will be filled in. By default, it will contain the following detailed information received from the corresponding Auditor alert and activity record: Alert Details: Who: %Who% Action: %Action% Object type: %ObjectType% What: %What% When: %When% Where: %Where% Workstation: %Workstation% Details: %Details% Data source: %DataSource% Monitoring plan: %MonitoringPlanName% Item: %Item% Sent by Netwrix Auditor from %Computer%
Severity Level	Specify what severity level will be assigned to the service tickets. Default is Medium.

Parameter	Description
Business Impact	Specify what business impact level will be assigned to the service tickets. Default is Medium.

Optionally, you can click the Create Test Ticket button — then a test ticket will be created in ConnectWise Manage to help you verify the connection and ticketing settings you configured. Its Summary field will contain *[Netwrix Auditor] Test Alert*; its Initial Description field will contain *This ticket was created to test the functionality of Netwrix Auditor Add-on for ConnectWise Manage*. Also, the test ticket will have a sample attachment (*TestAttachment.txt*).



Step 5 – Finally, at the **Summary** step, review the location of configuration file with the settings you specified: *C:\Addon\ITSM_CW\ConnectWiseSettings.xml*.



If needed, you can edit the configuration file manually. See the Connection and Ticketing Settings topic for additional information.

Click **Finish** to restart the add-on service so that the changes can take effect.

Transferring Configuration

If necessary, you can use configuration file created with this wizard as a template for multiple managed clients. Perform the following steps:

Step 1 – Open the file path provided at the **Summary** step of the wizard.

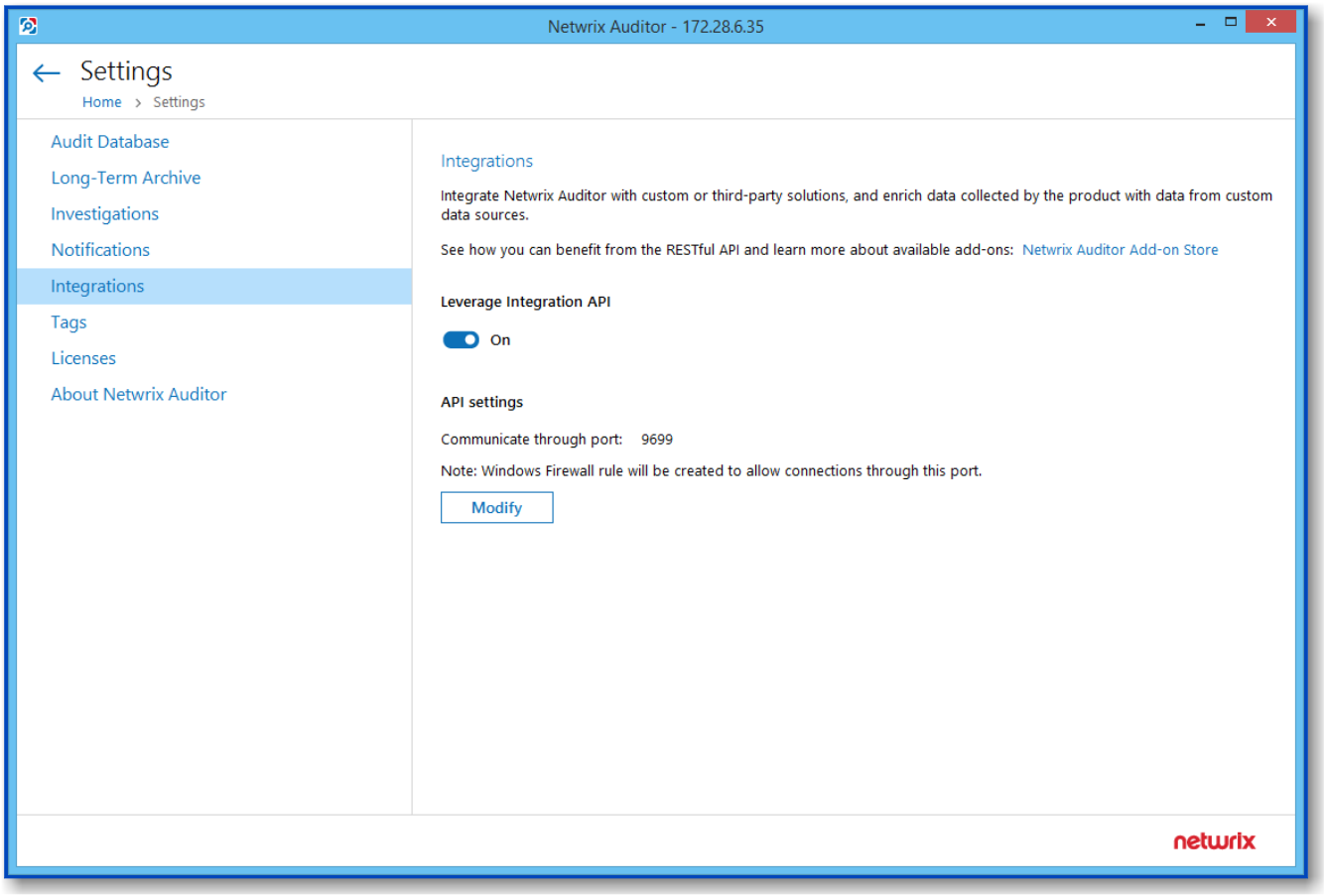
Step 2 – Locate the **ConnectWiseSettings.xml** file and copy it to the add-on folder on another client's server.

Step 3 – Then run ConfigureConnection.exe on that server to launch the configuration wizard and specify the necessary settings — for example, provide the managed client company name at the **Service Ticket Routing** step, and so on.

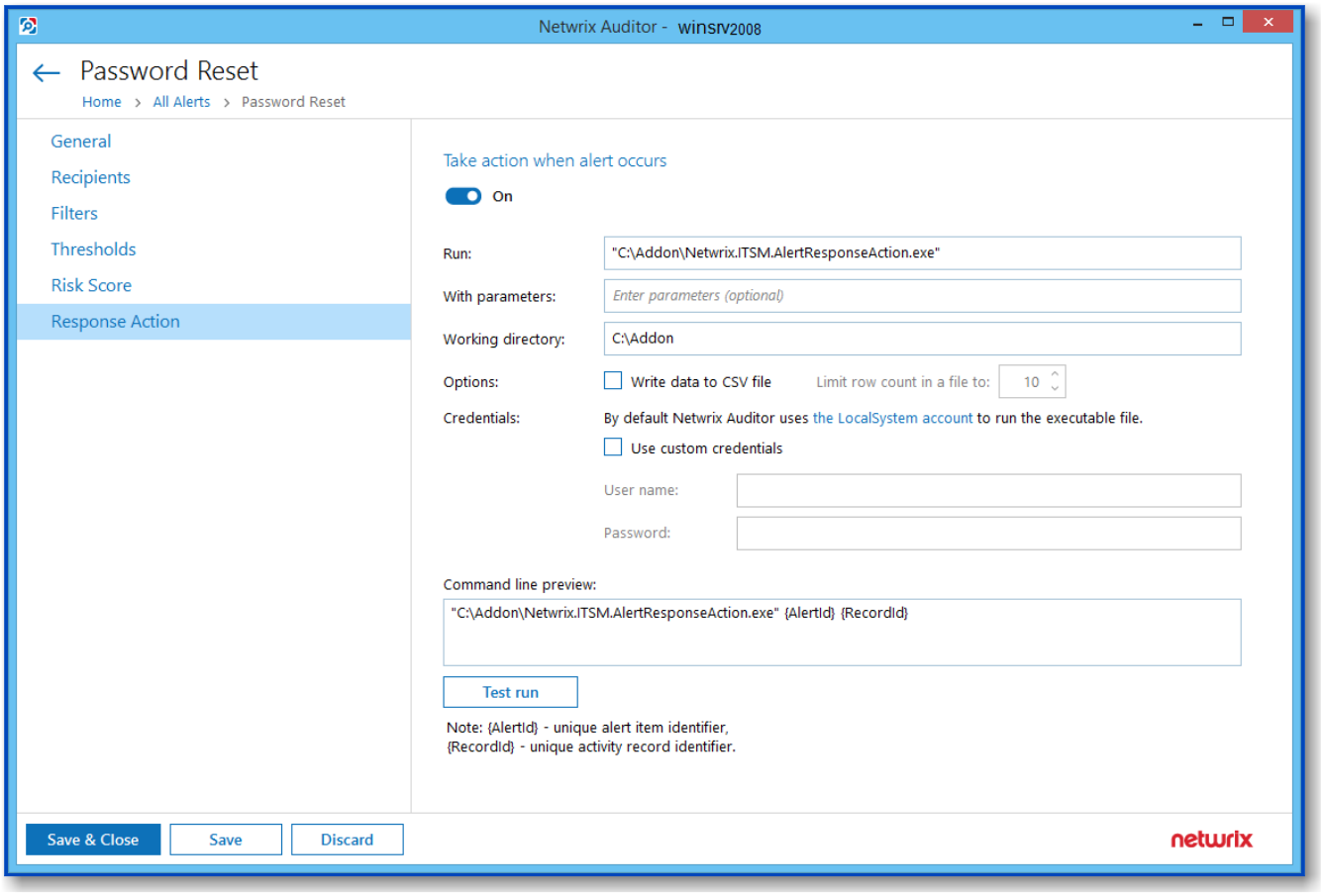
MSP Usage Example

Consider a situation when a password is reset for a user, computer, or **inetOrgPerson** account.

After deploying and configuring the add-on as described in this guide, the MSP (Managed Service Providers) staff member enabled Auditor integration feature:

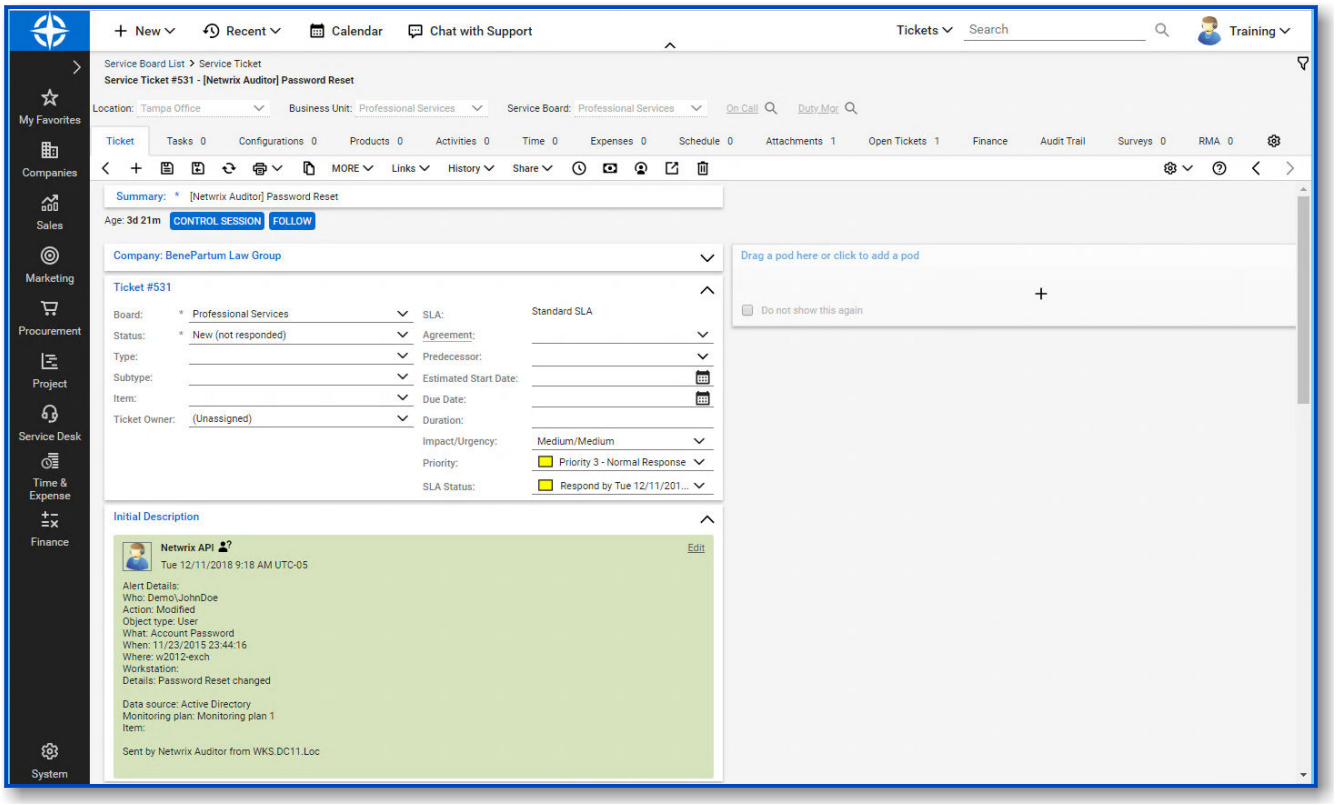


Also, she enabled the '**Password Reset**' alert from the Auditor predefined set of alerts and specified the add-on launch as response action.



Then a new ticket is automatically created shortly after any account password is reset.

All necessary details about the case are automatically entered into the ConnectWise ticket (*Initial Description* field), including the name of the workstation, the name of the account in question, and the time when the event occurred:



Connection and Ticketing Settings

It is recommended that you use configuration wizard to specify connection and ticketing settings. However, you can adjust them manually, using the information provided in this section.

Settings for ConnectWise Ticket Creation

Specify how data arriving from Auditor should be used to fill in ConnectWise ticket fields. For that, review `<TicketParameters>` section of the ConnectWiseSettings.xml file. The parameters inside this section correspond to ConnectWise ticket fields and use the same naming (e.g., priority, urgency).

Each `<TicketParameter>` includes the `<Name>↙Name>` and `<Value>↙Value>` pair that defines a ConnectWise ticket field and a value that will be assigned to it. For most parameters, default values are provided. Add more ticket parameters or update values if necessary.

<Name>	<Value>	Description
Summary	[Netwrix Auditor] %AlertName%	Instructs the system to fill in the Summary ticket field with the Auditor alert name (e.g., *[Netwrix Auditor] Password Reset)*.
InitialDescription	Alert Details: Who: %Who% Action: %Action% Object type: %ObjectType% What: %What% When: %When% Where: %Where% Workstation: %Workstation% Details: %Details% Data source: %DataSource% Monitoring plan: %MonitoringPlanName% Item: %Item% Sent by Netwrix Auditor from %Computer%	Instructs the system to fill in the InitialDescription ticket field with the Auditor activity record data. To read more about activity records, see the Reference for Creating Activity Records topic for additional information. You may need to fill in the internal description intended for use by MSP only (this description will not be visible to managed clients), perform the following steps: **Step 1 –** Run the configuration wizard (or modify *ConnectWiseSettings.xml*) to specify the settings you need. **Step 2 –** Then open *ConnectWiseSettings.xml* for edit. **Step 3 –** Locate the **InitialDescription** parameter and change the Name attribute to *initialInternalAnalysis*.
Impact/Urgency	Medium	Instructs the system to set ticket Impact/Urgency to *Medium*.

Parameters for Handling Related Tickets

Review the <CorrelationTicketFormat> section. It shows what information about related tickets will be included in your current ticket. Update the template if necessary.

CorrelationTicketFormat	Description
Previous incident for the same alert type: **Id: %id%**	The service will automatically substitute parameters from this section with values from a related ticket.

Parameters for Reopening Tickets

Review the <ReopenTicketOptions> section. It defines the tickets the add-on can reopen automatically.

Name	Description
ClosedTicketStates **TicketState**	Lists closed ticket statuses. By default, resolved, closed, and canceled tickets can be reopened. To specify a new status, provide its ID in the <TicketState> tag (e.g., 8 for canceled).
NewState	Defines a ticket status once it is reopened. By default, is set to *new*. To specify another status, provide its ID in the <NewState> tag (e.g., *1* for *new*).

When finished, save your changes to configuration file.

Remember to restart the add-on service every time you update any of configuration files.

Review Other Parameters

You can update other parameters with your own values if necessary; however, it is recommended that you contact Netwrixbefore modifying this section.

Name	Description
IgnoreUploadAttachmentError	Instructs the add on to ignore the attachment upload errors. • If false, a corresponding error message will be displayed. • If true, the file that failed to upload will be stored to the **MissingAttachments** subfolder in the add-on folder. Error message will not appear on the screen; instead, the following record will be written to the add-on log: *Attached files for ticket id: {0} dumped: '{attachmentPath}'* Default parameter value is **true**.

You can also review the `<TicketParameterRefs>` section. It shows information related to ConnectWise Manage objects.

Example:

```
<TicketParameterRefs>
 <TicketParameterRef>
  <Name>company</Name>
   <TicketParameters>
    <TicketParameter>
     <Name>id</Name>
     <!--My.Sample.Company-->
     <Value>42</Value> - enter ID of the company-ticket originator
    </TicketParameter>
```

```
    </TicketParameters>
  </TicketParameterRef>
  <TicketParameterRef>
    <Name>board</Name>
    <TicketParameters>
      <TicketParameter>
        <Name>id</Name>
        <!--Professional Services-->
        <Value>1</Value> - enter ID of the service board for the tickets
      </TicketParameter>
    </TicketParameters>
  </TicketParameterRef>
  <TicketParameterRef>
    <Name>priority</Name>
  <TicketParameters>
  <TicketParameter>
    <Name>id</Name>
    <!--Priority 3 - Normal Response-->
    <Value>4</Value>
  </TicketParameter>
</TicketParameters>
</TicketParameterRef>
<TicketParameterRef>
  <Name>team</Name>
  <TicketParameters>
```

```
    <TicketParameter>

     <Name>id</Name>

     <!--Service Team-->

     <Value>25</Value> - enter ID of the service team responsible for
     resolution

    </TicketParameter>

   </TicketParameters>

  </TicketParameterRef>

</TicketParameterRefs>
```

Operational Settings

This section describes how to configure settings of the main add-on component, Netwrix Auditor **ConnectWise Manage Integration Service**, required for its operation, including connection to Auditor Server, activity records processing, queuing and forwarding, ticket creation, and so on.

For that, follow the steps:

Step 1 – Navigate to the add-on folder and select ITSMSettings.xml.

Step 2 – Define operational parameters such as Auditor connection settings, the number of tickets the service can create per hour, ability to reopen closed tickets, etc. For most parameters, default values are provided. You can adjust them depending on your execution scenario and security policies. Use the following format: `<parameter>value<parameter>`.

Parameter	Default value	Description
NetwrixAuditorHost	https://localhost:9699	The add-on runs on the computer where Auditor Server resides and uses the default Integration API port (TCP port **9699**). To specify a non-default port, provide a new port number (e.g., *https://localhost:8788*).

Parameter	Default value	Description
		The add-on must always run locally, on the computer where Auditor Server resides.
NetwrixAuditorUserName	—	Unless specified, the Netwrix Auditor **ConnectWise Manage Integration Service** runs under the LocalSystem account. If you want this service to use another account to connect to Auditor Server, specify the account name in the *DOMAIN\username* format in this parameter value. The user account for running the service and connecting to Auditor Server must be granted the Global administrator role in Auditor or be a member of the Netwrix Auditor **Administrators** group. It must also have sufficient permissions to create files on the local computer.
NetwrixAuditorPassword	—	Provide a password for the account. Unless an account is specified, the service runs under the LocalSystem account and does not require a password.
TicketFloodLimit	10	Specify the maximum number of standalone tickets the service can create during TicketFloodInterval. If a ticket flood limit is reached, the service writes all new alerts into a single ticket.

Parameter	Default value	Description
TicketFloodInterval	3600	Specify the time period, in seconds. During this time period, the service can create as many tickets as specified in TicketFloodLimit. The default value is 3600 seconds, i.e., 1 hour.
ConsolidationInterval	900	Specify the time period, in seconds. During this time period, the service does not process similar alerts as they happen but consolidates them before updating open tickets. The default values is 900 seconds, i.e., 15 minutes. This option works in combination with UpdateTicketOnRepetitiveAlertsand is helpful if you want to reduce the number of ticket updates on ConnectWise Manage side. I.e., this option defines the maximum delay for processing alerts and updating existing tickets. Tickets for new alert types are created immediately. For example, a new alert is triggered —the service opens a new ticket. The alert keeps firing 20 times more within 10 minutes. Instead of updating the ticket every time, the service consolidates alerts for 15 minutes, and then updates a ticket just once with all collected data.
CheckAlertQueueInterval	5	Internal parameter. Check and process the alert queue every N seconds; in seconds.

Parameter	Default value	Description
UpdateTicketOnRepetitiveAlerts	true	Instead of creating a new ticket, update an existing active ticket if a similar alert occurs within UpdateInterval. To open a new ticket for every alert, set the parameter to *"false"*.
ReopenTicketOnRepetitiveAlerts	true	Instead of creating a new ticket, reopen an existing ticket that is in a closed state (be default, closed, canceled, and resolved) if a similar alert occurs within UpdateInterval. This option works only when UpdateTicketOnRepetitiveAlerts is set to *"true"*. If you want to reopen closed tickets, you must be granted the right to perform Write operations on inactive tickets.
UpdateInterval	86400	Specify the time period, in seconds. If a similar alert occurs in less than N seconds, it is treated as a part of an existing ticket. The default value is 86400 seconds, i.e., 24 hours. If an alerts is triggered after the UpdateInterval is over, a new ticket is created.
EnableTicketCorrelation	true	Review history and complement new tickets with information about similar tickets created previously.

Parameter	Default value	Description
		This information is written to the Description field. This option is helpful if you want to see if there is any correlation between past tickets (from the last month, by default) and a current ticket.
CorrelationInterval	2592000	Specify the time period, in seconds. During this time period, the service treats similar tickets as related and complements a new ticket with data from a previous ticket. The default value is 2592000 seconds, i.e., 1 month. Information on alerts that are older than 1 month is removed from internal service storage.
ProcessActivityRecordQueueInterval	5	Internal parameter. Process activity record queue every N seconds; in seconds.
DisplayOnlyFirstActivityRecord	true	Add only the first activity record in the work notes, activity records that update this ticket will be added as attachments to this ticket. If false, all activity records will be displayed in the ticket work notes.
ActivityRecordRequestsRetention		
RequestLimit	5000	Internal parameter. The maximum number of activity record requests

Parameter	Default value	Description
		the service can store in its internal memory. Once the limit is reached, the service clears activity record requests starting with older ones.
RequestLimitInterval	604800	Internal parameter. The service can store the activity record requests not older than N seconds; in seconds. Older activity record requests are cleared.
ActivityRecordWebRequests		
RequestLimit	200	Internal parameter. The maximum number of activity records the service can retrieve in a single request.
RequestTimeout	180	Internal parameter. By default, 3 minutes. Defines the connection timeout.
TicketRequestsRetention		
RequestLimit	300000	Internal parameter. The maximum number of ticket requests the service can store in its internal memory. Once the limit is reached, the service clears ticket requests starting with older ones.
RequestLimitInterval	604800	Internal parameter. The service can store the ticket requests not older

Parameter	Default value	Description
		than N seconds; in seconds. Older tickets requests are cleared.

Step 3 – Restart the service every time you update ITSMSettings.xml configuration file.

Ctera

The add-on works in collaboration with Netwrix Auditor, supplying data about activity on your Ctera-based devices. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a service, this add-on facilitates the data transition from Ctera-based systems to Netwrix Auditor. All you have to do is provide connect ion details and specify parsing rules.

On a high level, the add-on works as follows:

1. The add-on listens to the specified UDP ports and captures designated Syslog messages.
2. The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.
3. Using the Integration API, the add-on sends the activity records to the Netwrix Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the NIntegration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor Server side	• The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP **9699** port (default Integration API port) is open for inbound connections. • The user writing data to the Audit Database is granted the **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.
The computer where the add-on will be installed	• The UDP 514 port is open for inbound connections. • .Net Framework 4.7.2 and above is installed. Review the following Microsoft technical article for additional information on how to install .Net Framework 4.7.2: Microsoft .NET Framework 4.7.2 offline installer for Windows.

Configure Logging for CTERA Edge Filer

Prior to start using the Add-On, configure syslog logging settings on your CTERA Edge Filers. See the Configuring Syslog Settings article on the CTERA product documentation portal for detailed instructions.

Accounts and Rights

By default, the add-on will run under the *Local System* account. The add-on and Auditor must be installed on the same server.

Considerations and Limitations

- The Add-On must be deployed in the same subnet as CTERA Edge Filer and Auditor.
- If the monitoring plan name in the <*NetwrixAuditorPlan*> add-on configuration parameter is specified incorrectly, this may lead to temp files generation and, therefore, to inefficient disk space usage.
- If you are using Netwrix Auditor for Network Devices, the 514 UDP port may be already in use, and you should specify another port when configuring the add-on settings (see the Install Add-On and Define Parameters topics for additional information). Another option is to install the add-on and Auditor Server on different machines.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Install Add-On

Follow the steps to install the Add-On:

Step 1 – Navigate to your add-on package.

Step 2 – Unzip the Add-On to a desired folder.

Step 3 – Run the installation package.

Step 4 – Accept the license agreement and follow the instructions of the setup wizard.

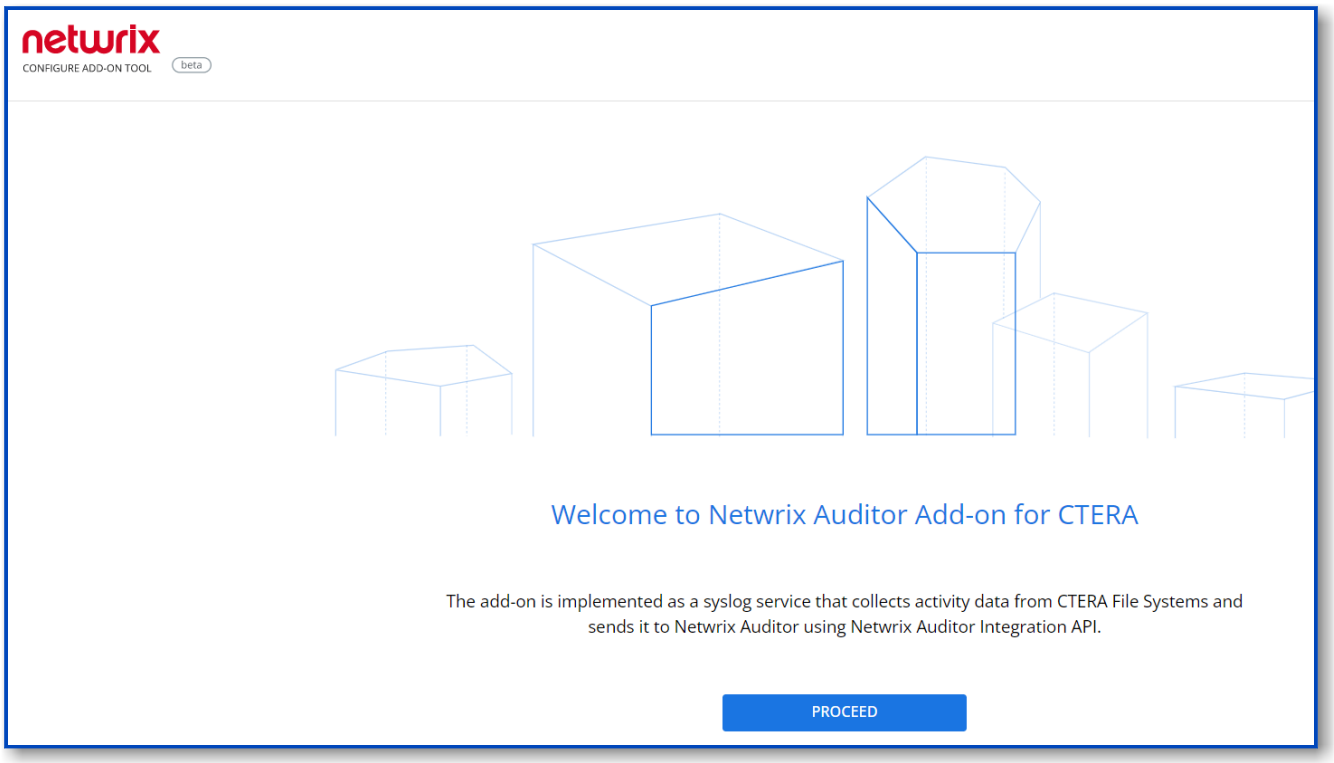
Step 5 – On the **Destination Folder** step, specify the installation folder (*C:\Program Files (x86)\Netwrix Add-ons\<Add-on name>* by default).

Step 6 – Click **Install**.

Step 7 – When done, click **Finish**.

Define Parameters

The configuration wizard opens in the default web browser:



Click **Proceed** and complete the following fields:

Option	Description
Specify General Settings	
Listed UDP port	Specify UDP port for listening incoming events. (**514** by default).
Auditor Endpoint	Auditor Server IP address and port number followed by endpoint for posting Activity Records.

Option	Description
	Assumes that the add-on runs on the computer hostingAuditor Server and uses default port *9699*. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15*, *EnterpriseNAServer*, *WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). **NOTE:** Do not modify the endpoint part (*/netwrix/api*)
Certificate Thumbprint	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Auditor certificate via Windows Certificate Store. • `AB:BB:CC`—Check Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
Specify Active Directory credentials	
Username	Provide the name of the account under which the service runs. Unless specified, the service runs under the account currently logged on.
Password	Provide the password for the selected account.
Auditor Monitoring Plan settings	

Option	Description
Auditor Plan	Unless specified, data is written to **Netwrix_Auditor_API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add- on, make sure a dedicated plan is created in Auditor, the Netwrix **API** data source is added to the plan and enabled for monitoring. Otherwise, the add- on will not be able to write data to the Audit Database.
Auditor Plan Item	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. **NOTE:** Make sure to create a dedicated item inAuditor in advance.
Accept List	
Address	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only. **NOTE:** Events collected from any other source will be ignored.

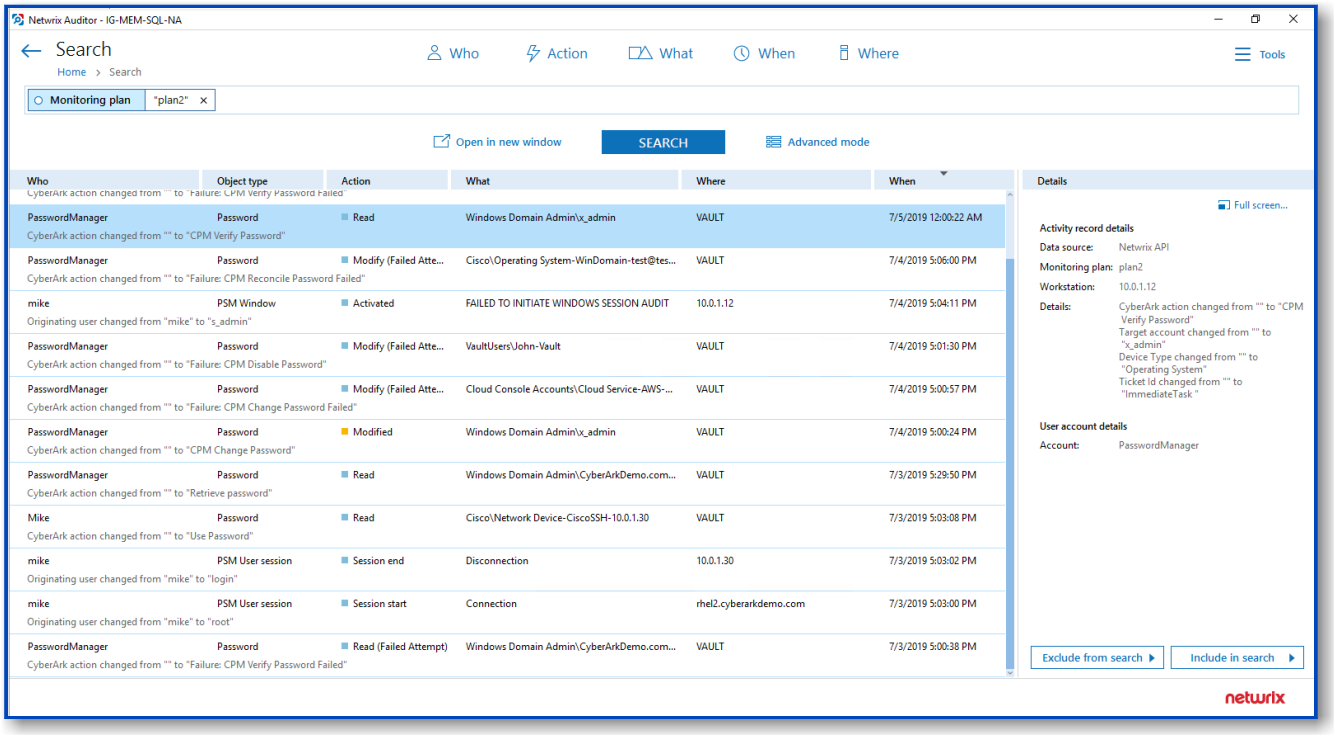
Click **Run** to start collecting data with the Add-On.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You can apply a filter to narrow down your search results to the Netwrix **API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:

  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.

  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See the following topics for additional information:

- Alerts
- View and Search Collected Data
- Subscriptions

CyberArk Privileged Access Security

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.

CyberArk offers its Privileged Access Security (PAS) solution for managing the privileged accounts and SSH Keys. It enables organizations to manage and monitor all activities associated with the privileged identities, for example, Windows server administrator, root on a UNIX server, etc. A featured set of the Privileged Access Security tools includes, in particular:

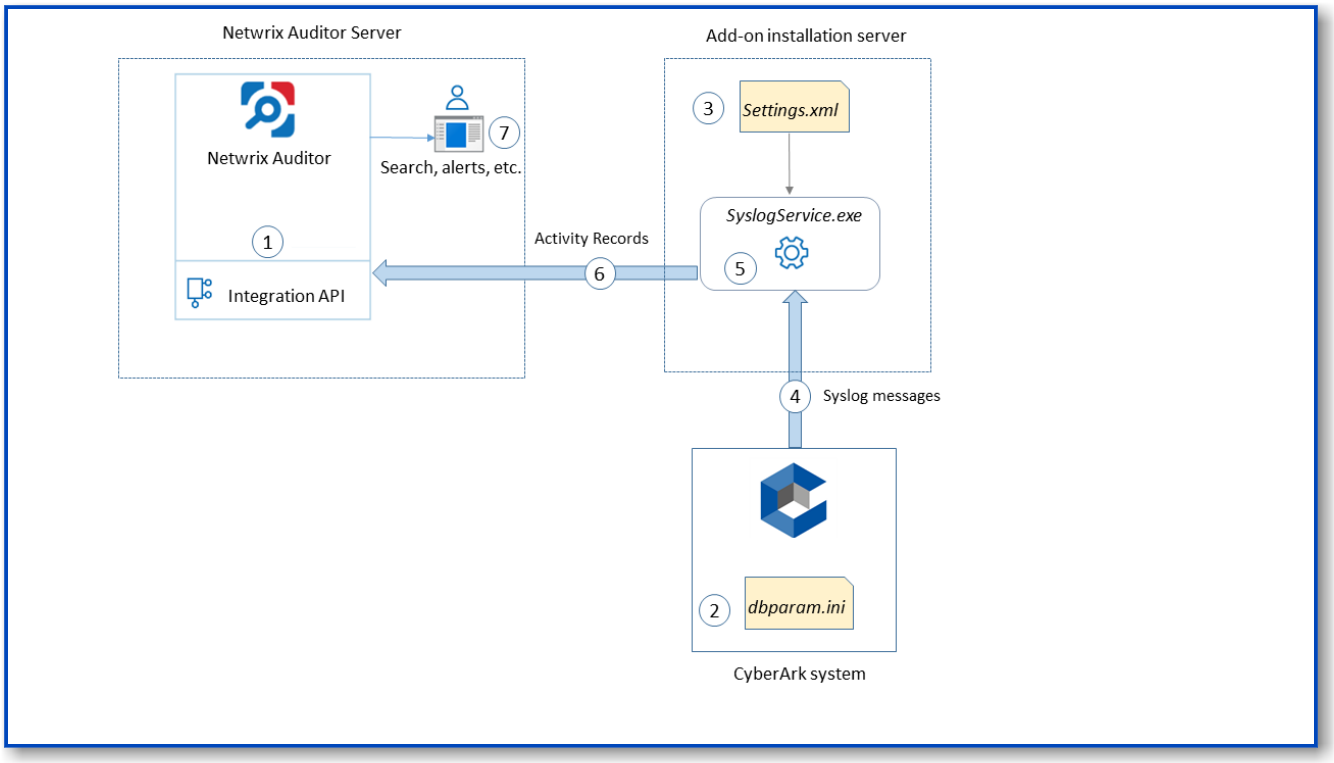
- **Privileged Session Manager** - a tool that enables users to securely connect to remote targets with a standard remote desktop client application, providing isolated sessions.
- **Enterprise Password Vault** – a tool for storage and centralized management of the privileged accounts; it supports automated changes and logging of the activities associated with all types of privileged passwords and SSH Keys. This tool also includes Central Policy Manager service.

Major benefit of the integrated solution implemented with the Add-On is the increased visibility into actions related to CyberArk tools, in particular:

- Visibility into the user account behind the respective isolated session controlled by Privileged Session Manager
- Visibility into the password-related activities, e.g. password retrieval and further actions made to target application or system, and automatic password update for managed accounts in Enterprise Password Vault and Central Policy Manager.

How It Works

The add-on is implemented as a syslog service that collects activity data from CyberArk system (PAS) and sends it to Auditor using the Integration API.



The add-on operates as a syslog listener for the CyberArk system. On a high level, the solution works as follows:

1. An IT administrator configures Integration API settings to enable data collection and storage to the Audit Databasefor further reporting, search, etc.

   It is recommended to create a dedicated monitoring plan in Auditor and add a dedicated item of **Integration** type to it — then you will be able to filter data in reports and search results by monitoring plan/item name.

2. On the CyberArk server, the administrator opens the **dbparam.ini** file and specifies the parameters for syslog message forwarding, including add-on installation server settings, the IDs of events to be monitored, etc.

   See the Monitored Events topic for additional information on the events supported for monitoring out of the box.

3. On the add-on installation server, the administrator runs the installation file and configures the Add-On parameters in the configuration wizard.
4. The add-on starts collecting and forwarding activity data: it listens to the specified UDP port and captures designated syslog messages (CyberArk events).

5. The add-on processes these events into Auditor-compatible format – activity records. Each activity record contains the *Who-What-When-Where-Action* information (that is, user account, time, action, and other details).

6. Using the Integration API, the add-on sends the activity records to Auditor Server that writes them to the Audit Database and Long-Term Archive. Data is sent periodically, by default every 5 seconds.

   See the Integration API topic for additional information on the structure of the activity record and the capabilities of the Integration API.

7. Users open Auditor Client to work with collected data:
   - Search for file changes using certain criteria
   - Export data to PDF or CSV files
   - Save search results as reports
   - Subscribe to search results
   - Configure and receive alerts

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

Where	Prerequisite to check
The Auditor Server side	• The Integration API and Audit Database settings are configured in Auditor Server settings. See the Prerequisites and Audit Database topics for additional information. • The **TCP 9699** port must be open on Windows firewall for inbound connections. • User account under which data will be written to the Audit Database requires the **Contributor** role in Auditor. See the Role-Based Access and Delegation for additional information. Alternatively, you can grant it the **Global administrator** role, or add that account to the **NETWRIX AUDITOR Administrators** group.
The machine where the Add-On will be installed (Auditor Server is recommended)	• The **UDP 514** port must be open on Windows firewall for inbound connections.

Where	Prerequisite to check
	If you are using Netwrix Auditor for Network Devices, this port may be already in use, and you should provide another one. Another option is to install the add-on and Auditor Server on different machines. • .Net Framework 4.7.2 and above is installed. Review the following Microsoft technical article for additional information on how to install .Net Framework 4.7.2: Microsoft .NET Framework 4.7.2 offline installer for Windows.
CyperArk PAS	Version 10.10.

Accounts and Rights

By default, the add-on will run under the *Local System* account. So, if the add-on and Auditor will be running on different machines, the corresponding computer account will require at least the **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information.

In case the add-on and Auditor are installed on the same server, no special settings are needed.

Considerations and Limitations

- The Add-On must be deployed in the same subnet as CyberArk PAS and Auditor.
- If the monitoring plan name in the <*NetwrixAuditorPlan*> add-on configuration parameter is specified incorrectly, this may lead to temp files generation and, therefore, to inefficient disk space usage.
- If you are using Netwrix Auditor for Network Devices, the 514 UDP port may be already in use, and you should specify another port when configuring the add-on settings (see Deploy the Add-On and Add-On Parameters topics for additional information). Another option is to install the add-on and Auditor Server on different machines.

Compatibility Notice

Netwrix Auditor add-on for CyberArk is compatible with CyberArk Privileged Access Security (PAS) 10.10 and with Netwrix Auditor 9.8 and later.

Add-On Parameters

To configure the add-on parameters, you need to edit the **Settings.xml** file in the add-on folder. You must define connection details: Auditor Server host, endpoint, etc.

Most parameters are optional; you can skip or define parameters depending on your execution scenario and security policies.

The service uses the default values unless parameters are explicitly defined (<*parameter*>**value**</*parameter*>).

Parameters in **Settings.xml** can be grouped as follows:

- **General parameters** that affect add- on execution. They are listed in the table below.
- Settings for a certain event source (within the *Source* section) that can override general settings.
- **Internal parameters** that should not be modified in most cases. They are listed in the topic.

Parameter	Default value	Description
General parameters		
ListenUdpPort	514	Specify UDP port for listening to the incoming syslog events.
NetwrixAuditorEndpoint	https://localhost:9699/netwrix/api/v1/activity_records	Auditor Server IP address and port number followed by endpoint for posting Activity Records.

Parameter	Default value	Description
		Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15, EnterpriseNAServer, WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). Do not modify the endpoint part (/ netwrix/api . . . .)
NetwrixAuditorCertificateThumbprint	NOCHECK	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check the certificate via Windows Certificate Store. • `AB:BB:CC.`—Check the certificate thumbprint identifier. • `NOCHECK`—Do not check the certificate. Make sure to select this parameter if you plan to specify servers by their IP.
NetwrixAuditorPlan	—	Unless specified, data is written to Netwrix_Auditor_API database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this

Parameter	Default value	Description
		case, data will be written to a database linked to this plan. If you select a plan name in the add-on, make sure a dedicated plan is created in Auditor, the Netwrix API data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
NetwrixAuditorPlanItem	—	Unless specified, data is not associated with a specific monitoring plan and thus cannot be filtered by item name. Specify an item name here. Make sure to create a dedicated item in Auditor in advance.
EventStorePath	—	Select where to store temporary files of syslog messages before the add-on sends them to Auditor Server. Netwrix recommends to store these files in the same directory with the add-on (SyslogService.exe).
LogLevel	warning	Specify logging level: • none • info • warning (used by default) • error • debug

Parameter	Default value	Description
WriteCriticalIssues ToEventLog	0	Instructs the add-on to write important events (like service start or critical issue) not only to its own log but also to Netwrix event log. • 1=yes • 0=no (default)
Parameters within SourceList **You can specify parsing rules for each specific event source and define parameters to override general settings, such as time zone, default plan name, etc.**		
NetwrixAuditorPlan	—	When specified, overrides the general settings.
NetwrixAuditorPlanItem	—	When specified, overrides the general settings.
AppNameRegExp	—	Custom regular expression pattern that will be used to retrieve the application name from your syslog messages. The add-on will match the application name and the files with syslog parsing rules to be applied. The pattern you provide here must match the application name in your custom rule file. Unless specified, RFC 3164/5424 format is used.

Parameter	Default value	Description
AppNameGroupID	—	Define application name value by Group ID only if messages are not formatted in accordance with RFC 3164/5424. Otherwise, leave the default value.
RuleFileList **PathFile**	cyberark-v2.xml	Specify paths to XML file(s) with regular expression parsing rules. You can create a custom file or use rules provided out of the box. Currently, the **cyberark-v2.xml** rule file is shipped with this add-on. You can specify several rule files. The service will check if the AppName parameter in the first rule file matches the AppNameRegExp and AppNameGroupID regular expression in this file. If not, the service will proceed to the next rule file.
AcceptList **Address**	—	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only. Events collected from any other source will be ignored. The *Address* parameter may be followed by optional attributes that override parameters specified above: • *naplan*—A name of associated monitoring plan

Parameter	Default value	Description
		• *naplanitem*—A name of associated item For example: <Address naplan="NFSmonitoring" naplanitem="NFS">172.28.3.15 ↙Address>

Remember to save **Settings.xml** after editing is complete.

After you modify parameters in the **Settings.xml** file, remember to save the changes and then restart the add-on main service (*SyslogService.exe*) for them to take effect.

Add-on Internal Parameters

Internal parameters listed in the table below are intended for performance tuning. In most cases the default values should be used.

Parameter	Default value	Description
EventsFromMemoryFirst	1	Instructs the add-on to save events to temporary storage only if there is no free space in queues: • 1=yes • 0=no
ConcurrentSend	-1	Specifies the number of threads for concurrent forwarding of events to Auditor. Default value is -1 (switch off concurrent forwarding).

Parameter	Default value	Description
SenderSleepTime	30	Specifies the retry interval in seconds to send messages to Auditor (30 - 3600 seconds).
TaskLimit	8	Specifies the number of threads and queues for concurrent handling of events.
QueueSizeLimit	100	Specifies the maximum number of events to keep in queue before saving to temporary storage or sending to Netwrix API.
QueueTimeLimit	5	Specifies the length of timeout before events from queue (not full) are saved to temporary storage or sent to Netwrix API: • From 5 to 300 – timeout in seconds. • -1 – disable timeout.

Deploy the Add-On

Follow the steps to deploy the Add-On:

Step 1 – Prepare Auditorfor data processing.

Step 2 – Configure Syslog message forwarding in CyberArk.

Step 3 – Download the Add-On.

Step 4 – Install Add-on.

Step 5 – Configure Add-on parameters

Prepare Auditor for Data Processing

In Auditor client, go to the Integrations section and verify Integration API settings:

1. Make sure the **Leverage Integration API** is switched to **ON**.
2. Check the TCP communication port number – default is **9699**.

See the Prerequisites topic for additional information.

By default, activity records are written to *Netwrix_Auditor_API* database which is not associated with a specific monitoring plan.

Optionally, you can create a dedicated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. Target it at Netwrix API data source and enable for monitoring. Add a dedicated item of *Integration* type to the plan for data to be filtered by item name. See the Integration API topic for additional information.

In such scenario, you will need to specify this monitoring plan in the *naplan* and *naplanitem* attributes of the <*AcceptList*> ® <*Address*> configuration parameters. See the Add-On Parameters topic for additional information.

Configure Syslog Message Forwarding in CyberArk

On the CyberArk side, you need to specify the server that will receive Syslog messages from CyberArk, process them and forward to Auditor Server. This will be the add-on installation server (the machine where *SyslogService.exe* runs).

Follow the steps to configure Syslog message forwarding in CyberArk.

Step 1 – Log in to your CyberArk system.

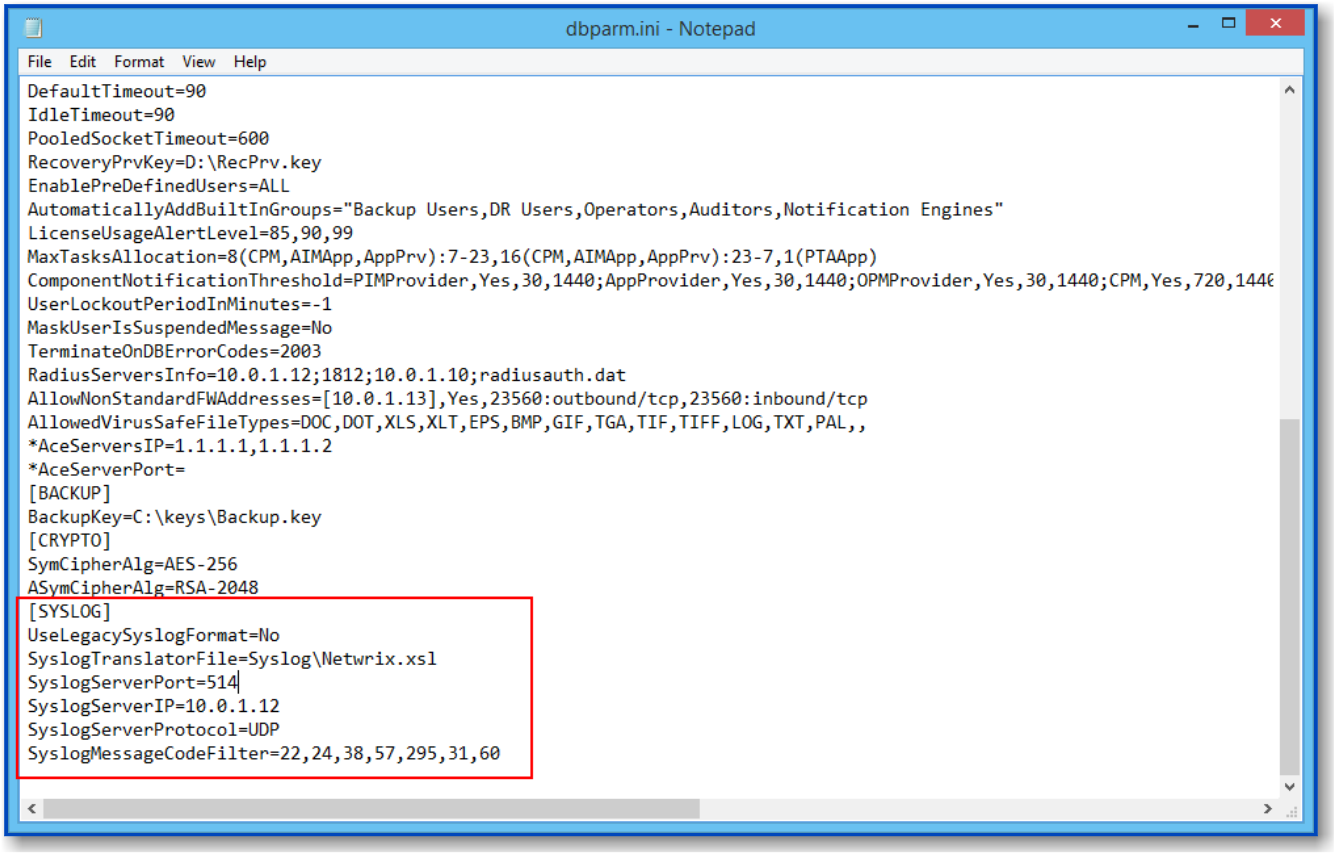
Step 2 – On the CyberArk server, locate the *%Program Files (x86)%\PrivateArk\Server\Conf* folder and open the **dbparam.ini** file for editing.

Step 3 – Go to the **[SYSLOG]** section and configure the following parameters:

- **SyslogTranslatorFile** – relative path to **Netwrix.xsl** file. You will need to create this file manually and copy the content of **SyslogTranslator.sample.xsl** file into it. This sample file

is provided by CyberArk. By default, it is located in the *%Program Files (x86) %\PrivateArk\Server\Syslog* folder. Place the *Netwrix.xsl* file there, too, so that default relative path should be *\Server\Syslog*.

- **SyslogServerPort** – communication port of the syslog server (i.e. add-on installation server). Default is **514**. Note that if you are using Netwrix Auditor for Network Devices, this port may be already in use, and you should provide another one.
- **SyslogServerIP** - IP address of the add-on installation server.
- SyslogServerProtocol – communication protocol for data transfer between CyberArk system and the add-on. Specify **UDP** protocol.
- **SyslogMessageCodeFilter** - IDs of events to forward. The add-on will only collect and process events you specify in this parameter. For the full list of supported events, see Monitored Events. Use comma as a separator.



Step 4 – Save the **dbparam.ini** file.

Download the Add-On

Step 1 – Download the distribution package **Netwrix_Auditor_Add-on_for_CyberArk_PAS.zip**.

Step 2 – Unpack it to a folder on the computer where you plan to deploy the add-on.

Remember, deploy the add-on on the same machine with the *Auditor* Server.

Install Add-On

Follow the steps to install the Add-On:

Step 3 – Navigate to your add-on package.

Step 4 – Unzip the Add-On to a desired folder.

Step 5 – Run the installation package.

Step 6 – Accept the license agreement and follow the instructions of the setup wizard.

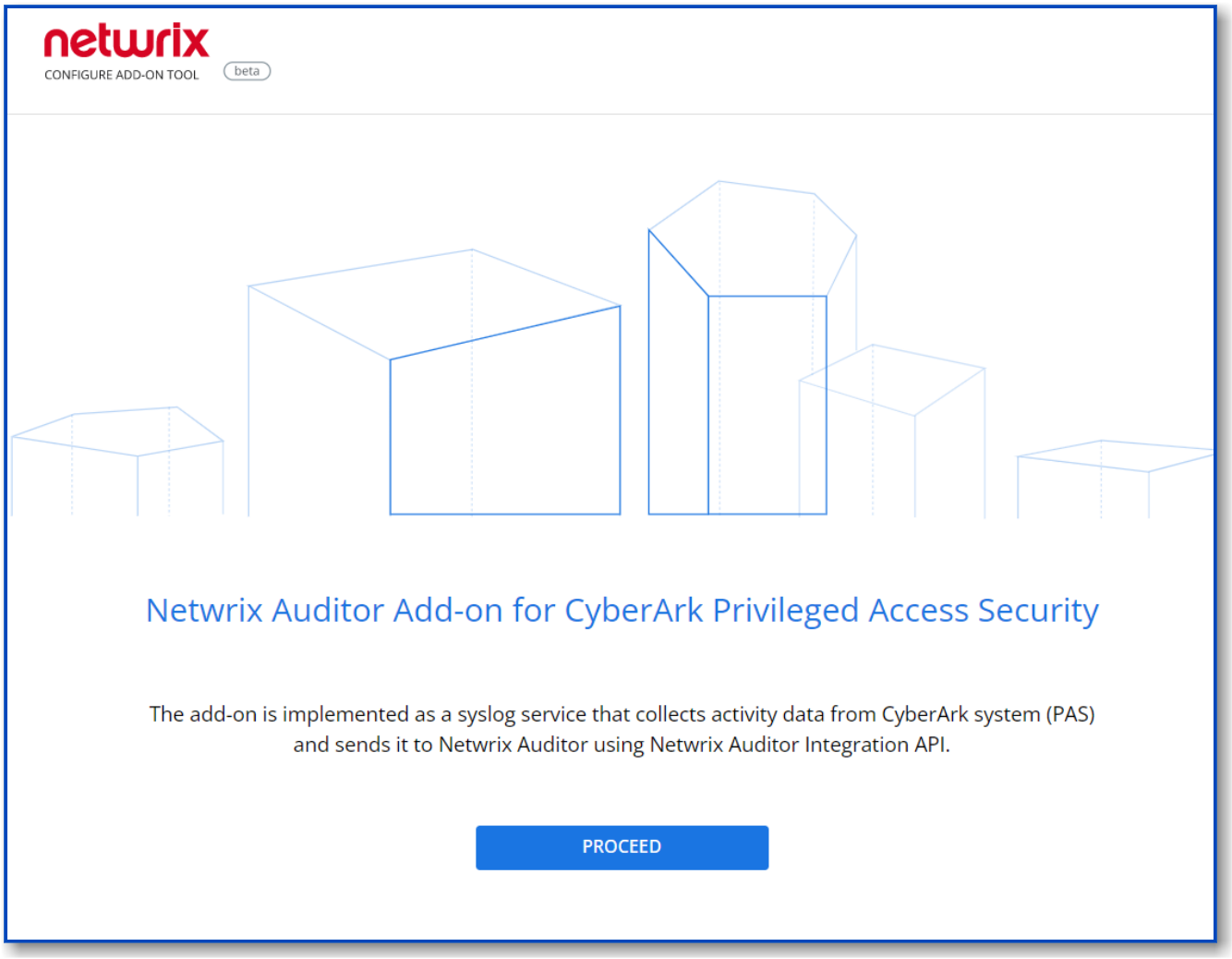
Step 7 – On the **Destination Folder** step, specify the installation folder (*C:\Program Files (x86)\Netwrix Add-ons\<Add-on name>* by default).

Step 8 – Click **Install**.

Step 9 – When done, click **Finish**.

Configure Add-on Parameters

The configuration wizard opens in the default web browser:



Click **Proceed** and complete the following fields:

Option	Description
Specify General Settings	
Listed UDP port	Specify UDP port for listening incoming events. (**514** by default).
Auditor Endpoint	Auditor Server IP address and port number followed by endpoint for posting Activity Records.

Option	Description
	Assumes that the add-on runs on the computer hostingAuditor Server and uses default port *9699*. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15*, *EnterpriseNAServer*, *WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). **NOTE:** Do not modify the endpoint part (*/netwrix/api*)
Certificate Thumbprint	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Auditor certificate via Windows Certificate Store. • `AB:BB:CC`—Check Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
Specify Active Directory credentials	
Username	Provide the name of the account under which the service runs. Unless specified, the service runs under the account currently logged on.
Password	Provide the password for the selected account.
Auditor Monitoring Plan settings	

Option	Description
Auditor Plan	Unless specified, data is written to **Netwrix_Auditor_API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add- on, make sure a dedicated plan is created in Auditor, the Netwrix **API** data source is added to the plan and enabled for monitoring. Otherwise, the add- on will not be able to write data to the Audit Database.
Auditor Plan Item	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. **NOTE:** Make sure to create a dedicated item inAuditor in advance.
Accept List	
Address	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only. **NOTE:** Events collected from any other source will be ignored.

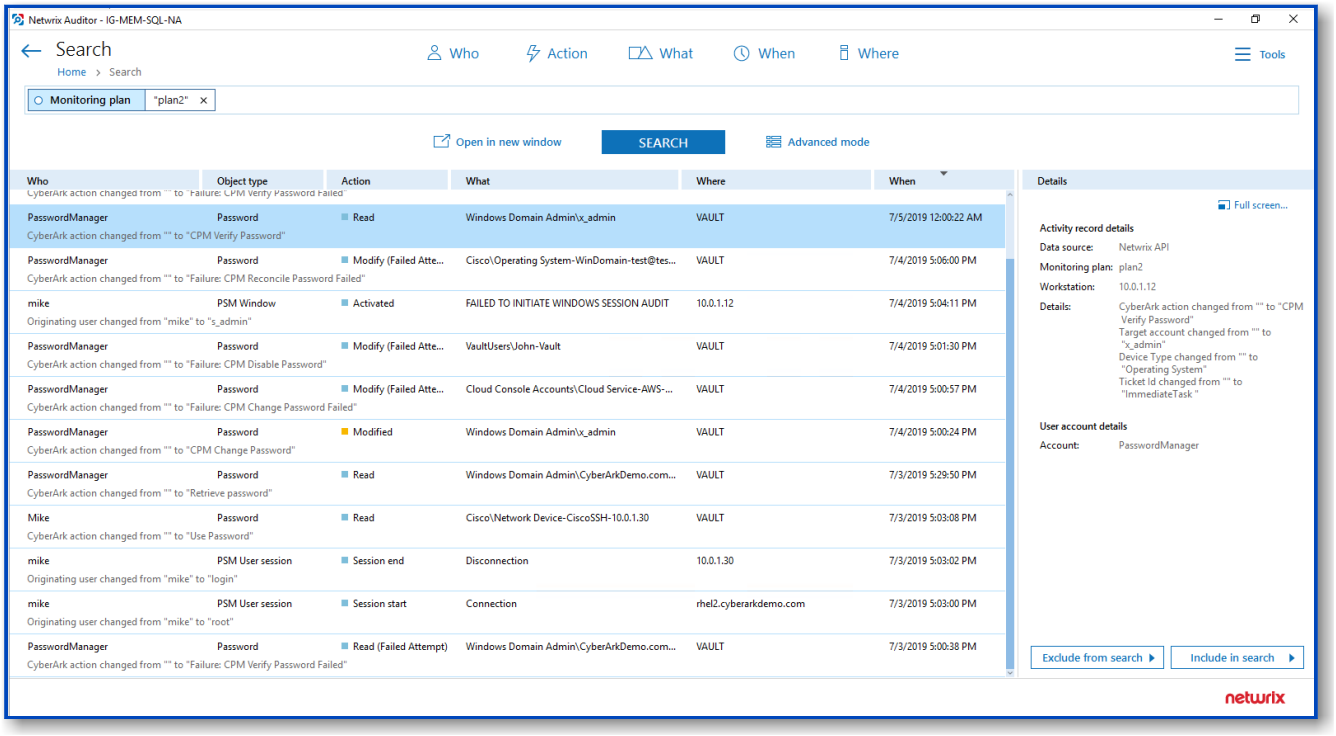
Click **Run** to start collecting data with the Add-On.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You can apply a filter to narrow down your search results to the Netwrix **API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:

  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.

  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See the following topics for additional information:

- Alerts
- View and Search Collected Data
- Subscriptions

Monitored Events

The Add-On supports monitoring of the following syslog events from CyberArk PAS:

Event ID	Description
22	Password verification by Central Policy Manager (success)
24	Password stored in EPV changed by Central Policy Manager (success)
31	Password reconciliation by Central Policy Manager (success)
38	Password verification by Central Policy Manager (failure)
57	Password stored in Enterprise Password Vault changed by Central Policy Manager (failure)
60	Password reconciliation by Central Policy Manager (failure)
130	Password stored in Enterprise Password Vault disabled by Central Policy Manager
295	User retrieved a password stored in Enterprise Password Vault

Event ID	Description
300	User session started in Privileged Session Manager
302	User session ended in Privileged Session Manager
308	User used a password stored in Enterprise Password Vault
411	A window was activated by user in Privileged Session Manager

Maintenance and Troubleshooting

The Add-On operations are logged into the **SyslogService.txt** file. This file is located in the same folder as **SyslogService.exe.**

To change the add-on logging level, use the **LogLevel** parameter in the **Settings.xml** file.

- It is recommended that before the first run you set this parameter to debug. This will facilitate operations tracking and possible problem solving.
- After that it is strongly recommended to re-set this parameter to `error` to prevent the uncontrolled log growth.

If you cannot see collected data in Auditor, check the following:

1. In Auditor settings, go to the **Integrations** section and make sure the **Leverage Integration API** is switched to **ON**. Check the communication port number – default is **9699**.
2. If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
3. Verify the parameters you provided in **Settings.xml** and **dbparam.ini**.

Hyper-V SCVMM

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 analytic to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Microsoft System Center Virtual Machine Manager (SCVMM) is a solution for configuring and managing virtualized infrastructure components across on-premises, service provider, and the Azure cloud environment. These components include virtualization servers, networking components and storage resources.

Virtualization teams, Managed Service Providers and other IT professionals need to detect who does what in the SCVMM-managed virtual infrastructure. For that, a unified audit trail is required, supporting detailed SCVMM monitoring and effective response to changes.

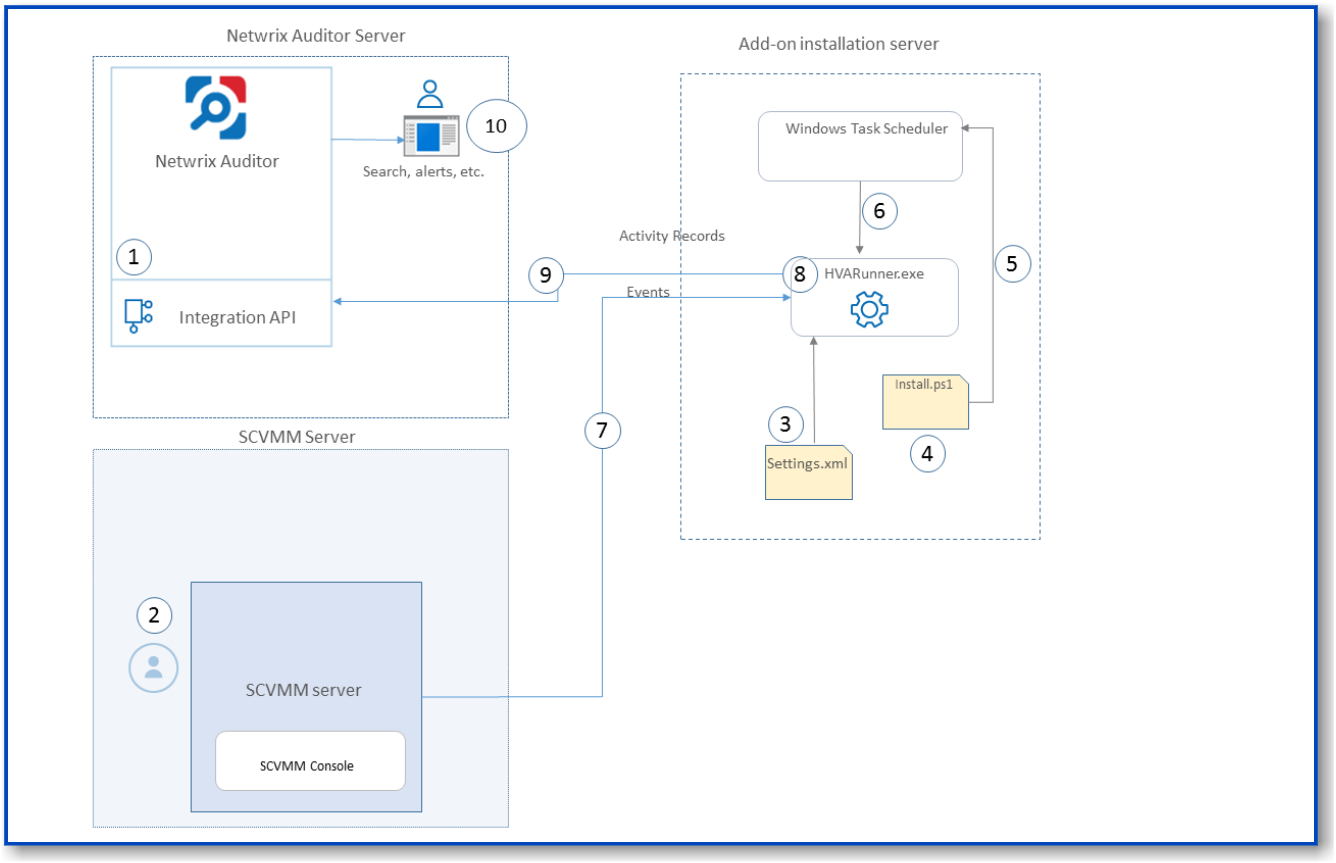
For that purpose, you can use a specially designed add-on. It works in collaboration with Netwrix Auditor, supplying data about operations on your SCVMM server to Netwrix database. Aggregating data into a single audit trail simplifies the analysis, makes activity monitoring more cost-effective, and helps you keep tabs on your virtual infrastructure.

Major benefits:

- Gain a high-level view of the data you store
- Detect unauthorized activity that might threaten your data

How It Works

The add-on is implemented as a stand-alone application that collects activity data from Virtual Machine Manager and sends it to Auditor using the Integration API.



On a high level, the solution works as follows:

1. An IT administrator configures the Integration API settings to enable data collection and storage to the Netwrix database for further reporting, search, etc.

   It is recommended to create a dedicated monitoring plan in Auditor and add a dedicated item of **Integration** type to it — then you will be able to filter data in reports and search results by monitoring plan or item name.

2. On SCVMM side, the IT administrator prepares a dedicated user account for accessing SCVMM server. This account requires administrative rights.
3. Then the IT administrator opens the settings.xml configuration file and specifies the necessary parameters for add-on operation, including Netwrix Auditor server settings, etc.

4. The IT administrator selects the deployment scenario and runs install.ps1 PowerShell script file to deploy and configure the add-on components on the target server.

5. This script creates a Windows scheduled task that will run periodically (every 15 minutes) to collect audit data from VMM server.

   See the Monitoring Scope for additional information on the default list of the events supported out-of-the box.

6. The add-on component **HVARunner.exe** starts collecting activity data from VMM. Data communication is performed using TCP protocol.

7. The add-on processes this data into Auditor-compatible format (Activity Records). Each Activity Record contains the Who-What-When-Where-Action information (that is, initiator's account, time, action, and other details).

   See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Integration API.

8. The add-on uses the Integration API to send the Activity Records to Auditor Server, where this data becomes available for search, reporting and alerting.
9. Users open Auditor Client to work with collected data:
   - Search for file changes using certain criteria
   - Export data to PDF or CSV files
   - Save search results as reports
   - Subscribe to search results
   - Configure and receive alerts

Add-on Delivery Package

The add-on delivery package is a ZIP archive comprising several files, including DLLs, configuration and executable files. The latter ones are listed in the table below.

File name	Description
install.ps1	PowerShell script that installs the add-on components and creates a scheduled task for data collection.
settings.xml	Contains parameters for the add-on service operation.
HVARunner.exe	Main add-on component, responsible for audit data collection from SCVMM.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
Auditor Server	• Integration API and Audit Database settings are configured in Auditor Server settings. See the Prerequisites and Audit Database topics for additional information. • The **TCP 9699** port must be open on Windows firewall for inbound connections. • User account under which data will be written to the Audit Database requires the **Contributor** role in Netwrix Auditor. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant it the **Global administrator** role, or add that account to the **Netwrix Auditor Administrators** group.
Add-on installation server, i.e. the machine where the add-on will be installed	• The **TCP 5985** port must be open on Windows firewall for inbound connections. • NET Framework 4.5 or later.
Microsoft System Center Virtual Machine Manager	SCVMM versions: • 2019 • 2016
Virtualization hosts	• Microsoft Hyper-V (hardware and nested-virtualization) • VMware ESXi

Accounts and Rights

It is recommended to create a dedicated account for running the add-on.

This account should have the following minimal rights and permissions:

- **Administrator** role in SCVMM
- **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information.

Considerations and Limitations

- By default, the add-on is targeted at a single SCVMM server.
- If Auditor Server becomes unavailable for some time, the add-on will reset the last data collection and will run it anew during the next scheduled interval.

Compatibility Notice

The add-on is compatible with:

- Microsoft System Center Virtual Machine Manager 2019 and 2016
- Netwrix Auditor 9.9 and later

Add-On Parameters

To configure the add-on parameters, you need to edit the **settings.xml** file in the add-on folder. You must define connection details: Auditor Server host, user credentials, etc.

Most parameters are optional, the service uses the default values unless parameters are explicitly defined (<*parameter*>**value**</*parameter*>). You can skip or define parameters depending on your execution scenario and security policies.

Parameter	Default value	Description
NetwrixIntegration		

Parameter	Default value	Description
NetwrixAuditorEndpoint	https://localhost:9699/netwrix/api/v1/activity_records	Auditor Server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15, EnterpriseNAServer, WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). Do not modify the endpoint part (/netwrix/api . . . .)
NetwrixAuditorCertificateThumbprint	NOCHECK	Auditor Certificate Thumbprint Property. Possible values: • AB:BB:CC.—Check Auditor server certificate thumbprint identifier. • NOCHECK—Do not check Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
NetwrixAuditorDateTimeFormat	yyyy-MM-ddTHH:mm:ssZ	Auditor time format. By default, set to zero offset.

Parameter	Default value	Description
NetwrixAuditorPlan	—	Unless specified, data is written to Netwrix_Auditor_API database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. If you select a plan name in the add-on, make sure a dedicated plan is created in Auditor, the Netwrix API data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
NetwrixAuditorPlanItem	—	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. Make sure to create a dedicated item in Auditor in advance.
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN\username* format. The account must be assigned the Contributor role in Netwrix Auditor.

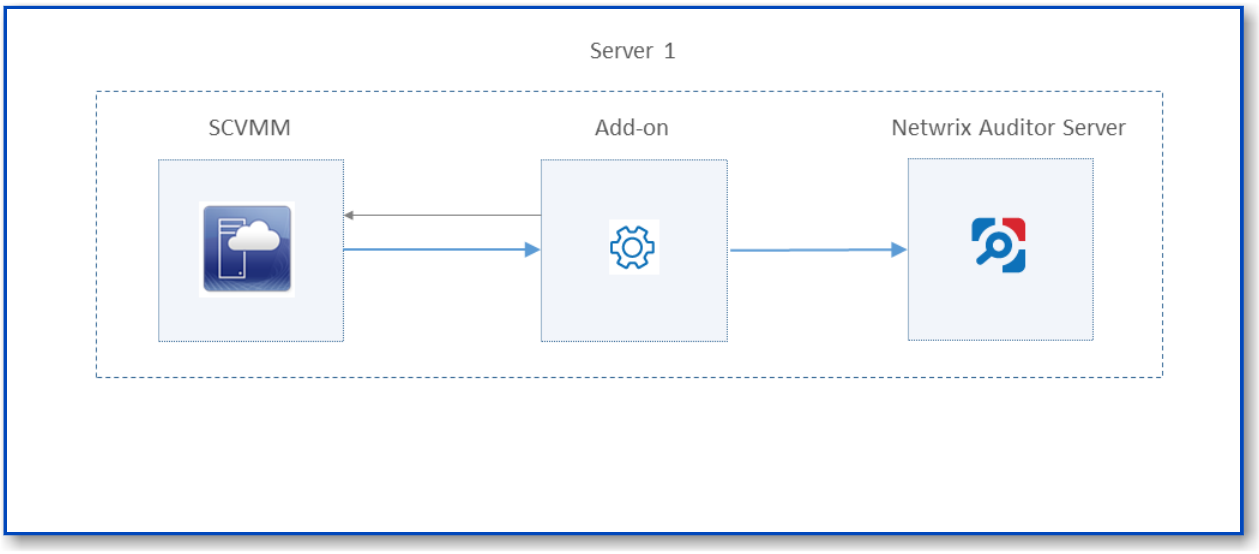
Parameter	Default value	Description
NetwrixAuditorUserPassword	Current user credentials	Unless specified, the add-on runs with the current user credentials. Provide a different password if necessary.
DataCollection		
DataCollectionServer	(empty)	Specify SCVMM server to collect data from. You can use IP address, FQDN or NETBIOS name. For localhost, leave this parameter empty.
DataCollectionUserName	(empty)	Specify user account that will be used for data collection from SCVMM server. To use the account currently logged in, leave this parameter empty. Make sure the account has administrative rights on that server (see the Accounts and Rights topic for additional information).
DataCollectionPassword		Specify user account password.
ShortTermFolder	ShortTerm	Specify path to the short-term archive (Netwrix Auditor working folder). You can use full or relative path.

Remember to save **settings.xml** after editing is complete.

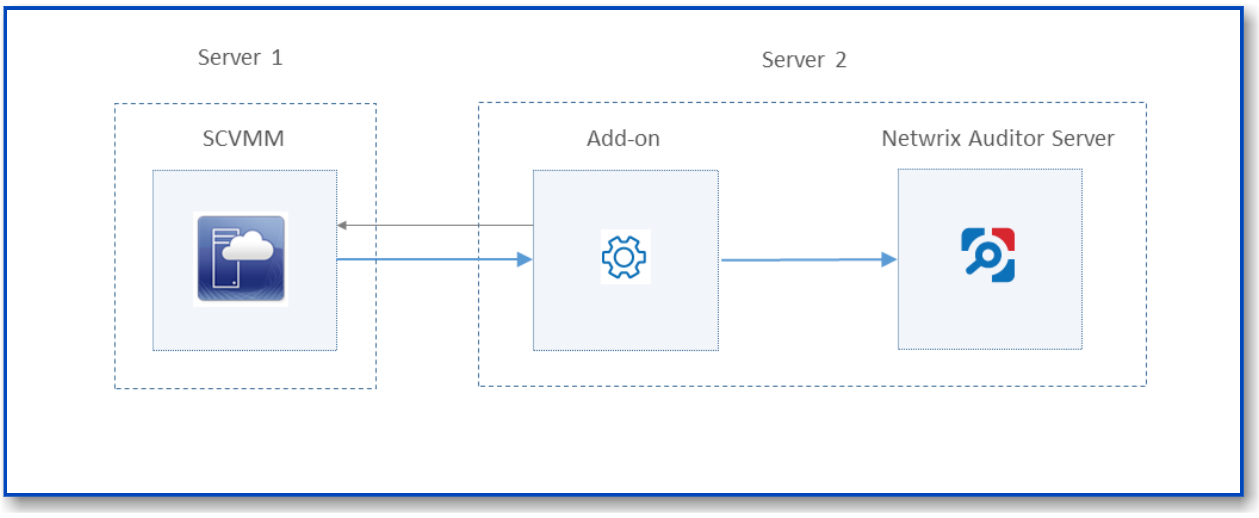
Deployment Scenarios

The add-on can be deployed on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed, or on a remote server. Also, consider different SCVMM deployment scenarios. Possible deployment options are as follows (here it is assumed that the add-on is installed together with Auditor server):

1. Add-on running on the same machine as SCVMM server (with Management Console):

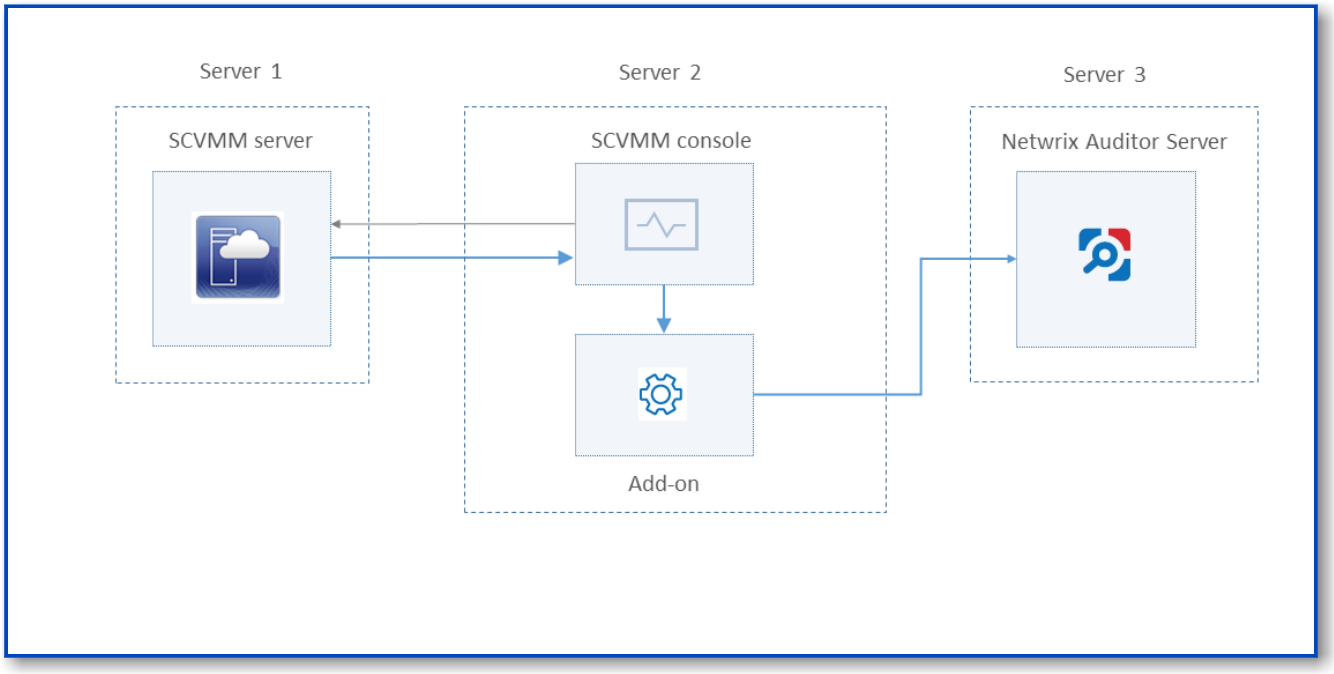


2. Add-on and SCVMM server (with Management Console) running on different machines:



In this scenario, the account used to access SCVMM server must be a member of the *Remote Management Users* local group on the SCVMM server.

3. Add-on running on the same machine as SCVMM Management Console; SCVMM server running on the remote machine:



In this scenario, make sure to specify SCVMM server address in the **DataCollectionServer** parameter (not the machine where SCVMM console runs) in the **settings.xml** configuration file. See the Add-On Parameterstopic for additional information.

Depending on the deployment scenario you choose, you will need to define a set of the add-on parameters. Several examples are provided below.

In the certain scenarios you may need to configure not all parameters but only some of them.

Example 1

- The add-on runs on the Auditor server.
- The *System* account is used to launch the add-on via Task Scheduler (default configuration).
- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/
activity_records↙NetwrixAuditorEndpoint>

<NetwrixAuditorUserName↗

<NetrixAuditorPassword↗
```

Configuration parameters **NetwrixAuditorUserName** and **NetrixAuditorPassword** are not required.

Example 2

- The add-on runs on the Auditor server with the explicitly specified user credentials.
- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/
activity_records↙NetwrixAuditorEndpoint>

<NetwrixAuditorUserName>SecurityOfficer↙NetwrixAuditorUserName>

<NetwrixAuditorPassword>NetwrixUser↙NetwrixAuditorPassword>
```

Example 3

- The add-on runs on the machine with SCVMM.
- The *System* account is used to launch the add-on via Task Scheduler (default configuration).
- Configuration parameters to specify in **settings.xml**:

```
<DataCollectionServer↗

<DataCollectionUserName↗

<DataCollectionPassword↗
```

Credentials for **Data Collection Server** (that is, SCVMM) are not required.

Example 4

- SCVMM and/or Auditor run on the machines other than the add-on server.
- In this case, the corresponding set of credentials (for **Data Collection Server** and/or Netwrix Auditor) must be specified explicitly.
- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/
activity_records↙NetwrixAuditorEndpoint>
```

```
<NetwrixAuditorUserName>SecurityOfficer↙NetwrixAuditorUserName>

<NetrixAuditorPassword>NetwrixUser↙NetrixAuditorPassword>

<DataCollectionServer>SCVMMServer↙DataCollectionServer>

<DataCollectionUserName>SCVMMAdmin↙DataCollectionUserName>

<DataCollectionPassword>Password↙DataCollectionPassword>
```

Deploy the Add-On

Follow the step to deploy the Add-On:

Step 1 – Prepare Netwrix Auditor for Data Processing.

Step 2 – Download the Add-On.

Step 3 – Configure Parameters for Data Collection.

Step 4 – Register Windows Scheduled Task.

Prepare Netwrix Auditor for Data Processing

In Auditor client, go to the Integrations section and verify Integration API settings:

1. Make sure the **Leverage Integration API** is switched to **ON**.
2. Check the TCP communication port number – default is **9699**.

See the Prerequisites topic for additional information.

By default, activity records are written to *Netwrix_Auditor_API* database which is not associated with a specific monitoring plan.

Optionally, you can create a dedicated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. Target it at Netwrix API data source and enable for monitoring. Add a dedicated item of *Integration* type to the plan for data to be filtered by item name. See the Integration API topic for additional information.

In such scenario, you will need to specify this monitoring plan in the *NetwrixAuditorPlan* and *NetwrixAuditorPlanItem* parameters in the **settings.xml** file. See the Add-On Parameters topic for additional information.

Download the Add-On

1. Download the distribution package **Netwrix_Auditor_Add-on_for_Microsoft_SCVMM.zip**.
2. Unpack it to a folder on the computer where you plan to deploy the add-on.

Configure Parameters for Data Collection

In the add-on folder, open the **settings.xml** file and configure the add-on parameters for data collection, as listed below.

See the Add-On Parameterstopic for the full list of configuration parameters.

Parameter	Default value	Description
DataCollectionServer	(empty)	Specify SCVMM server to collect data from. You can use IP address, FQDN or NETBIOS name. For *localhost*, leave this parameter empty.
DataCollectionUserName	(empty)	Specify user account that will be used for data collection from SCVMM server. To use the account currently logged in, leave this parameter empty.s Make sure the account has administrative rights on that server (see the Accounts and Rights topic for additional information).

Parameter	Default value	Description
DataCollectionPassword		Specify user account password.
ShortTermFolder	ShortTerm	Specify path to the short-term archive (Netwrix Auditor working folder). You can use full or relative path.

Save the **settings.xml** file. New configuration settings will be applied automatically at the next data collection.

For the full list of parameters, see the Add-On Parameters topic for additional information.

Register Windows Scheduled Task

Run the **install.ps1** PowerShell script from the add-on folder. It will configure and register a Windows scheduled task that will run periodically every 15 min to retrieve audit data from SCVMM.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You might want to apply a filter to narrow down your search results to the Netwrix API data source only.

- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.

    - To create an alert on the specific occurrences, click **Create alert**.
    - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in. See the Administration topic for additional information.

Monitoring Scope

Review a full list of the events that can be monitored using the add-on.

Object Type	Reported Action	Reported Properties
Virtual Machine	• Create/Delete • Clone • Migrate • Rename • Create/Delete Checkpoint • Hardware Configuration change	• Name • Checkpoint Name & Description • Number Of Processors • Memory Size (Allocated, Max) • VHD Location, Max size • Network Name • Switch Name
Hypervisor (Host)	• Create/Delete • Move • Hardware Configuration change • State change	• Name • Number Of Processors • RAM Memory Size • Host Disk Capacity
Host Cluster	• Create/Delete • Move	• Name
Host Group	• Create/Delete	• Name

Object Type	Reported Action	Reported Properties
	• Move • Rename	
Private Cloud	• Create/Delete • Rename	• Name
VM Network	• Create/Delete • Rename	• Name
User Role	• Rename • Add/Remove Members • Add/Remove Scopes • Permissions change	• Name • Scope • Permissions • Members

Maintenance and Troubleshooting

If you cannot see collected data in Auditor, check the following:

- Add-on account has sufficient rights to access SCVMM and Auditor.
- In Netwrix Auditor settings, go to the **Integrations** section and make sure the **Leverage Integration API** is switched to **ON**. Check the communication port number – default is **9699**.
- If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
- Verify the parameters you provided in **settings.xml**.

Monitor Several SCVMM

Follow the steps If you need to monitor more than one SCVMM:

Step 1 – Deploy one more add-on instance to the server where the first add-on instance is already installed. Be sure to use a different installation folder.

Step 2 – Open the **settings.xml** file and configure the new add-on instance to work with the second SCVMM server.

Step 3 – Open the **install.ps1** file for the new add-on for edit.

Step 4 – Modify the default scheduled task name:

```
$name = "NetwrixAuditor Add-on for Microsoft SCVMM"
```

Step 5 – Save and then launch the updated **install.ps1** file.

Modify Task Schedule

Follow the steps if you need to modify the task schedule:

Step 1 – Open **install.ps1** for edit.

Step 2 – Modify the default scheduled task schedule:

```
$task.Triggers.Repetition.Interval = "PT15M"
```

Step 3 – Save and then launch the updated **install.ps1** file.

Alternatively, you can use **Windows Task Scheduler**.

- If the solution was deployed using the third scenario (that is, SCVMM server and add-on are running on different machines), then the following error may be written in the solution log:

The WinRM client cannot process the request.

See the Deployment Scenariostopic for additional information.

If the authentication scheme is different from Kerberos, or if the client computer is not joined to a domain, then HTTPS transport must be used or the destination machine must be added to the **TrustedHosts** list. To configure this list, use **winrm.cmd**.

Computers included in the **TrustedHosts** list might not be authenticated. To get more information about their settings, you can run the following command:

```
winrm help config
```

For details on remote troubleshooting and authentication issues, see the following Microsoft article: about_Remote_Troubleshooting.

To work around, add the remote SCVMM server to the **TrustedHosts** list on the machine were the add-on runs. For that, use the following commands:

```
winrm quickconfig

Set-Item WSMan:\localhost\Client\TrustedHosts -Value "ServerNameOrIP"
```

here:

`ServerNameOrIP` – SCVMM server name or IP address.

IBM QRadar

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the IBM QRadar SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.

2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.

3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.\

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted`

On...	Ensure that...
	• The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting the Auditor Server and uses default port 9699.

Parameter	Default value	Description
		If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN**username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

In-Script Parameters

You may also need to modify the parameters that define how EventIDs should be generated for exported events, though their default values address most popular usage scenarios. In-script

parameters are listed in the table below. To modify them, open the script for edit and enter the values you need.

Once set, these parameter values must stay unchanged until the last run of the script — otherwise dynamically calculated EventIDs will be modified and applied incorrectly.

Parameter	Default value	Description
EventID generation		
GenerateEventId	True	Defines whether to generated unique EventIDs. Possible parameter values: • True — generate unique EventIDs using Activity Record fields • False — do not generate a unique ID, set EventID=0 for all cases EventID is generated through CRC32 calculation that involves the following Activity Record field values: • ObjectType • Action • DataSource (optional, see below for details) Only the lowest 16 bits of the calculation result are used. See the Activity Records topic for additional information.
IncludeDataSourceToMakeEventId*	True	Defines whether the DataSource field of Activity Record should be used in the EventID calculation. This parameter is applied only if GenerateEventId is set to *TRUE*.

Parameter	Default value	Description
SetDataSourceAsEventCategory	True	Defines whether to fill in Event Category event field with a numeric value derived from the DataSource field of Activity Record. Possible parameter values: • True — generate a numeric value for Event Category using Activity Record field • False — do not generate a numeric value, set Event Category=1 for all cases The Event Category field value is generated through CRC32 calculation that involves the DataSource field of Activity Record. Only the lowest 9 bits of the calculation result are used.
SetDataSourceAsEventSource	False	Defines whether to fill in the Event Source event field with the value from the DataSource field of Activity Record. Possible parameter values: • True — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by $EventSourcePrefix. Default prefix is *NA*, for example:*NA Windows Server* • False — set Event Source to *Netwrix_Auditor_Integration_API* for all cases If the script cannot fill in the Event Source for some DataSource, the default value

Parameter	Default value	Description
		Netwrix_Auditor_Integration_API will be used. If the event source for particular DataSource does not exist in the Netwrix_Auditor_Integration event log, elevated privileges are required for add-on execution.

* When configuring the **IncludeDataSourceToMakeEventId** parameter, consider that the *Object Type - Action* pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding DataSource from calculation may lead to the same EventID (duplicates). See the Run the Add-On with PowerShell topic for additional information about duplicates.

Choose Appropriate Execution Scenario

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1`
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_ QRadar.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

Scenario	Example
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_ QRadar.ps1 -NetwrixAuditorHost 172.28.6.15`
The add-on exports Activity Records from a remote Auditor Server using explicitly defined credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_ QRadar.ps1 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-
on_for_IBM_QRadar.ps1 - NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor **Integration** event log will be created and filled with events.

By default, the Netwrix Auditor **Integration** event log size is set to **1GB**, and retention is set to "*Overwrite events as needed*". See the Integration Event Log Fields topic for additional information.

NOTE: Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt** file. It defines mapping between the Activity Records and related Event IDs . You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt** file.

Similarly, the add-on also creates the **Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt** file that defines mapping between the Data Source and related Category ID.

Applying Filters

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.
- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_IBM_QRadar.ps1" -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

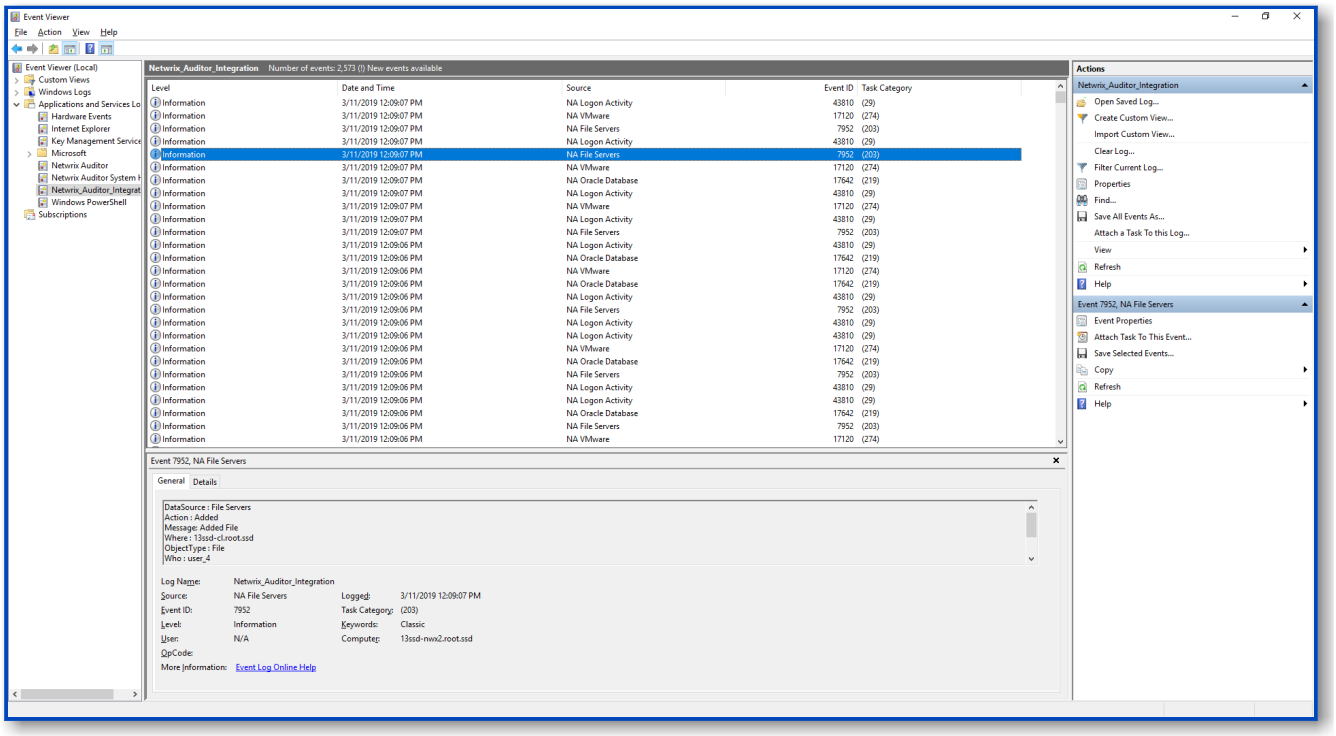
Work with Collected Data

Follow the steps to work with collected data:

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the Event Viewer dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** >Netwrix Auditor Integration log.

Step 3 – Review events.



Now you can augment Windows event log with data collected by the Auditor.

Integration Event Log Fields

This section describes how the add-on fills in the Netwrix Auditor **Integration** event log fields with data retrieved from Activity Records.

The Activity Record structure is described in the Reference for Creating Activity Recordstopic.

Event log field name	Filled in with value	Details
Source	**NA{Data Source Name}** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter.
EventID	**{Calculated by add-on}** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*).
Task Category	**{DataSource ID}** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter.

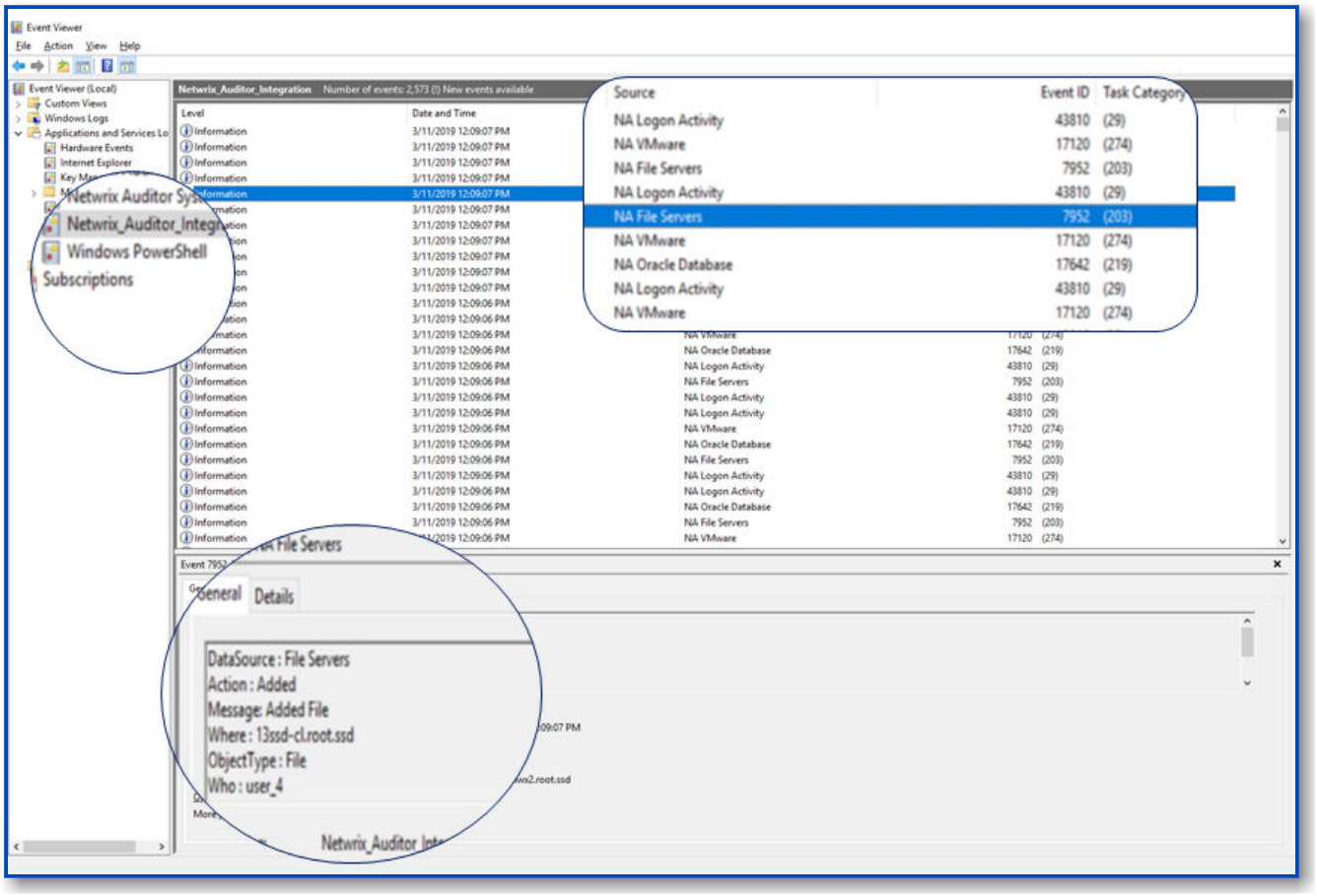
See the Define Parameters topic for additional information.

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}
Action	{Action}
Message	{Action ObjectType}
Where	{Where}

Entry in EventData	Activity Record field
ObjectType	{ObjectType}
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

Details are filled in only if this Activity Record field is not empty.



Intel Security

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the Intel Security SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.

On...	Ensure that...
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting the Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN**username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

In-Script Parameters

You may also need to modify the parameters that define how EventIDs should be generated for exported events, though their default values address most popular usage scenarios. In-script parameters are listed in the table below. To modify them, open the script for edit and enter the values you need.

Once set, these parameter values must stay unchanged until the last run of the script — otherwise dynamically calculated EventIDs will be modified and applied incorrectly.

Parameter	Default value	Description
EventID generation		
GenerateEventId	True	Defines whether to generated unique EventIDs. Possible parameter values: • True — generate unique EventIDs using Activity Record fields • False — do not generate a unique ID, set EventID=0 for all cases EventID is generated through CRC32 calculation that involves the following Activity Record field values: • ObjectType • Action • DataSource (optional, see below for details) Only the lowest 16 bits of the calculation result are used. See the Activity Records topic for additional information.
IncludeDataSourceToMakeEventId*	True	Defines whether the DataSource field of Activity Record should be

Parameter	Default value	Description
		used in the EventID calculation. This parameter is applied only if GenerateEventId is set to *TRUE*.
SetDataSourceAsEventCategory	True	Defines whether to fill in Event Category event field with a numeric value derived from the DataSource field of Activity Record. Possible parameter values: • True — generate a numeric value for Event Category using Activity Record field • False — do not generate a numeric value, set Event Category=1 for all cases The Event Category field value is generated through CRC32 calculation that involves the DataSource field of Activity Record. Only the lowest 9 bits of the calculation result are used.
SetDataSourceAsEventSource	False	Defines whether to fill in the Event Source event field with the value from the DataSource field of Activity Record. Possible parameter values: • True — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by $EventSourcePrefix. Default prefix is *NA*, for example:*NA Windows Server*

Parameter	Default value	Description
		• False — set Event Source to *Netwrix_Auditor_Integration_API* for all cases If the script cannot fill in the Event Source for some DataSource, the default value *Netwrix_Auditor_Integration_API* will be used. If the event source for particular DataSource does not exist in the Netwrix_Auditor_Integration event log, elevated privileges are required for add-on execution.

* When configuring the **IncludeDataSourceToMakeEventId** parameter, consider that the *Object Type - Action* pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding DataSource from calculation may lead to the same EventID (duplicates). See the Run the Add-On with PowerShell topic for additional information about duplicates.

Choose Appropriate Execution Scenario

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Intel_Security.ps1`

Scenario	Example
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Intel_Security.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Intel_Security.ps1-NetwrixAuditorHost 172.28.6.15`
The add-on exports Activity Records from a remote Auditor Server using explicitly defined credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Intel_Security.ps1-NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

To run the script with PowerShell:

Step 1 – On computer where you want to execute the add-on, start **Windows PowerShell**.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-
on_for_Intel_Security.ps1 - NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*\), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*\").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor **Integration** event log will be created and filled with events.

By default, the Netwrix Auditor **Integration** event log size is set to 1GB, and retention is set to "*Overwrite events as needed*". See the Integration Event Log Fields topic for additional information.

NOTE: Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt** file. It defines mapping between the Activity Records and related Event IDs . You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt** file.

Similarly, the add-on also creates the **Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt** file that defines mapping between the Data Source and related Category ID.

Applying Filters

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.
- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_Intel_Security.ps1" -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

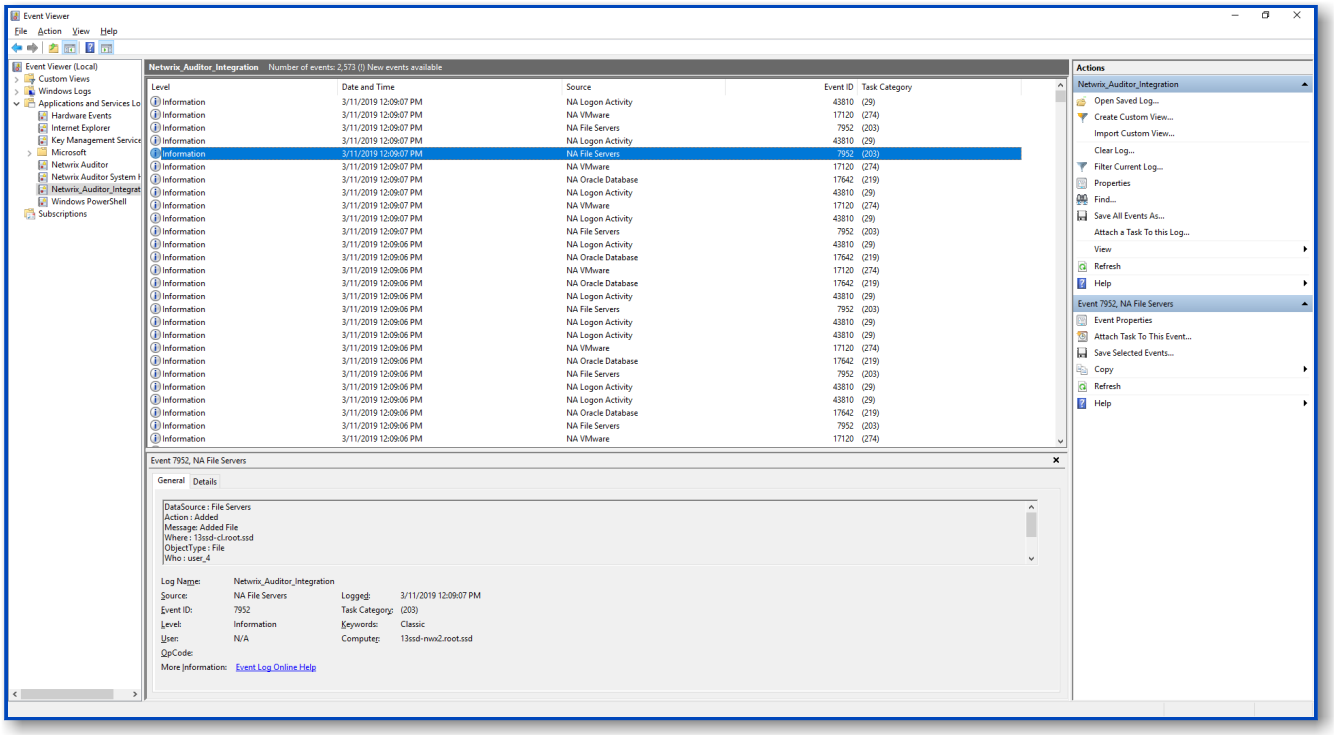
Work with Collected Data

Follow the steps to work with collected data:

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the Event Viewer dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** >Netwrix Auditor Integration log.

Step 3 – Review events.



Now you can augment Windows event log with data collected by the Auditor.

Integration Event Log Fields

This section describes how the add-on fills in the Netwrix Auditor **Integration** event log fields with data retrieved from Activity Records.

The Activity Record structure is described in the Reference for Creating Activity Recordstopic.

Event log field name	Filled in with value	Details
Source	**NA{Data Source Name}** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter.
EventID	**{Calculated by add-on}** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*).
Task Category	**{DataSource ID}** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter.

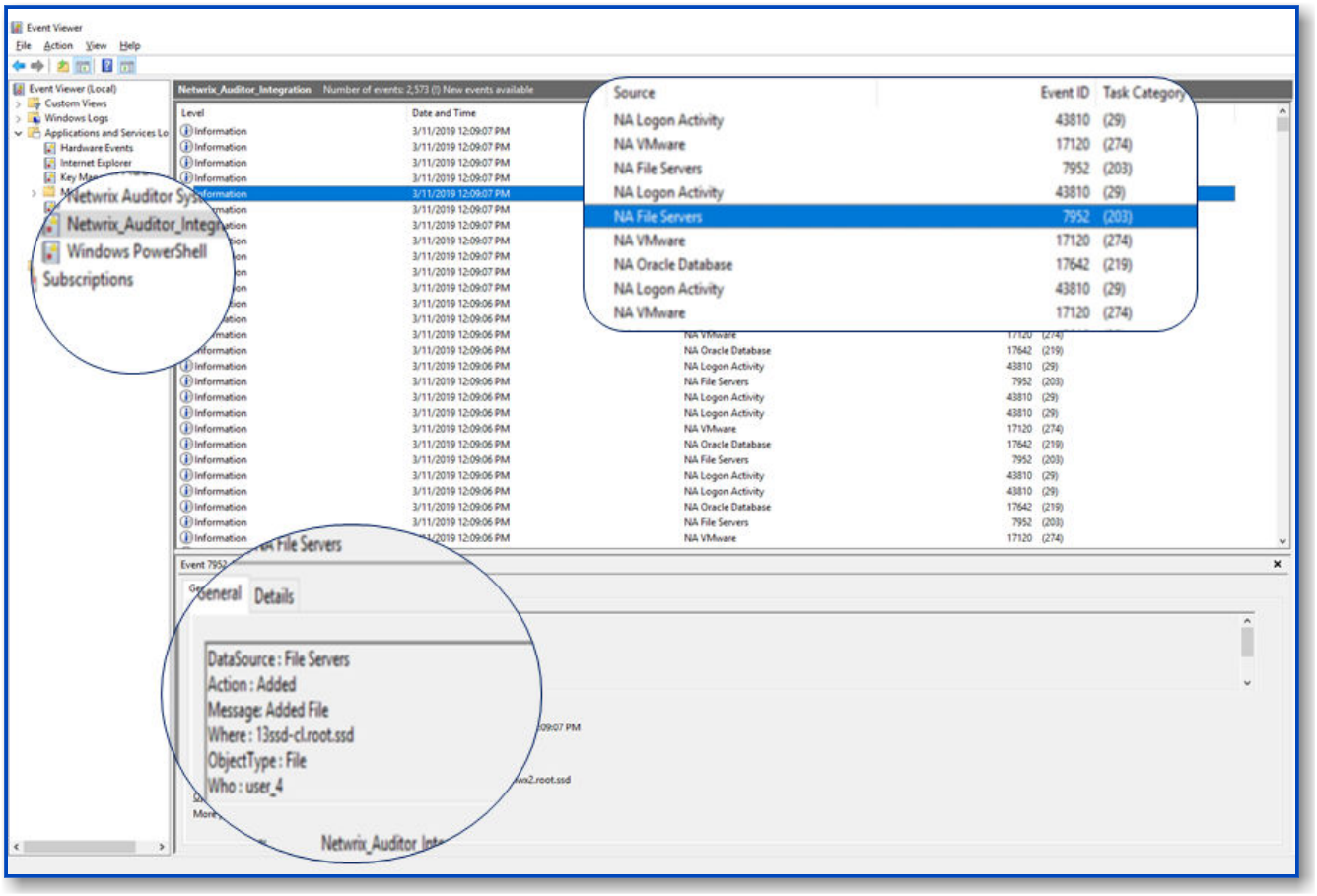
See the Define Parameters topic for additional information.

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}
Action	{Action}
Message	{Action ObjectType}

Entry in EventData	Activity Record field
Where	{Where}
ObjectType	{ObjectType}
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

Details are filled in only if this Activity Record field is not empty.



Linux Generic Syslog

The add-on works in collaboration with Netwrix Auditor, supplying data about activity on your Linux-based devices. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a service, this add-on facilitates the data transition from Linux-based systems to Netwrix Auditor. All you have to do is provide connect ion details and specify parsing rules.

On a high level, the add-on works as follows:

1. The add-on listens to the specified UDP ports and captures designated Syslog messages.

   Out of the box, messages from Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE42, and Ubuntu 16 are supported. For other distributions, deployment of the rsyslog package may be required. You can edit the add-on configuration to extend the captured message list.

2. The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.

3. Using the Integration API, the add-on sends the activity records to the Netwrix Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the NIntegration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Netwrix Auditor Server side	• The Audit Database settings are configured in Auditor Server. • The TCP **9699** port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Contributor role in Auditor. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
The computer where the add-on will be installed	• The UDP 514 port is open for inbound connections. **CAUTION:** UPD 514 port can only be used by one service, otherwise the following error will occur: `[ERROR] Error occurred when starting the syslog udp`

On...	Ensure that...
	`listener. Only one usage of each socket address (protocol/network address/port) is normally permitted` • .Net Framework 3.5 SP1, 4.0, 4.5, or 4.6 is installed.

On the target syslog-based platform	Outbound UDP 514 port must be enabled.
	
	The **Syslog daemon** must be configured to redirect events. The procedure below explains how to configure redirection.
	
	NOTE: Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu 16 are supported out of the box. For other distributions, deployment of the rsyslog package may be required.
	
	• On Red Hat Enterprise Linux 7, perform the following steps:
	
	Step 1 – Open the **/ etc/ rsyslog.conf** file.
	
	Step 2 – Add the following line:
	
	`auth.*;authpriv.* @name:514;RSYSLOG_SyslogProtocol23Format`
	
	where **name** is a FQDN, Net BIOSname or IP address of the computer where Netwrix Auditor Server is installed. For example:
	
	`auth.*;authpriv.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format`
	
	Step 3 – Launch the **RHEL console** and execute the following command:
	
	`service rsyslog restart`

On...	Ensure that...

	• On Ubuntu 16, perform the following steps:
	
	Step 1 – Navigate to the **/ etc/ rsyslog.d/ 50-default.conf** file.
	
	Step 2 – Add the following line:
	
	`auth.*;authpriv.* @name:514;RSYSLOG_SyslogProtocol23Format`
	
	where **name** is a FQDN, Net BIOSname or IP address of the computer where Netwrix Auditor Server is installed. For example:
	
	`auth.*;authpriv.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format`
	
	Step 3 – Launch the **UBUNTU console** and execute the following command:
	
	`service rsyslog restart`

Install Add-On

Follow the steps to install the Add-On:

Step 1 – Navigate to your add-on package.

Step 2 – Unzip the Add-On to a desired folder.

Step 3 – Run the installation package.

Step 4 – Accept the license agreement and follow the instructions of the setup wizard.

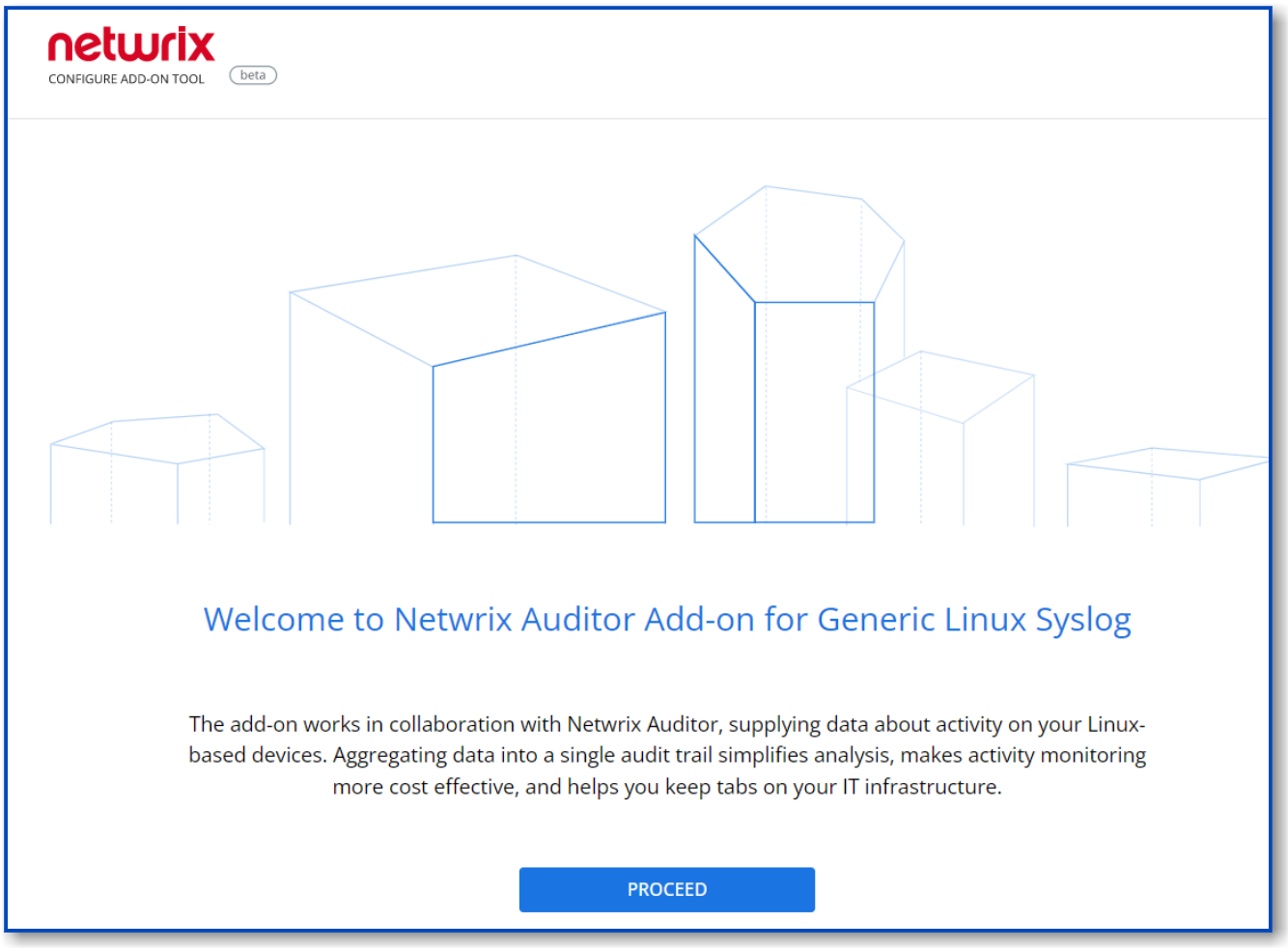
Step 5 – On the **Destination Folder** step, specify the installation folder (*C:\Program Files (x86)\Netwrix Add-ons\<Add-on name>* by default).

Step 6 – Click **Install**.

Step 7 – When done, click **Finish**.

Define Parameters

The configuration wizard opens in the default web browser:



Click **Proceed** and complete the following fields:

Option	Description
Specify General Settings	

Option	Description
Listed UDP port	Specify UDP port for listening incoming events. (**514** by default).
Auditor Endpoint	Auditor Server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hostingAuditor Server and uses default port *9699*. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15*, *EnterpriseNAServer*, *WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). **NOTE:** Do not modify the endpoint part (*/ netwrix/ api*)
Certificate Thumbprint	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Auditor certificate via Windows Certificate Store. • `AB:BB:CC`—Check Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
Specify Active Directory credentials	

Option	Description
Username	Provide the name of the account under which the service runs. Unless specified, the service runs under the account currently logged on.
Password	Provide the password for the selected account.
Auditor Monitoring Plan settings	
Auditor Plan	Unless specified, data is written to **Netwrix_Auditor_API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add- on, make sure a dedicated plan is created in Auditor, the Netwrix **API** data source is added to the plan and enabled for monitoring. Otherwise, the add- on will not be able to write data to the Audit Database.
Auditor Plan Item	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. **NOTE:** Make sure to create a dedicated item inAuditor in advance.
Accept List	
Address	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only.

Option	Description
	NOTE: Events collected from any other source will be ignored.

Click **Run** to start collecting data with the Add-On.

Work with Collected Data

Follow the steps to search for collected data:

Step 1 – Start the Auditor client and navigate to **Search**.

Step 2 – Click **Search**.

NOTE: You might want to apply a filter to narrow down your search results to the Netwrix API data source only.

Expand List of Gathered Events

Based on the activity you get, you may want to adjust the processing rules, add other relevant events, etc. To do that, copy and edit the file with processing rules, and then restart the service.

LogRhythm

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the LogRhythm SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information.

On...	Ensure that...
	Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting the Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN**username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.

Parameter	Default value	Description
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

In-Script Parameters

You may also need to modify the parameters that define how EventIDs should be generated for exported events, though their default values address most popular usage scenarios. In-script parameters are listed in the table below. To modify them, open the script for edit and enter the values you need.

Once set, these parameter values must stay unchanged until the last run of the script — otherwise dynamically calculated EventIDs will be modified and applied incorrectly.

Parameter	Default value	Description
EventID generation		
GenerateEventId	True	Defines whether to generated unique EventIDs. Possible parameter values: • True — generate unique EventIDs using Activity Record fields • False — do not generate a unique ID, set EventID=0 for all cases EventID is generated through CRC32 calculation that involves the following Activity Record field values: • ObjectType • Action

Parameter	Default value	Description
		• DataSource (optional, see below for details) Only the lowest 16 bits of the calculation result are used. See the Activity Records topic for additional information.
IncludeDataSourceToMakeEventId*	True	Defines whether the DataSource field of Activity Record should be used in the EventID calculation. This parameter is applied only if GenerateEventId is set to *TRUE*.
SetDataSourceAsEventCategory	True	Defines whether to fill in Event Category event field with a numeric value derived from the DataSource field of Activity Record. Possible parameter values: • True — generate a numeric value for Event Category using Activity Record field • False — do not generate a numeric value, set Event Category=1 for all cases The Event Category field value is generated through CRC32 calculation that involves the DataSource field of Activity Record. Only the lowest 9 bits of the calculation result are used.
SetDataSourceAsEventSource	False	Defines whether to fill in the Event Source event field with the value

Parameter	Default value	Description
		from the DataSource field of Activity Record. Possible parameter values: • True — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by $EventSourcePrefix. Default prefix is *NA*, for example:*NA Windows Server* • False — set Event Source to *Netwrix_Auditor_Integration_API* for all cases If the script cannot fill in the Event Source for some DataSource, the default value *Netwrix_Auditor_Integration_API* will be used. If the event source for particular DataSource does not exist in the Netwrix_Auditor_Integration event log, elevated privileges are required for add-on execution.

* When configuring the **IncludeDataSourceToMakeEventId** parameter, consider that the *Object Type - Action* pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding DataSource from calculation may lead to the same EventID (duplicates). See the Run the Add-On with PowerShell topic for additional information about duplicates.*

Choose Appropriate Execution Scenario

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on theAuditorServer with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_LogRhythm.ps1`
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ LogRhythm.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ LogRhythm.ps1- NetwrixAuditorHost 172.28.6.15`
The add-on exports Activity Records from a remote Auditor Server using explicitly defined credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ LogRhythm.ps1- NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run the script with PowerShell.

Step 1 – On computer where you want to execute the add-on, start **Windows PowerShell**.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-on_for_LogRhythm.ps1
- NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*\), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*\").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor Integration event log will be created and filled with events.

By default, the Auditor Integration event log size is set to 1GB, and retention is set to "*Overwrite events as needed*". See the Integration Event Log Fields topic for additional information.

NOTE: Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt** file. It defines mapping between the Activity Records and related Event IDs . You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt** file.

Similarly, the add-on also creates the **Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt** file that defines mapping between the Data Source and related Category ID.

Applying Filters

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will

export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.

- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

Automate Add-On Execution

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-`

Option	Value
	on_for_LogRhythm.ps1" -NetwrixAuditorHost 172.28.6.15

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

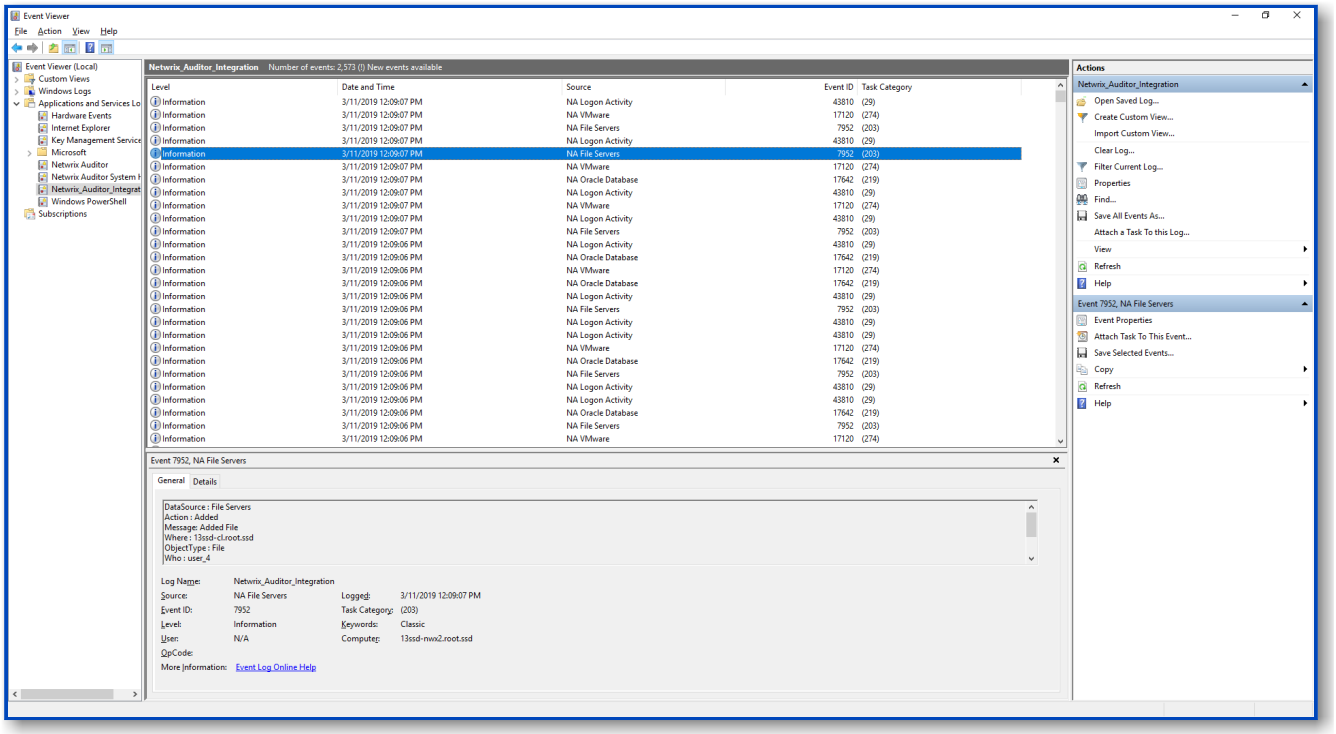
Work with Collected Data

Follow the steps to work with collected data.

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the Event Viewer dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** >Netwrix Auditor Integration log.

Step 3 – Review events.



Now you can augment Windows event log with data collected by the Auditor.

Integration Event Log Fields

This section describes how the add-on fills in the Netwrix Auditor **Integration** event log fields with data retrieved from Activity Records.

The Activity Record structure is described in the Reference for Creating Activity Recordstopic.

Event log field name	Filled in with value	Details
Source	**NA{Data Source Name}** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter.
EventID	**{Calculated by add-on}** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*).
Task Category	**{DataSource ID}** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter.

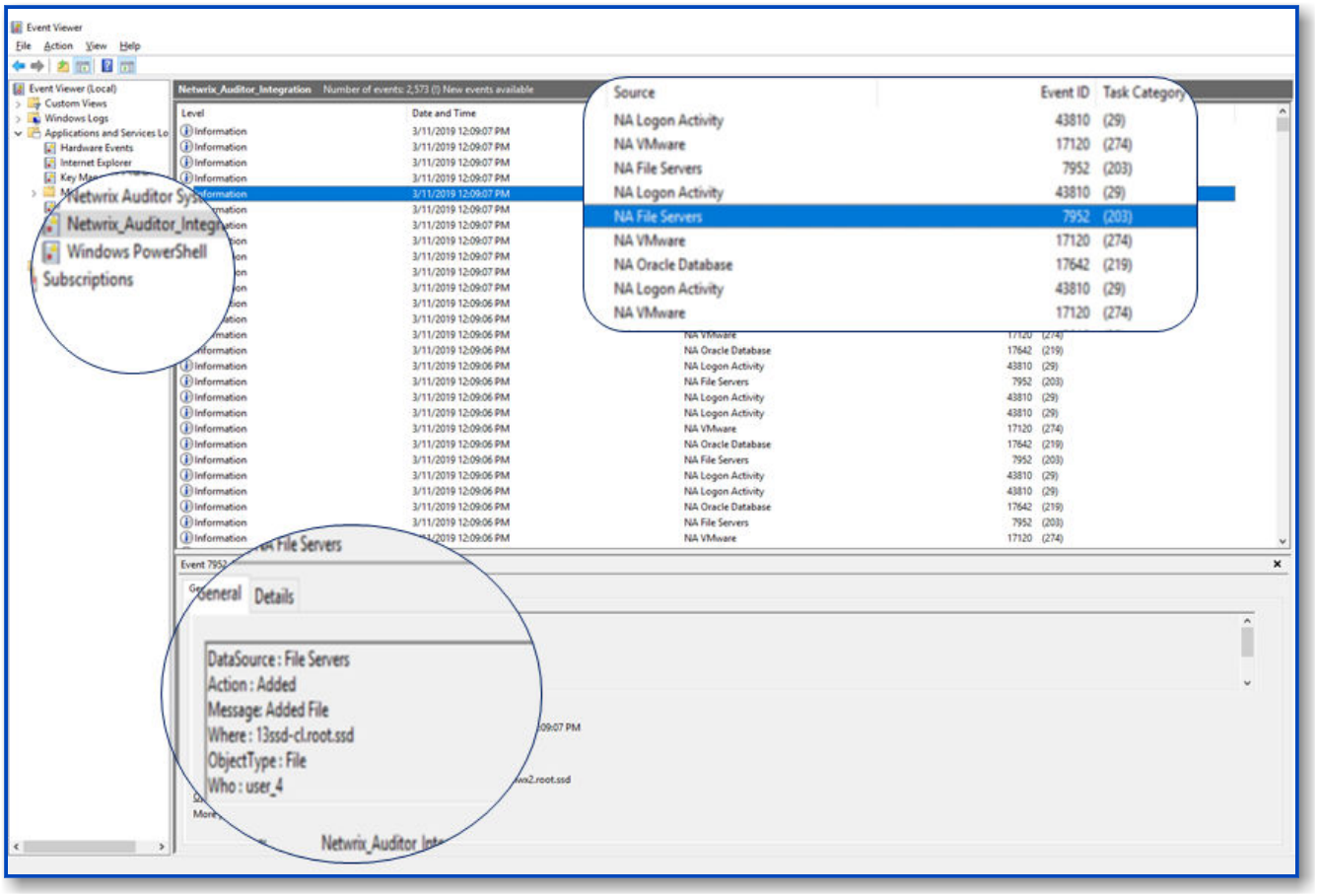
See the Define Parameters topic for additional information.

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}

Entry in EventData	Activity Record field
Action	{Action}
Message	{Action ObjectType}
Where	{Where}
ObjectType	{ObjectType}
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

Details are filled in only if this Activity Record field is not empty.



Nasuni

The add-on works in collaboration with Netwrix Auditor, supplying data about activity on your Nasuni-based devices. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a service, this add-on facilitates the data transition from Nasuni-based systems to Netwrix Auditor. All you have to do is provide connect ion details and specify parsing rules.

On a high level, the add-on works as follows:

1. The add-on listens to the specified UDP ports and captures designated Syslog messages.
2. The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.
3. Using the Integration API, the add-on sends the activity records to the Netwrix Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the NIntegration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor Server side	• The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP **9699** port (default Integration API port) is open for inbound connections. • The user writing data to the Audit Database is granted the **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.
The computer where the add-on will be installed	• The UDP 514 port is open for inbound connections. • .Net Framework 4.7.2 and above is installed. Review the following Microsoft technical article for additional information on how to install .Net Framework 4.7.2: Microsoft .NET Framework 4.7.2 offline installer for Windows.

Configure Logging for

Follow the steps to configure the syslog integration.

Step 1 – Log in to the Nasuni Management Console and go to the **Console Settings** > **Syslog Exports**.

Step 2 – In the Network section, specify the **IP Address** and **Port** and save the configuration.

Step 3 – Configure log settings:

- Set **Send Auditing Messages** to "*ON*";
- Set **Logging Facility** to default "*Local0 (16)*";
- Set **Log Level for Audit Message** to "*Info*".

Step 4 – Enable auditing:

1. On the Volumes tab, open **Auditing**.
2. Choose the volume you wish to be audited and click **Edit Volumes**.
3. Select the **Auditing Enabled** option and choose which Event Types you wish to be reported.
4. Hit the **Save Auditing Settings** button.

Accounts and Rights

By default, the add-on will run under the *Local System* account. The add-on and Auditor must be installed on the same server. If a specific account is designated to run the add-on, it needs local admin privileges.

Considerations and Limitations

- The Add-On must be deployed in the same subnet as Nasuni NAS & File Server Silo Consolidation and Auditor.
- If the monitoring plan name in the <*NetwrixAuditorPlan*> add-on configuration parameter is specified incorrectly, this may lead to temp files generation and, therefore, to inefficient disk space usage.

- If you are using Netwrix Auditor for Network Devices, the 514 UDP port may be already in use, and you should specify another port when configuring the add-on settings (see the Install Add-On and Define Parameters topics for additional information). Another option is to install the add-on and Auditor Server on different machines.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Install Add-On

Follow the steps to install the Add-On:

Step 1 – Navigate to your add-on package.

Step 2 – Unzip the Add-On to a desired folder.

Step 3 – Run the installation package.

Step 4 – Accept the license agreement and follow the instructions of the setup wizard.

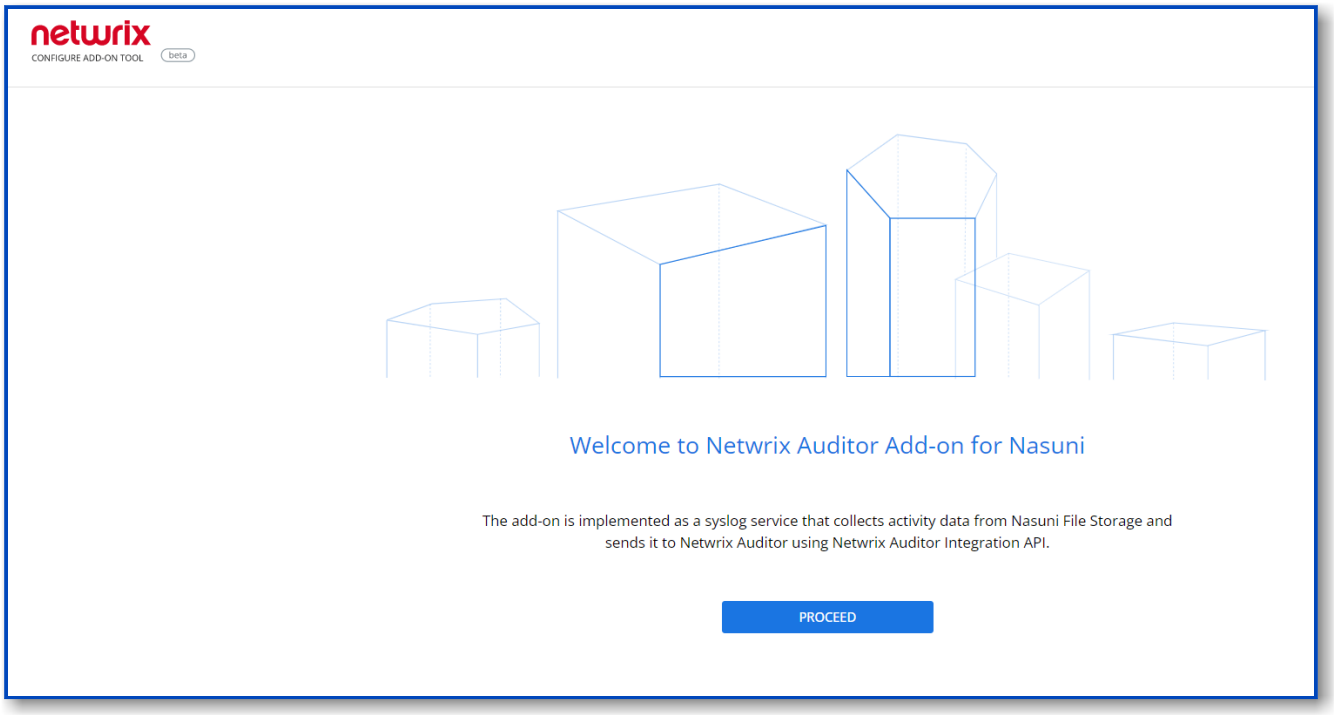
Step 5 – On the **Destination Folder** step, specify the installation folder (*C:\Program Files (x86)\Netwrix Add-ons\<Add-on name>* by default).

Step 6 – Click **Install**.

Step 7 – When done, click **Finish**.

Define Parameters

The configuration wizard opens in the default web browser:



Click **Proceed** and complete the following fields:

Option	Description
Specify General Settings	
Listed UDP port	Specify UDP port for listening incoming events. (**514** by default).
Auditor Endpoint	Auditor Server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hostingAuditor Server and uses default port *9699*. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15*, *EnterpriseNAServer*, *WKS.enterprise.local*).

Option	Description
	To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). **NOTE:** Do not modify the endpoint part (*/netwrix/api*)
Certificate Thumbprint	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Auditor certificate via Windows Certificate Store. • `AB:BB:CC`—Check Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
Specify Active Directory credentials	
Username	Provide the name of the account under which the service runs. Unless specified, the service runs under the account currently logged on.
Password	Provide the password for the selected account.
Auditor Monitoring Plan settings	
Auditor Plan	Unless specified, data is written to **Netwrix_Auditor_API** database and is not associated with a specific monitoring plan.

Option	Description
	Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add- on, make sure a dedicated plan is created in Auditor, the Netwrix **API** data source is added to the plan and enabled for monitoring. Otherwise, the add- on will not be able to write data to the Audit Database.
Auditor Plan Item	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. **NOTE:** Make sure to create a dedicated item inAuditor in advance.
Accept List	
Address	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only. **NOTE:** Events collected from any other source will be ignored.

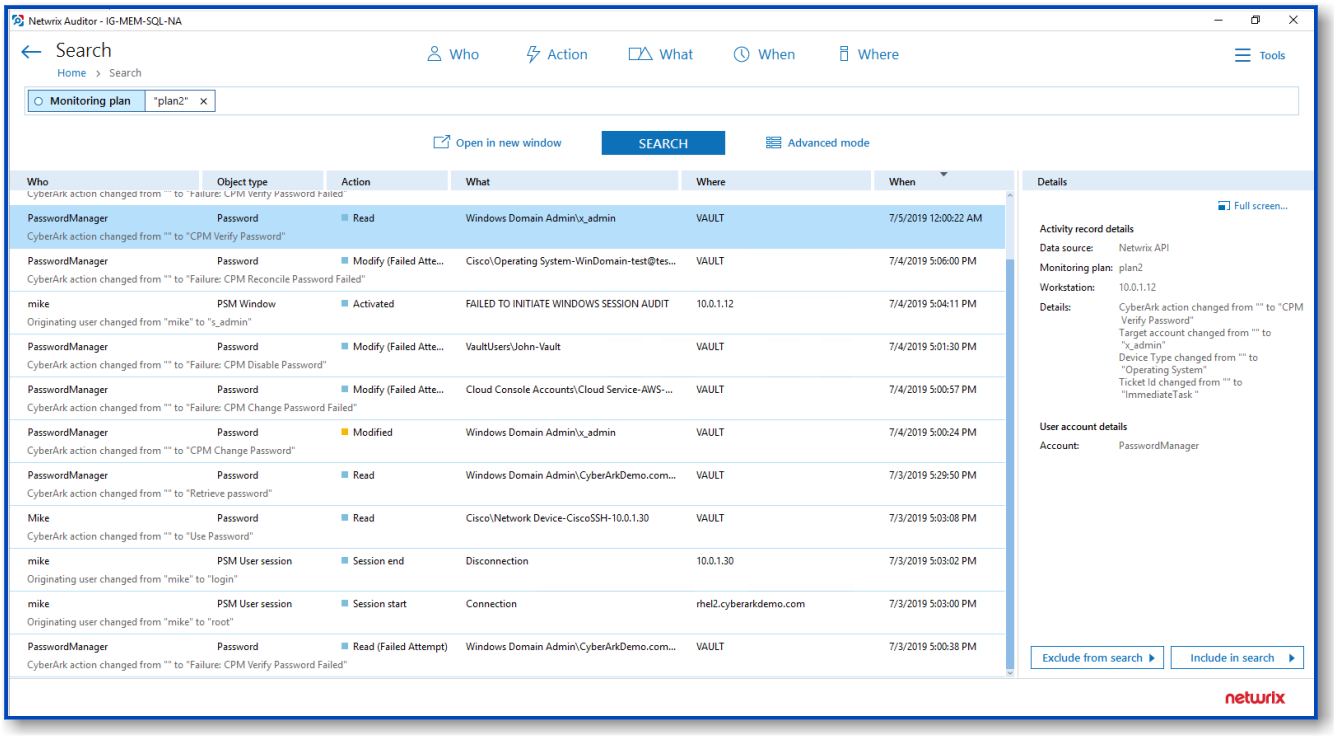
Click **Run** to start collecting data with the Add-On.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You can apply a filter to narrow down your search results to the Netwrix **API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
    - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
    - To create an alert on the specific occurrences, click **Create alert**.
    - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See the following topics for additional information:

- Alerts
- View and Search Collected Data
- Subscriptions

Nutanix AHV

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.

Nutanix AHV is a virtualization platform within the Nutanix Enterprise Cloud architecture. It provides facilities for VM deployment, operation and centralized management. Nutanix AHV is a fully integrated component of the Nutanix Enterprise Cloud.

Virtualization teams, Managed Service Providers and other IT professionals need to detect who does what in the Nutanix Hyperconverged infrastructure. For that, a unified audit trail is required, supporting detailed Nutanix monitoring and effective response to changes.

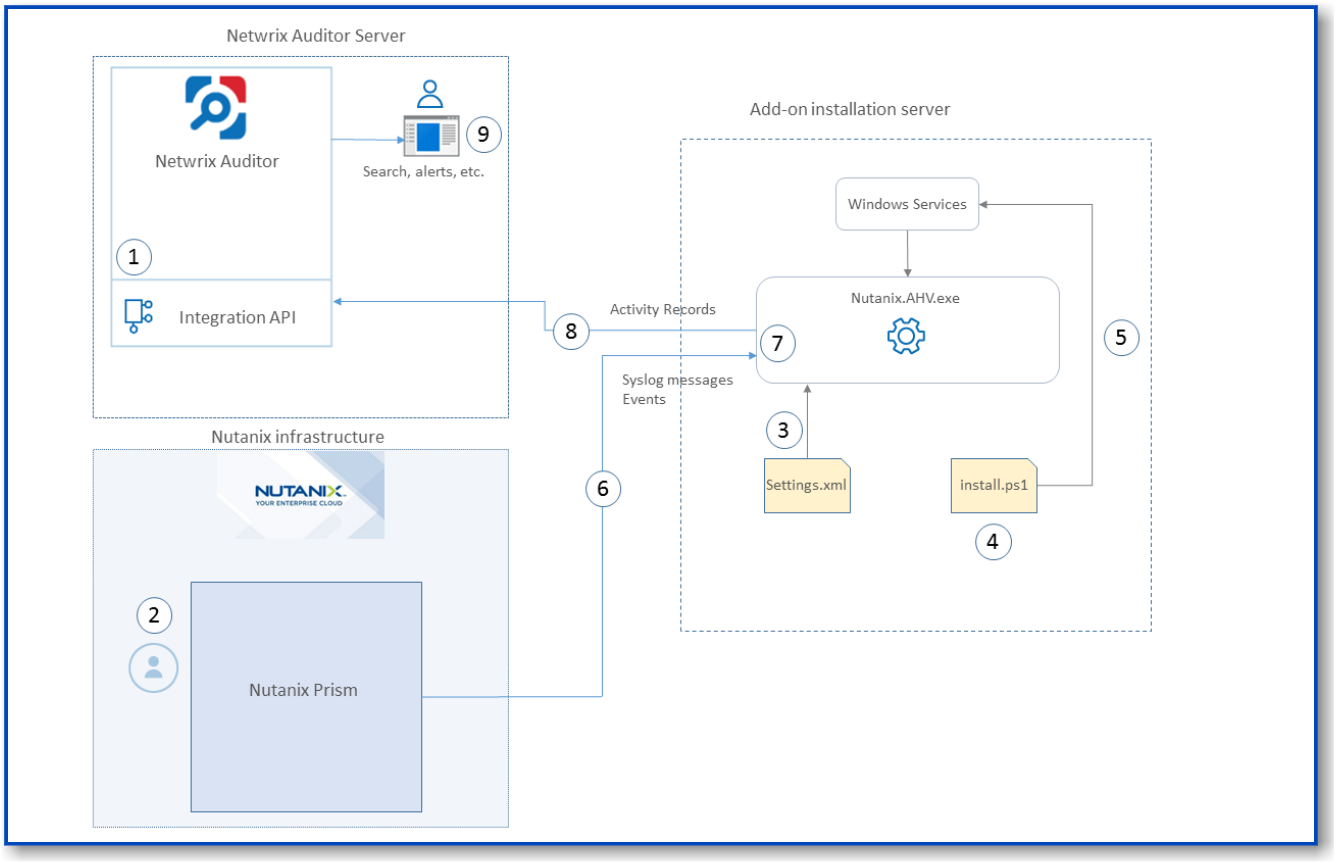
For that purpose, you can use a specially designed add-on that supports audit for Nutanix AHV and Nutanix Prism/Element. The add-on works in collaboration with Auditor, supplying data about operations on your Nutanix AHV to Netwrix database. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost-effective, and helps you keep tabs on your IT infrastructure.

Major benefits:

- Gain a high-level view of the data you store
- Detect unauthorized activity that might threaten your data

How it works

The add-on is implemented as a Syslog service that collects activity data from Nutanix infrastructure and sends it to Netwrix Auditor using the Integration API.



On a high level, the solution works as follows:

1. An IT administrator configures the Integration API settings to enable data collection and storage to Netwrix database for further reporting, search, etc.

   It is recommended to create a dedicated monitoring plan in Netwrix Auditor and add a dedicated item of **Integration** type to it — then you will be able to filter data in reports and search results by monitoring plan/item name.

2. On Nutanix side, the IT administrator prepares a dedicated user account for accessing Nutanix Prism Central/Element and configures Syslog server (IP, port, etc.).
3. The administrator opens the Settings.xml configuration file and specifies the necessary parameters for add-on operation, Netwrix Auditor settings, etc. The add-on will operate as a Syslog listener for Nutanix server.
4. The administrator runs the Netwrix.IntegrationConfiguration.exe file and provides credentials to connect to Prism Central server.

5. The administrator selects the deployment scenario and runs the **install.ps1** PowerShell script file to deploy and configure the add-on components on the target server.

6. In particular, the script deploys and starts **Netwrix Auditor Add-on for Nutanix AHV** Windows Service— this is the main add-on component, responsible for audit data collection and forwarding.

7. The add-on starts collecting and forwarding activity data from Nutanix Prism server: it listens to the specified UDP port and captures designated Syslog event messages and also collects activity data using Nutanix REST API.

   Syslog event data communication is performed using UDP version of Syslog protocol. See the Monitoring Scope topic for additional information on the default list of events supported out-of-the box.

8. The add-on processes the incoming Syslog messages and activity data collected using Nutanix REST API into NAuditor -compatible format (Activity Records). Each Activity Record contains the Who-What-When-Where-Action information (that is, initiator's account, time, action, and other details).
9. Using the Integration API, the add-on sends the activity records to Auditor Server that writes them to the Audit Database and Long-Term Archive. Data is sent periodically, by default every second.

   See the Integration API topic for additional information on the Activity Record structure and capabilities of the Integration API.

10. Users open Auditor Client to work with collected data:
    - Search for file changes using certain criteria
    - Export data to PDF or CSV files
    - Save search results as reports
    - Subscribe to search results
    - Configure and receive alerts

Add-on Delivery Package

The add-on delivery package is a ZIP archive that includes the following files:

File name	Description
Install.ps1	PowerShell script that creates windows service to execute add-on.
Settings.xml	Contains parameters for the add-on service operation.

File name	Description
Netwrix.IntegrationConfiguration.exe	Add-on component responsible for accessing Prism Central server.
Netwrix.Nutanix.IntegrationService.exe	Main add-on component, responsible for audit data collection from Nutanix AHV.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

Where	Prerequisite to check
Auditor Server side	• Auditor version 9.9 or later. • Netwrix Integration API and Audit Database settings are configured properly in Netwrix Auditor. See the Prerequisites and Audit Database topics for additional information. • The **TCP 9699** port must be open on Windows firewall for inbound connections. • User account under which data will be written to the Audit Database requires the **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant it the **Global administrator** role, or add that account to the **NETWRIX AUDITOR Administrators** group.
The machine where the add-on will be installed	• Any of the following Windows OS versions: ◦ Windows Server 2012 R2 (or later) ◦ Windows 8.1 (or later)

Where	Prerequisite to check
	• The **UDP** port must be open on Windows firewall for inbound connections. • .NET Framework versions 4.5 or later
Nutanix Prism server	Nutanix AOS 5.11, 5.15, or 5.20

Accounts and rights

It is recommended to create a dedicated account for running **install.ps1** and **Netwrix Auditor Add-on for Nutanix AHV** (main service of the solution). The service will connect to Auditor Server using this account, so at least the **Contributor** role in Auditor is required for it. See the Role-Based Access and Delegation topic for additional information.

This service account requires the **User Admin** role in Nutanix Prism. You will be prompted for the corresponding set of credentials when you run the **install.ps1** script (see Steps 4 and 5 of the Deploy the Add-On). User name and password for connection to Nutanix Prism server will be then encrypted and stored in the solution configuration.

Considerations and limitations

- By default, the add-on is targeted at a single Nutanix Prism Central/Element server.
- Netwrix add-on must be deployed in the same subnet as Nutanix Prism Central/Element server.
- Please be aware that monitoring of actions performed on the add-on installation server is not supported.

Upgrade Path

To upgrade from versions released earlier than August 2020, do the following:

1. Stop and remove the **Netwrix Auditor Add-on for Nutanix AHV** service.
2. Download and unpack the new add-on package to the same location as the earlier version.

3. Run the **install.ps1** PowerShell script file from the new add-on version on the target server.

Compatibility notice

The add-on is compatible with Nutanix AOS 5.15 and Nutanix AOS 5.20, and with Auditor 10.0 and later.

Deploy the Add-On

Follow the steps to deploy the Add-On:

Step 1 – Prepare Auditorfor data processing.

Step 2 – Configure message forwarding for Nutanix Prism.

Step 3 – Download the Add-On.

Step 4 – Configure Add-On parameters.

Step 5 – Connect to Prism Central Server.

Step 6 – Register the Add-On

Prepare Auditor for Data Processing

In Auditor client, go to the Integrations section and verify Integration API settings:

1. Make sure the **Leverage Integration API** is switched to **ON**.
2. Check the TCP communication port number – default is **9699**.

See the Prerequisites topic for additional information.

By default, activity records are written to *Netwrix_Auditor_API* database which is not associated with a specific monitoring plan.

Optionally, you can create a dedicated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. Target it at Netwrix API data source and enable for monitoring. Add a dedicated item of *Integration* type to the plan for data to be filtered by item name. See the Integration API topic for additional information.

In such scenario, you will need to specify this monitoring plan in the *MonitoringPlan* and *MonitoringPlanItem* attributes in the add-on configuration parameters. See **Step 4** below for details.

Configure Message Forwarding for Nutanix Prism

To provide for interaction and data flow between Nutanix Prism and the Add-On, you should set up the add-on installation server as a remote Syslog listener for Nutanix Prism. For that remote Syslog server, you will need to specify the IP address and port for inbound messages. Depending on Nutanix Prism server you are using (Element/Central), follow the related procedure below.

Procedure for Nutanix Prism Element

Follow the steps If you are using Nutanix Prism Element.

Step 1 – Connect to a Controller VM (or Nutanix Prism) by SSH or via web console and execute the `ncli` command.

Step 2 – Find the IP address of the Controller VM in Nutanix web console under **Settings** > **General** > **Configure CVM**.

Procedure for Nutanix Command-Line Interface

Alternatively, you can download and install the *ncli* (Nutanix command-line interface) on any server in your infrastructure, as described in the Nutanix Command-Line Interface (nCLI) article, and connect to a Controller VM in your cluster.

Follow the steps if you are using Nutanix command-line interface.

Step 1 – Disable it temporarily until you configure a new remote Syslog listener. By default, the remote Syslog listening server is enabled. For that, run the following command in ncli:

```
ncli> rsyslog-config set-status enable=false
```

Step 2 – Create a remote Syslog server — a remote server that will operate as a Syslog listener, receiving the Syslog messages from Nutanix server. In the integration solution deployment, it will be the add-on installation server. Run the following command in *nlci*:

```
ncli> rsyslog-config add-server name=<CustomServerName> ip-
address=<RemoteIP> port=<Port> network-protocol=udp
```

here:

- `CustomServerName` — remote server that will receive the syslog messages (i.e., server on which the add-on will be deployed)
- `RemoteIP` — remote server IP address
- `Port` — Destination port number on the remote server

Step 3 – To ensure the server was created successfully, review the list of servers. For that, run the following command:

```
ncli> rsyslog-config ls-servers
```

The server will be added to the cluster automatically.

Step 4 – Instruct the AUDIT module of Nutanix solution to forward its log information to the new remote syslog listener, and specify the logging level. For that, run the following command:
`ncli> rsyslog-config add-module server-name=<CustomServerName> module-name=AUDIT include-monitor-logs=false level=notice`

Step 5 – Finally, enable syslog forwarding to remote server: `ncli> rsyslog-config set-status enable=true`

This syslog server will be added to the cluster automatically.

Procedure for Nutanix Prism Central

First, provide the new remote Syslog server settings to Nutanix Prism server that will forward Syslog messages. For that, follow the steps below:

Step 1 – Log in to Nutanix Prism Central.

Step 2 – Select **Settings** > **Email and Alerts** > **Syslog Server**.

Step 3 – Click **Configure Syslog Server**.

Step 4 – Enter remote Syslog server settings you specified at Step 2:

- **Server Name** — name of the remote server.
- **IP Address** — server IP address.
- **Port**— port for incoming messages

Step 5 – Select **UDP** as communication protocol.

Step 6 – Click **Configure**.

Next, for the most detailed logs to be sent to remote Syslog server, set the logging level in Prism to *5* (*Notice*). For that, follow the steps below:

Step 1 – Select **Data Source** and click **Edit**.

Step 2 – Select **Audit** module and select **5 - Notice** level.

Step 3 – Finally, click **Save**.

Download the Add-On

Download the distribution package from the Netwrix website and unpack it to a folder on the computer where you plan to deploy the add-on.

Customers who are logged in to the Netwrix Customer Portal can download the latest version of their software products from the My Products page: https://www.netwrix.com/my_products.html. See the Customer Portal Access topic for information on how to register for a Customer Portal account.

Configure Add-On Parameters

Open the add-on folder and edit the **settings.xml** file to configure the add-on parameters:

Parameter	Default value	Description
NetwrixAuditorIntegration		
NetwrixAuditorEndpoint	https://localhost:9699/netwrix/api/v1/activity_records	Auditor server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**. If you want to run the add-on on another machine, provide a name of the computer where Auditor

Parameter	Default value	Description
		Server resides (e.g., *172.28.6.15, EnterpriseNAServer, WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). Do not modify the endpoint part (/ netwrix/api . . . .)
CertificateThumbprint	NOCHECK	Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Netwrix Auditor certificate via Windows Certificate Store. • `AB:BB:CC.`—Check Netwrix Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Netwrix Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
DateTimeFormat	yyyy-MM-ddTHH:mm:ssZ	Auditor time format. By default, set to zero offset.
MonitoringPlan	—	Unless specified, data is written to Netwrix_Auditor_API database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this

Parameter	Default value	Description
		case, data will be written to a database linked to this plan. If you select a plan name in the add-on, make sure a dedicated plan is created in Auditor, the Netwrix API data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
MonitoringPlanItem	—	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. Make sure to create a dedicated item in Auditor in advance.
UserName	Current user credentials	Credentials to access Auditor server. Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor server, specify the account name in the *DOMAIN\username* format.
Password	Current user credentials	Unless specified, the service runs with the current user credentials. Provide a different password if necessary.

Parameter	Default value	Description
ARsNumberAtTime		Maximum number of Audit Records that can be sent to Auditor at a time.
ARsSendingPeriodicity		Periodic time interval for sending Activity Records (in seconds).
PauseWhenSendingFailed		Pause after a failed attempt to send Activity Records (in seconds).
DataCollection		
ListenUDPPort	514	UDP port for receiving incoming Syslog messages. Make sure that this port is not used by any other add-ons or applications (for example, Netwrix Auditor for Network Devices); otherwise specify another port here.
StateUpdatingPeriodicity		Periodic time interval for updating state of clusters (in seconds).
EventsReadingPeriodicity		Periodic time interval for reading events (in seconds). Target endpoint: */api/nutanix/v2.0/events*

Parameter	Default value	Description
PageLength		The number of objects loaded with one request.
ShortTermFolder		Short term folder for collected data (full or local path).

If you modify parameters in the **settings.xml** file, remember to save the changes and then restart the **NETWRIX AUDITOR Add-on for Nutanix AHV** service for them to take effect.

If you need to change user name or password for accessing Prism Central, you should run Netwrix.IntegrationConfiguration.exe file that will prompt you for the new credentials (see step 5 below). Then restart the Netwrix Auditor Add-on for Nutanix AHV service for the changes to take effect.

Connect to Prism Central Server

Run the Netwrix.IntegrationConfiguration.exe file and specify the following:

- Prism IP address – IP address of Prism Cental server.
- User name – Specify a user name to connect to Prism Central server.
- Password – Specify password fof the account used to connect to Prism Central server.

These parameters will be configured automatically by **install.ps1** script. If you need to modify it later, use this configurator from the add-on package.

Credentials for connection to Nutanix Prism server will be then encrypted and stored in the solution configuration. Consider that user account should have the **User Admin** role in Nutanix Prism.

Register the Add-On

Run the **install.ps1** PowerShell script to register the add-on service. You will be also prompted to specify credentials for accessing Nutanix Prism Central. These credentials will be encrypted

and used for secure communication. If you need to modify them later, run the Netwrix.IntegrationConfiguration.exe file from the add-on package.

Deployment Scenarios

The Add-On can run on any computer in your environment, except for the machine where your Nutanix Prism Central/Element runs. Depending on the deployment scenario you choose, you will need to define a different set of parameters

Possible deployment options are as follows:

1. Add-on running on the same machine as Auditor Server.
2. Add-on running on the remote machine.

Example 1

- The add-on runs on the Auditor Server.
- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/
activity_records↙NetwrixAuditorEndpoint>

<NetwrixAuditorUserName↗

<NetrixAuditorPassword↗
```

Configuration parameters **NetwrixAuditorUserName** and **NetwrixAuditorPassword** are not required.

You will be prompted for the corresponding set of credentials (user name and password) when you run the **install.ps1** script. For that, use the Netwrix Auditor **Add-on for Nutanix AHV Configurator** tool (see steps 4 and 5 of the Deploy the Add-On). Credentials for connection to Nutanix Prism server will be then encrypted and stored in the solution configuration. Consider that user account should have the **User Admin** role in Nutanix Prism.

Example 2

- The add-on runs on the Auditor Server with the explicitly specified user credentials, or on the remote machine.

- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/
activity_records↙NetwrixAuditorEndpoint>

<NetwrixAuditorUserName>SecurityOfficer↙NetwrixAuditorUserName>

<NetwrixAuditorPassword>NetwrixUser↙NetwrixAuditorPassword>
```

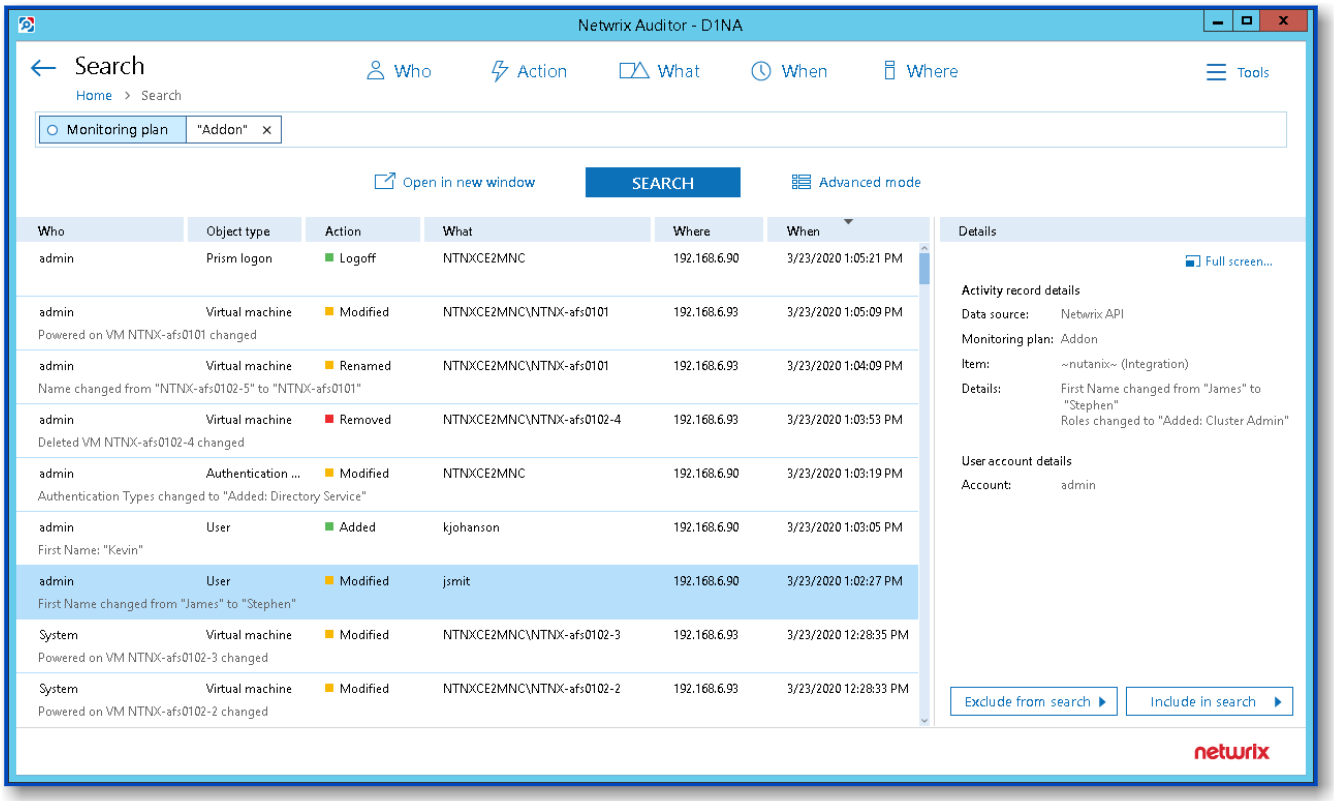
Netwrix recommends to create a special user account with permissions to access Auditor and Nutanix server.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You might want to apply a filter to narrow down your search results to the Netwrix**API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See the following topics for additional information:

- Alerts
- View and Search Collected Data
- Subscriptions

Monitoring Scope

Review a full list of object types and activities monitored on Nutanix Prism with the add-on.

Object	Action	Property
Virtual Machine[1]	Create/Delete Clone Migrate Rename State change (Power off/on, Pause etc.) Restore from snapshot Hardware Configuration change	Name MAC Address VLAN Name Connection State Number Of Processors Cores Per Processor Memory Size (MiB) Disk Size (Bytes) Host IP

Object	Action	Property
Host (Node) [2]	Add[3]/Remove[4]	IP[5]
Host Cluster	-	-
VM Network (Subnet)	-	-
Local User[2]	• Create/Delete • Properties change[6] • Roles change[6] • Log in/out • Password Change	• Username • First Name[6] • Last Name[6] • Email[6] • Language[6] • Roles[6]
Authentication Configuration[2]	• Authentication type change	• Authentication Types

[1]— Syslog

[2] — Events (API v2.0)

[3]— User not applicable

[4]—Host remove event consist of 2 events (see Appendix B):

- Host marked for removal: this event has a “Who”
- Host deleted: this event occurs when the host deletion task completes.

[5]—The host add event contains the IP address of the host Controller VM, and not the host IP address.

[6]—UI API

.

Maintenance and Troubleshooting

If you cannot see collected data in Auditor, check the following:

- Service account has sufficient rights to access Auditor.
- In Auditor settings, go to the **Integrations** section and make sure the **Leverage Integration API** is switched to **ON**. Check the communication port number – default is **9699**.
- If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
- Verify the parameters you provided in **settings.xml**.

Also, remember that events from the remote Syslog server (add-on installation server) are not collected.

Currently, the add-on supports only one Prism installation (Central or Element). To monitor more than one Prism Central/Element, you can copy the add-on to another folder, configure **settings.xml** as described in this document and modify **install.ps1** to rename the service:

Step 1 – Deploy one more add-on instance to the server where the first add-on instance is already installed. Be sure to use a different installation folder.

Step 2 – Open **settings.xml** and configure the new add-on instance to work with the second Prism server.

Step 3 – Open **install.ps1** for the new add-on for edit.

Step 4 – Modify the default service name:

```
$name = "enter_new_name"
```

Step 5 – Save and then launch the updated **install.ps1** file.

Okta

The add-on works in collaboration with Netwrix Auditor, supplying data about activity on your Okta-based devices. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a service, this add-on facilitates the data transition from Okta-based systems to Netwrix Auditor. All you have to do is provide connect ion details and specify parsing rules.

On a high level, the add-on works as follows:

1. The add-on listens to the specified UDP ports and captures designated Syslog messages.

2. The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.

3. Using the Integration API, the add-on sends the activity records to the Netwrix Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the NIntegration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor Server side	• .NET Framework 4.5 or later is installed. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP **9699** port (default Integration API port) is open for inbound connections. • The user writing data to the Audit Database is granted the **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.

Accounts and Rights

By default, the add-on will run under the *Local System* account. So, if the add-on and Auditor will be running on different machines, the corresponding computer account will require at least the **Contributor** role in Auditor. See the Role-Based Access and Delegation topic for additional information.

In case the add-on and Auditor are installed on the same server, no special settings are needed.

Considerations and Limitations

- The Add-On must be deployed in the same subnet as Okta and Auditor.
- If the monitoring plan name in the <*NetwrixAuditorPlan*> add-on configuration parameter is specified incorrectly, this may lead to temp files generation and, therefore, to inefficient disk space usage.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Deploy the Add-On

Follow the steps to deploy the Add-On.

Step 1 – Download the distribution package **Netwrix_Auditor_Add-on_for_Okta.zip**.

Step 2 – Unpack it to a folder on the computer where you plan to deploy the add-on.

Remember, deploying the add-on on the same machine with the *Auditor* Server.

Step 3 – Run the **NetwrixOktaAddon.exe** and follow the installation steps:

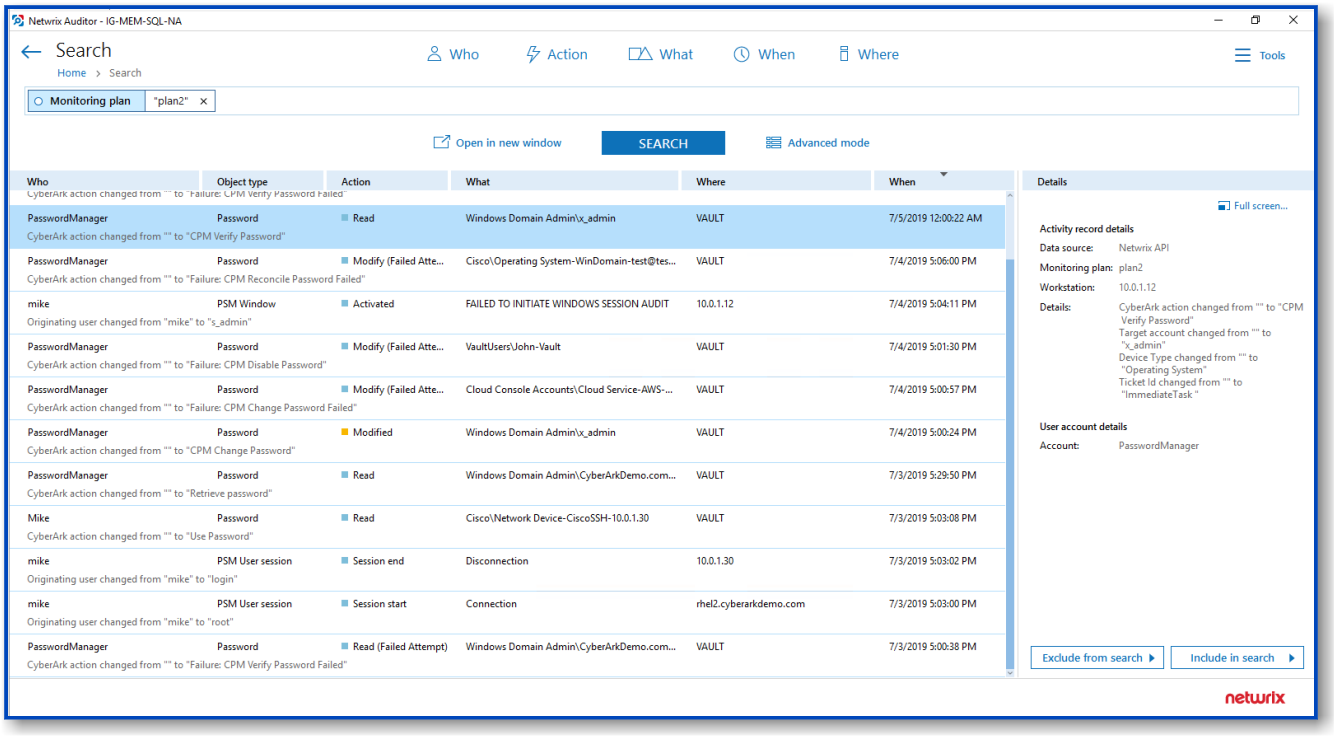
Option	Description
Okta Connection Settings	Specify server address in the '*https://example.okta.com/*' format and SSWS token.
Netwrix Connection Settings	Specify settings to connect to Auditor: • Server address – provide the address of the Auditor Server host. • Username – Provide the name of the account used to connect to Auditor. • Password – Provide password for this account.
Summary	Review the Add-On settings.

Work with Collected Data

To leverage data collected with the add-on, you can do the following in Auditor:

- Search for required data. For that, start Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You can apply a filter to narrow down your search results to the Netwrix **API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
    - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
    - To create an alert on the specific occurrences, click **Create alert**.
    - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See the following topics for additional information:

- Alerts
- View and Search Collected Data
- Subscriptions

Privileged User Monitoring on Linux and Unix Systems

The add-on works in collaboration with Auditor, supplying data about privileged user activity on Linux and Unix. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost effective, and helps you keep tabs on privilege elevation on your Linux and Unix-based devices. For example, it helps monitor the usage of SUDO as well as remote access with openSSH.

On a high level, the add-on works as follows:

1. The add-on listens to the specified UDP ports and captures designated Syslog messages.

   Out of the box, messages from Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu 16 are supported. For other distributions, deployment of the rsyslog package may be required. You can edit the add-on configuration to extend the captured message list.

2. The add-on processes these events into Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.

3. Using the Integration API, the add-on sends the activity records Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor Server side	• The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP **9699** port (default Integration API port) is open for inbound connections. • The user writing data to the Audit Database is granted the **Contributor** role in Auditor. See the

On...	Ensure that...
	Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.
The computer where the service will be installed	• The UDP 514 port is open for inbound connections. • .Net Framework 4.7.2 and above is installed. Review the following Microsoft technical article for additional information on how to install .Net Framework 4.7.2: Microsoft .NET Framework 4.7.2 offline installer for Windows.
The target syslog-based platform	The **Syslog daemon** is configured to redirect events. The procedure below explains how to configure redirection: **NOTE:** Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu 16 are supported out of the box. For other distributions, deployment of rsyslog package may be required. • On Red Hat Enterprise Linux 7: • Open the **/etc/rsyslog.conf** file. • Add the following line: `auth.*;authpriv.* @name:514;RSYSLOG_SyslogProtocol23Format` where `name` is a FQDN, NetBIOS name or IP address of the computer where Netwrix Auditor Server is installed. For example:

On...	Ensure that...
	`auth.*;authpriv.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format` • Launch the **RHEL console** and execute the following command: `service rsyslog restart`. • On Ubuntu 16: • Navigate to the **/etc/rsyslog.d/50-default.conf** file. • Add the following line: `auth.*;authpriv.* @name:514;RSYSLOG_SyslogProtocol23Format` where `name` is a FQDN, NetBIOS name or IP address of the computer where Netwrix Auditor Server is installed. For example: `auth.*;authpriv.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format` • Launch the **UBUNTU console** and execute the following command: `service rsyslog restart`.

See the the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Integration API

Install the Add-On

To install the Add-On, perform the following steps:

Step 1 – Navigate to your add-on package.

Step 2 – Unzip the Add-On to a desired folder.

Step 3 – Run the installation package.

Step 4 – Accept the license agreement and follow the instructions of the setup wizard.

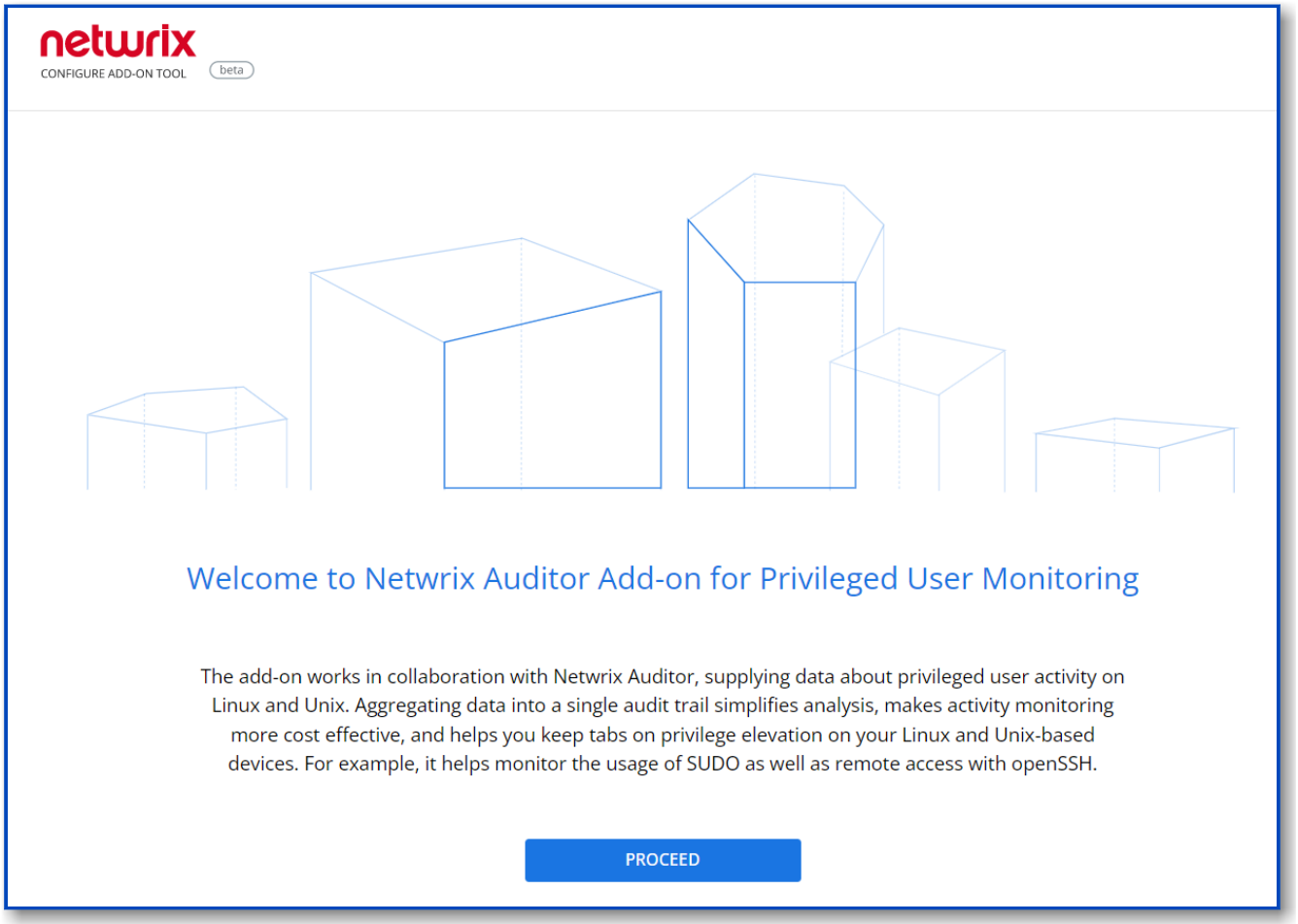
Step 5 – On the **Destination Folder** step, specify the installation folder (*C:\Program Files (x86)\Netwrix Add-ons\<Add-on name>* by default).

Step 6 – Click **Install**.

Step 7 – When done, click **Finish**.

Define Parameters

The configuration wizard opens in the default web browser:



Click **Proceed** and complete the following fields:

Option	Description
Specify General Settings	
Listed UDP port	Specify UDP port for listening incoming events. (**514** by default).
Auditor Endpoint	Auditor Server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hostingAuditor Server and uses default port *9699*. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15*, *EnterpriseNAServer*, *WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). **NOTE:** Do not modify the endpoint part (*/netwrix/api*)
Certificate Thumbprint	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Auditor certificate via Windows Certificate Store. • `AB:BB:CC`—Check Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
Specify Active Directory credentials	

Option	Description
Username	Provide the name of the account under which the service runs. Unless specified, the service runs under the account currently logged on.
Password	Provide the password for the selected account.
Auditor Monitoring Plan settings	
Auditor Plan	Unless specified, data is written to **Netwrix_Auditor_API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add- on, make sure a dedicated plan is created in Auditor, the Netwrix **API** data source is added to the plan and enabled for monitoring. Otherwise, the add- on will not be able to write data to the Audit Database.
Auditor Plan Item	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. **NOTE:** Make sure to create a dedicated item inAuditor in advance.
Accept List	
Address	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only.

Option	Description
	NOTE: Events collected from any other source will be ignored.

Click **Run** to start collecting data with the Add-On.

Work with Collected Data

Follow the steps to work with collected data:

Step 1 – Start the Auditor client and navigate to **Search**.

Step 2 – Click **Search**.

NOTE: You might want to apply a filter to narrow down your search results to the NetwrixAPI data source only.

Qumulo

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.

Qumulo Hybrid Cloud File Storage delivers real-time visibility, scale, and control of data across on-prem and cloud. Qumulo customers understand storage at a granular level; programmatically configure and manage usage, capacity, and performance; and are continuously delighted with new capabilities, 100% usable capacity and direct access to experts. More information at www.qumulo.com.

To control who does what in the IT infrastructure that includes Qumulo Hybrid Cloud File Storage, organizations need to monitor file-related activity. A typical case is when a user has renamed a directory at the top level, and other users are unable to locate their files anymore. Thus, IT specialists require a way to monitor, search and get notifications on certain file activity so that they can take corrective measures.

For that purpose, you can use a specially designed Netwrix Auditor add-on for Qumulo. It works in collaboration with Netwrix Auditor, supplying data about file operations on your Qumulo

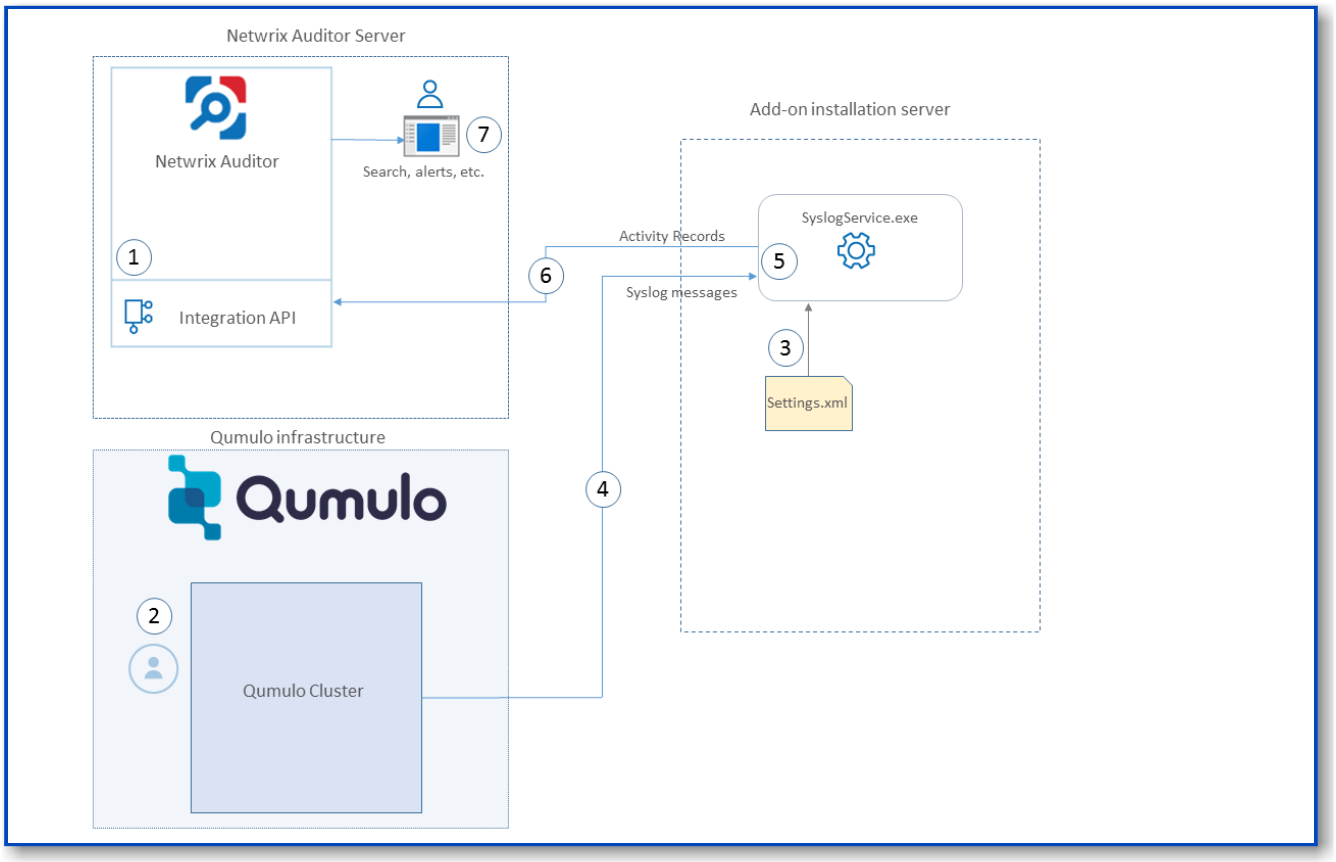
Cluster to Netwrix database. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost-effective, and helps you keep tabs on your IT infrastructure.

Major benefits:

- Gain a high-level view of the data you store
- Detect unauthorized activity that might threaten your data

How it Works

The add-on is implemented as a Syslog service that collects activity data from Qumulo Cluster and sends it to Auditor using the Integration API.



On a high level, the solution works as follows:

1. An IT administrator configures the Integration API settings to enable data collection and storage to the Netwrix database for further reporting, search, etc.

It is recommended to create a dedicated monitoring plan in Netwrix Auditor and add a dedicated item of **Integration** type to it — then you will be able to filter data in reports and search results by monitoring plan/item name.

2. On the Qumulo side, the IT administrator prepares Syslog configuration settings.
3. Then the administrator opens the settings.xml configuration file and specifies the necessary parameters for add-on operation, including Qumulo Cluster as the source of Syslog messages, Auditor settings, etc. The add-on will operate as a Syslog listener for the Qumulo Cluster.

4. The add-on starts collecting and forwarding activity data: it listens to the specified TCP port and captures the designated Syslog messages. Data communication is performed using the TCP version of Syslog protocol.

5. The add-on processes these Syslog messages into Auditor-compatible format (Activity Records). Each Activity Record contains the "Who-What-When-Where-Action" information (that is, initiator's account, time, action, and other details).
6. Using the Integration API, the add-on sends the activity records to Auditor Server that writes them to the **Netwrix_Auditor_API** database (SQL server database) and file-based Long-Term Archive. Data is sent periodically, by default every 5 seconds. For more information on the Activity Record structure and capabilities of the Integration API, refer to the Integration API topic.
7. Users open Auditor Client to work with collected data:
   - Search for file changes using certain criteria
   - Export data to PDF or CSV files
   - Save search results as reports
   - Subscribe to search results
   - Configure and receive alerts

Add-on Delivery Package

The add=on delivery package is a ZIP archive that includes the following files:

File name	Description
install.cmd	Command file that installs and enables Netwrix Syslog service.
settings.xml	Contains parameters for the add-on service operation.

File name	Description
SyslogService.exe	The Syslog service – main add-on component, implemented as a Syslog service.
SyslogService.exe.config	Add-on configuration data.

You will also need the **qumulo.xml** file that contains rules for processing Qumulo events. This file is shipped separately.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

Where	Prerequisite to check
The Auditor Server side	• Auditor version is 9.96 or higher. • Integration API settings and **Netwrix_Auditor_API** database are configured properly. See Configure Integration API and Audit Database. • The **TCP 9699** port must be open on Windows firewall for inbound connections. • User account under which data will be written to **Netwrix_Auditor_API** database requires the *Contributor* role in Netwrix Auditor. See Role-Based Access and Delegation. Alternatively, you can grant it the **Global administrator** role, or add that account to the *Netwrix Auditor Administrators* group.

Where	Prerequisite to check
The machine where the add-on will be installed	• The **TCP 9905** port must be open on Windows firewall for inbound connections. • .NET Framework 4.5 or later must be installed.
Qumulo Cluster	Qumulo core version 3.0.5.

Accounts and rights

It is recommended to create a dedicated account for running **install.cmd** and **SyslogService.exe**. The service will connect to Auditor Server using this account, so at least the **Contributor** role in Auditor is required for it. See Role-Based Access and Delegation for more information.

Considerations and limitations

- For events received with NFS3 protocol, the *posix uid* will be displayed instead of the initiator's account name in the "*Who*" field of the Auditor search results and activity summaries.
- If the initiator's account name could not be resolved, then Windows SID or Qumulo auth ID will be displayed in the the "*Who*" field of the search results and activity summaries.
- Currently, not every detail about permission and attribute changes may be provided by Qumulo Cluster, so they cannot be reported by Auditor.
- If the monitoring plan name in the add-on configuration parameter is specified incorrectly, this may lead to temp files generation and, therefore, to inefficient disk space usage.

Compatibility Notice

(Undefined variable: Add-on.Addon_Qumulo) is compatible with Qumulo core 3.0.5 and with Netwrix Auditor 9.96 and later.

Deployment Scenarios

The Add-On can run on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed, or on a remote server. Depending on the deployment scenario you choose, you will need to define a different set of parameters

Netwrix suggests the following scenarios:

Scenario	Example: Parameters updated in default settings.xml
The add-on runs on the Netwrix Auditor Server with the current user credentials.	<Address>172.28.4.15↙Address> <Address>172.28.3.18↙Address>
The add-on runs on the Netwrix Auditor Server with the explicitly specified user credentials.	<NetwrixAuditorUserName>SecurityOfficer↙NetwrixAuditorUserName> <NetwrixAuditorPassword>NetwrixUser↙NetwrixAuditorPassword> <Address>172.28.4.15↙Address>
The add-on runs on a remote computer. Data is written to a remote Netwrix Auditor repository with the current user credentials.	<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/activity_records↙NetwrixAuditorEndpoint> <Address>172.28.4.15↙Address>
The add-on runs on a remote computer. Data is written to a remote Netwrix Auditor repository with the explicitly specified user credentials.	<NetwrixAuditorEndpoint>https://172.28.6.19:9699/netwrix/api/v1/activity_records↙NetwrixAuditorEndpoint> <NetwrixAuditorUserName>NetwrixUser↙NetwrixAuditorUserName>

Scenario	Example: Parameters updated in default settings.xml
	<NetwrixAuditorPassword>NetwrixIsCool↙NetwrixAuditorPassword> <Address>172.28.4.15↙Address>

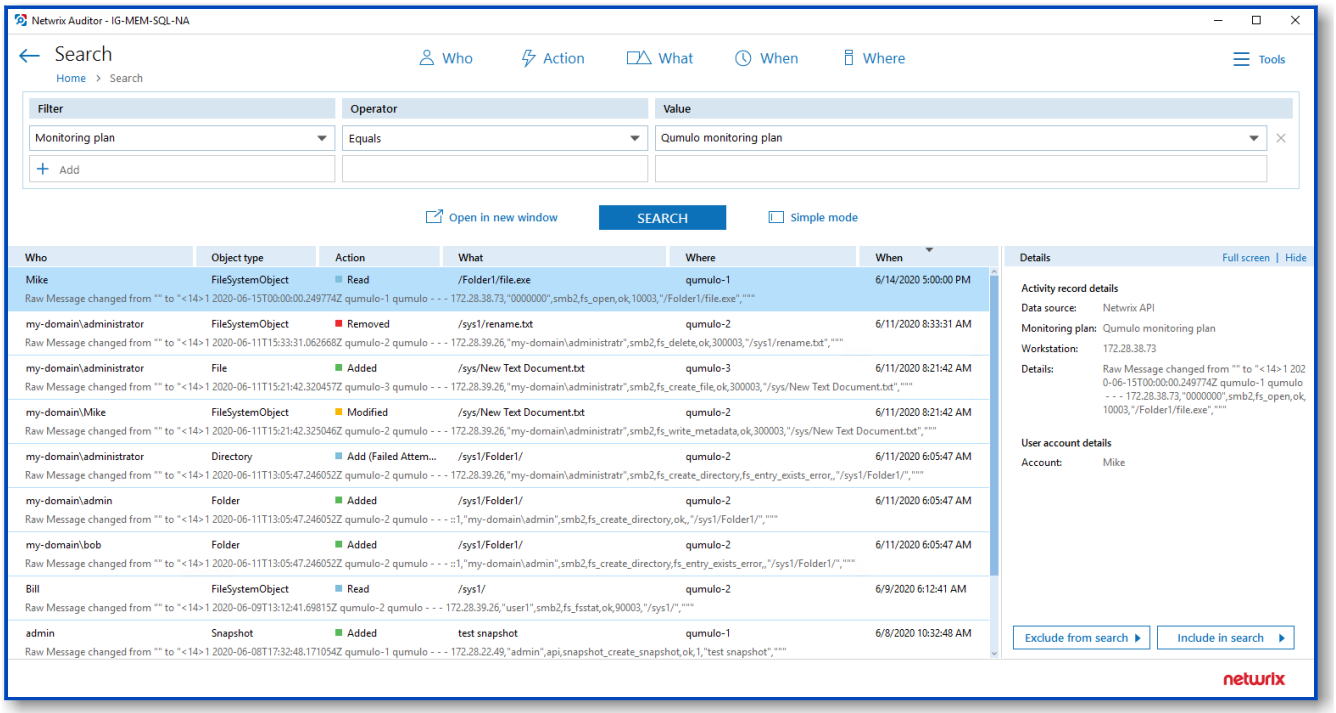
For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Working with Collected Data

To leverage data collected with the add-on, you can do the following in Netwrix Auditor:

- Search for required data. For that, start Netwrix Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

You might want to apply a filter to narrow down your search results to the Netwrix API data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

Add-On Parameters

To configure the add-on parameters, you need to edit the **settings.xml** file in the add-on folder. You must define connection details: Netwrix Auditor Server host, user credentials, etc.

Most parameters are optional, the service uses the default values unless parameters are explicitly defined (<*parameter*>**value**</*parameter*>). You can skip or define parameters depending on your execution scenario and security policies.

Parameters in **settings.xml** can be grouped as follows:

- General parameters that affect add- on execution. They are listed in the table below.
- Settings for a certain event source (within the *Source* section) that can override general settings.
- Internal parameters that should not be modified in most cases. They are listed in .

Parameter	Default value	Description
General parameters		
ListenTcpPort	9905	Specify TCP port for listening incoming syslog events.
NetwrixAuditorEndpoint	https://localhost:9699/netwrix/api/v1/activity_records	Netwrix Auditor Server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**.

Parameter	Default value	Description
		If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15, EnterpriseNAServer, WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*). Do not modify the endpoint part (/ netwrix/api . . . .)
NetwrixAuditorCertificateThumbprint	NOCHECK	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Netwrix Auditor certificate via Windows Certificate Store. • `AB:BB:CC.`—Check Netwrix Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Netwrix Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN\username* format. The account must be assigned the Contributor role in Netwrix Auditor.

Parameter	Default value	Description
NetwrixAuditorUserPassword	Current user credentials	Unless specified, the service runs with the current user credentials. Provide a different password if necessary.
NetwrixAuditorDateTimeFormat	yyyy-MM-ddTHH:mm:ssZ	Netwrix Auditor time format. By default, set to zero offset.
NetwrixAuditorPlan	—	Unless specified, data is written to Netwrix_Auditor_API database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. If you select a plan name in the add-on, make sure a dedicated plan is created in Auditor, the Netwrix API data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
NetwrixAuditorPlanItem	—	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. Make sure to create a dedicated item in Netwrix Auditor in advance.
EventStorePath	—	Select where to store temporary files of syslog messages before the add-on sends them to Netwrix Auditor Server.

Parameter	Default value	Description
		Netwrix recommends not to store these files out of the service directory.
LogLevel	error	Specify logging level: • none • info • warning • error (used by default) • debug
WriteCriticalIssues ToEventLog	0	Instructs the add-on to write important events (like service start or critical issue) not only to its own log but also to Netwrix event log. • 1=yes • 0=no (default)
Parameters within SourceList You can specify parsing rules for each specific event source and define parameters to override general settings, such as time zone, default plan name, etc.		
NetwrixAuditorPlan	—	When specified, overrides the general settings.
NetwrixAuditorPlanItem	—	When specified, overrides the general settings.
DefaultTsTimezone	—	Define the time zone of syslog events. By default, set to zero offset (UTC).
AppNameRegExp	—	Define a custom regular expression pattern to retrieve the application name from your syslog messages. Unless specified, RFC 3164/5424 format is used.

Parameter	Default value	Description
		If you provide a pattern for application name, this name will be used to determine what rule file will be used to parse syslog messages. The pattern you provide here must match the application name in your custom rule file.
AppNameGroupID	—	Define application name value by Group ID only if messages are not formatted in accordance with RFC 3164/5424. Otherwise, leave the default value.
RuleFileList PathFile	qumulo.xml	Specify paths to XML file(s) with regular expression parsing rules. You can create a custom file or use rules provided out of the box. Currently, the **qumulo.xml** rules file is provided by Qumulo. You can specify several rule files. The service will check if the AppName parameter in the first rule file matches the **AppNameRegExp** and **AppNameGroupID** regular expression in this file. If not, the service will proceed to the next rule file.
AcceptList Address	—	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only. Events collected from any other source will be ignored. The Address parameter may be followed by optional attributes that

Parameter	Default value	Description
		override parameters specified above: • naplan—A name of associated monitoring plan • naplanitem—A name of associated item • tstimezone—Timezone for Qumulo Cluster For example: <Address naplan="NFSmonitoring" naplanitem="NFS" tstimezone="GMT StandardTime">172.28.3.15 </Address>

After you modify parameters in the **settings.xml** file, remember to save the changes and then restart (Undefined variable: Add-on.Addon_Qumulo) service (**SyslogService.exe**) for them to take effect.

Add-on Internal Parameters

Internal parameters listed in the table below are intended for performance tuning. In most cases the default values should be used.

Parameter	Default value	Description
EventsFromMemoryFirst	1	Instructs the add-on to save events to temporary storage only if there is no free space in queues: • 1=yes • 0=no

Parameter	Default value	Description
ConcurrentSend	-1	Specifies number of threads for concurrent forwarding of events to Auditor. Default value is -1 (switch off concurrent forwarding).
ListenTcpAddress	0.0.0.0	Defines destination IP address. In case of multiple network cards, you can specify certain IP address here to listen to its messages only.
SenderSleepTime	30	Specifies retry interval in seconds to send messages to Auditor (30 - 3600 seconds).
TaskLimit	8	Specifies number of threads and queues for concurrent handling of events.
QueueSizeLimit	1000	Specifies maximum number of events to keep in queue before saving to temporary storage or sending to Netwrix API.
QueueTimeLimit	5	Specifies the length of timeout before events from queue (not full) are saved to temporary storage or sent to Netwrix API: • From 5 to 300 — timeout in seconds. • -1 — disable timeout.

Monitoring Scope

Review a full list of all events Netwrix Auditor can collect on Qumulo Cluster.

Event	Description
fs_create_directory	A new directory was created.
fs_create_file	A new file was created.
fs_create_hard_link	A new hard link was created.
fs_create	A filetype other than one of the types captured above was created.
fs_delete	An entity (file, link, directory) was deleted from the file storage.
fs_rename	An entity (file, link, directory) from the file storage was renamed.
fs_read_data	Read operation was performed.
fs_write_data	Write operation was performed.
fs_write_metadata	Write operation was performed (metadata was written).

Event	Description
nfs_create_export	Created NFS Export that the client will mount to.
nfs_delete_export	Removed NFS Export that the client will mount to.
nfs_modify_export	Modified NFS Export that the client will mount to.
nfs_mount	Mount to NFS share.
replication_create_source_relationship	A replication object was created.
replication_delete_source_relationship	A replication object was deleted.
replication_modify_source_relationship	A replication object was modified.
smb_create_share	A new SMB file share was created.
smb_delete_share	An SMB file share was deleted.
smb_modify_share	An SMB file share was modified.
snapshot_create_snapshot	A snapshot was created.

Event	Description
snapshot_delete_snapshot	A snapshot was deleted.
snapshot_modify_snapshot	A snapshot was modified.

Maintenance and Troubleshooting

(Undefined variable: Add-on.Addon_Qumulo) operations are logged into the **SyslogService.txt** file. This file is located in the same folder as **SyslogService.exe.**

To change the add-on logging level, use the **LogLevel** parameter in the **settings.xml** file.

- It is recommended that before the first run you set this parameter to debug. This will facilitate operations tracking and possible problem solving.
- After that it is strongly recommended to re-set this parameter to `error` (default value) to prevent the uncontrolled log growth.

If you cannot see collected data in Netwrix Auditor, check the following:

1. Service account has sufficient rights to access Netwrix Auditor.
2. In Netwrix Auditor settings, go to the **Integrations** section and make sure the **Leverage Integration API** is switched to **ON**. Check the communication port number – default is **9699**.
3. If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
4. Verify the parameters you provided in **settings.xml**.

RADIUS Server

Netwrix Auditor Add-on for RADIUS Server tracks user and device logon activity on a Windows Server where the Remote Authentication Dial-In User Service (RADIUS) is running.

RADIUS Protocol

RADIUS is a client-server network protocol that enables secure authentication, authorization, and account management through special network access servers called gateways. The protocol works as follows: When a user tries to access network resources through a gateway that has the RADIUS client component enabled, the gateway sends a request to the RADIUS server. The RADIUS server identifies the user or device and either accepts or rejects the connection request, and then logs the attempt for future reference.

Because it enhances security and scalability, the RADIUS protocol is widely used in enterprise network environments to provide authentication and authorization for a variety of network access servers, such as VPN or dial-in servers and wireless access points. It helps organize and centralize sign-in procedures and improve overall security. In a Windows Server environment, the RADIUS server is provided by the Network Policy Server (NPS).

In addition to providing user authentication and authorization, a RADIUS server can grant or deny access to a connecting device based on network policies. Companies leverage these policies to empower users to connect to the corporate infrastructure using their personal devices, while disallowing potentially vulnerable and unsafe devices to minimize risk.

Netwrix Auditor Add-on

Regular review of logon activity is essential for gaining complete visibility into your account management

procedures and ensuring that all activity is traceable and compliant with your policies. For example, logons from unusual locations or devices can be a sign of user account compromise or identity theft, and an unexpectedly high number of logon failures can indicate an intrusion attempt. Careful review of successful and failed logons from both Active Directory and RADIUS servers helps security operations teams detect these signs and react promptly to security threats.

Netwrix Auditor Add-on for RADIUS Server works in collaboration with Netwrix Auditor for Active Directory, collecting additional data that augments the data collected by Netwrix Auditor. Aggregating data into a single audit trail simplifies logon activity analysis and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on automates the acquisition of RADIUS logon events and their transition to Netwrix Auditor. All you have to do is provide connection details and schedule the script for execution. Netwrix recommends running this add-on in addition to the Active Directory auditing provided by Netwrix Auditor.

On a high level, the add-on works as follows:

1. The add-on connects to the Security event log on the RADIUS server and collects logon-related events.
2. The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, logon status, time, and other details. Where applicable, the cause for logon failure and the name of network policy are included in the Activity Record.
3. Using the Netwrix Auditor Integration API, the add-on sends the successful and failed logon events to the Netwrix Auditor server, which writes them to the Long-Term Archive and the Audit Database.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor Server side	• Auditor version is **9.8** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.

On...	Ensure that...
The RADIUS server	• The **Remote Event Log Management (RPC)** inbound firewall rule is enabled. • The account collecting RADIUS logon events is member of the **Domain Users** group and have the **Manage auditing and security log** right.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

Parameter	Default value	Description
Connection to Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the DOMAIN\username format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor Client Users group on the computer hosting Auditor Server.

Parameter	Default value	Description
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.
NetwrixAuditorPlan	–	Unless specified, data is written to **Netwrix_ Auditor_API** database and is not associated with a specific monitoring plan. Specify a name of associated monitoring plan in Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add-on, make sure a dedicated plan is created in Auditor, the Netwrix API data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
RADIUSHost	localhost	Assumes that the script runs on the RADIUS server. If you want to run a script on another machine, provide a name of the computer where RADIUS server resides (e.g., 172.28.6.16, EnterpriseNPS, NPS.enterprise.local).
RADIUSUserName	Current user credentials	Unless specified, the script runs with the current user credentials.

Parameter	Default value	Description
		If you want the script to use another account to access the RADIUS server, specify the account name in the DOMAIN\username format. **NOTE:** The account must be a member of the **Domain Users** group and have the **Manage auditing and security log** right.
RADIUSPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

Choose Appropriate Execution Scenario

Auditor Add-on for RADIUS Server runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on your RADIUS server.

Depending on the execution scenario you choose, you have to define a different set of script parameters. See the Define Parameters topic for additional information.

Netwrixsuggests the following execution scenarios:

Scenario	Example
The add-on runs on theAuditor Server with the current user credentials. **Data is collected from a remote RADIUS server and written to a local repository.**	`C:\Add-ons\Netwrix_Auditor_Add-on_for_RADIUS_Server.ps1 -RADIUSHost 172.28.6.16`

Scenario	Example
The add-on runs on the Auditor Server with explicitly defined credentials. Collected data is written to a remote Auditor Server.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ RADIUS_Server.ps1 -NetwrixAuditorHost 172.28.6.15`
The add-on runs on the Auditor Server with the current user credentials. Data is collected from a remote RADIUS server with explicitly defined credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ RADIUS_Server.ps1 -RADIUSHost 172.28.6.16 -RADIUSUserName enterprise\NSPuser -RADIUSPassword SuperStrictPassword`
The add-on runs on a remote computer with the current user credentials. Data is collected from a remote RADIUS server and written to a remote Auditor repository.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ RADIUS_Server.ps1 -NetwrixAuditorHost 172.28.6.15 -RADIUSHost 172.28.6.16`
The add-on runs on a remote computer. Data is collected from a remote RADIUS server with RADIUS server credentials and is written to a remote Auditor repository with Auditor credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_ RADIUS_Server.ps1 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool -RADIUSHost 172.28.6.16 -RADIUSUserName enterprise\NSPuser -RADIUSPassword SuperStrictPassword`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run the script with PowerShell.

Step 1 – On computer where you want to execute the add-on, start **Windows PowerShell**.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-
on_for_for_RADIUS_Server.ps1 - NetwrixAuditorHost 172.28.6.15 -RADIUSHost
172.28.6.16
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Auditor Audit Database execution may take a while. Ensure the script execution completed successfully.

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new events.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

To create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.Select **Create Task**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrix recommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_RADIUS_ Server.ps1" -NetwrixAuditorHost 172.28.6.15 -RADIUSHost 172.28.6.16`

Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

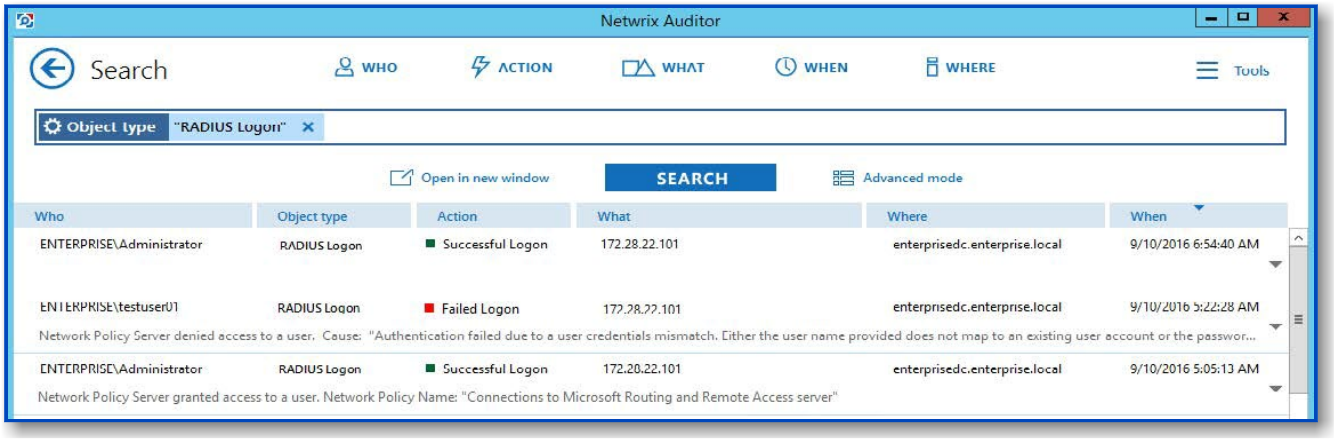
Work with Collected Data

Auditor provides a convenient interface for reviewing RADIUS server logons. Once the script execution completed, you can start analyzing user activity data with Netwrix search.

Follow the steps to see results.

Step 1 – Start the Auditor client and navigate to Search.

Step 2 – Click **Search**.



NOTE: You might want to apply a filter to narrow down your search results to the RADIUS Logon object type only.

Create Custom Report

To speed up data review process and help you find the latest logons faster, Netwrix created an additional script, **Netwrix_Auditor_Saved_Search_for_RADIUS_Server_Logons.ps1**. It is shipped with the add-on and creates the RADIUS server logons since yesterday custom search-based report in the Auditor client.

Follow the steps to create a custom report with the script.

Step 1 – Copy the **Netwrix_Auditor_Saved_Search_for_RADIUS_Server_Logons.ps1** script to the Auditor Server.

Step 2 – Start **Windows PowerShell** and specify a path to the script.

Step 3 – Run the script.

NOTE: The user running the script must be a member of the **Netwrix Auditor Administrators** group.

After running the script, the RADIUS server logons since yesterday custom report appears in **Reports** > **Custom**. You can access the search instantly to receive it on a regular basis.

Clicking the saved search tile opens the search with preset filters, which shows RADIUS logon activity data for 2 days (yesterday and today).

Troubleshoot Issues

Error in PowerShell	Resolution
`New-Object : Exception calling ".ctor" with "1" argument(s): "Attempted to perform an unauthorized operation."`	The account specified for collecting events on the RADIUS server does not have sufficient rights and permissions or the password is incorrect. • Check the password for this account. • Select the account that belongs to the **Domain Users** group and has the **Manage auditing and security log** right in domain where the RADIUS server resides.
`New-Object : Exception calling ".ctor" with "1" argument(s): "The RPC server is unavailable"`	The firewall on the RADIUS server blocks the script execution. On the server, navigate to the **Help Protect your computer with Windows Firewall** page, select **Advanced Settings** and enable the **Remote Event Log Management (RPC)** inbound rule.

ServiceNow Incident Management

The add-on works in collaboration with Netwrix Auditor, supplying data on suspicious activity or improper actions right to your helpdesk action center. Aggregating data into a single trail

simplifies incident processing and handling, makes IT service management more cost effective, and helps address threats as soon as possible.

Implemented as a service, this add-on facilitates the data transition from Netwrix Auditor to ServiceNow ITSM system. The service automatically creates incident tickets in your system and updates them with subsequent events. All you have to do is provide connection details and specify what actions should lead to ticket creation.

On a high level, the add-on works as follows:

1. The add-ons comes with a special set of alerts developed by Netwrix industry experts. With a help of a straight- forward command- line tool, you upload these alerts to Netwrix Auditor and enable integration with add-on.

2. Whenever the alert is triggered, the add-on retrieves an Activity Records for this action using the Netwrix Auditor Integration API. Each Activity Record contains the user account, action, time, and other details.

3. The add-on creates an incident ticket in ServiceNow, populates it with data that was available in the alert, and assigns to a proper team. Now, you can process a ticket as usual.

   To prevent ticket overflow, the service provides an advanced flood suppression mechanism.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor Server side	• Auditor version is **9.8** or later. • The Audit Database settings are configured in the Auditor. See the Audit Databasetopic for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in

On...	Ensure that...
	the Auditor or is a member of the Netwrix Auditor Client Users group. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
On the ServiceNow side	• ServiceNow version should be any of the following: ◦ Helsinki ◦ Istanbul ◦ Kingston ◦ London **NOTE:** Currently, Jakarta version has only experimental support. • A new user is created and has sufficient permissions to create tickets and update them. The **itil** role is recommended. If you want to reopen closed tickets, you must be granted the right to perform **Write** operations on inactive incidents.

See the Integration API topic for additional information.

Install Add-On

After downloading the add-on package from Netwrix add-on store, copy it to the a computer where the Auditor Server resides. Unpack the ZIP archive to a folder of your choice; by default, it will be unpacked to the **Netwrix_Auditor_Add-on_for_ITSM** folder.

The main component of the add- on is implemented as a service named Netwrix Auditor **ITSM Integration Service**. This service will run on the computer where the Auditor Server works, and will use the default Integration API port **9699**. Unless specified, the service will run under the **LocalSystem** account.

To use the add-on, you should check the prerequisites and specify configuration settings, as described in the next sections. After that, run the installer that will apply settings and start the service. See the Deploy the Service topic for additional information.

Define Parameters

General

Perform the following steps to define general parameters for the Add-On:

Step 1 – Navigate to your add-on folder and select the **ITSMSettings.xml** file.

Step 2 – Define general parameters such as Auditor connection parameters, the number of tickets the service can create per hour, ability to reopen closed tickets, etc. For most parameters, default values are provided.

Step 3 – Provide new values as follows: `<parameter>value</parameter>`. You can skip or define parameters depending on your execution scenario and security policies.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	• The add-on runs on the computer where the Auditor Server resides and uses the default Integration API port **9699**. To specify a non-default port, provide a new port number (e.g., *https://localhost:8788*). • The add- on must always run locally, on the computer

Parameter	Default value	Description
		where the Auditor Server resides.
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs under the **LocalSystem** account. If you want the add-on to use another account to connect to the Auditor Server, specify the account name in the *DOMAIN\username* format. Alternatively, after deploying the **Netwrix Auditor ITSM Integration Service** service, specify an account in its properties. The account must be assigned the Global reviewer role in the Auditor or be a member of the Netwrix Auditor**Administrators** group. The user must have sufficient permissions to create files on the computer.
NetwrixAuditorPassword	–	Provide a password for the account. Unless an account is specified, the service runs under the **LocalSystem** account and does not require a password.
TicketFloodLimit	10	Specify the maximum number of standalone tickets the service can create during **TicketFloodInterval**. If a ticket flood limit is reached, the service writes all new alerts into a single ticket.

Parameter	Default value	Description
TicketFloodInterval	3600	Specify the time period, in seconds. During this time period, the service can create as many tickets as specified in **TicketFloodLimit**. The default value is 3600 seconds, i.e., 1 hour.
ConsolidationInterval	900	Specify the time period, in seconds. During this time period, the service does not process similar alerts as they happen but consolidates them before updating open tickets in your ITSM. The default values is 900 seconds, i.e., 15 minutes. This option works in combination with **UpdateTicketOnRepetitiveAlerts** and is helpful if you want to reduce the number of ticket updates on ITSM side. I.e., this option defines the maximum delay for processing alerts and updating existing tickets. Tickets for new alert types are created immediately. For example, a new alert is triggered —the service opens a new incident ticket. The alert keeps firing 20 times more within 10 minutes. Instead of updating the ticket every time, the service consolidates alerts for 15 minutes, and then updates a ticket just ones with all collected data.
CheckAlertQueueInterval	5	Internal parameter. Check and process the alert queue every N seconds; in seconds.

Parameter	Default value	Description
UpdateTicketOnRepetitiveAlerts	true	Instead of creating a new ticket, reopen an existing ticket that is in a closed state (be default, closed, canceled, and resolved) if a similar alert occurs within **UpdateInterval**. This option works only when **UpdateTicketOnRepetitiveAlerts** is set to "*true*". **NOTE:** If you want to reopen closed tickets, you must be granted the right to perform **Write** operations on inactive incidents.
UpdateInterval	86400	Specify the time period, in seconds. If a similar alert occurs in less than N seconds, it is treated as a part of an existing incident. The default value is 86400 seconds, i.e., 24 hours. If an alerts is triggered after the **UpdateInterval** is over, a new ticket is created.
EnableTicketCorrelation	true	Review history and complement new tickets with information about similar tickets created previously. This information is written to the **Description** field. This option is helpful if you want to see if there is any correlation between past incidents (occurred during last month, by default) and a current incident.

Parameter	Default value	Description
CorrelationInterval	2592000	Specify the time period, in seconds. During this time period, the service treats similar tickets as related and complements a new ticket with data from a previous ticket. The default value is 2592000 seconds, i.e., 1 month. Information on alerts that are older than 1 month is removed from internal service storage.
ProcessActivityRecordQueueInterval	5	Internal parameter. Process Activity Record queue every N seconds; in seconds.
DisplayOnlyFirstActivityRecord	true	Add only the first Activity Record in the work notes, Activity Records that update this ticket will be added as attachments to this ticket. If false, all Activity Records will be displayed in the ticket work notes.
ActivityRecordRequestsRetention		
RequestLimit	5000	Internal parameter. The maximum number of Activity Record requests the service can store in its internal memory. Once the limit is reached, the service clears Activity Record requests starting with older ones.
RequestLimitInterval	604800	Internal parameter. The service can store the Activity Record requests not older than N seconds; in

Parameter	Default value	Description
		seconds. Older Activity Record requests are cleared.
ActivityRecordWebRequests		
RequestLimit	200	Internal parameter. The maximum number of Activity Records the service can retrieve in a single request.
RequestTimeout	180	Internal parameter. By default, 3 minutes. Defines the connection timeout.
TicketRequestsRetention		
RequestLimit	300000	Internal parameter. The maximum number of ticket requests the service can store in its internal memory. Once the limit is reached, the service clears ticket requests starting with older ones.
RequestLimitInterval	604800	Internal parameter. The service can store the ticket requests not older than N seconds; in seconds. Older tickets requests are cleared.

NOTE: Stop and then restart the service every time you update any of configuration files.

ServiceNow Parameters

Follow the steps to define ServiceNow parameters:

Step 1 – Navigate to your add-on folder and select **ServiceNowSettings.xml**.

Step 2 – Define parameters such as ServiceNow connection parameters inside the `<Connection>` section.

Step 3 – Provide new values as follows: `<paramenter>value↙parameter>`.

<Connection> parameter	Default value	Description
URL	—	Provide a link to your ServiceNow system (e.g., *https://enterprise.service-now.com*).
UserName	—	Specify a user account. Make sure the user has sufficient permissions to create tickets and update them. The **itil** role is recommended. **NOTE:** If you want to reopen closed tickets, you must be granted the right to perform **Write** operations on inactive incidents.
Password	—	Provide a password.

Step 4 – Review the `<TicketParameters>` section. The parameters inside this section correspond to ServiceNow ticket fields and use the same naming (e.g., priority, urgency). To find out a field name in ServiceNow, switch to XML view (on the ticket header, navigate to Show XML).

Each `<TicketParameter>` includes the `<Name>↙Name>` and `<Value>↙Value>` pair that defines a ServiceNow ticket field and a value that will be assigned to it. For most parameters, default values are provided. Add more ticket parameters or update values if necessary.

NOTE: The template remains the same for all alerts and cannot be adjusted per individual alerts.

Name	Value	Description
short_description	[Netwrix Auditor] %AlertName%	Sets **Short** description to alert title (e.g., *[Netwrix Auditor] ITSM Add-On: User Account Locked Out)*.
category	software	Sets the incident **Category** to "*Software*".
impact	1	Sets **Impact** to "*1 – High*".
urgency	1	Sets **Urgency** to "*1 – High*".
severity	1	Sets **Severity** to "*1 – High*".
assignment_ group	d625dccec0a8016700a22a0 f7900d06	Sets **Assignment** group to "*Service Desk*". **NOTE:** You cannot use a group name as a value. Provide its guid instead.
description	%AlertDescription% %PreviousTicketReference%	Provides an alert description and references to related tickets in **Description**.
work_notes	Alert Details: ...	Adds the full alert text to Work notes, including data source, who, what, where, etc.

Name	Value	Description
		To find out what is included in the alert details, see the **ServiceNowSettings.xml** file. **NOTE:** You can write alert details in the **Additional comments** field instead of Work notes. To do this, rename `<Name>work_notes↙Name>` into `<Name>comments↙Name>`. If you want to write alert details into both fields, create a copy of `<TicketParameter>` entry containing work_notes and `<Name>work_notes↙Name>` into `<Name>comments↙Name`. To skip alert details, remove entries for work_notes or comments.

Step 5 – Review the `<CorrelationTicketFormat>` section. It shows what information about related tickets will be included in your current ticket. Update the template if necessary.

CorrelationTicketFormat	Description
Previous incident for the same alert type: **Number: %number%** **Opened: %opened_at%** **Assigned to: %assigned_to%** **Assignment group: %assignment_group%** **State: %state%**	Each `%parameter%` corresponds to a ServiceNow ticket field. The service will automatically substitute these parameters with values from a related ticket. Rearrange fields or add more if necessary. To find out a field name in ServiceNow, switch to XML view (on the ticket header, navigate to **Show XML**).

Step 6 – Review the `<ReopenTicketOptions>` section. It defines the tickets the add- on can reopen automatically.

Name	Description
ClosedTicketStates **TicketState**	Lists ticket statuses. Only tickets with this status can be reopened. By default, resolved, closed, and canceled tickets can be reopened. To specify a new status, provide its ID in the `<TicketState>` tag (e.g., 8 for canceled).
NewState	Defines a ticket status once it is reopened. By default, new. To specify another status, provide its ID in the `<NewState>` tag (e.g., 1 for new).

NOTE: Stop and then restart the service every time you update any of configuration files.

Integrate Alerts with Add-On

The add-on is shipped with a special set of alerts developed by Netwrixindustry experts. These alerts are helpful for handling some routine cases that require service manager's attention, e.g., account lockouts, changes to administrative groups. The alerts have preset filters and can be easily uploaded to Auditor, and then integrated with the add-on and your ServiceNow system. These alerts have ITSM Addon prefix in their names.

Alternatively, you can integrate any default Auditor alert or your custom-built alerts with the addon.

By default, none of the alerts are integrated with add-on. To instruct the add-on to create tickets for alerts, you should enable integration. Netwrix provides a command-line tool for enabling integration with the add-on.

NOTE: Make sure to turn on alerting in Auditor. You should manually set the state to "**On**" for all alerts you want to integrate with the add-on.

Perform the following steps to integrate alerts with the add-on:

Step 1 – On the computer where the Auditor Server is installed, start the **Command Prompt** and run the **Netwrix.ITSM.AlertsUploaderTool.exe** tool. The tool is located in the add-on folder. For example:

```
C:\>cd C:\Add-on
```

```
C:\Add-on\Netwrix.ITSM.AlertsUploaderTool.exe
```

Step 2 – Execute one of the following commands depending on your task.

To...	Execute...
Upload alert set shipped with the addon to Auditor	`Netwrix.ITSM.AlertsUploaderTool.exe /UploadTemplates` Once uploaded, the alerts appear in the **All Alerts** list in Auditor, their names start with "*ITSM add-on*". Make sure to set their state to "**On**" (turn them on) manually.
Review alert list and their integration status	`Netwrix.ITSM.AlertsUploaderTool.exe /List` You will see the full list of Auditor alerts, with an enabled or disabled integration status for each alert.

Enable integration	`Netwrix.ITSM.AlertsUploaderTool.exe /Update "<Alert Name>" Enable`
	
	where `<Alert Name>` is the name of the alert you want to integrate with the add-on. Provide alert names as they appear in Auditor.
	
	NOTE: You can enable integration with one alert at a time.
	
	For example:
	
	`Netwrix.ITSM.AlertsUploaderTool.exe /Update "ITSM Add-On: User Account Locked Out" Enable`

Disable integration	`Netwrix.ITSM.AlertsUploaderTool.exe /Update "<Alert Name>" Disable`

To...	Execute...
	where <Alert Name> is the name of the alert for which you want to disable integration. **NOTE:** You can disable integration with one alert at a time. For example: Netwrix.ITSM.AlertsUploaderTool.exe /Update "ITSM Add-On: User Account Locked Out" Disable

Deploy the Service

Follow the steps to deploy the service.

Step 1 – Locate the add-on folder on the computer where the Auditor Server resides.

Step 2 – Run the **install.cmd** file. The file deploys and enables the Auditor **ITSM Integration Service**.

NOTE: Stop and then restart the service every time you update any of configuration files.

Configure Integration Service to Use Proxy

If you are using a proxy to provide access to the Internet, consider that the Auditor ITSM Integration Service will need some additional configuration for proxy server to be detected properly. The reason is that this service runs under the **LocalSystem** account (non-interactive), which requires proxy settings to be specified manually. See the following Microsoft article for additional information: HTTP proxy.

Follow the step to configure integration service settings.

Step 3 – Navigate to the add-on folder (default name is *Netwrix_Auditor_Add-on_for_ITSM*) and select the **Netwrix.ITSM.IntegrationService.exe.config** service configuration file.

NOTE: If Auditor ITSM Integration Service is running, stop it before modifying configuration file.

Step 4 – Open this XML file for edit and add the following section:

```
<system.net>
 <defaultProxy>
 <proxy
  proxyaddress="http://<ip_address>:<port>"
  usesystemdefault="True"
  autoDetect="False" />
 </defaultProxy>
</system.net>
```

Here:

Parameter	Description
proxyaddress	Specify default proxy address and connection port, e.g., *http://172.28.13.79:8080*
usesystemdefault	Set to **True** to allow Internet Explorer proxy settings to be overwritten with custom settings.
autoDetect	Set to **False**.

Step 5 – Start the Auditor ITSM Integration Service.

SIEM

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the AlienVault USM SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

Netwrix Auditor Activity Records to Event Log Add-on

On...	Ensure that...
The Auditor side	• Auditor version is **9.8** or later.

On...	Ensure that...
	• The Audit Database settings are configured in Auditor Server. • The TCP 9699 port (default Integration API port) is open for inbound connections. The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Netwrix Auditor Alerts to Event Log Add-on

On...	Ensure that...
The Auditor Server side	• Auditor version is **9.96** or 10. • The alert response action settings in Auditor Server are configured as follows: ◦ **Take action when alert occurs** is switched **ON** ◦ **Run** field contains the path to Windows PowserShell: `C:\Windows\System32\WindowsPowerShell` ◦ **With parameters** field contains the required parameters, including the path to **Netwrix_Auditor_Alerts_to_Event_Log_Add-on.ps1** file. Example: `-File C:\Netwrix_Auditor_Add-on_for_SIEM\Netwrix_Auditor_Alerts_to_on.ps1 -NetwrixPathToCsvData` For details on script parameters, see the section below. ◦ **Write data to CSV file** option is selected ◦ **Command line preview** looks like this:`C:\Windows\System32\WindowsPowerShe -File C:\Netwrix_Auditor_Add-on_for_SIEM\Netwrix_Auditor_Alerts_to_on.ps1 -NetwrixPathToCsvData {CsvFile}` • By default, the executable file will be launched under the *LocalSystem* account. If you want to use another account, make sure it has **Log on as batch job** privilege on Netwrix Auditor server. You may want to perform the test run after configuring the script as the alert response action. If so, consider that current user account (logged on to Auditor client) must have local **Administrator** privileges on AuditorServer where the executable file is located.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Activity Records to Event Log Add-on

On a high level, this add-on works as follows:

1. The add-on connects to the Auditor server and retrieves audit data using the Integration API.

2. The add-on processes Netwrix Auditor -compatible data (Activity Records) into log events that work as input for Windows event log. Each event contains the user account, action, time, and other details.

3. The add-on creates a special Windows event log named Netwrix_Auditor_Integration and stores events there. These events are structured and ready for integration with Windows event log.

For more information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API, refer to Integration API.

Netwrix Auditor Alerts to Event Log Add-on

This add-on works as response action to the alert, as follows:

1. The administrator enables and configured response action for selected alert, as described in the following topic: Configure a Response Action for Alert. Make sure to provide correct path to the script file and to select the Write data to CSV file option.
2. When the alert is triggered, the script starts - it retrieves audit data (activity record fields) from the CSV file and processes it into log events. Each event contains the user account, action, time, and other details.

3. The add-on creates a special Windows event log named Netwrix_Auditor_Integration and stores events there. These events are structured and ready for integration with SIEM system.

See the Configure a Response Action for Alert topic for additional information on the alert response actions and CSV file.

Configuration

Activity Records to Event Log Add-on Connection

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for more information.

Parameter	Default value	Description
Connection to Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15, EnterpriseNAServer, WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account

Parameter	Default value	Description
		name in the *DOMAIN**username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

In-Script Parameters

You may also need to modify the parameters that define how EventIDs should be generated for exported events, though their default values address most popular usage scenarios. In-script parameters are listed in the table below. To modify them, open the script for edit and enter the values you need.

Once set, these parameter values must stay unchanged until the last run of the script — otherwise dynamically calculated EventIDs will be modified and applied incorrectly.

Parameter	Default value	Description
EventID generation		
GenerateEventId	True	Defines whether to generated unique EventIDs. Possible parameter values: • True — generate unique EventIDs using Activity Record fields

Parameter	Default value	Description
		• False — do not generate a unique ID, set EventID=0 for all cases EventID is generated through CRC32 calculation that involves the following Activity Record field values: • ObjectType • Action • DataSource (optional, see below for details) Only the lowest 16 bits of the calculation result are used. See the Activity Records topic for additional information.
IncludeDataSourceToMakeEventId	True	Defines whether the DataSource field of Activity Record should be used in the EventID calculation. This parameter is applied only if GenerateEventId is set to TRUE. *Object Type - Action* pair may be identical for several data sources (e.g., Object='User' and Action='Added'); thus, excluding DataSource from calculation may lead to the same EventID (duplicates). See the Export Activity Records topic for additional information..
SetDataSourceAsEventCategory	True	Defines whether to fill in Event Category event field with a numeric value derived from the **DataSource** field of Activity Record.

Parameter	Default value	Description
		Possible parameter values: • True — generate a numeric value for Event Category using Activity Record field • False — do not generate a numeric value, set Event Category=1 for all cases The Event Category field value is generated through CRC32 calculation that involves the **DataSource** field of Activity Record. Only the lowest 9 bits of the calculation result are used.
SetDataSourceAsEventSource	False	Defines whether to fill in the Event Source event field with the value from the **DataSource** field of Activity Record. Possible parameter values: • True — fill in the Event Source with the value from DataSource field of Activity Record, adding the prefix defined by $EventSourcePrefix. Default prefix is *NA*, for example:*NA Windows Server* • False — set Event Source to *Netwrix_Auditor_Integration_API* for all cases If the script cannot fill in the Event Source for some DataSource, the default value *Netwrix_Auditor_Integration_API* will be used. If the event source for particular **DataSource** does not exist in the

Parameter	Default value	Description
		Netwrix_Auditor_Integration event log, elevated privileges are required for add-on execution.

Alerts to Event Log Add-on Settings

This add-on requires you to specify the following parameter:

Parameter	Description	Example
NetwrixPathToCsvData	Specify path to the auxiliary CSV file storing the data of activity records associated with the alert.	`%ProgramData%\Netwrix Auditor\AuditCore\AuditArchive\Al`

Choose Appropriate Execution Scenario

Netwrix Auditor Activity Records to Event Log Add-on

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Configuration topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1`
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1 Netwrix Auditor add-on for SIEM`
The add-on exports Activity Records from a remote Auditor server using explicitly defined credentials and writes data to a local event log.	`C:\Add-ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1 Netwrix Auditor add-on for SIEM- NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Alerts to Event Log Add-on

The script will be executed on Auditor Server.

By default, Auditor uses the *LocalSystem* account to run PowerShell scripts. If you want to use another account, in the alert settings go to **Response Action**, select the **Use custom**

credentials checkbox and specify user name and password. Make sure this account has **Log on as batch job** privilege. See the Configure a Response Action for Alert topic for additional information.

Export Activity Records

Export Activity Records Associated with the Alert

To export only important audit data, that is, the Activity Records that led to the alert triggering, configure the alert response action, providing path to **Netwrix_Auditor_Alerts_to_Event_Log_Add-on.ps1**. See the SIEM topic for additional information.

Export Activity Records in Bulk

As said, Netwrix recommends exporting the most important data, using the script described above. However, if you need to export all Activity Records in bulk, follow the recommendations below.

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters—the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.
```

```
PS C:\Users\AddOnUser> C:\Add-
ons\Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on.ps1.ps1
```

If the script path contains spaces (e.g., `C:\Netwrix Add-ons\`), embrace it in double quotes and insert the ampersand (&) symbol in front (e.g., `& "C:\Netwrix Add-ons\"`).

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor Integration event log will be created and filled with events.

By default, the Netwrix Auditor Integration event log size is set to *1GB*, and retention is set to *"Overwrite events as needed"*. See the Integration Event Log Fields topic for additional information.

Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt** file. It defines mapping between the Activity Records and related Event IDs .

You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt** file.

Similarly, the add-on also creates the **Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt** file that defines mapping between the Data Source and related Category ID.

Apply Filters

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.
- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, you can schedule a daily task for running the Activity Records to Event Log add-on.

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.Task Scheduler.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to *"Start a program"*.
Program/script	Input *"Powershell.exe"*.
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Audit_Records_to_Event_Log_Add-on.ps1"`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

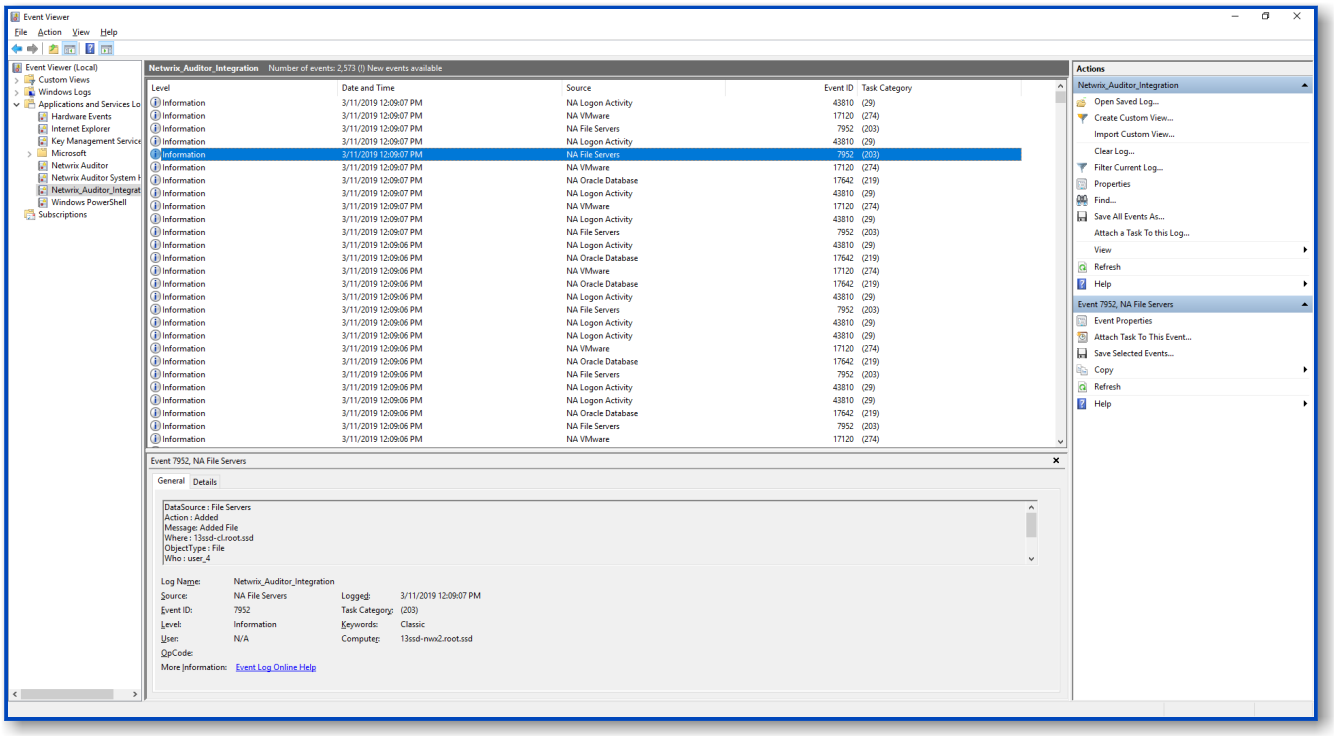
Work with Collected Data

Follow the steps to work with collected data:

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the Event Viewer dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** >Netwrix Auditor Integration log.

Step 3 – Review events.



Now you can augment Windows event log with data collected by the Auditor.

Integration Event Log Fields

This section describes how the add-on fills in the Netwrix Auditor **Integration** event log fields with data retrieved from Activity Records.

The Activity Record structure is described in the Reference for Creating Activity Recordstopic.

Event log field name	Filled in with value	Details
Source	**NA{Data Source Name}** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter.
EventID	**{Calculated by add-on}** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*).
Task Category	**{DataSource ID}** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter.

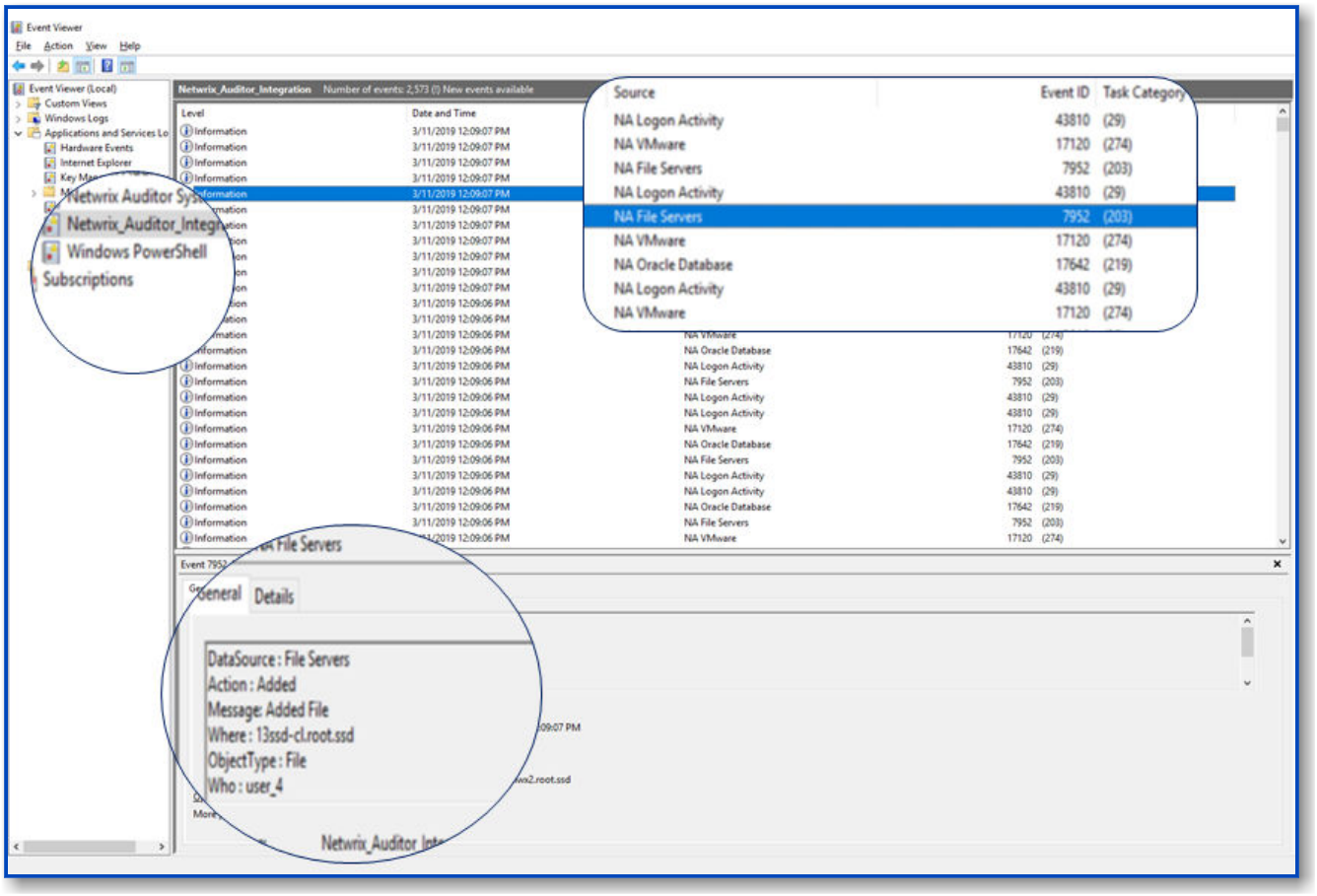
See the Configuration topic for additional information.

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}
Action	{Action}
Message	{Action ObjectType}
Where	{Where}

Entry in EventData	Activity Record field
ObjectType	{ObjectType}
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

Details are filled in only if this Activity Record field is not empty.



SIEM Generic Integration for CEF Export

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the CEF Export SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.

On...	Ensure that...
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters—the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Parameter	Default value	Description
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Auditor Server and uses default port **9699**. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., *172.28.6.15, EnterpriseNAServer, WKS.enterprise.local*). To specify a non-default port, provide a server name followed by the port number (e.g., *WKS.enterprise.local:9999*).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account name in the *DOMAIN\username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials.

Parameter	Default value	Description
		Provide a different password if necessary.
OutputFolder	—	Provide a path to the folder to store CEF log files. This is a mandatory parameter.

Choose Appropriate Execution Scenario

Netwrix Auditor Netwrix Risk Insights runs on any computer in your environment. For example, you can run the add-on on the computer where Netwrix Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Activity Records are exported to a local folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Addon.ps1 -OutputFolder C:\CEF_Export -OutputFolder C:\CEF_Export`
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Addon.ps1 -OutputFolder C:\CEF_Export -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

Scenario	Example
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Addon.ps1 -OutputFolder C:\CEF_Export -NetwrixAuditorHost 172.28.6.15`
The add-on exports Activity Records from a remote Auditor Server using explicitly defined credentials and writes data to a local folder.	`C:\Add-ons\Netwrix_Auditor_CEF_Export_Addon.ps1 -OutputFolder C:\CEF_Export -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.
```

```
PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_CEF_Export_Add-on.ps1
-OutputFolder C:\CEF_Export -NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The CEF log file will be created in the destination folder. Note that details (or 'msg' in CEF terms) exceeding 16000 symbols are trimmed.

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".

Option	Value
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_CEF_Export_Add-on.ps1" -OutputFolder C:\CEF_Export -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

Work with Collected Data

Follow the steps to work with collected data:

Step 1 – Navigate to the destination folder and open a CEF log file.

Step 2 – Review audit data exported from the Audit Database. For example, review this CEF-formatted string:

```
CEF:0|Netwrix|Active Directory|1.0|Added|Added user|0|
shost=enterprisedc.enterprise.local cat=user suser=enterprise\
\administrator filePath=\\local\\enterprise\\users\\newuser start=Mar 28
2017 14:01:48
```

Now you can feed your SIEM solutions with data collected by Auditor.

SIEM Generic Integration for Event Log Export

Netwrix Auditor helps you protect and get most from your SIEM investment. The Event Log Export Add-on works in collaboration with Netwrix Auditor , supplying additional data that augments the data collected by SIEM.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to SIEM. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Auditor Server and retrieves audit data using the Integration API.

2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for SIEM. Each event contains the user account, action, time, and other details.

3. The add-on creates a special Windows event log (Netwrix_Auditor_Integration) and stores events there. These events are structured and ready for integration with SIEM.

For more information on the structure of the Activity Record and the capabilities of the Integration API, refer to the Integration API topic.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later.

On...	Ensure that...
	• The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging the Integration API. Download the latest add- on version in the Add- on Store. See the Integration API topic for additional information about schema updates.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See Choose Appropriate Execution Scenario for additional information.

First provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined.

Parameter	Default value	Description
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting Auditor Server and uses default port 9699. If you want to run the add- on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials.

Parameter	Default value	Description
		If you want the add-on to use another account to connect to Auditor Server, specify the account name in the DOMAIN\username format. **NOTE:** The account must be assigned the **Global reviewer** role in Auditor or be a member of the **Netwrix Auditor Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

Choose Appropriate Execution Scenario

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Auditor Server with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Event_Log_Export_Add-on.ps1`
The add-on runs on the Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Event_Log_Export_Add-on.ps1`

Scenario	Example
	-NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool
The add-on exports Activity Records from a remote Auditor Server using current user credentials and writes data to a local event log.	C:\Add-ons\Netwrix_Auditor_Event_Log_Export_Add-on.ps1 -NetwrixAuditorHost 172.28.6.15
The add-on exports Activity Records from a remoteAuditor Server using explicitly defined credentials and writes data to a local event log.	C:\Add-ons\Netwrix_Auditor_Event_Log_Export_Add-on.ps1 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

Follow the steps to run add-on with PowerShell:

Step 1 – On computer where you want to execute the add-on, start Windows PowerShell.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Event_Log_Export_Add-
on.ps1 - NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor **Integration** event log will be created and filled with events.

By default, the Netwrix Auditor **Integration** event log size is set to **1GB**, and retention is set to "*Overwrite events as needed*".

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".

Option	Value
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Event_Log_Export_Add-on.ps1" -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

Work with Collected Data

Follow the steps to work with collected data:

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the **Event Viewer** dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** > **Netwrix_Auditor_Integration log**.

Step 3 – Review events.

Now you can augment SIEM with data collected by Auditor.

Solarwinds Log and Event Manager

Netwrix Auditor Add-on for SIEM helps you to get most from your SIEM investment. This topic focuses on the Solarwinds Log & Event Manager SIEM solution.

The add-on works in collaboration with Netwrix Auditor, supplying additional data that augments the data collected by the SIEM solution.

The add-on enriches your SIEM data with actionable context in human-readable format, including the before and after values for every change and data access attempt, both failed and successful. Aggregating data into a single audit trail simplifies analysis, makes your SIEM more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a PowerShell script, this add-on facilitates the audit data transition from Netwrix Auditor to the SIEM solution. All you have to do is provide connection details and schedule the script for execution.

On a high level, the add-on works as follows:

1. The add-on connects to the Netwrix Auditor server and retrieves audit data using the Netwrix Auditor Integration API.
2. The add-on processes Netwrix Auditor-compatible data (Activity Records) into log events that work as input for the SIEM solution. Each event contains the user account, action, time, and other details.
3. The add-on creates a special Windows event log named **Netwrix_Auditor_Integration** and stores events there. These events are structured and ready for integration with the SIEM solution.

See the Integration API topic for additional information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Auditor server side	• Auditor version is **10.0** or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information.

On...	Ensure that...
	• The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
The computer where the script will be executed	• PowerShell **3.0** or later must be installed. • .NET **4.5** or later must be installed. • Execution policy for powershell scripts is set to *"Unrestricted"*. Run Windows PowerShell as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the write permission on the script folder—the add-on creates a special .bin file with the last exported event. • The user running the script must be a member of the Domain Users group. • At least the first script run should be performed under the account with elevated privileges, as it will be necessary to create event log file and perform other required operations.

Compatibility Notice

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store.

Define Parameters

Before running or scheduling the add-on, you must define connection details: Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See the Choose Appropriate Execution Scenario topic for additional information.

Parameter	Default value	Description
Connection to Netwrix Auditor		
NetwrixAuditorHost	localhost:9699	Assumes that the add-on runs on the computer hosting the Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Auditor Server, specify the account

Parameter	Default value	Description
		name in the *DOMAIN\username* format. The account must be assigned the Global reviewer role in Auditor or be a member of the Netwrix Auditor **Client Users** group on the computer hosting Auditor Server.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

In-Script Parameters

Choose Appropriate Execution Scenario

Auditor Add-on for the SIEM solution runs on any computer in your environment. For example, you can run the add-on on the computer where Auditor is installed or on a remote server. Depending on the execution scenario you choose, you have to define a different set of parameters. See the Define Parameters topic for additional information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Netwrix Auditor Server with the current user credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Solarwinds_Log_and_Event_Manager.ps1`
The add-on runs on the Netwrix Auditor Server with explicitly defined credentials. Activity Records are exported to a local event log.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Solarwinds_Log_and_Event_Manager.ps1`

Scenario	Example
	-NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool
The add-on exports Activity Records from a remote Netwrix Auditor Server using current user credentials and writes data to a local event log.	C:\Add-ons\Netwrix_Auditor_Add-on_for_Solarwinds_Log_and_Event_Manager.ps1 -NetwrixAuditorHost 172.28.6.15
The add-on exports Activity Records from a remote Netwrix Auditor Server using explicitly defined credentials and writes data to a local event log.	C:\Add-ons\Netwrix_Auditor_Add-on_for_Solarwinds_Log_and_Event_Manager.ps1 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool

For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to both Auditor data and event log and use it for running the script.

Run the Add-On with PowerShell

First, provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters— the script uses a default value unless a parameter is explicitly defined. If necessary, modify the parameters as required.

To run the script with PowerShell:

Step 1 – On computer where you want to execute the add-on, start **Windows PowerShell**.

Step 2 – Type a path to the add-on. Or simply drag and drop the add-on file in the console window.

Step 3 – Add script parameters. The console will look similar to the following:

```
Windows PowerShell
```

```
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-
on_for_Solarwinds_Log_and_Event_Manager.ps1 - NetwrixAuditorHost
172.28.6.15
```

NOTE: If the script path contains spaces (e.g., *C:\Netwrix Add-ons*), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., & "*C:\Netwrix Add-ons*").

Step 4 – Hit **Enter**.

Depending on the number of Activity Records stored in Netwrix Auditor Audit Database execution may take a while. Ensure the script execution completed successfully. The Netwrix Auditor **Integration** event log will be created and filled with events.

By default, the Netwrix Auditor **Integration** event log size is set to 1GB, and retention is set to "*Overwrite events as needed*". See the Integration Event Log Fields topic for additional information.

NOTE: Event records with more than 30,000 characters length will be trimmed.

At the end of each run, the script creates the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDs.txt** file. It defines mapping between the Activity Records and related Event IDs . You can use this file to track possible duplicates of Event IDs created at each script execution. Duplicates, if any, are written to the **Netwrix_Auditor_Event_Log_Export_Add-on_EventIDsDuplicates.txt** file.

Similarly, the add-on also creates the **Netwrix_Auditor_Event_Log_Export_Add-on_CategoriesIDs.txt** file that defines mapping between the Data Source and related Category ID.

Applying Filters

Every time you run the script, Auditor makes a timestamp. The next time you run the script, it will start retrieving new Activity Records. Consider the following:

- By default, the add-on does not apply any filters when exporting Activity Records. If you are running the add-on for the first time (there is no timestamp yet) with no filters, it will export Activity Records for the last month only. This helps to optimize solution performance during the first run. At the end of the first run, the timestamp will be created, and the next run will start export from that timestamp.
- However, if you have specified a time period for Activity Records to be exported, then this filter will be applied at the add-on first run and the runs that follow.

Automate Add-On Execution

To ensure you feed the most recent data to your SIEM solution, Netwrix recommends scheduling a daily task for running the add-on.

Perform the following steps to create a scheduled task:

Step 1 – On the computer where you want to execute the add-on, navigate to **Task Scheduler**.

Step 2 – On the **General** tab, specify a task name. Make sure the account that runs the task has all necessary rights and permissions.

Step 3 – On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from Auditor and saved to event log. Netwrixrecommends scheduling a daily task.

Step 4 – On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to "*Start a program*".
Program/script	Input "*Powershell.exe*".
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_Solarwinds_Log_and_Event_Manager.ps1" -NetwrixAuditorHost 172.28.6.15`

Step 5 – Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

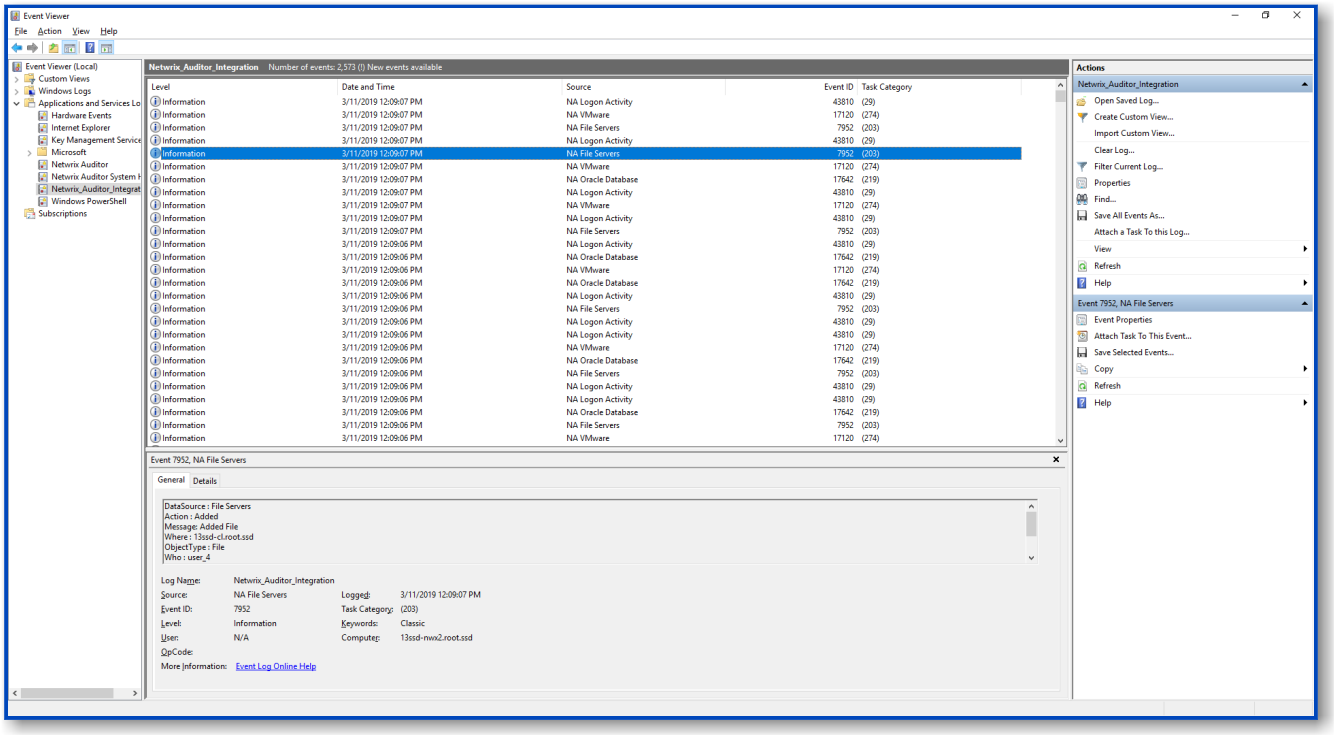
Work with Collected Data

Follow the steps to work with collected data:

Step 1 – On the computer where you executed the add-on, navigate to **Start** > **All Programs** > **Event Viewer**.

Step 2 – In the Event Viewer dialog, navigate to **Event Viewer (local)** > **Applications and Services Logs** >Netwrix Auditor Integration log.

Step 3 – Review events.



Now you can augment Windows event log with data collected by the Auditor.

Integration Event Log Fields

This section describes how the add-on fills in the Netwrix Auditor **Integration** event log fields with data retrieved from Activity Records.

The Activity Record structure is described in the Reference for Creating Activity Recordstopic.

Event log field name	Filled in with value	Details
Source	**NA{Data Source Name}** -OR- **Netwrix _Auditor_Integration_API**	Depending on *SetDataSourceAsEventSource* in-script parameter.
EventID	**{Calculated by add-on}** -OR- **0**	Depending on *GenerateEventId* in-script parameter (calculation result also depends on *IncludeDataSourceToMakeEventId* parameter — if *GenerateEventId* = *True*).
Task Category	**{DataSource ID}** -OR- **1**	Depending on *SetDataSourceAsEventCategory* in-script parameter.

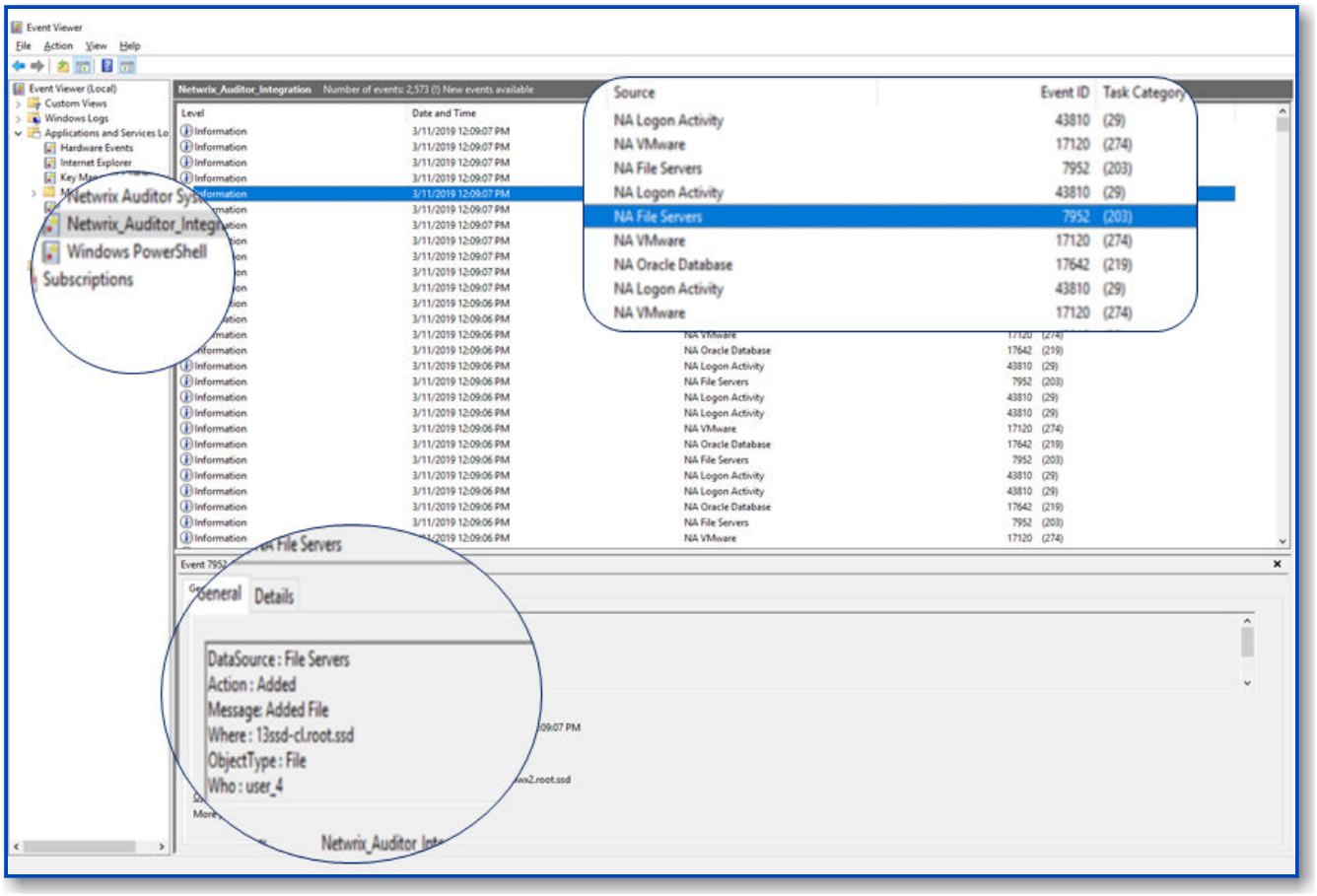
See the Define Parameters topic for additional information.

EventData is filled in with data from the Activity Record fields as follows:

Entry in EventData	Activity Record field
DataSource	{DataSource}
Action	{Action}
Message	{Action ObjectType}
Where	{Where}

Entry in EventData	Activity Record field
ObjectType	{ObjectType}
Who	{Who}
What	{What}
When	{When}
Workstation	{Workstation}
Details	{Details}

Details are filled in only if this Activity Record field is not empty.



Splunk

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.

Splunk is a log management solution that enables search and visualization of data collected from the company's IT assets.

Netwrix Auditor add-on for Splunk works as an integration solution for both products: it instructs Splunk to pull the audit data collected by Netwrix Auditor and stored to the audit databases in Netwrix-compatible form (activity records). This data is saved in the event log format recognized by Splunk and also mapped to the CIM data models — for normalization and better correlation with other log sources. With that automated flow, you can use Splunk Enterprise as your single pane of glass for aggregated data analysis. This makes the IT infrastructure monitoring more efficient and helps you keep tabs on your IT assets.

The major benefits- are:

- Aggregated audit data from the variety of sources available from a single console
- Efficient search through the audit data

Compatibility notice

Netwrix Auditor add-on for Splunk is compatible with the following products:

- Splunk Enterprise 8.0.6 and 8.2.1
- Netwrix Auditor 9.96 and above

Supported data sources

Netwrix Auditor add-on for Splunk supports and provides CIM data models mapping for the following Netwrix Auditor data sources:

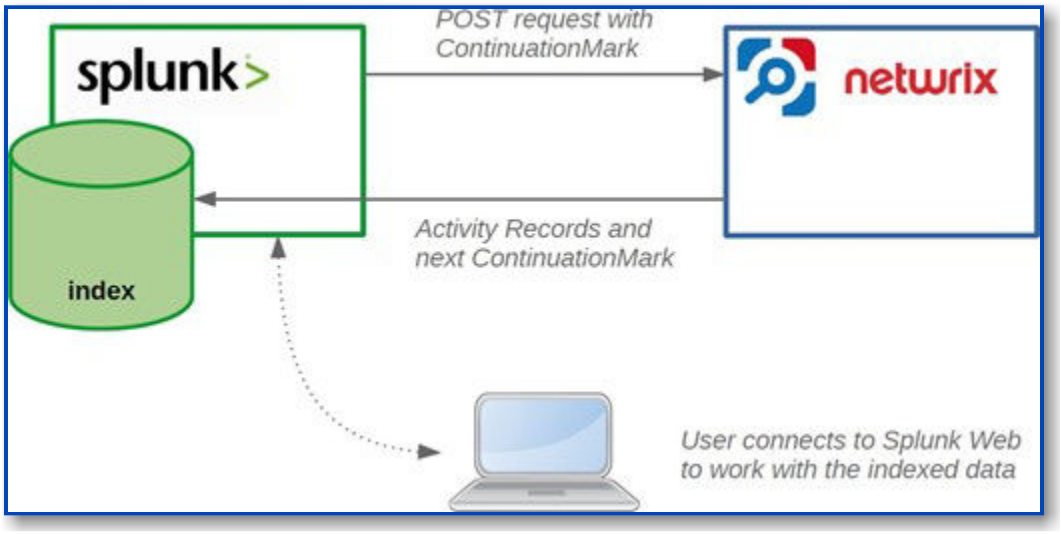
Netwrix Auditor data source	CIM Data Model
Active Directory	Authentication Change
Exchange	Change Email
Exchange Online	Change Email

Netwrix Auditor data source	CIM Data Model
File Servers	Change Endpoint
Microsoft Entra ID	Authentication Change
SharePoint	Change
SharePoint Online	Change
SQL Server	Authentication Change
VMware	Authentication Change
Windows Server	Change

See CIM Data Model Mapping for details.

How It Works

Netwrix Auditor add-on for Splunk allows pulling activity records data from the Netwrix Auditor via its Integration API. Data is retrieved in JSON format, transferred over HTTPS and stored to Splunk index.



To learn more about Netwrix Auditor activity records, see the Activity Records topic for additional information.

For this data to be provided to Splunk, it adds a new Splunk source type, performing additional data parsing and field extraction. The audit data is also mapped into the Common Information Model (CIM) data models — for normalization and better correlation with other log sources.

On a high level, the solution works in the following steps.

Step 1 – An IT administrator configures Netwrix Auditor Integration API settings to enable sharing Netwrix Auditor data with external applications.

Step 2 – On the Splunk side, the IT administrator installs and configures the add-on, providing the necessary parameters for its operation: Netwrix Auditor Integration API host and account to access it with sufficient access rights.

Step 3 – The IT administrator prepares a Splunk index to store the data that will be collected from Netwrix Auditor.

Step 4 – Splunk starts pulling activity records via Netwrix Auditor Integration API by sending POST requests with Continuation Mark. Data is received in JSON format and stored in the specified Splunk index — to make it available for further search by Splunk.

Step 5 – When search is performed, Splunk attempts to extract additional information available in the audit data and to map it to CIM data models.

User opens Splunk Enterprise to work with collected data:

- Search for the activity records in the specified index or data model
- Create reports and dashboards in Splunk

Report and dashboard creation in Splunk is outside the scope of this guide.

Add-on delivery package

Netwrix Auditor add-on for Splunk delivery package is a ZIP archive that includes the following files:

File name	Description
ta-netwrix-auditor-add-on-for- splunk-1.6.1.spl	Netwrix Auditor add-on for Splunk package.

Prerequisites

Before running the add-on, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
Auditor Server side	• Auditor version is 9.8 or later. • The Audit Database settings are configured in Auditor Server. See the Prerequisites and Audit Database topics for additional information. • The TCP 9699 port (default Auditor Integration API port) is open for inbound connections. • The user retrieving data from the Audit Database is granted the Global reviewer role in Auditor or is a member of the Netwrix Auditor

On...	Ensure that...
	Client Users group. See the Role-Based Access and Delegation topic for additional information. Alternatively, you can grant the Global administrator role or add the user to the Netwrix Auditor Administrators group. In this case, this user will have the most extended permissions in the product.
Splunk Enterprise	• Splunk version is 8.0.6 or higher. • Splunk Common Information Model add-on version 4.17.0 or higher. • Splunk Administrator or any other account with permissions to add add-ons, create indexes and data inputs. • The TCP 9699 port must be open on firewalls between Splunk and Netwrix Auditor server.

Considerations and limitations

- If the information is not available in the activity record received from Auditor, it will also not be available in Splunk.
- CIM might not have data models for some of the activity records received from Auditor; such information can only be accessed in Splunk using search by index.

Deployment Procedure

Prepare Netwrix Auditor for data processing

In Netwrix Auditor client, go to the Integrations section and verify Integration API settings:

1. Make sure the Leverage Integration API is switched to ON.
2. Check the TCP communication port number – default is 9699.

For more information, see the Prerequisites Configure Integration APIAudit Databasetopic for additional information.

Download the add-on

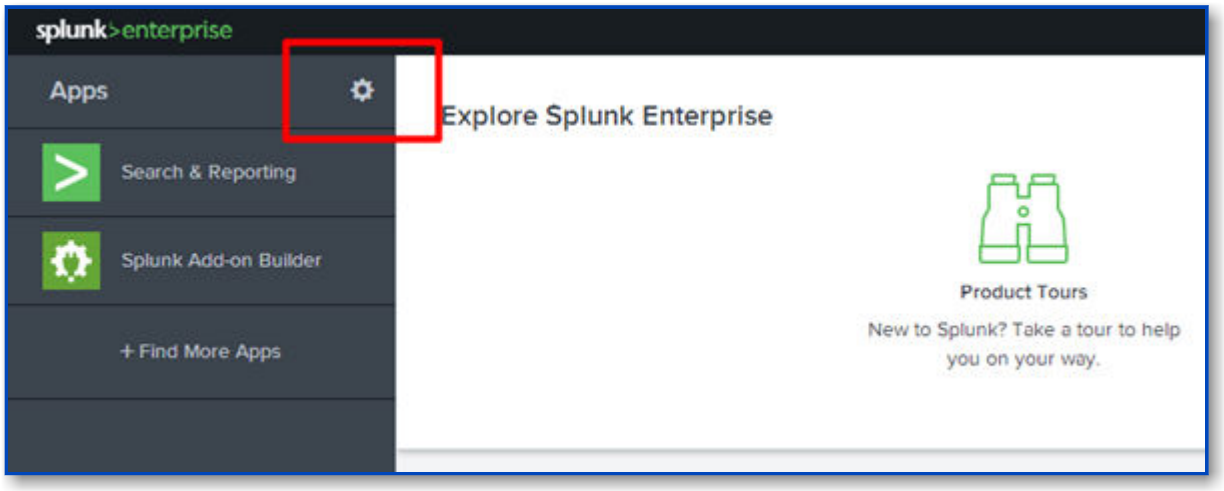
1. Download the distribution package Netwrix_Auditor_Add-on_for_Splunk.zip.
2. Unpack it to a folder on the computer from which you can access Splunk Web.

Install the add-on

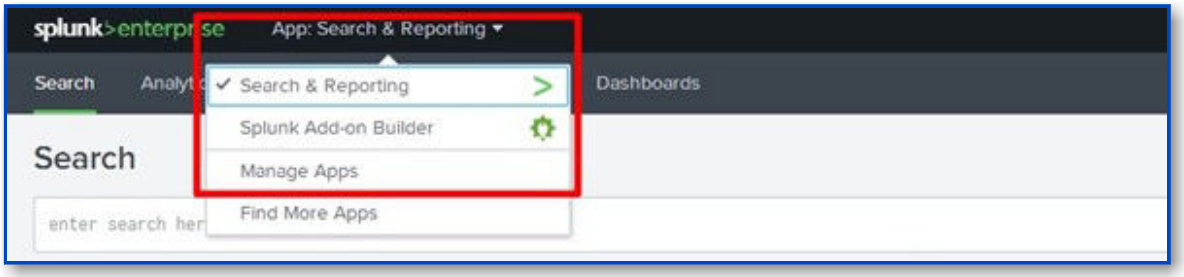
1. Login to Splunk Web using Splunk Administrator account.
2. Open the Splunk Apps

   settings in any of the following ways:

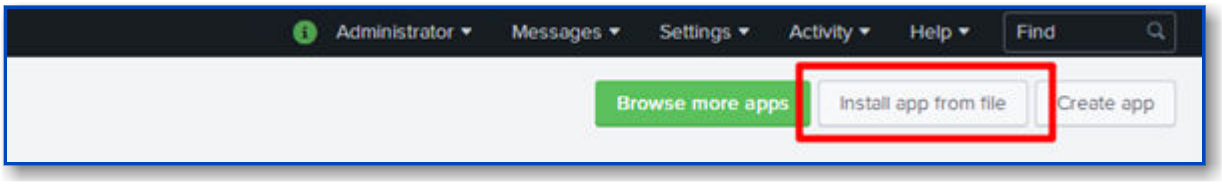
   - When on the main Explore Splunk Enterprise screen, click on the gear icon at the top of the left Apps panel:



- When on any other screen, you can expand the drop-down list at the top panel and choose Manage Apps:

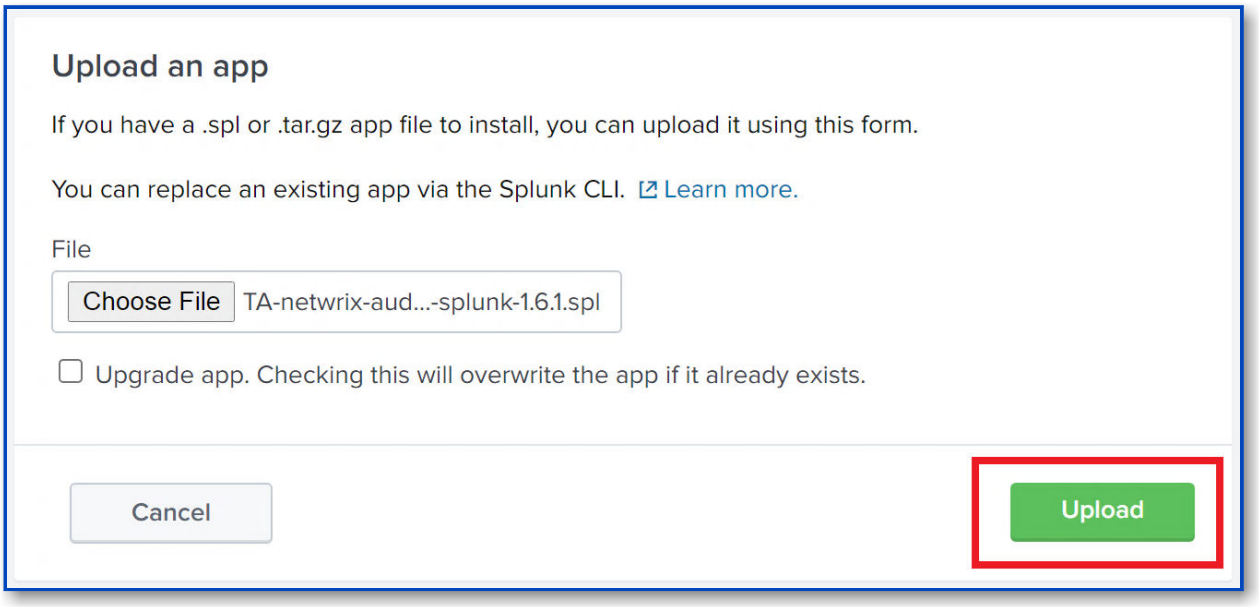


3. On the Apps screen, click Install app from file:



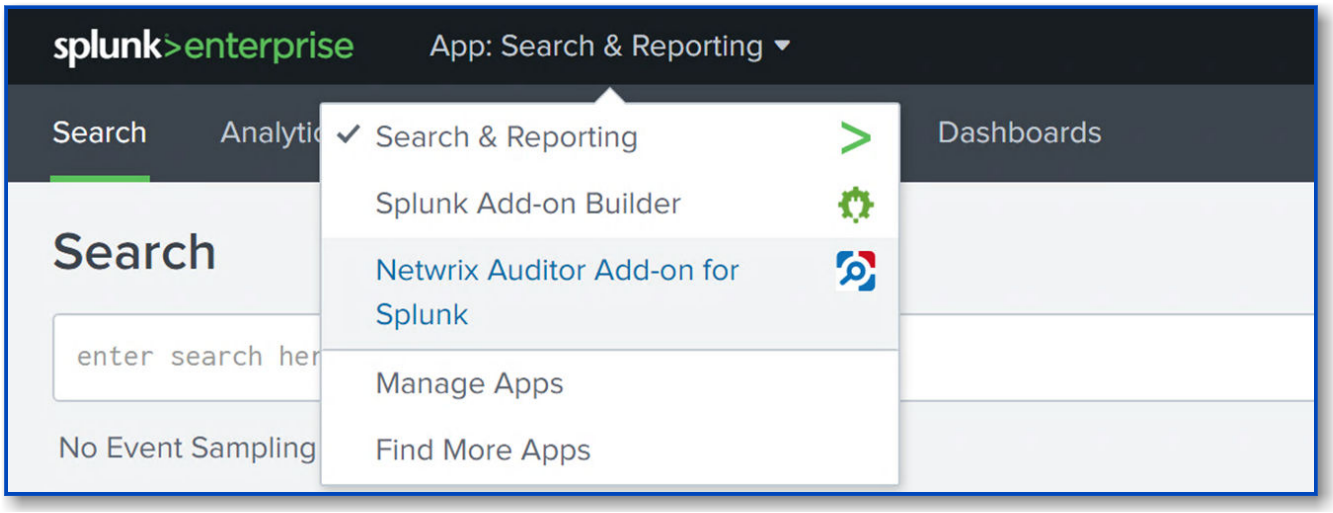
4. Click Choose File, navigate to the folder where you unpacked the add-on package, select the ta- netwrix-auditor-add-on-for-splunk-1.6.1.spl file and click Open.

5. Click Upload:



The Upload button text will change to "*Processing...*". When the installation is complete, you will see an invitation to reboot Splunk. This is optional unless you plan to create index configuration in the add-on folder. In addition, Splunk might not display add-on's icon until restart.

The installed add-on should appear in the Apps list in Splunk.



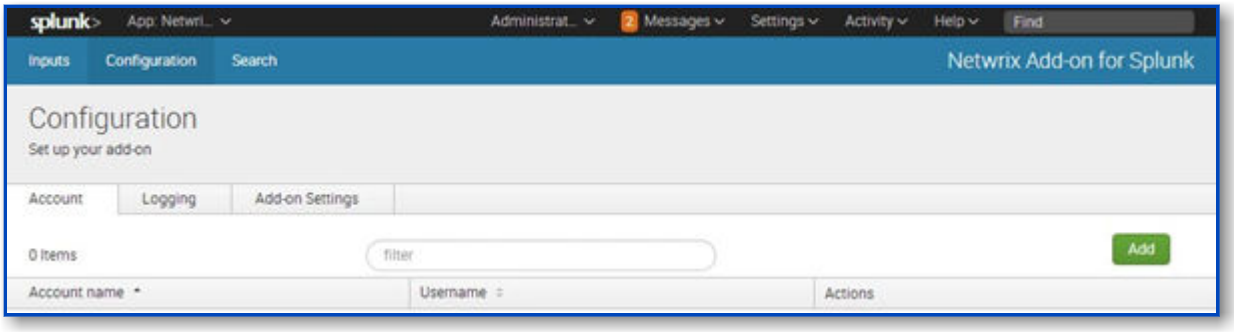
Prepare for using Netwrix Auditor Integration API

Make sure you have the following information required for the add-on configuration:

- User name and password for the account you will be using to access the Netwrix Auditor Integration API
- Netwrix Auditor Integration API host name or IP address
- TCP port used by Integration API (default port is 9699)

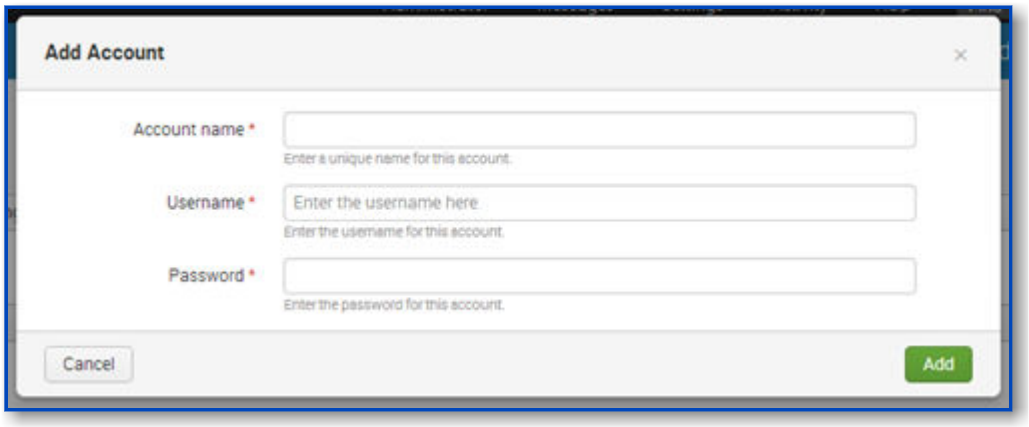
Configure the add-on

1. From the Explore Splunk Enterprise or from the drop-down list on the top Splunk panel, open Netwrix Auditor add-on for Splunk and navigate to the Configuration page:



2. Configure the account:

    1. On the Configuration page, open the Account section.

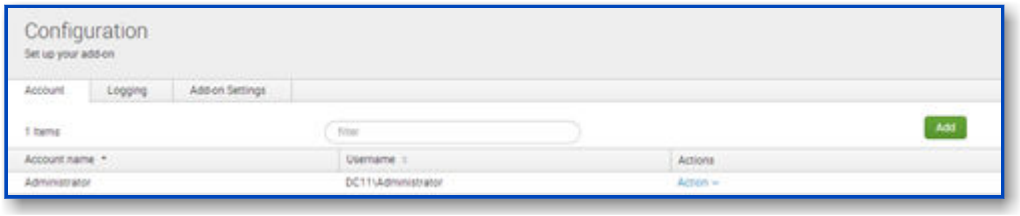


    2. Click Add and populate the fields:

        - For the Account name provide a unique name for the account that will be visible to the add-on users

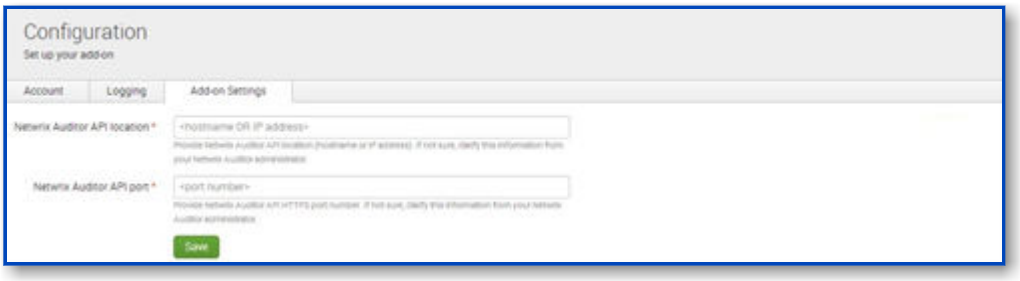
- In the Username field insert the user name of the account that will be used to access Netwrix Auditor Integration API. If a domain account is used, make sure to use the *DOMAIN\User* format.
- In the Password field insert the account's password

3. Click the Add button. The added account should appear in the list:



3. Configure the Netwrix Auditor Integration API location:

1. On the Configuration page open the Add-on Settings section:



2. In the Netwrix Auditor API location field provide the hostname or IP address of your Netwrix Auditor Integration API host (that is, Netwrix Auditor server).
3. In the Netwrix Auditor API port field provide the TCP port used by Netwrix Auditor Integration API; by default it is 9699.

   Make sure that your Netwrix Auditor Integration API is configured to use HTTPS protocol.
4. Press the Save button.

Configure data input

Splunk uses indexes to store data and manage access to it. While you can send Netwrix Auditor data to one of the existing indexes it is strongly recommended to create a separate index.

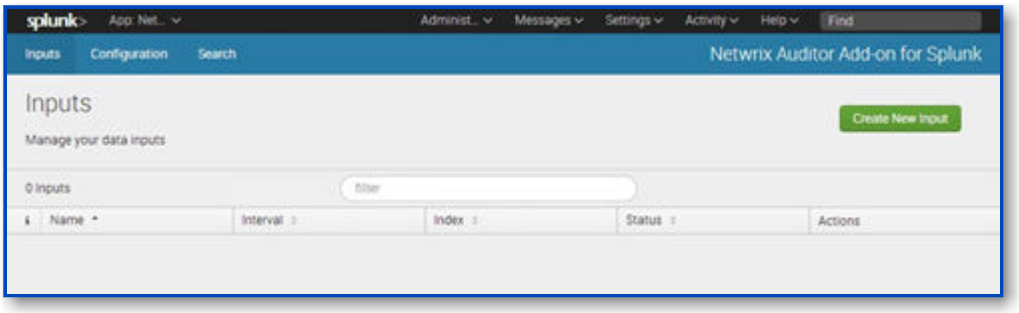
1. Create a new index to store data from Netwrix Auditor:

1. In Splunk expand the Settings drop-down menu and click on the Indexes option under the DATA section.
2. Press the New Index button to create an index.
3. Provide the new index parameters:
   - Index name — it will be used in searches
   - App — points where the index configuration is stored; choosing Search & Reporting is recommended
   - Check if you need to provide custom location for the Home, Cold and Thawed paths; by default they are in the Splunk program folder
   - Set the Max Size of Entire Index to match the expected volume of logs from Netwrix Auditor
   - By default, Splunk deletes old events when the size of the index exceeds its max value; if you want Splunk to archive them instead specify the Frozen Path

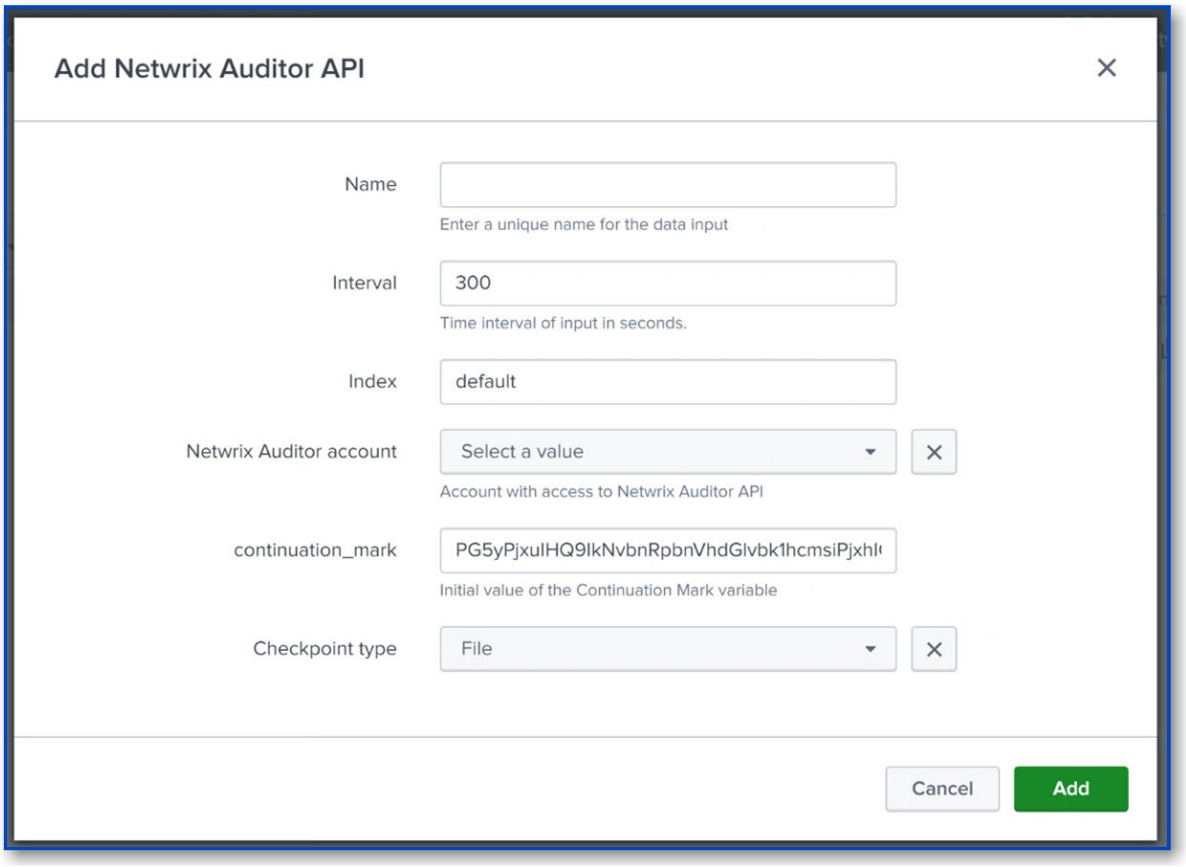
     Detailed Splunk index creation and management is outside of scope of this guide.

     Please refer to the Managing Indexers and Clusters of Indexers manual for additional details on indexes.

2. Create a data input:
   1. Open Netwrix Auditor add-on for Splunk, go to the Inputs section



   2. Click Create New Input.



3. Provide the new data input parameters:

   - Name of the new data input
   - Set the interval (period) for Splunk to periodically request new data from Netwrix Auditor Integration API. Recommended period is 300 seconds.
   - Select the index that will be used to store the collected data
   - Select account with access to Netwrix Auditor Integration API
   - If not following the upgrade procedure, keep the default value for Continuation Mark. This field should never be empty.
   - Checkpoint type specifies location for continuation mark data. File is recommended. Do not change this setting unless advised accordingly by your Splunk Administrator.

4. Click the Add button.

Upgrade procedure

If you were using the older (Windows event log-based) version of Netwrix Auditor add-on for Splunk and plan to migrate to the new version, remember to take the additional steps described below. They will help to ensure imported data consistency and avoid excessive operations. Otherwise, the new add-on will pull Netwrix Auditor's activity data that had already been imported into your Splunk system by the old add-on.

1. Stop the old version of Netwrix Auditor add-on for Splunk. Typically, this can be done via Windows Scheduled Tasks.
2. Locate the Netwrix_Auditor_Activity_Records_to_Event_Log_Add-on_Cookie.bin file in the installation directory of the old add-on for Splunk. Store that file content to a safe location.
3. Install the new add-on. When prompted for Continuation Mark, enter that Netwrix_Auditor_ Activity_Records_to_Event_Log_Add-on_Cookie.bin file content (see the Configure data inputConfigure data inputstep).

Work with Collected Data

Review the examples below for the possible scenarios on how to work with collected data.

Example 1: Search by Index

Follow the steps to search by index:

Step 1 – Navigate to the Search page of the add-on or Search & Reporting Splunk app

Step 2 – Enter the search command:

```
index=<your_netwrix_index>
```

for example:

```
index=netwrix
```

Step 3 – Press the Last 24 hours button and choose All time time range.

Step 4 – Press the search button; you should see list of the events currently indexed in Splunk.

Step 5 – Click on the arrow button next to any of the returned event to expand the list of parsed fields and confirm that fields are populated properly.

If you do not see any fields, make sure that you are running the search in Smart or Verbose mode.

Follow the steps to get all user account creation events from Microsoft Entra ID (formerly Azure AD) ports .

Step 1 – Navigate to the **Search** page of the add-on or **Search & Reporting** Splunk app

Step 2 – Enter the search command:

```
index=netwrix Action=”Added” ObjectType=”user”

| table Who Action ObjectType What Where
```

Step 3 – Press the Last 24 hours button and choose All time time range.

Example 2: Use Netwrix Auditor Fields in Index Search

Follow the steps to use Auditor fields in index search:

Step 1 – Navigate to the **Search** page of the add-on or **Search & Reporting** Splunk app

Step 2 – Enter the search command:

```
| datamodel <data_nodel_name> search

| search sourcetype=netwrix
```

for example:

```
| datamodel Authentication search

| search sourcetype=netwrix
```

Step 3 – Press the Last 24 hours button and choose All time time range.

Step 4 – Press the search button; you should see list of the events currently indexed in Splunk and mapped to the selected data model.

Step 5 – Click on the arrow button next to any of the returned event to expand the list of parsed fields and confirm that fields are populated properly.

Example 3: Use CIM Data Model Search and Data Model Fields

Follow the steps to get all events for account deletion:

Step 1 – Navigate to the Search page of the add-on or Search & Reporting Splunk app

Step 2 – Enter the search command:

```
| datamodel Change search

| search sourcetype=netwrix All_Changes.action=”deleted”

| table All_Changes.vendor_product All_Changes.action All_Changes.src
All_Changes.dest All_Changes.user All_Changes.object
All_Changes.object_attrs
```

Step 3 – Press the Last 24 hours button and choose All time time range.

CIM Data Model Mapping

The Splunk Common Information Model (CIM) is installed with an add-on and adds a set of data models that allow data normalization to simplify search.

The CIM contains a number of standard data models that can be used for search. Each of them has predefined set of standard fields common for different data sources.

Netwrix Auditor Add-on for Splunk will map some of the Activity Records that match certain scenario to the respective CIM data models.

Criteria	Data model	Description
DataSource IN ("Microsoft Entra ID", "Logon Activity", "SQL Server", "VMware") Action="Successful Logon"	Authentication > Authentication > Successful_Authentication	Successful login events
DataSource IN ("Microsoft Entra ID", "Logon Activity", "SQL Server", "VMware") Action="Failed Logon"	Authentication > Authentication > Failed_ Authentication	Failed login events
DataSource IN ("Active Directory", "Microsoft Entra ID", "Exchange*") Action="Added" ObjectType IN ("user", "computer",	Change > All_Changes > Account Management > Created Accounts	Account creation events

Criteria	Data model	Description
"inetorgperson", "service principal", "mail contact", "mail user")		
DataSource IN ("Active Directory", "Microsoft Entra ID", "Exchange*") Action IN ("Modified", "Moved") ObjectType IN ("user", "computer", "inetorgperson", "service principal", "mail contact", "mail user")	Change > All_Changes > Account Management > Updated Accounts	Account update events
DataSource IN ("Active Directory", "Microsoft Entra ID", "Exchange*") Action="Removed" ObjectType IN ("user", "computer", "inetorgperson", "service principal", "mail contact", "mail user")	Change > All_Changes > Account Management > Deleted Accounts	Account deletion events
DataSource IN ("Active Directory", "Microsoft Entra ID", "Exchange*", "File Servers") Action IN ("Added", "Modified", "Moved", "Removed") NOT ObjectType IN ("user", "computer", "inetorgperson", "service principal", "mail contact", "mail user")	Change > All_Changes	All other – not related to accounts – changes
DataSource IN ("Active Directory", "Microsoft Entra ID", "Exchange*") ObjectType IN ("user", "computer", "inetorgperson", "service principal", "mail contact", "mail user") is_ lockout=1	Change > All_Changes > Account Management > Locked Accounts	Account lockout events
DataSource IN ("Active Directory", "Microsoft Entra ID", "Exchange*") Action IN ("Added", "Modified", "Removed") is_audit=1	Change > All_Changes > Auditing Changes	Changes to audit settings or policies
DataSource="Exchange*" ObjectType="Mailbox Item" Action IN ("Sent", "Removed")	Email > All Email	Information related to sent or received emails
DataSource="File Server" Action IN ("Added". "Modified", "Moved", "Removed", "Renamed") ObjectType IN ("file", "folder")	Endpoint > Filesystem	Changes to file shares

Maintenance and Troubleshooting

Splunk records service logs to the _internal index. Follow the steps to troubleshoot data input from Netwrix Auditor API:

Step 1 – Navigate to the Search page of the add-on or Search & Reporting Splunk app.

Step 2 – Enter the search command:

```
index=_internal "<data_input_name>"
```

For example:

```
index=_internal "<netwrix_data_input>"
```

Step 3 – Press the Last 24 hours button and choose Last 15 minutes time range.

Step 4 – Press the search button; you should see list of the events with Splunk service information.

When the add-on operates normally there should be no errors and the following types of events should appear regularly:

- Regular events from **splunk\ta-netwrix-auditor-add-on-for-splunk_netwrix_auditor_api_input_** source with POST requests to the Netwrix Auditor API.
- Regular events from **splunk\ta-netwrix-auditor-add-on-for-splunk_netwrix_auditor_api_input_** source with checkpoint update with new ContinuationMarks received from Netwrix Auditor API.
- Events from **\splunk\metrics.log* source with information about indexed volumes.

Account Lockout Examiner

Overview

Netwrix Account Lockout Examiner helps IT administrators to discover why an Active Directory account keeps locking out, so they can quickly identify the lockout reason and restore normal operations.

You can investigate lockouts originating from the following sources:

- Applications running on workstations
- Microsoft Exchange ActiveSync devices
- Microsoft Outlook Web Access (including mobile devices)
- Mistyped credentials (interactive logons with incorrect password)
- Terminal Server Sessions
- Windows Credential Manager
- Windows Task Scheduler
- Windows Services

Upgrade recommendations

Since the functionality of older and newer versions does not match one-to-one (see Feature comparison of Netwrix Account Lockout Examiner 4.1 and 5.x), there is no upgrade path for **Netwrix Account Lockout Examiner 4.1**.

Though its users can continue working with that older version, we recommend to use the latest Netwrix Account Lockout Examiner to benefit from the variety of its new features and enhanced usability.

Feature comparison of Netwrix Account Lockout Examiner 4.1 and 5.x

Netwrix Account Lockout Examiner 5.1 and later is not an evolutionary update, but rather a total revamp of version 4.1. Hence, the functionality of the older and newer versions does not match one-to-one. Feature comparison is provided in the table below.

Feature	Version 4.1	Version 5.x
Network/domain configuration		
Support for multi-domain (Root-Child) configurations	No	Yes
Lockout sources		
Applications running on workstations	No	Yes
Microsoft Exchange ActiveSync devices	No	Yes
Microsoft Outlook Web Access (incl. mobile devices)	No	Yes
Mistyped credentials (interactive logons with incorrect password)	Yes	Yes
Terminal Server Sessions	Yes	Yes
Windows Credential Manager	No	Yes
Windows Task Scheduler	Yes	Yes
Windows Services	Yes	Yes
User experience		
Easy to install	-	Yes
Ease of troubleshooting	-	Yes
Workflow		
Ability to unlock account & reset password	Yes	No
Web-based helpdesk portal	Yes (paid version only)	No
Email alerts	Yes	No – check Netwrix Auditor for monitoring and alerting capabilities
Online monitor on critical account status	Yes	No – check Netwrix Auditor for monitoring and alerting capabilities

Users of Account Lockout Examiner 4.1 can continue using that older version, as there is no upgrade path, just a new installation of the latest version.

We welcome any feedback and ideas you might have. You can check in on Netwrix page at Spiceworks or submit direct feedback via this link.

Planning and Preparation

Before you start using Netwrix Account Lockout Examiner, check the prerequisites and set up your environment, as described in this section.

System requirements

Make sure that the machine where you plan install the solution meets the system requirements listed below.

Hardware:

Specification	Requirement
CPU	min 1.5 GHz
Memory	1 GB RAM
Disk space	20 MB

Software:

Specification	Requirement
OS	Both 32-bit and 64-bit of the following operating systems are supported: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows 10 • Windows 8.1

Accounts and rights

1. The computer where **Account Lockout Examiner** will run must be a member of the domain where lockouts happen.
2. The account used to run the application must be a member of the following groups:

1. **Domain Admins** group (to retrieve the necessary data from domain controllers.)
2. Local **Administrators** group on the workstation where lockouts happen (to access the Security event log.)

In the environments with root/child domains, the account used to run Account Lockout Examiner should be a member of the local **Administrators** group on the workstations in both root and child domains.

Licensing

Account Lockout Examiner is shipped with a free pre-configured license that will be valid until a newer version becomes available. You will be notified on the new version release by the corresponding message displayed in the product. Then you will need to download that new version.

Target infrastructure

For the solution to connect to and retrieve the necessary information from the Windows machines that may become the potential lockout reasons, your infrastructure should meet the requirements listed below.

Target systems and platforms

The following Windows machines are supported as examination targets:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 10
- Windows 8.1

The solution can work with the following Exchange Server versions to retrieve information needed for lockout reason detection:

- Exchange Server 2019
- Exchange Server 2016
- Exchange Server 2013

Inbound firewall rules

Make sure the following **Inbound** firewall rules are enabled on the Domain Controllers and domain computers:

- File and Printer Sharing (Echo Request - ICMPv4-In)
- Remote Event Log Management (RPC)
- Remote Service Management (NP-In)
- Remote Scheduled Tasks Management (RPC)
- Remote Volume Management (RPC -EPMAP)
- Windows Management Instrumentation (WMI-In)

Ports

The following **TCP** ports should be open on the Domain Controllers and domain computers:

- Port **135** — for communication using RPC
- Dynamic ports **1024-65535** — for internal communication

Recommended network security settings

Security researches revealed that NTLM and NTLMv2 authentication is vulnerable to a variety of malicious attacks, including SMB replay, man-in-the-middle attacks, and brute force attacks.

To make Windows operating system use more secure protocols (e.g. Kerberos version 5), the outgoing NTLM authentication traffic should be disabled for the machine where Netwrix Account Lockout Examiner will run. (See also this Microsoft article.)

For that, you need to set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** policy setting to **Deny All**. This can be done locally on the machine hosting Netwrix Account Lockout Examiner, or via Group Policy.

To disable outgoing NTLM authentication traffic locally:

1. Run *secpol.msc*.
2. Browse to **Security Settings\Local Policies\Security Options**.
3. Set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** setting to **Deny All**.

To disable outgoing NTLM authentication traffic via Group Policy:

1. Open *gpmc.msc*.

2. Find the Group Policy Object (GPO) that is applied to the machine where Netwrix Account Lockout Examiner runs.
3. Edit this GPO. Browse to **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**.
4. Set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** setting to **Deny All**.
5. On the machine hosting Netwrix Account Lockout Examiner run the following command via the command prompt: `gpupdate /force`

Required audit settings

You can configure either **Advanced audit policies** or **Basic audit policies** for the target machines. See Scenario A or Scenario B, respectively.

Scenario A: Advanced audit policies

Enable the following **Advanced audit policies** for the target machines:

Audit entry	Event ID	Success/Failure
Account Logon		
Audit Credential Validation	4776	Failure
Audit Kerberos Authentication Service	4771	Failure
Audit Other Account Logon Events	4776	Failure
Account Management		
Audit User Account Management	4740	Success
Logon/Logoff		
Audit Logon	4625	Failure
Audit Account Lockout	4625	Failure

Scenario B: Basic audit policies

Enable the following **basic audit policies** for the target machines:

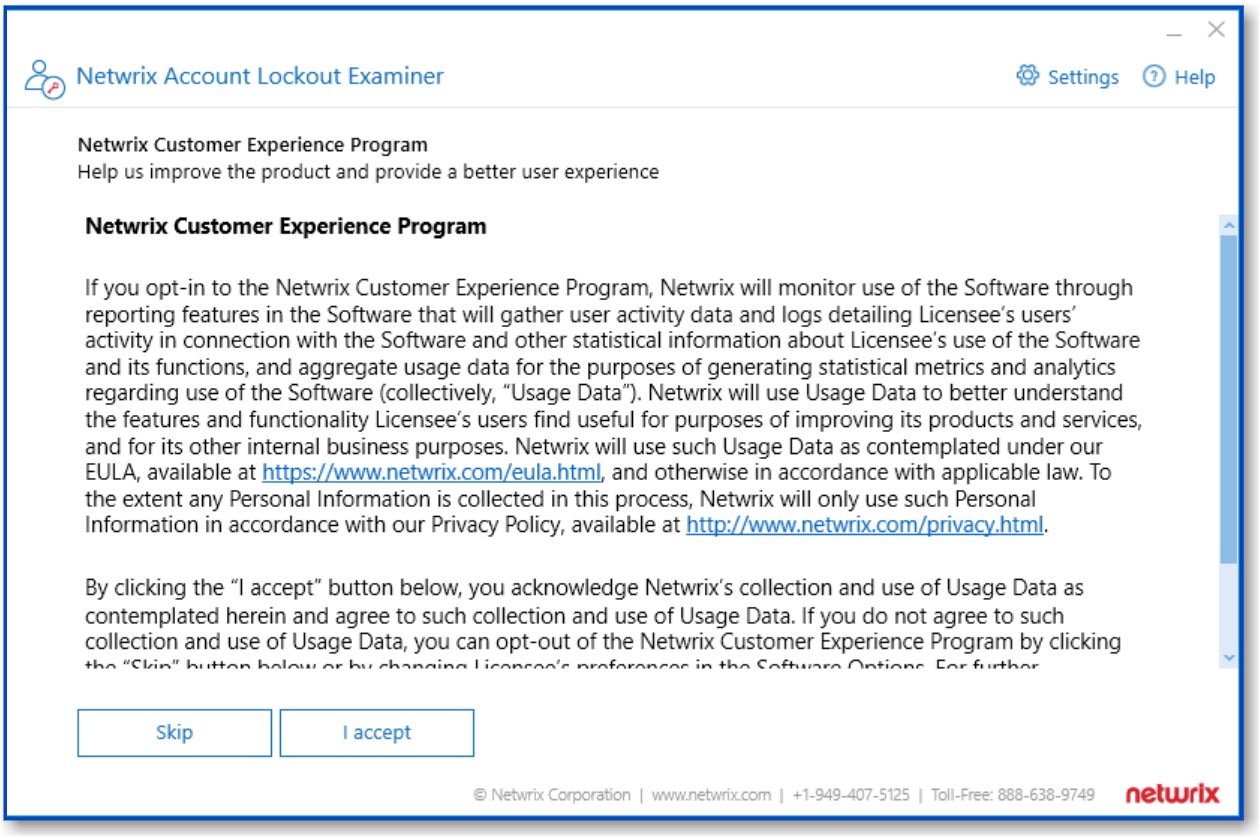
Audit entry	Event ID	Success/Failure
Audit logon events	4625	Failure
Audit account logon events	4776, 4771	Failure
Audit account management	4740	Success

Examining Lockouts

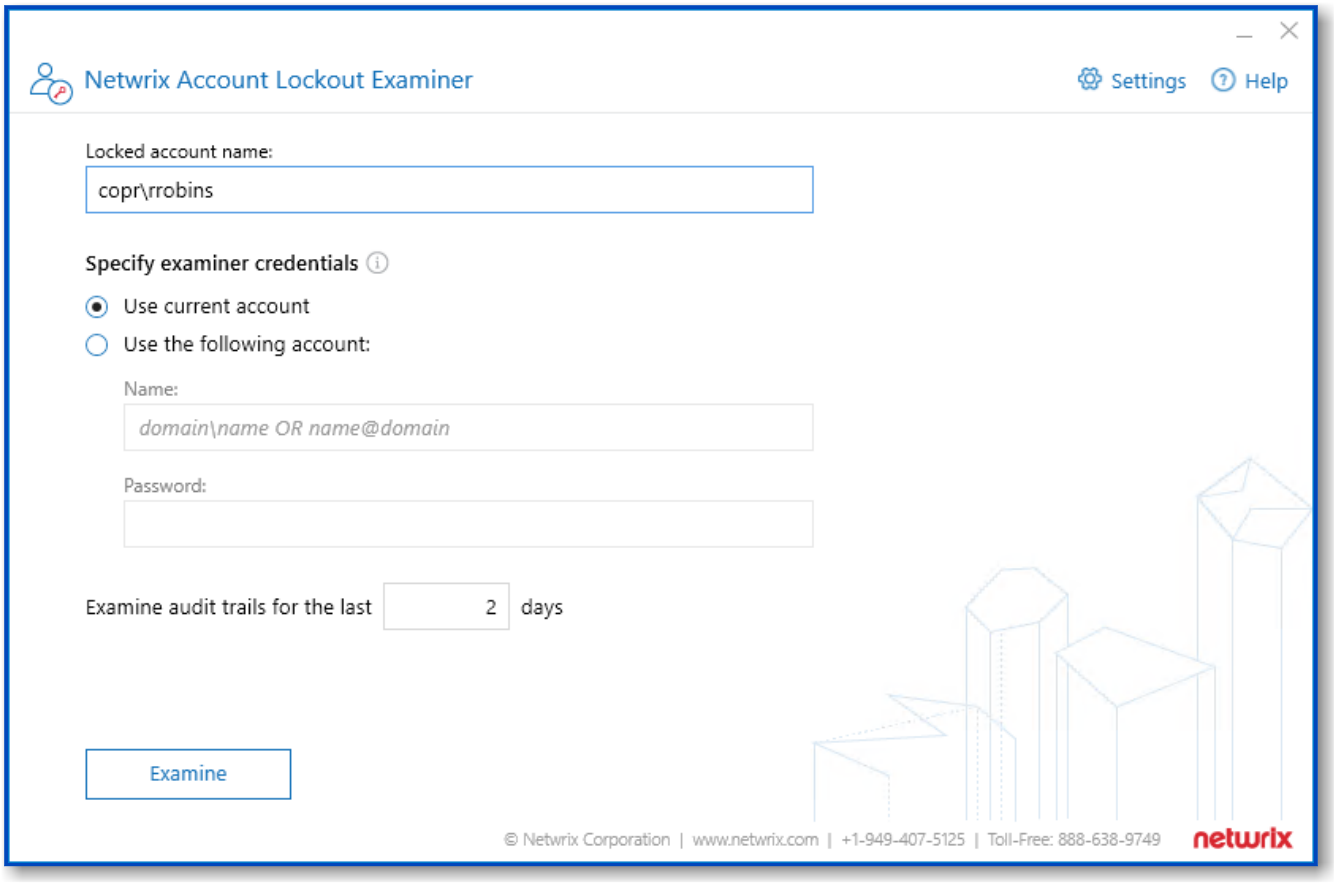
To start using **Netwrix Account Lockout Examiner**, download it from Netwrix web site. Once the download completes, run the executable from your browser menu or from your **Downloads** folder.

To find out why an Active Directory account was locked out, perform the following steps:

1. Set up the auditing as described in Planning and Preparation section.
2. Download the application onto a computer within the domain where lockouts happen.
3. Run the application. When prompted, accept the end-user license agreement.
4. If you wish, select to participate in Netwrix Customer Experience Improvement program. You can later change your preference using the product settings (see the next section for details).



5. In the main window, supply the name of the account that was locked out.
6. Specify examiner credentials – the user account that will be used to run the examination, access domain controllers, and so on. The account must be a member of the **Domain Admins** group.
7. Click **Examine**.



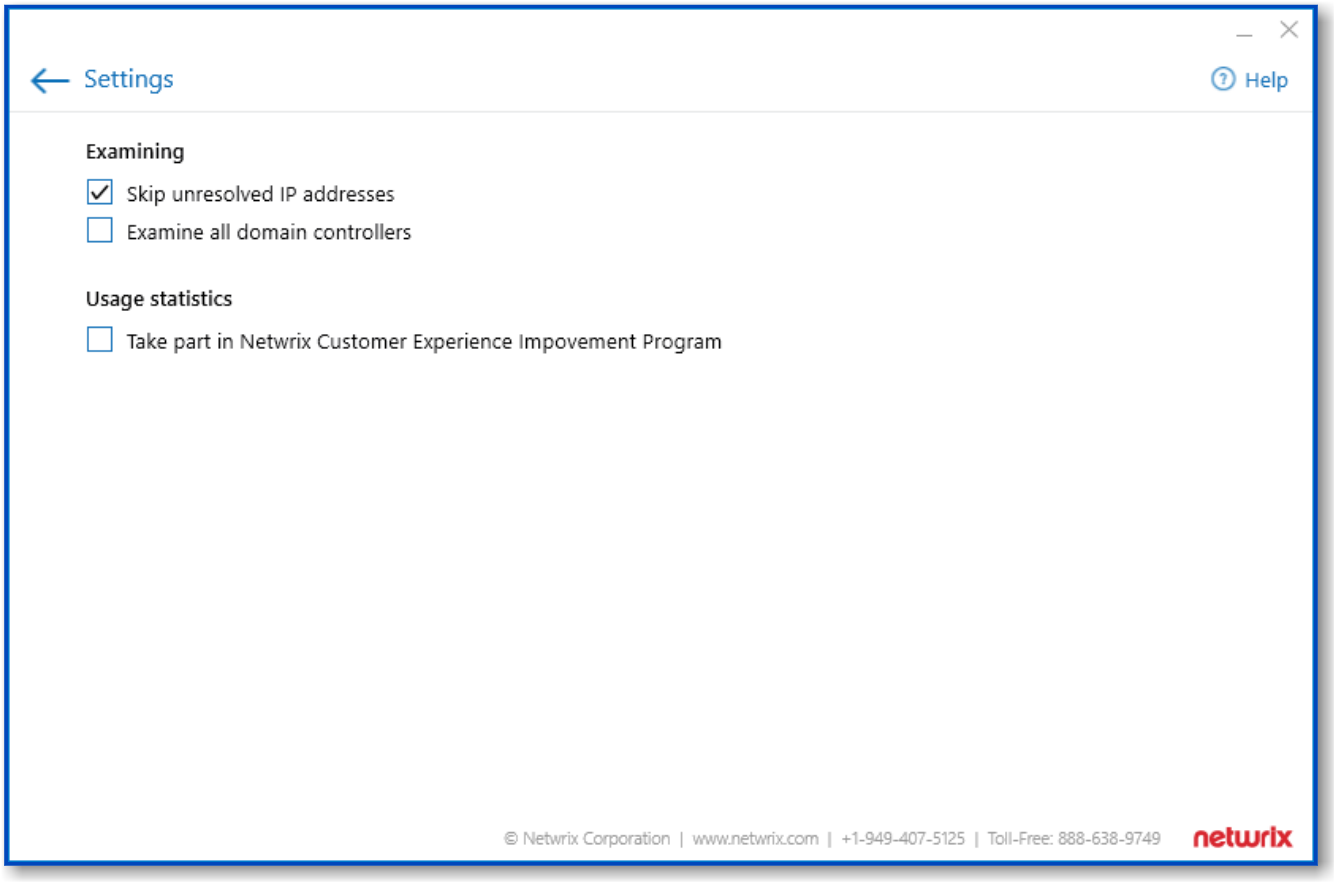
Once the examination completes, you will be presented with a list of reasons why the account you supplied is being locked out.

Modifying product settings

After you click **Settings** in the main window, you can apply the following options:

Option	Description	Default
Examining		
Skip unresolved IP addresses	For safety reasons, Netwrix Account Lockout Examiner by default does not connect to the unknown and potentially dangerous IP addresses. See this Knowledge Base article for more information.	Enabled
Examine all domain controllers	Select this option if you want to examine all domain controllers to detect potential lockout reason.	Disabled

Option	Description	Default
Usage statistics		
Take part in Netwrix Customer Experience Improvement program	Select this option to participate in the program. See this Knowledge Base article for more information on the program.	

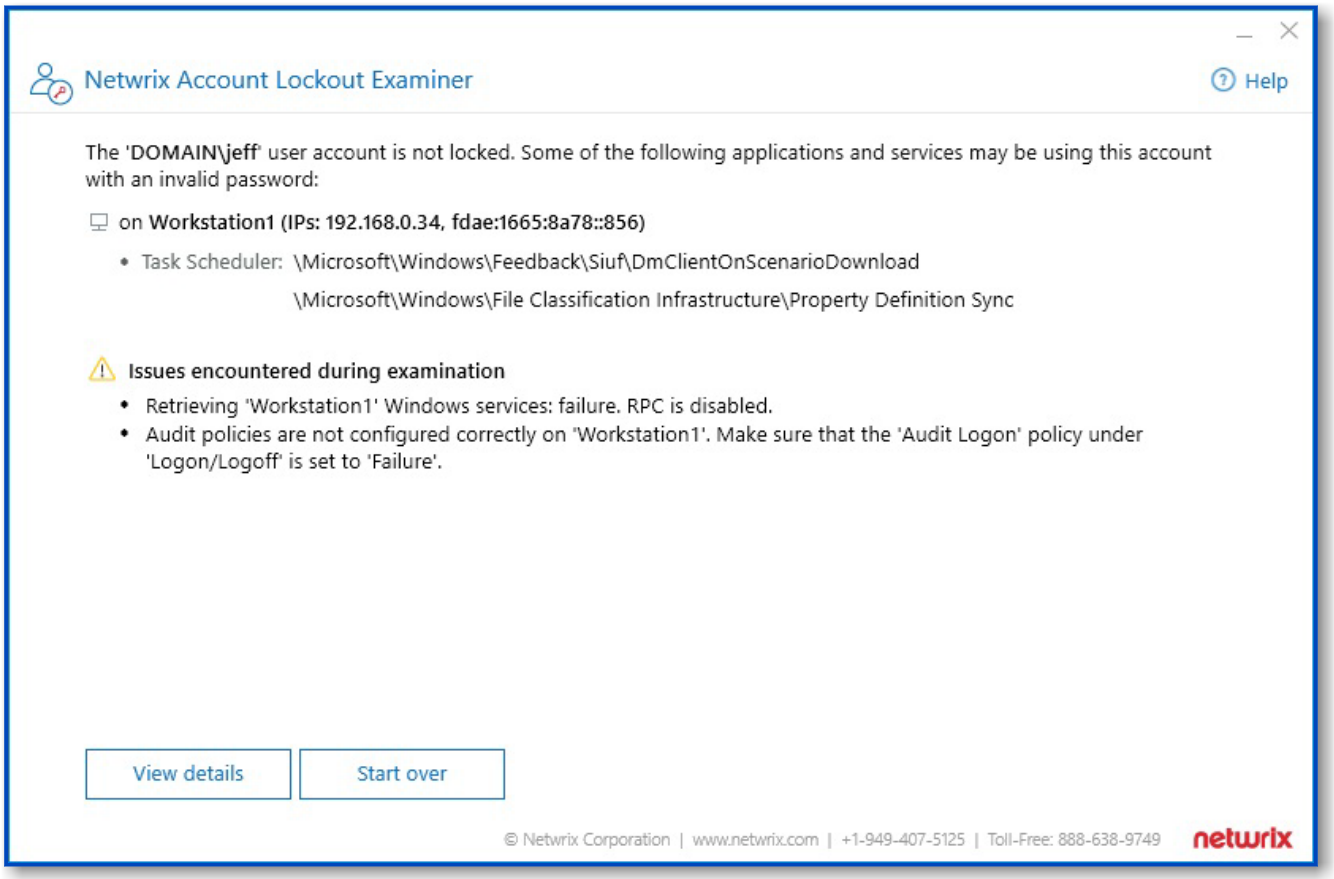


Troubleshooting

Log files of Netwrix Account Lockout Examiner can be found in the *%ProgramData%\Netwrix Account Lockout Examiner\Logs* folder.

Symptom	Cause	Solution
In the environments with root/child domains, you may receive the *"Could not query ComputerName. Access is denied."* error.	The account used to run Netwrix Account Lockout Examiner is not a member of the local **Administrators**	Make sure this account is included in the local **Administrators** group.

Symptom	Cause	Solution
	group on the workstations in both root and child domains. Administrative rights are required to access the Security Event logs on these workstations.	
Issues encountered during examination section is shown in the examination results.	Most probably this means that **Netwrix Account Lockout Examiner** cannot reach some of the data sources it needs.	• Check that you have configured the audit settings in the target domain as described in Required audit settings section. • Check that network connectivity between the Account Lockout Examiner machine and the domain controllers in your domain works properly.



We welcome any feedback and ideas you might have. Please take a minute to check in on Netwrix page at Spiceworks or submit direct feedback via this link.

Access Reviews

Netwrix Auditor supports integration with Netwrix Auditor Access Reviews, which enables business owners to conduct resource and group reviews and recommend changes. The integration is available for the following data sources:

- Active Directory
- Dell Data Storage (only Unity family)
- NetApp
- Nutanix Files
- Qumulo
- SharePoint Online
- Synology
- Windows File Servers

Getting Started

This workflow assumes you already have Netwrix Auditor installed with configured monitoring plans for a supported data source.

NOTE: Access Reviews is a separately licensed product and is not included with Netwrix Auditor. Make sure that you have the Access Reviews license enabled in Auditor.

See the Licenses topic for additional information.

Remember, there is one single Access Review license for all data sources that can send data to the application.

Follow the steps to use Netwrix Auditor Access Reviews in conjuction with Auditor.

Step 1 – Install Access Reviews on the same computer where Netwrix Auditor is installed. See the Installation Overview topic for prerequisites and additional information.

Step 2 – Configure Access Reviews. The Configuration interface is only available to users with the Administrator role. See the Administrator Overview topic for configuration settings and enabling user access.

Step 3 – Use the Access reviews configuration tool to setup the data flow from the Auditor database to the Access Reviews database. See the Select Data Sources topic for additional information.

NOTE: Data upload speed depends on the amount of collected data and Auditor collectors configuration.

Step 4 – Configure resource ownership through the Access Reviews Console. The Resource Owners interface is available to users with either the Security Team or Administrator role. Managing ownership is core component for the Access Reviews workflow. See the Resource Owners Overview topic for additional information.

NOTE: The Owners & Access Reviews topic and subtopics are written for the assigned owners. You can distribute the URL to this topic or download a PDF to be distributed to your assigned resource owners.

Step 5 – Configure and run reviews. The Entitlement Reviews interface is available to users with either the Security Team or Administrator role. See the Reviews Overview topic for additional information.

Netwrix Auditor Access Reviews is now configured and ready to use.

Considerations & Limitations

Review the following considerations:

1. Enabling State-in-Time data collection for your monitoring plans option is not required for the integration works properly.
2. The data collected by Auditor is updated at least once a day.
3. If a monitoring plan or a data source with enabled integration is deleted, all collected data will be removed from the Access Reviews database.
4. If there are errors in upload of data to the Access Reviews database, these errors are reflected in the Netwrix Auditor Health Log and text log files; status of items and data sources in Auditor is not affected by these errors.
5. Permissions-related considerations:

- For Windows File Servers, permission data for all items in this data source is sent to the Access Reviews application;
- Only effective top-level permissions are sent (share+NTFS);
- Permission data is sent per file server (entirely for each server);
- Transfer of permission data to the Access Reviews application is started when you enable the integration for a data source.

Getting Started

The Access Reviews application is installed with a Builtin Administrator account used to enable console access. Launch the Access Reviews Console using the desktop icon for the first time and set the password for the Builtin Administrator account. Then log in with that account. See the First Launch topic for additional information.

Initial Configuration

Next, configure the Access Reviews for your environment:

- Console Users — Grant users access to the application starting with an Administrator account. There are two levels of access: Administrator and Security Team. See the Console Access Page topic for information.
  - Optionally, disable the Builtin Administrator account. See the Modify the Builtin Administrator Account topic for additional information.
- Notification — Configure the Notification settings required in order for the application to send email. See the Notifications Page topic for information.

Enable Console Users

Access Reviews Console users granted one of the available roles should be notified.

RECOMMENDED: The notification should include:

- Why your organization is using Netwrix Auditor Access Reviews

- What they will be doing in the Access Reviews Console
- How to log into the Access Reviews Console, specifically what URL and credentials to use

You should also provide links to the appropriate topics based on the user's role:

- Security Team — Need topics that align to the work the will be doing in the Access Reviews Console:
  - Ownership Administrator — Send the URL link for the Resource Owners Overview topic
  - Review Administrator — Send the URL link for the Reviews Overview topic
- Administrator — Send the URL link for the Administrator Overview topic

Resource Ownership Configuration

Ownership of resources must be assigned in order to use the Access Reviews workflow:

- Resource Ownership — Assign ownership for resources to be managed through the application. See the Resource Owners Interface topic for additional information.
- Enable Owners — Send a notification to your owners about resource ownership with the application. See the Notification to Owners topic for additional information.

Access Reviews Workflow

The Access Reviews applicaton runs attestations on resources and groups with the assigned owners. The workflow consists of:

- Reviews — Configure reviews for resource Access or group Membership
- Owner Performs Review — Owners process the review, potentially recommending changes
- Review Administrator Approval — Review and process owner recommended changes

RECOMMENDED: Set expectations for response time from owners.

Reviews can be run multiple times, maintaining a historical record for each instance. See the Reviews Overview topic for additional information.

Installation Overview

The Netwrix Auditor Access Reviews application relies on collected and analyzed data that is stored in a Microsoft® SQL® Server database. Netwrix Auditor must be installed and collecting data before installing and using the Access Reviews application. The Access Reviews Configuration tool must be used after installation to complete the integration of these products.

NOTE: Access Reviews is a separately licensed product and is not included with Netwrix Auditor. Make sure that you have the Access Reviews license enabled in Auditor.

Prerequisites

The Access Reviews application must be installed on the same server as Netwrix Auditor.

Permissions

Permissions are needed to the Netwrix Auditor database and to Active Directory. This can be one account with sufficient rights to each or two separate accounts. For the purpose of this document, these will be referred to as the Database service account and the Active Directory service account.

- Database service account – This is the same account used by Netwrix Auditor for a database service account. This credential is required for installation.

  NOTE: Database connection via TLS 1.2 (SQL Native Client) is supported.

- Active Directory service account – The Access Reviews Console login authentication requires the Active Directory service account to have rights to "read" Active Directory. This credential is configured during installation based on the account used for connecting to the database. See the Active Directory Page topic for additional information.

Software Compatibility & Versions

For proper functionality, it is necessary for the version of the Access Reviews to be compatible with the existing Netwrix Auditor installation. If necessary, Netwrix Support can confirm whether the two product versions are compatible.

Latest Version Compatibility

Component	Current Version
Netwrix Auditor Console	10.7*
Netwrix Auditor Access Reviews	v12.0*

Last Updated 6/6/2022

See the Upgrade Procedure topic for additional information.

Supported Browsers

Supported browsers for the Access Reviews Console include:

- Google® Chrome®
- Microsoft® Edge®
- Mozilla® Firefox®

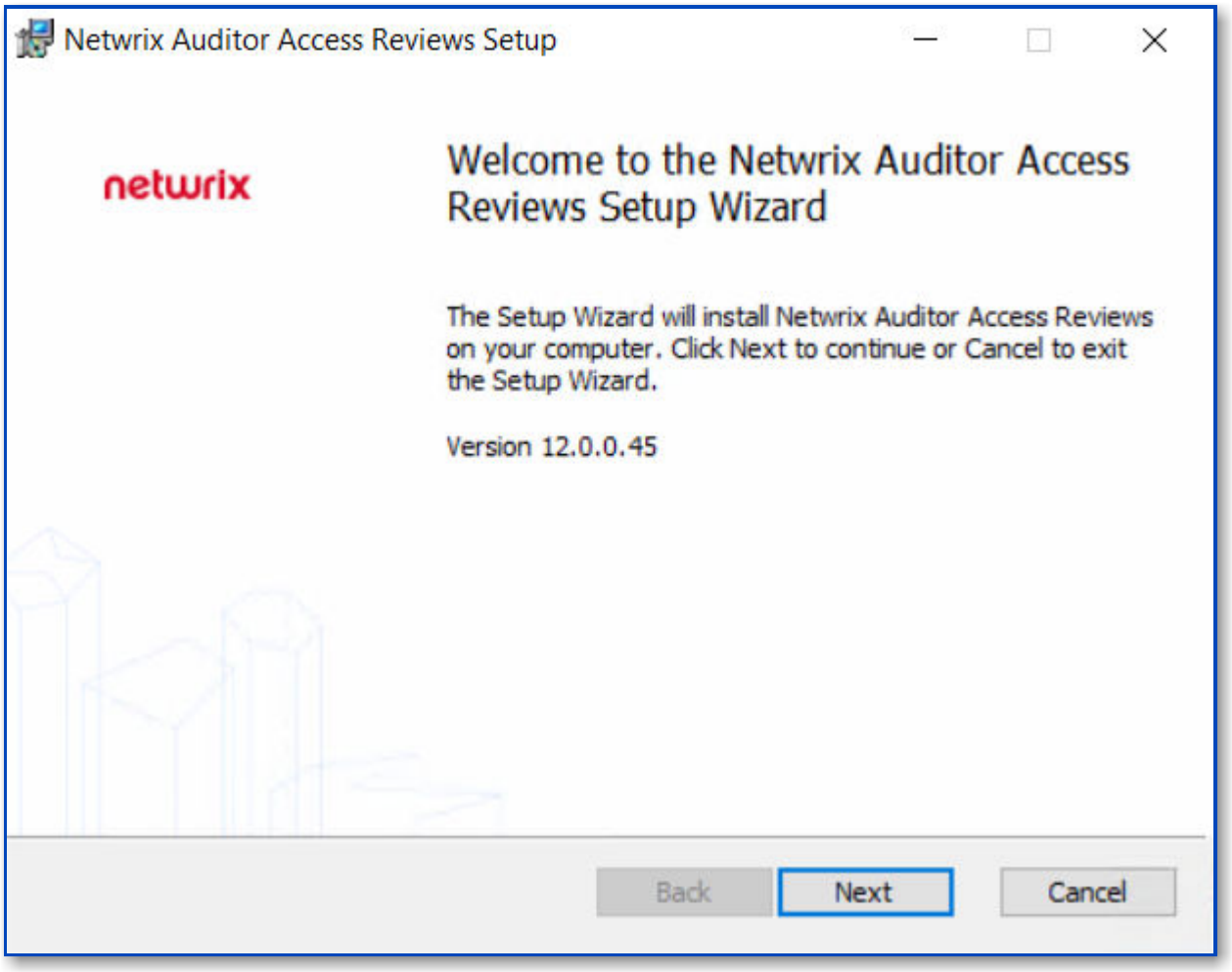
Screen Resolution Requirement

Supported screen resolution of 1368 x 768 or greater.

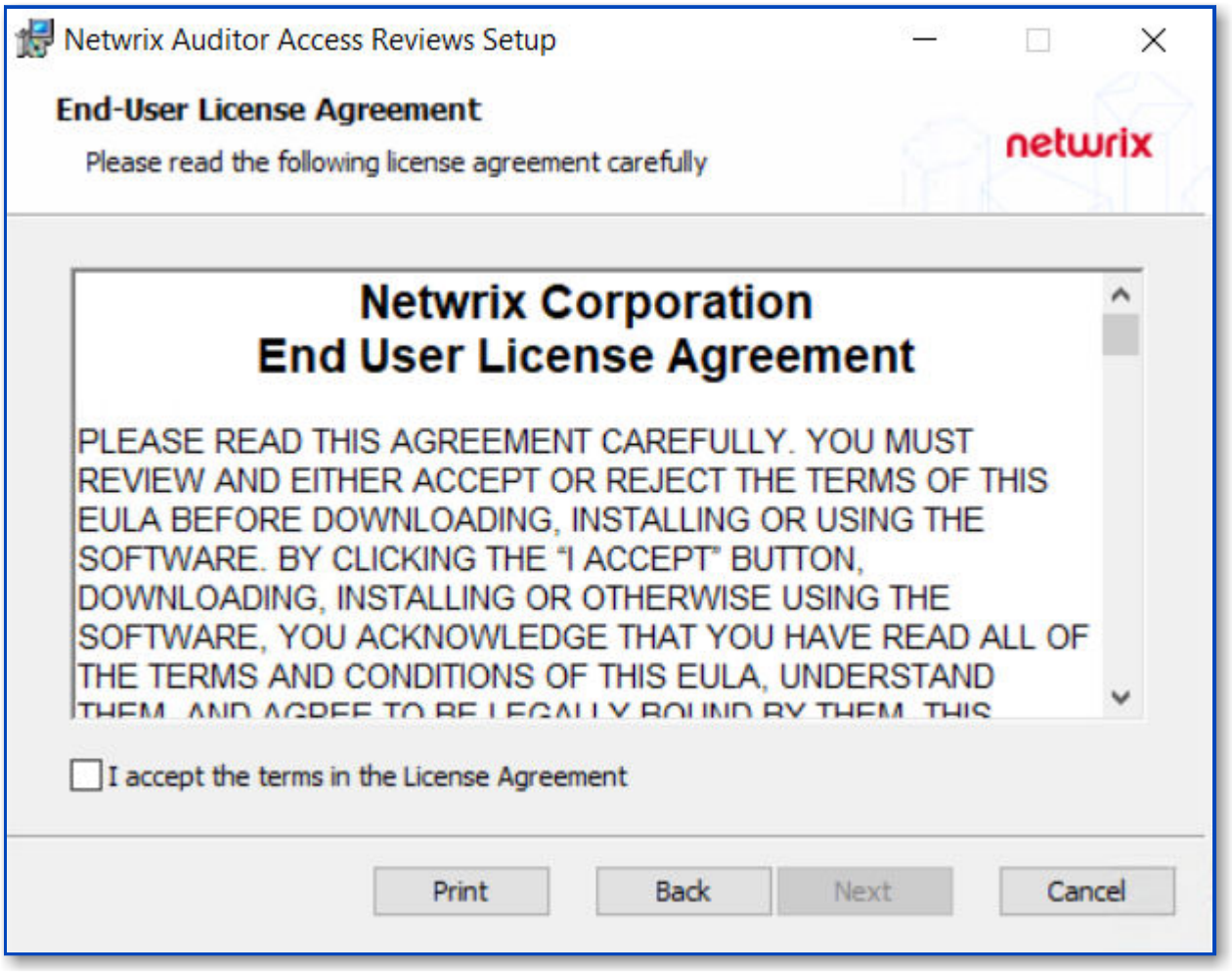
Install

Once the prerequisites have been met, follow the steps to install the Access Reviews application.

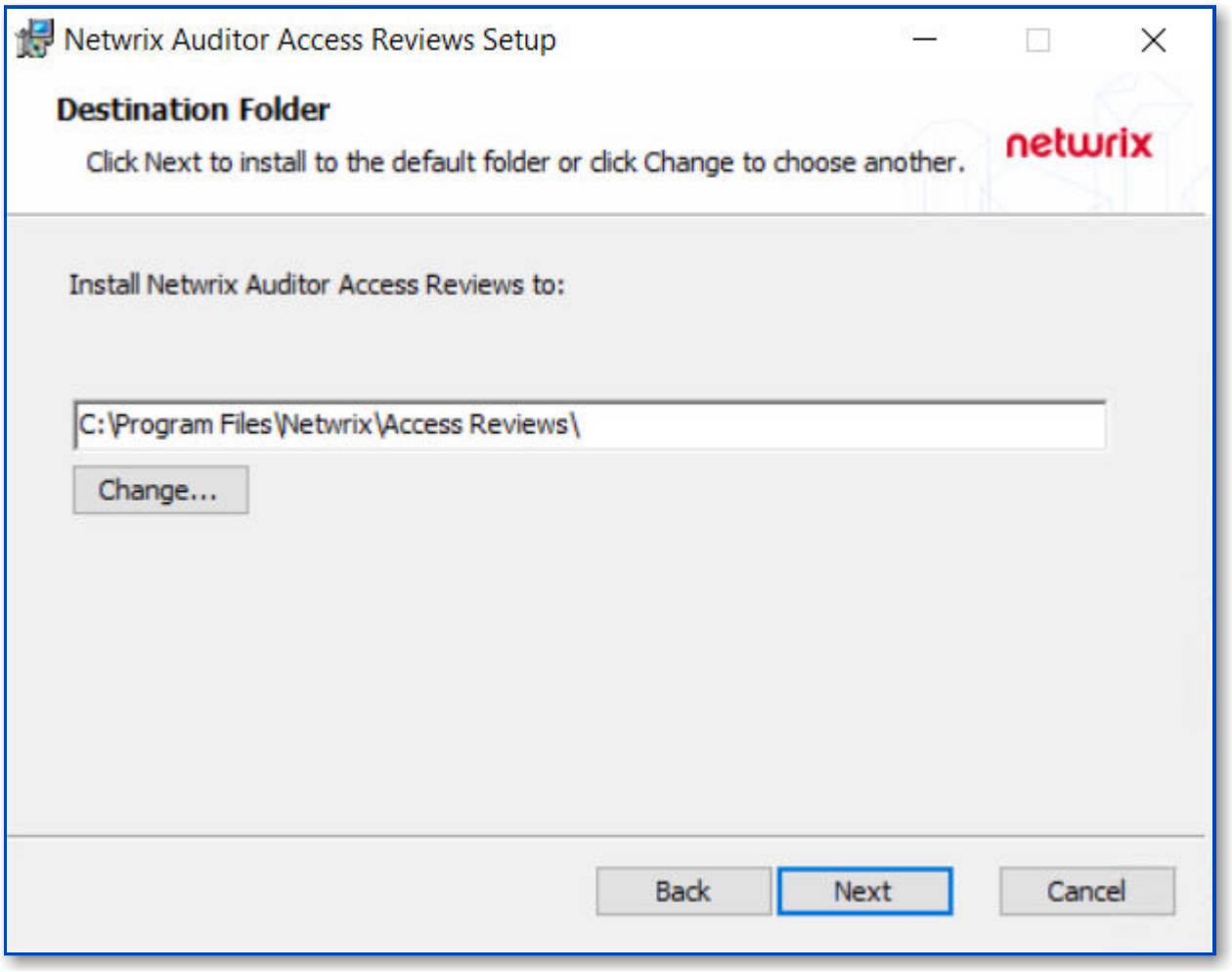
Step 1 – Run the `AccessReviews.exe` executable, and the Netwrix Auditor Access Reviews Setup wizard opens.



Step 2 – On the Welcome page, click the Next button to begin the installation process.

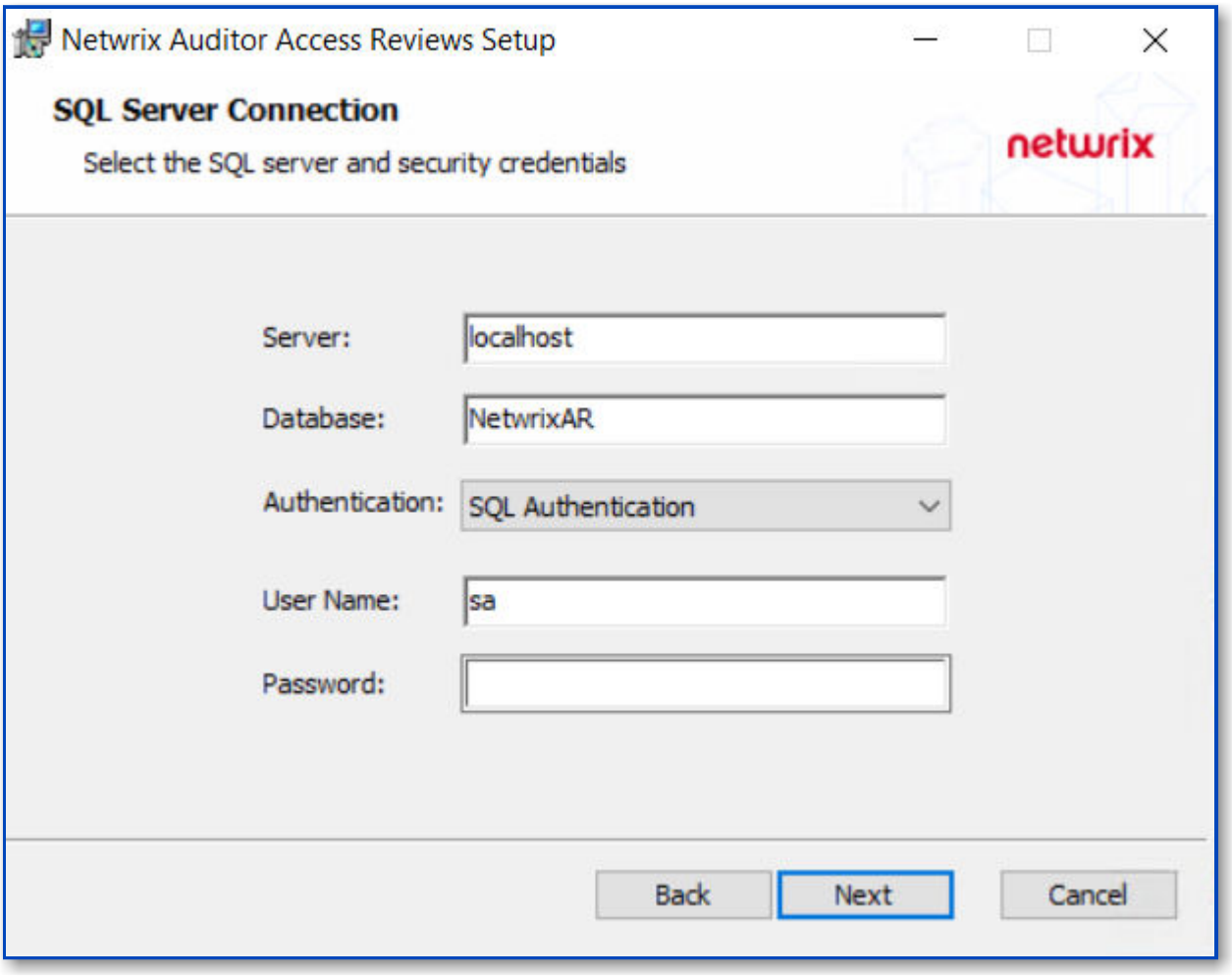


Step 3 – On the End-User License Agreement page, check the **I accept the terms in the License Agreement** box and click **Next**.



Step 4 – On the Destination Folder page, you can choose between the default destination folder and a custom folder. Click Change to browse for a different location. When the destination is set as desired, click **Next**.

NOTE: The default location is `C:\Program Files\Netwrix\Access Access Reviews\`. There are no specific requirements for changing the path.

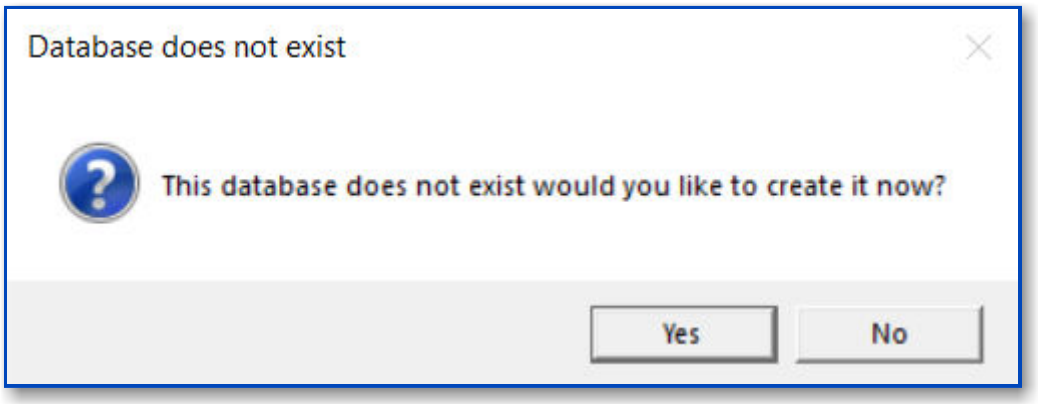


Step 5 – On the SQL Server Connection page, provide the required database information. Click Next to test the connection to the SQL Server.

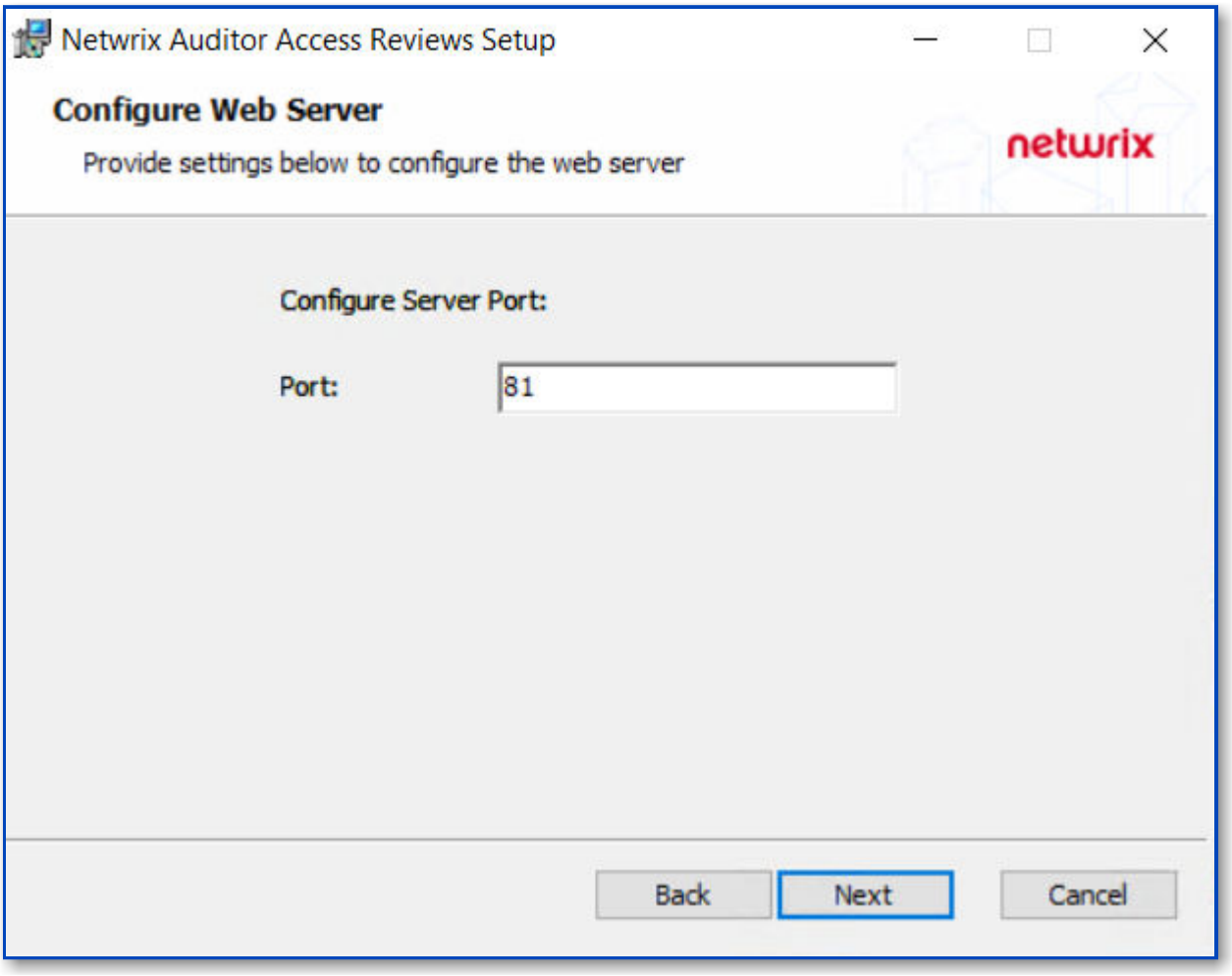
- Server — Enter the database server hostname (NetBIOS name, FQDN, or IP address) with the instance name or non-standard port, if applicable, in one of the following formats:
  - No named instance, use [SQLHostName], e.g. NT-SQL02
  - Named instance, use [SQLHostName]\[SQLInstanceName], e.g. NT-SQL02\Netwrix
  - No named instance with non-standard port, use [SQLHostName],[PortNumber], e.g. NT-SQL02,72
  - Named instance with non-standard port, use [SQLHostName]\[SQLInstanceName], [PortNumber], e.g. NT-SQL02\Netwrix,72
- Database — Enter the name of the database. By default, this is set to NetwrixAR.

- Authentication — Select the Database service account type from the drop-down menu. Then enter the account information in the **User Name** and **Password** fields.
  - For Windows Authentication — **User Name** format must be [DOMAIN]\[username] , e.g. NWXTECH\ad.bruce

NOTE: See the Database Page topic for additional information.

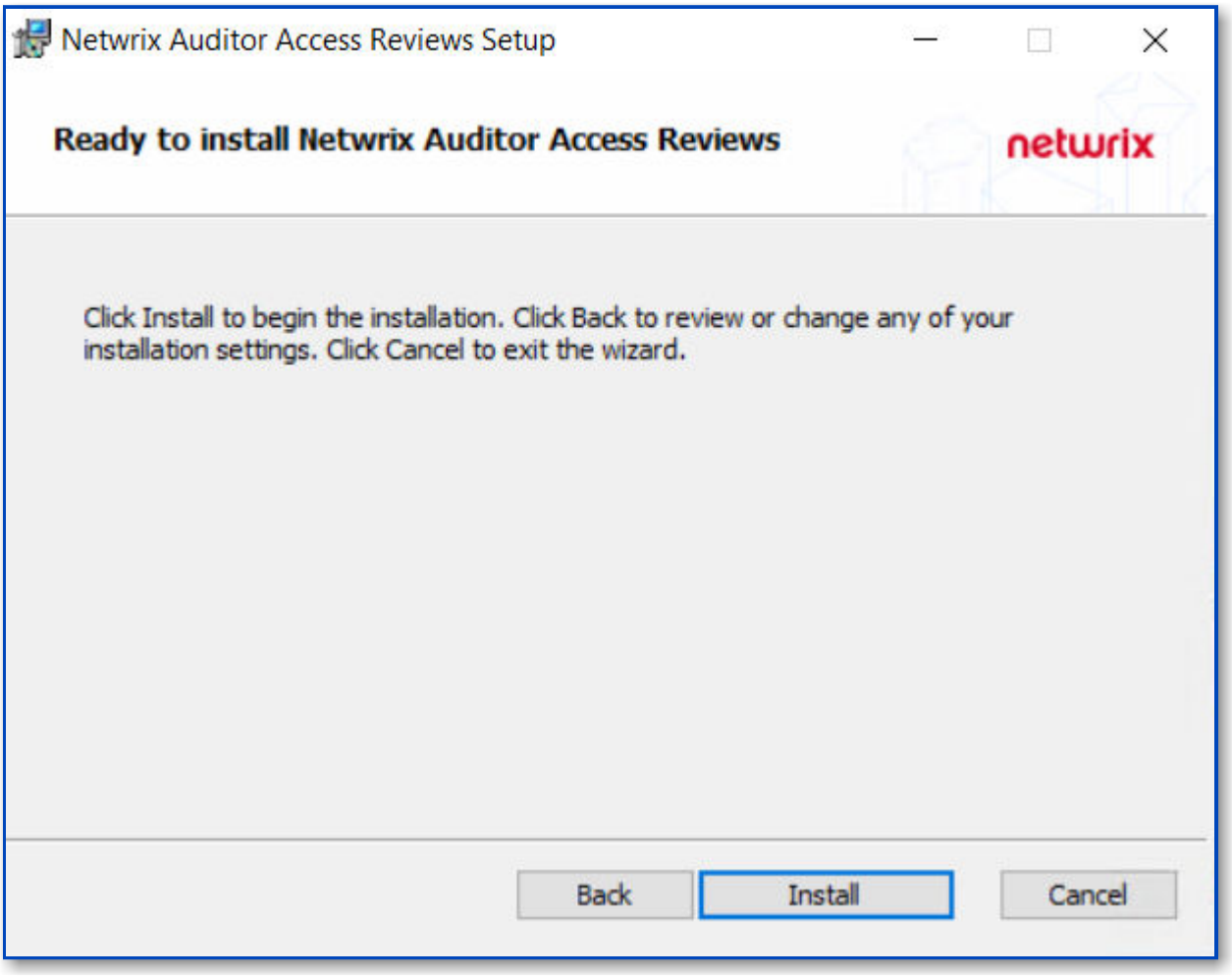


Step 6 – If there are no errors, you will be asked to confirm creation of the new database. Click **Yes**.

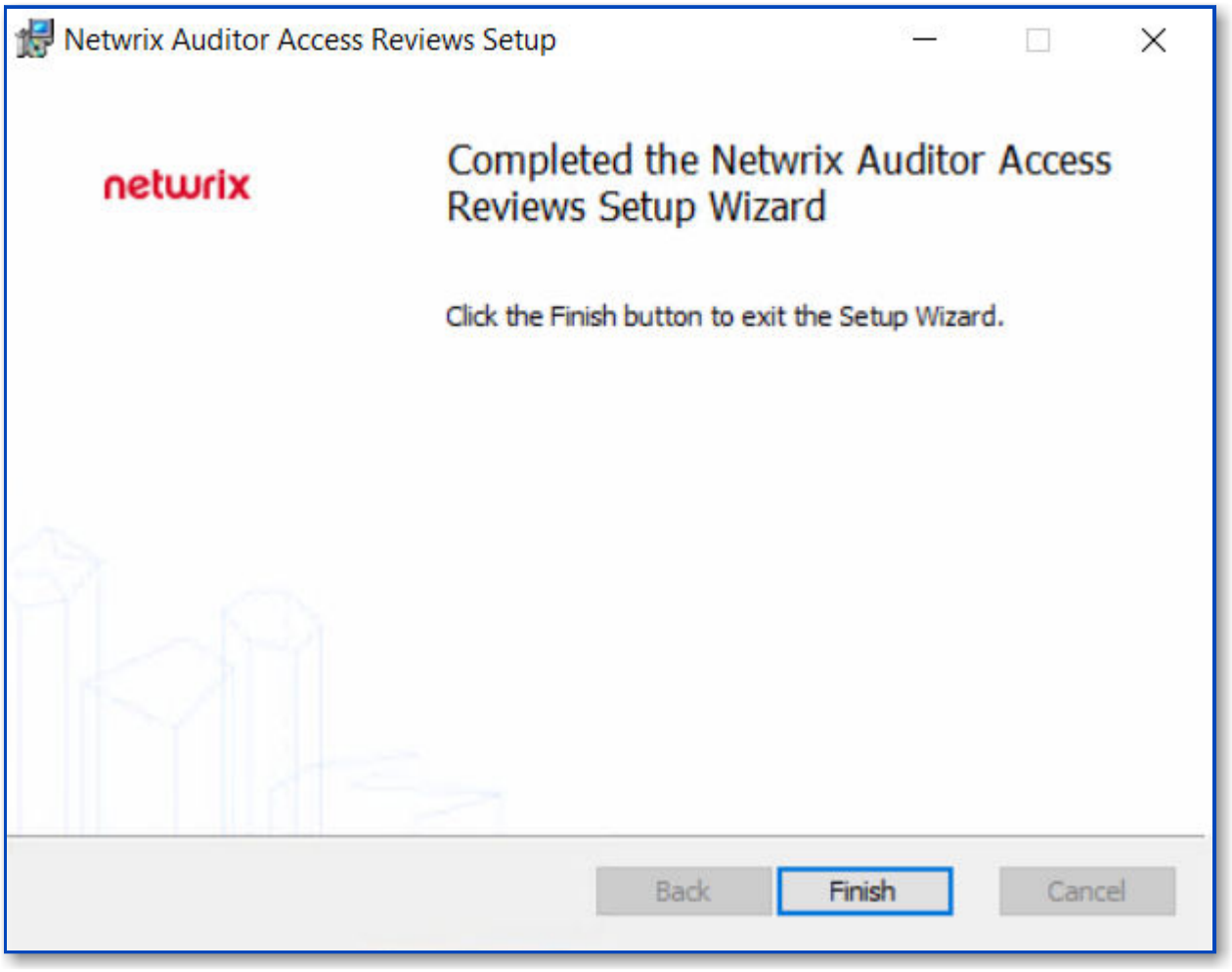


Step 7 – On the Configure Web Server page, you can choose between the default port and a custom port on which the application will be accessible. To change the port, enter a new port number in the field. When the port is set as desired, click **Next**.

NOTE: The default port is 81.



Step 8 – On the Ready to install page, click Install to begin the process.



Step 9 – Once the installation has successfully completed, click Finish to exit the wizard.

The installation wizard placed a Netwrix Auditor Access Reviews icon on the desktop. Now proceed to the First Launch topic for next steps.

Select Data Sources

Remember, the *Access Reviews* must already be installed on the *Auditor* server.

You can configure Netwrix Auditor Access Reviews in two ways:

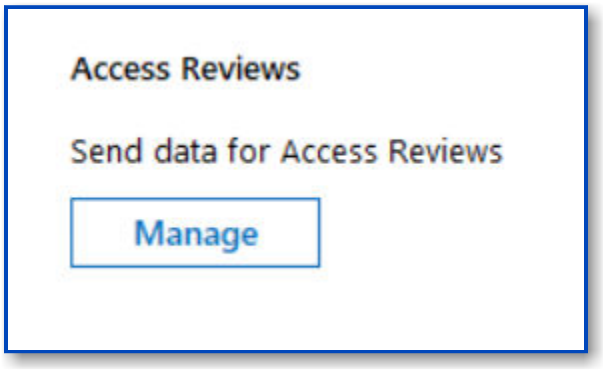
- Select Data Sources in the General Settings
- Select Data Sources in the Monitoring Plan

Select Data Sources in the General Settings

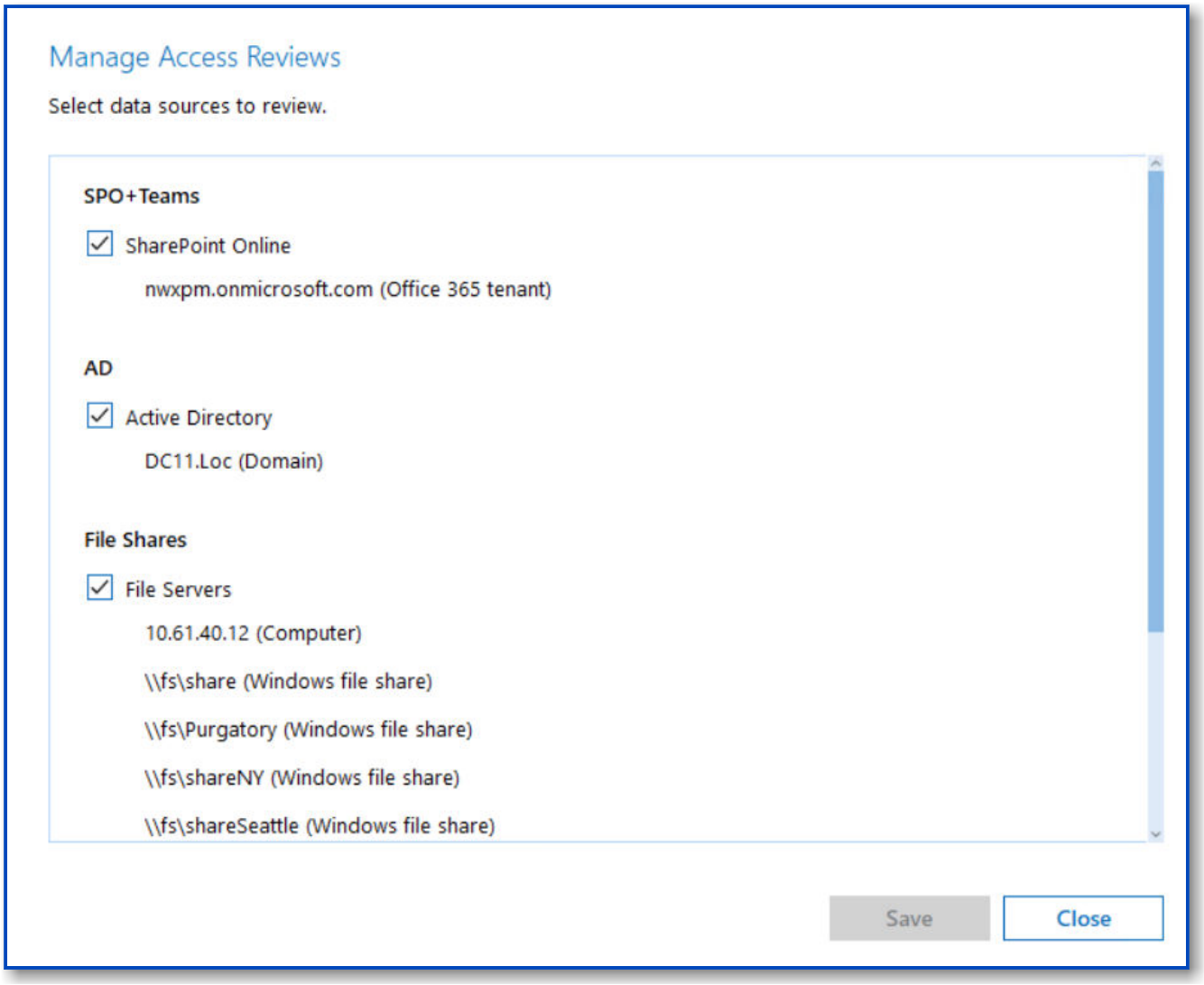
If you plan to use Access Reviews for multiple data sources, configure the settings to work with the data sources that you select.

Follow the steps to configure Access Reviews in the Netwrix Auditor.

Step 1 – Go to **Settings > General > Access Reviews**.



Step 2 – Click **Manage**.



Step 3 – Select the desired data sources to review.

Step 4 – Click **Save**.

Netwrix Auditor Access Reviews is configured and ready to use in the Netwrix Auditor.

Select Data Sources in the Monitoring Plan

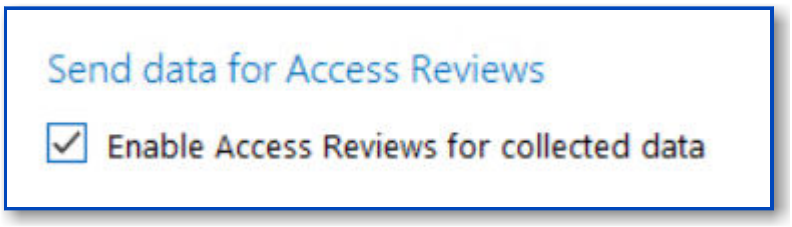
If you plan to use Access Reviews for a specific monitoring plan, configure Access Reviews in that monitoring plan.

Follow the steps to configure Access Reviews in the Netwrix Auditor.

Step 1 – Go to **Configuration > Monitoring plans**.

Step 2 – Double click the desired monitoring plan.

Step 3 – Click **Edit data source** button on the left.



Step 4 – Navigate to the Send data for Access Reviews and select the checkbox.

Step 5 – Click **Save** or **Save & Close**.

Netwrix Auditor Access Reviews is configured and ready to use in the Netwrix Auditor.

Secure Console Access

Enable Secure Sockets Layer (SSL) for secure, remote connections to the application web server. In order to enable SSL, you need to create a certificate and then bind it to the secure port.

NOTE: Organizations typically have one or more system administrators responsible for Public Key Infrastructure (PKI) and certificates. To continue with this configuration, it will first be necessary to confer with the PKI administrator to determine which certificate method will conform to the organization's security policies.

Follow the steps to enable SSL.

Step 1 – Create an SSL Binding.

Step 2 – Modify the AccessInformationCenter.Service.exe.Config File.

The Access Reviews application is now configured to use SSL for secure, remote connections.

Create an SSL Binding

You run a PowerShell command to create an SSL binding. The binding command has several environmental variables:

- The `$certHash` value is the `Thumbprint` value.

- The `$ip` value of the IP addresses. In the example script below, the value [0.0.0.0] is set for all IP addresses.
- The `$port` value must be accurate for your environment. The HTTP default port is 81. The HTTPS default is 481. However, it can be customized during installation.
- The `$guid` value is required for specifying a valid GUID value to identify the owning application for a binding purpose. It obtained from any valid GUID.

If you need to find the `$certHash` value of a certificate that was already created, run the PowerShell `dir` command below on the certificate's drive. This will output the Thumbprint (Hash) value and the certificate name:

```
dir cert:\localmachine\my
```

Replace the environmental variables in the example script below. Then Run the PowerShell command to create an SSL binding:

```
$guid = "1be32670-7644-4dce-9a5d-01643022074e"

$certHash = "03CFD5D51A0DAA2F3DCDA9407486B220449D0E92"

$ip = "0.0.0.0"

$port = "481"

"http add sslcert ipport=$($ip):$port certhash=$certHash appid={$guid}" |
netsh
```

The next step is to modify the `AccessInformationCenter.Service.exe.Config` file.

Modify the AccessInformationCenter.Service.exe.Config File

Follow the steps to modify the Modify the `AccessInformationCenter.Service.exe.Config` file for HTTPS.

Step 1 – Open the `AccessInformationCenter.Service.exe.Config` file in a text editor, e.g. Notepad. It is located in the installation directory:

```
...\Netwrix\Access Reviews
```

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2"/>
    </startup>
    <appSettings>
  <add key="ConfigurationVersion" value="2.0" />
  <add key="BindingUrl" value="http://+:81" />
  <add key="LogLevel" value="2" />
  <add key="DisclaimerMessage" value="" />
  <add key="AuthSessionTimeout" value="15" />
```

Step 2 – Change the `BindingUrl` key value to `"https://+:481"` (ensure the port number matches the port number used in the PowerShell command run to create the SSL Binding.

Step 3 – Save and close the file.

Step 4 – Restart the Netwrix Auditor Access Reviews service in Services Manager (`services.msc`).

The URL for the Access Reviews Console is now accessible `https://[Fully Qualified Domain Name for the Machine]:481` (if port 481 was used when creating the binding). For example, https://NEWYORKSRV10.NWXTech.com:481.

Upgrade Procedure

CAUTION: If you are upgrading from the Netwrix Access Information Center for Netwrix Auditor to the Netwrix Auditor Access Reviews application, see the Special Considerations topic for upgrade steps.

To upgrade the Access Reviews application to a newer version, simply run the new `AccessReviews.msi` executable. It is not necessary to uninstall the existing version. See the Install topic for additional information.

Remember, the *Access Reviews* version must align to the compatible *Netwrix Auditor* version.

When the installer is run over an existing version, the following is happening in the backend:

- During the installation process, a Backup folder is created in the Access Reviews installation directory

  `...\Netwrix\Access Reviews`

  - The Backup folder contains the files where various settings reside listed in the table below

- The backup folder files are copied over the default files laid down by the installer, preserving customized settings
- After the installation is complete, the Backup folder is removed

File	Location	Guidance
Email Templates (multiple files)	Located in the Backup folder	The HTML templates that are used to send notification email. These can be customized with logos or corporate branding.
AccessInformationCenter.Service.exe	Located in the Backup folder	Contains custom application settings and logging levels.
Version.txt	Located in the Backup folder	Indicates the version number associated with the backup contents.

Special Considerations

The originally released Netwrix Access Information Center has been rebranded to Netwrix Auditor Access Reviews. This rebranding project included changing the installation directory, the name of the service, and the default name of the database created by the installer. Follow the steps to replace Netwrix Access Information Center with Netwrix Auditor Access Reviews.

Step 1 – Install the Netwrix Auditor Access Reviews application on the same server where the Netwrix Access Information Center was installed. See the Install topic for additional information. On the SQL Server Connection page:

- Supply the information for the existing database. The default name for the original database was NetwrixAIC. However, it could have been Customized.
- Use the same credentials for the SQL Server Connection.

NOTE: The new destination folder will be `...\Netwrix\Access Reviews`.

Step 2 – Launch the application and reset the Builtin Administrator password. See the First Launch topic for additional information.

Step 3 – It will be necessary to add your Console Users again. See the Console Access Page topic for additional information.

Step 4 – It will be necessary to configure the Notification settings. See the Notifications Page topic for additional information.

Step 5 – If you have customized your email templates, it will be necessary to copy the Templates folder from the old `...\Netwrix\Access Information Center` installation directory to the new `...\Netwrix\Access Reviews` installation directory.

All of the resources with assigned owners will be visible on the Resource Owners tab. All reviews will be visible on the Entitlement Reviews tab.

After the upgrade has been confirmed to be successful, you can optionally remove/delete the old installation directory: `...\Netwrix\Access Information Center`.

Administrator Overview

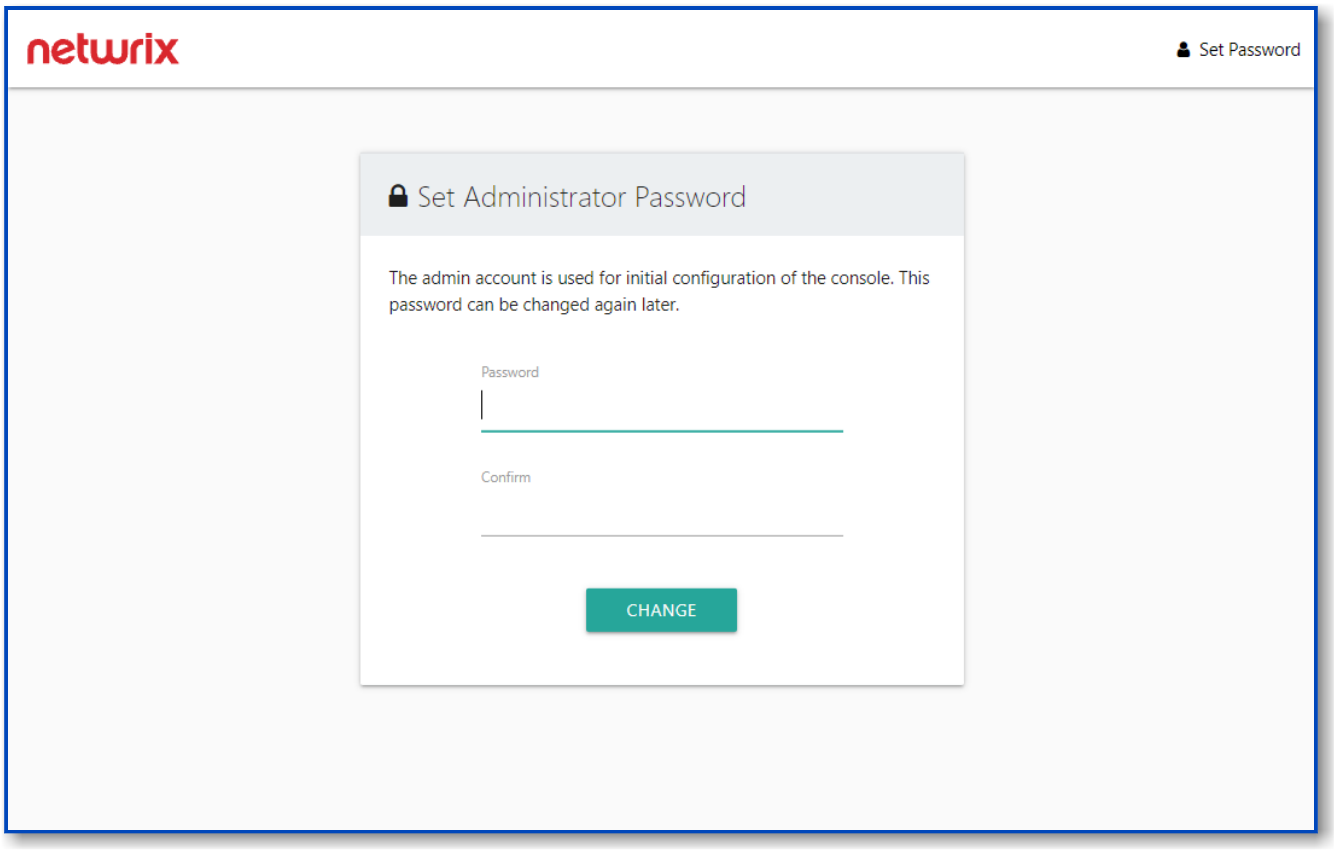
Access Reviews administrators have access to the Configuration interface where there application settings reside. This topic includes the following subtopics:

- Getting Started
- First Launch
- Navigation
- Configuration Interface Overview
- Additional Configuration Options
- URL & Login
- Troubleshooting

First Launch

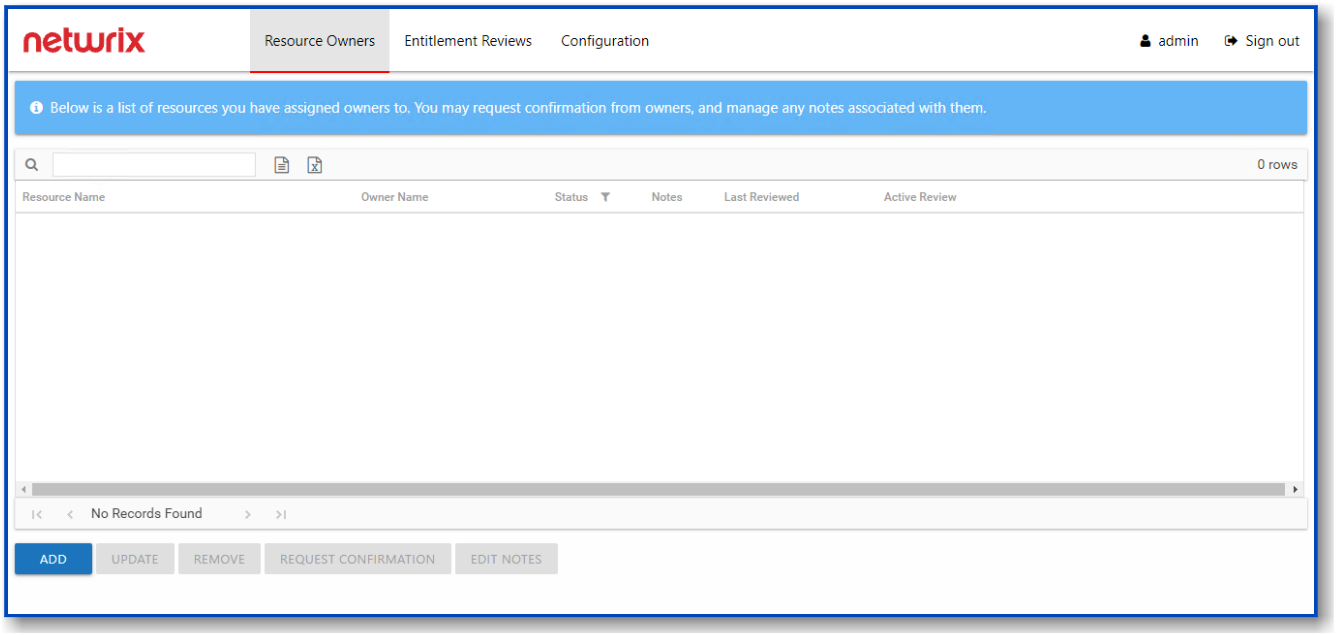
The installer places the following icon on the desktop which opens the Access Reviews Console:

Use this icon to launch the Access Reviews Console for the first time.



The Access Reviews application is installed with a Builtin Administrator account; "admin" is the User Name. You will be prompted to set the account's password. It must be eight or more characters long. After setting the password, you will need to login with the "admin" account.

Using the Configuration interface, the Builtin Administrator account can be disabled once a domain account has been granted the Administrator role. You can also change the password for the Builtin Administrator account. See the Modify the Builtin Administrator Account topic for additional information.



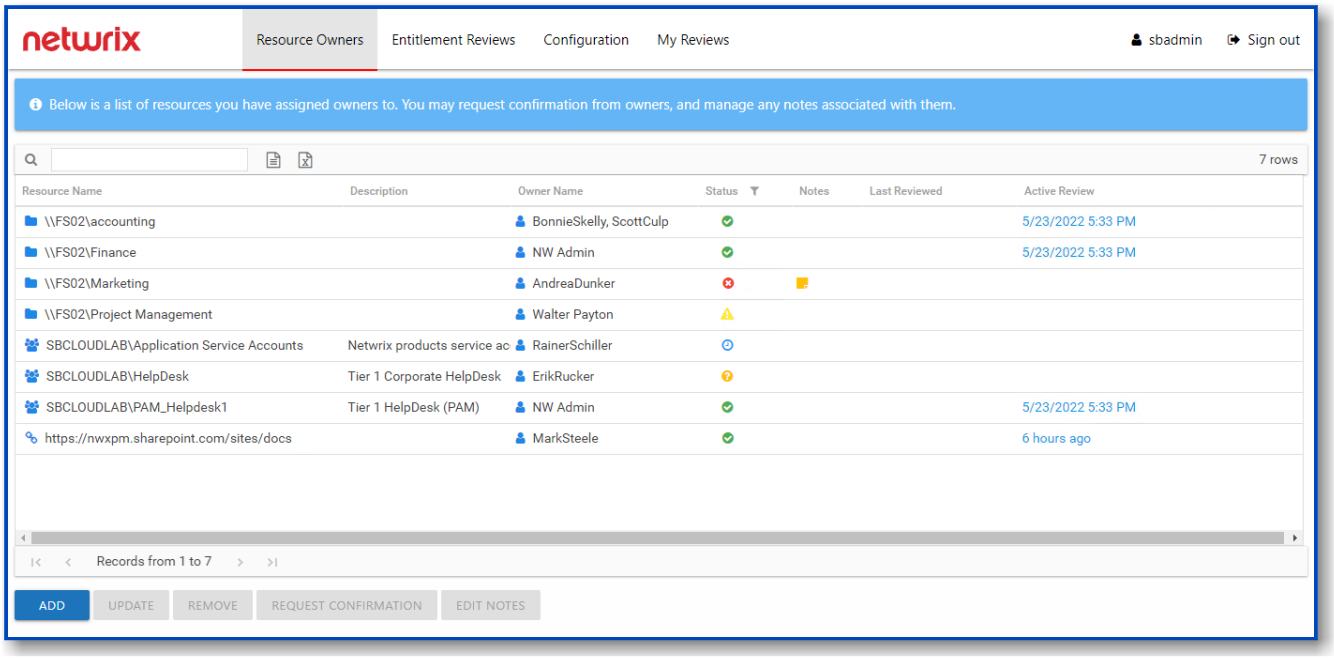
The Resource Owners interface opens. The first thing that should be done is to configure console access for domain users and configure notification settings. Select the Configuration tab. See the Console Access Page and Notifications Page topics for additional information.

The interfaces available to console users are controlled by the role assigned. Owners do not need to be assigned console access. See the URL & Login topic for information on how users will log in and where they are directed after login.

See the Navigation topic for information on each of the interfaces.

Navigation

The Access Reviews Console has four interfaces. Upon login, users granted console access are brought to the Resource Owners interface.



The signed in user is displayed in the upper-right corner, along with the **Sign out** link. The available interfaces change according to the role assigned to the user.

For Administrator Only

The Configuration tab opens the Configuration interface. Configure console access, Active Directory service account, notification settings, database access, and diagnostic logging level.

This interface is available only to users with the Administrator role. See the Configuration Interface Overview topic for additional information.

For Security Team & Administrator

The Resource Owners tab opens the Resource Owners interface. Manage resource ownership by assigning owners to resources and requesting ownership confirmation. Resources to be included in the Access Reviews workflow must first be assigned at least one owner within the Resource Owners interface. Assigned owners can log in to complete reviews.

This interface is available only to users with either the Security Team or Administrator role. See the Resource Owners Interface topic for additional information.

The Entitlement Reviews tab opens the Entitlement Reviews interface. Create and manage reviews. There are two types of reviews for resources being managed within the Access Reviews application: resource Access reviews and group Membership reviews. This does require the Access Reviews application to be configured to send notifications.

This interface is available only to users with either the Security Team or Administrator role. See the Entitlement Reviews Interface topic for additional information.

For Assigned Owner

The My Reviews tab opens the My Reviews interface. It is only visible if the logged in user is also an assigned owner of at least one resource. Assigned owners without a user role are directed to the My Reviews interface at login.

The My Reviews interface is available to any domain user who has been assigned ownership of a resource. See the Owners & Access Reviews topic for additional information.

Interface Quick Reference

The table below is a quick reference aligning each interface with its purpose, how to access it, and who has access to it:

Interface	Purpose	Opened By	Accessible To
Configuration	Configure console access, Active Directory service account, notification settings, database access, and diagnostic logging level.	**Configuration** tab	Administrator role
Resource Owners	Manage resource ownership by assigning owners to resources and requesting ownership confirmation.	**Resource Owners** tab	Administrator role Security Team role
Entitlement Reviews	Create and manage reviews.	**Entitlement Reviews** tab	Administrator role Security Team role

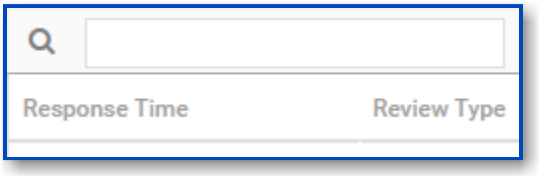
Interface	Purpose	Opened By	Accessible To
My Reviews	View and process pending reviews. Also view historical reviews.	**My Reviews** tab Direct from login for owners without a role	Assigned Resource Owners

Data Grid Features

The data grids within various tables have several features to improve your experience.

Search & Filter

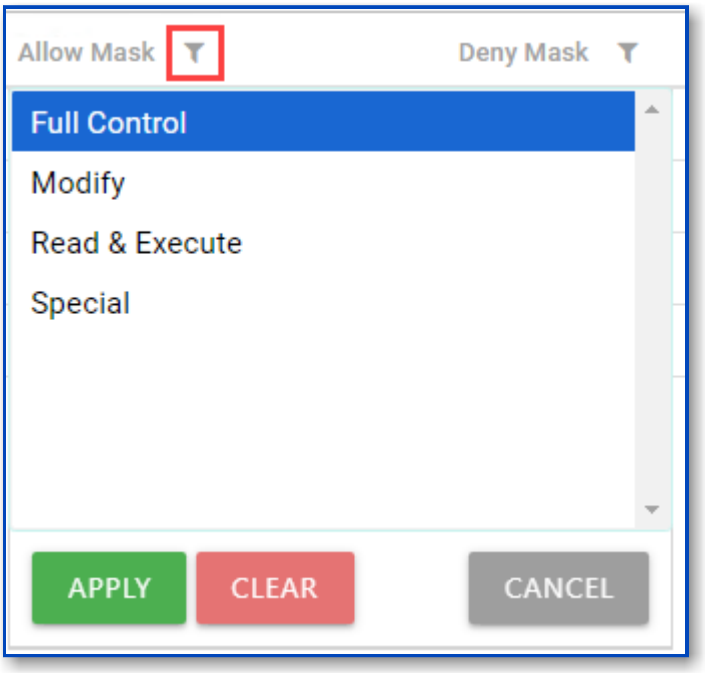
There is a Search box above a table's header row that can be used to filter the table data.



Begin typing in the Search box. The filter acts as a wildcard, filtering the table data as you type.

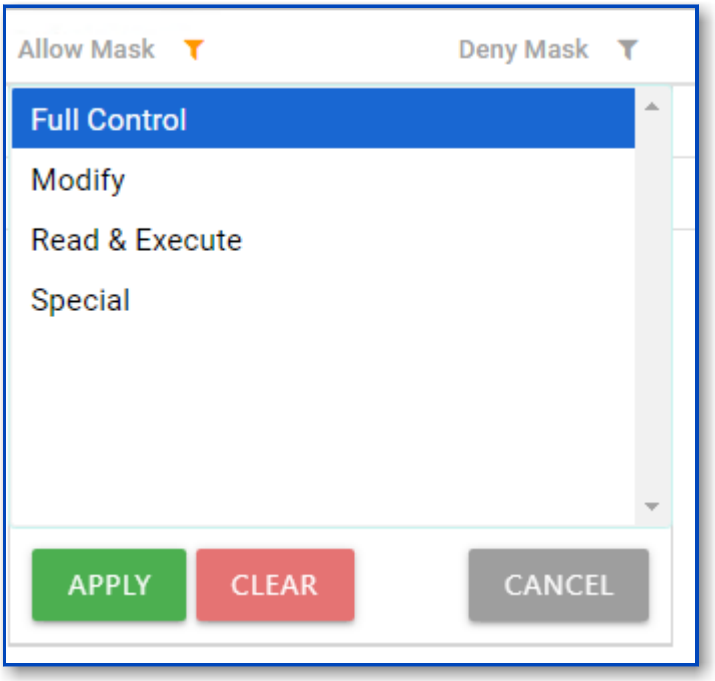
Column Filters

There is a filter icon to the right of each column name that can be used to apply a column specific filter. You can apply filters to multiple columns simultaneously.



Click the filter icon for the column you want to filter. Select the values you want to filter for from the list, and click **Apply**.

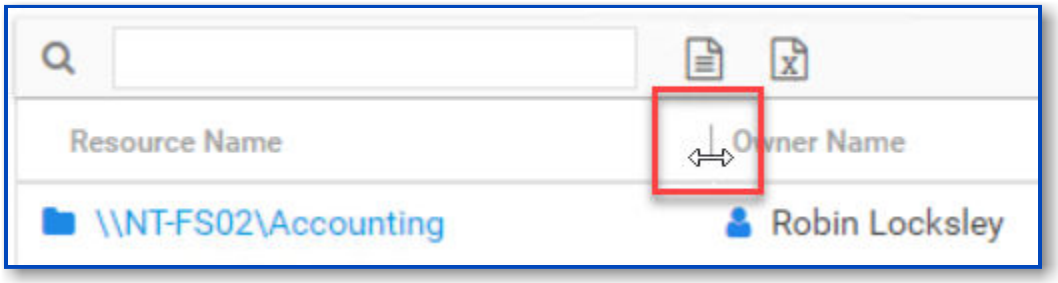
NOTE: Hold the **Shift** key and click the first and last values to select a group of adjacent values, or hold the **Ctrl** key and click each value to select multiple values individually.



The filter icon is highlighted orange for a column where a filter is applied. To clear an applied filter, click the filter icon and click **Clear**.

Resize Columns

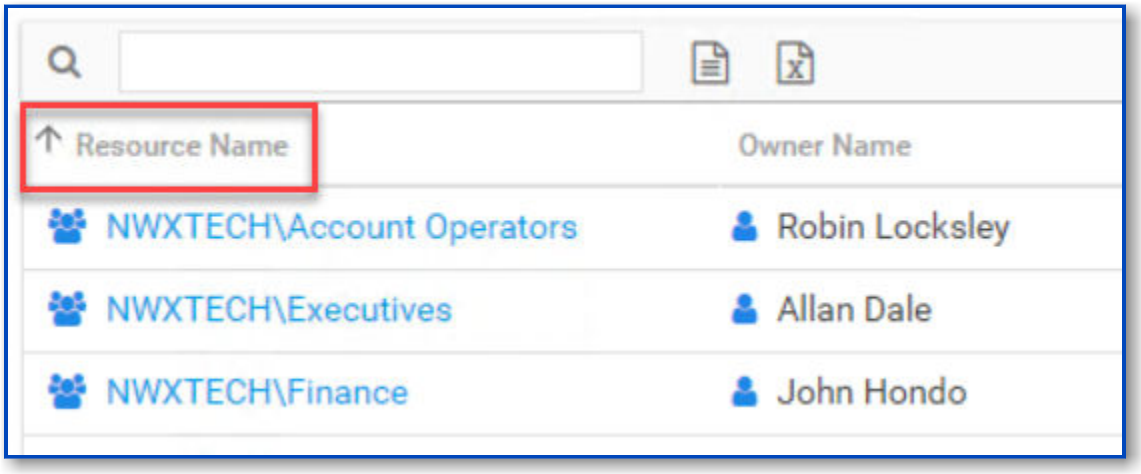
Table column widths can be resized to change the width.



Simply select the edges of the column headers and drag to the desired width.

Sort

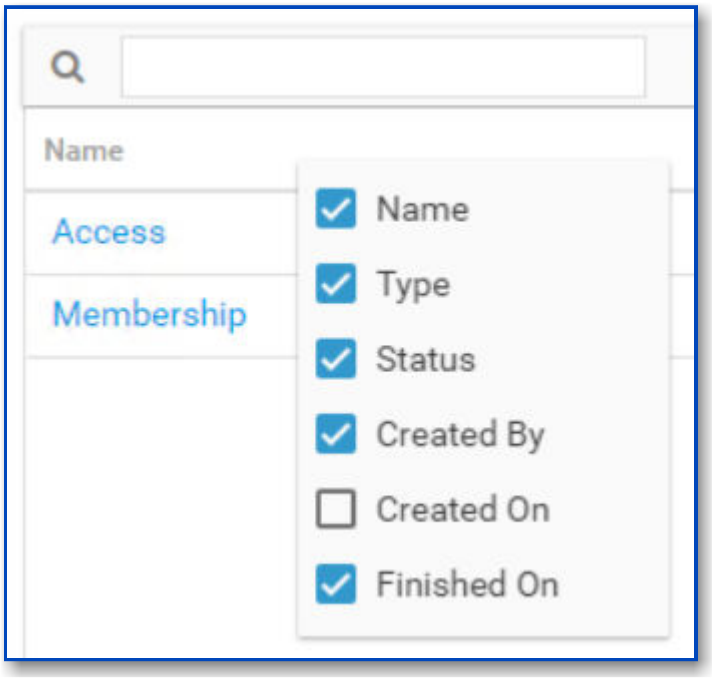
Data within a table can be sorted alphanumerically for a column.



Click on any column header. An arrow will appear next to the column name indicating the sort to be ascending or descending order.

Columns Selector

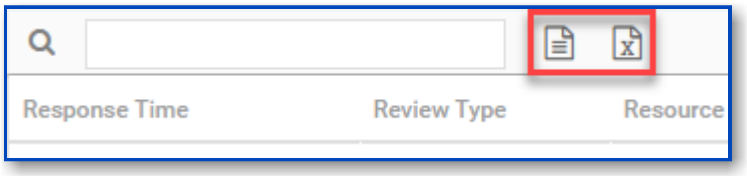
Columns can be hidden or unhidden. Available columns for a table are listed in the column selector menu that appears when you right-click on a column header.



The column selector menu shows all available columns for the table. Check columns are visible. Unchecked columns are hidden.

Exports

There are two export buttons above a table's header row that can be used to export the data currently displayed within the table.



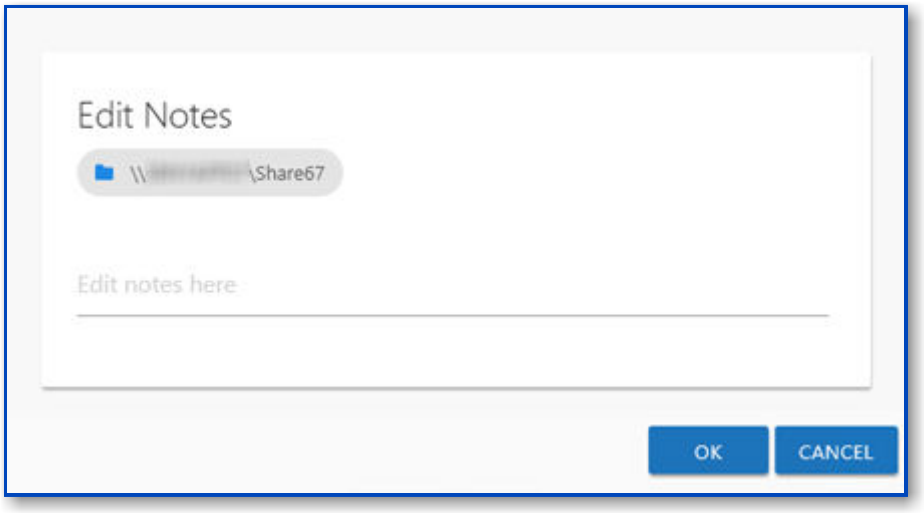
- CSV Export – Downloads the data within the table in a CSV file format
- Excel Export – Downloads the data within the table in an Excel file format

The export mimics the table with any sort, filter, or column modifications. The Excel or CSV file can then be distributed as desired. The Excel file presents an easy to read format, including information about the selected table and resource at the top. The CSV file displays column headers in the first row.

Edit Notes Window

The Edit Note window can be opened from a variety of interfaces. Follow the steps to add or edit a note.

Step 1 – Select the item in the interface and click Edit Notes. The Edit Notes window opens.



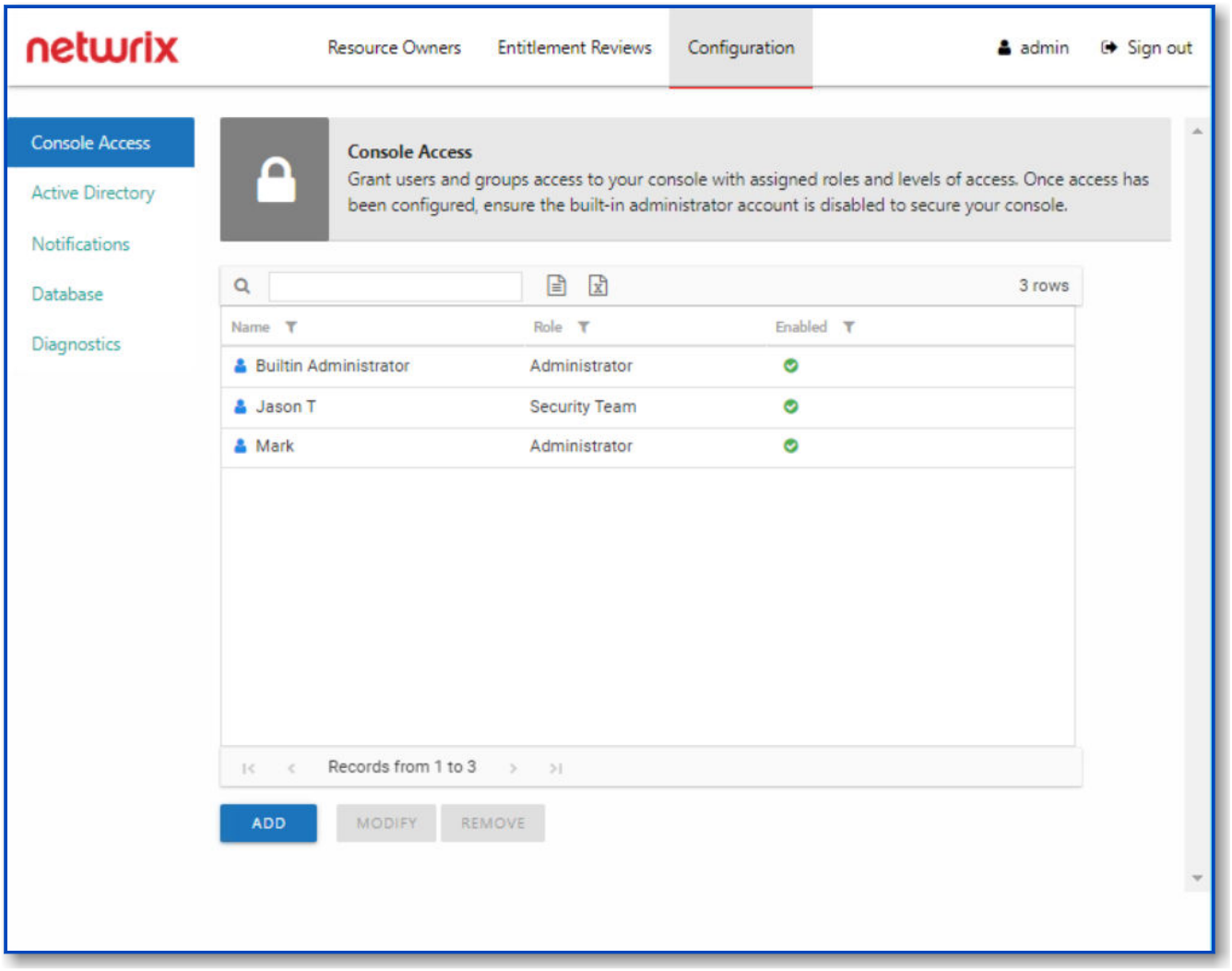
Step 2 – Type or edit the note in the textbox.

Step 3 – Click OK when finished. The Edit Notes window closes.

The user name and a date timestamp will appear at the beginning of each note added.

Configuration Interface Overview

The Configuration interface is available only to users with the Administrator role. It is opened by the **Configuration** tab.

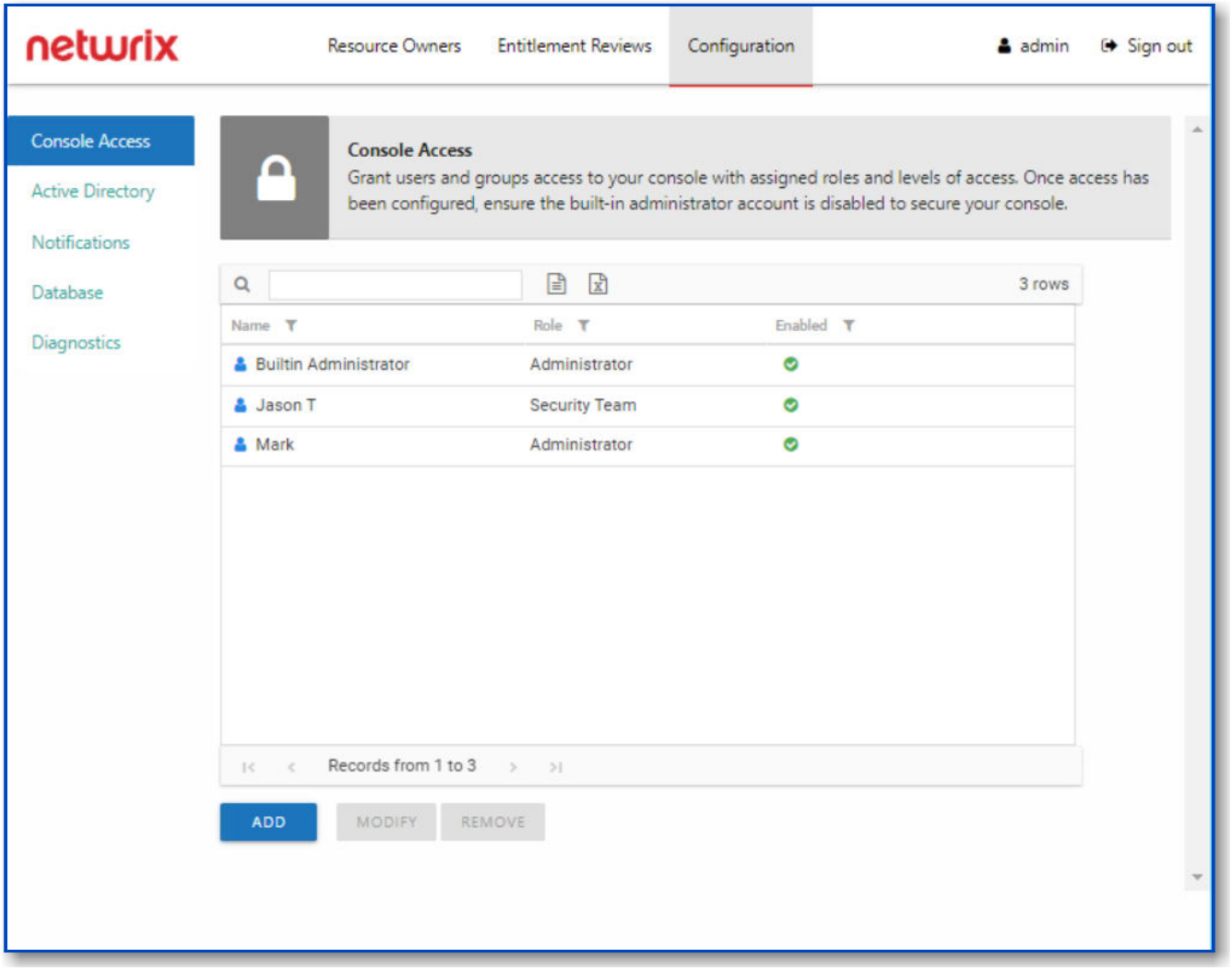


It has the following pages:

- Console Access Page – Grant users console access
- Active Directory Page – Configure the Active Directory service account used to add console users.
- Notifications Page – Configure the SMTP server, email security settings, notification options, and owner reminder settings
- Database Page – Configure the connection to the database
- Diagnostics Page – Download logs and enable debug log level for troubleshooting

Console Access Page

Console access is configured through the Configuration > Console Access page. Adding users to the Access Reviews Console requires the Active Directory service account to be configured.



There are two levels of access, or roles, which can be granted to domain users or groups:

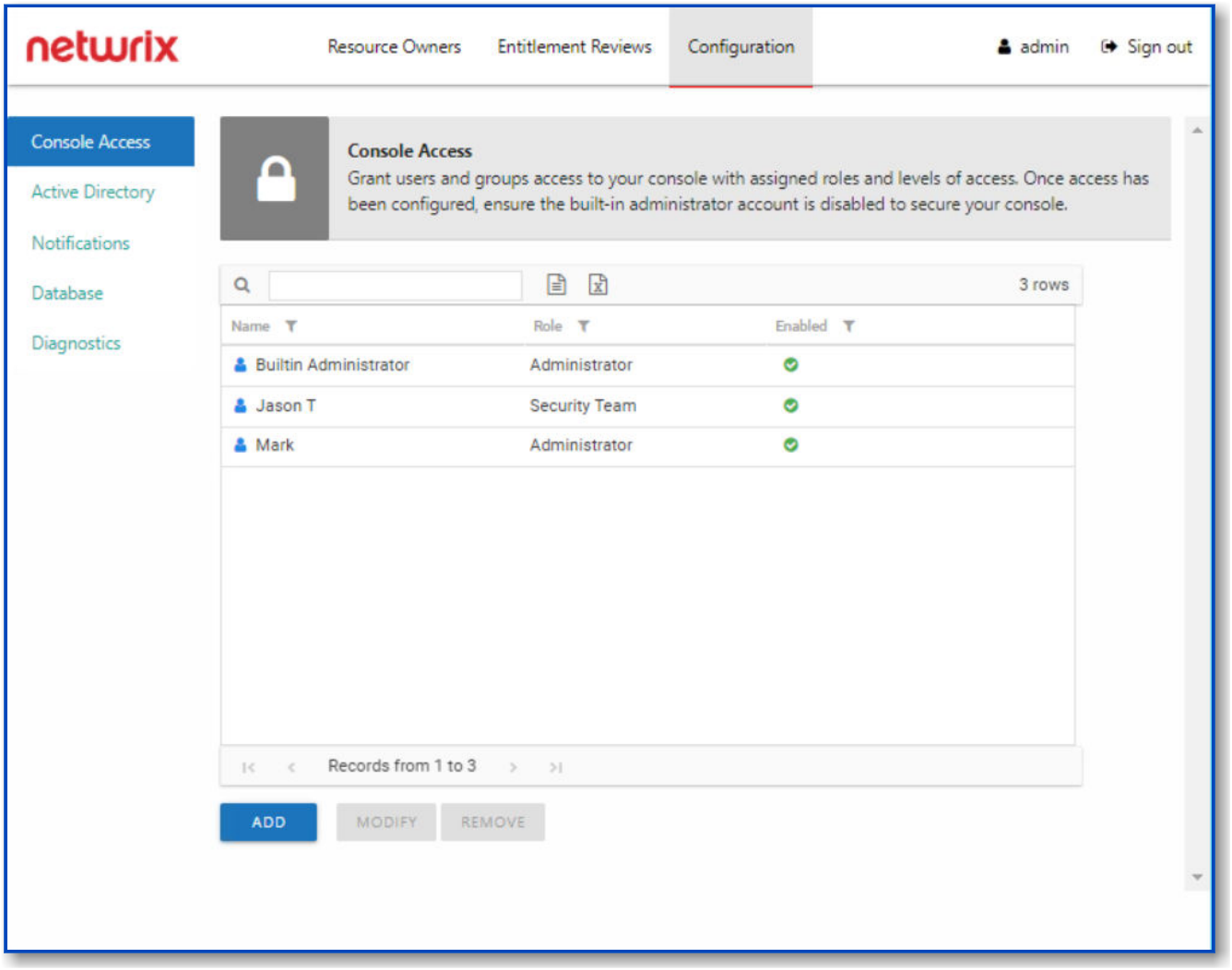
- Administrator – Role allows access to all interfaces including the Configuration interface
- Security Team – Role allows access to all interfaces except for the Configuration interface
    - In the Entitlement Reviews interface, this role can only view reviews that the logged in user has created.
    - Access can be limited by resource types (File System, SharePoint, or Active Directory)

CAUTION: Before disabling the Builtin Administrator account, it is necessary to first assign at least one domain user account to the Administrator role. Login with another Administrator account to disable the Builtin Administrator. Failure to do this could result in being locked-out of the Configuration interface. As an alternative to disabling this account, the password can be changed. See the Modify the Builtin Administrator Account topic for additional information.

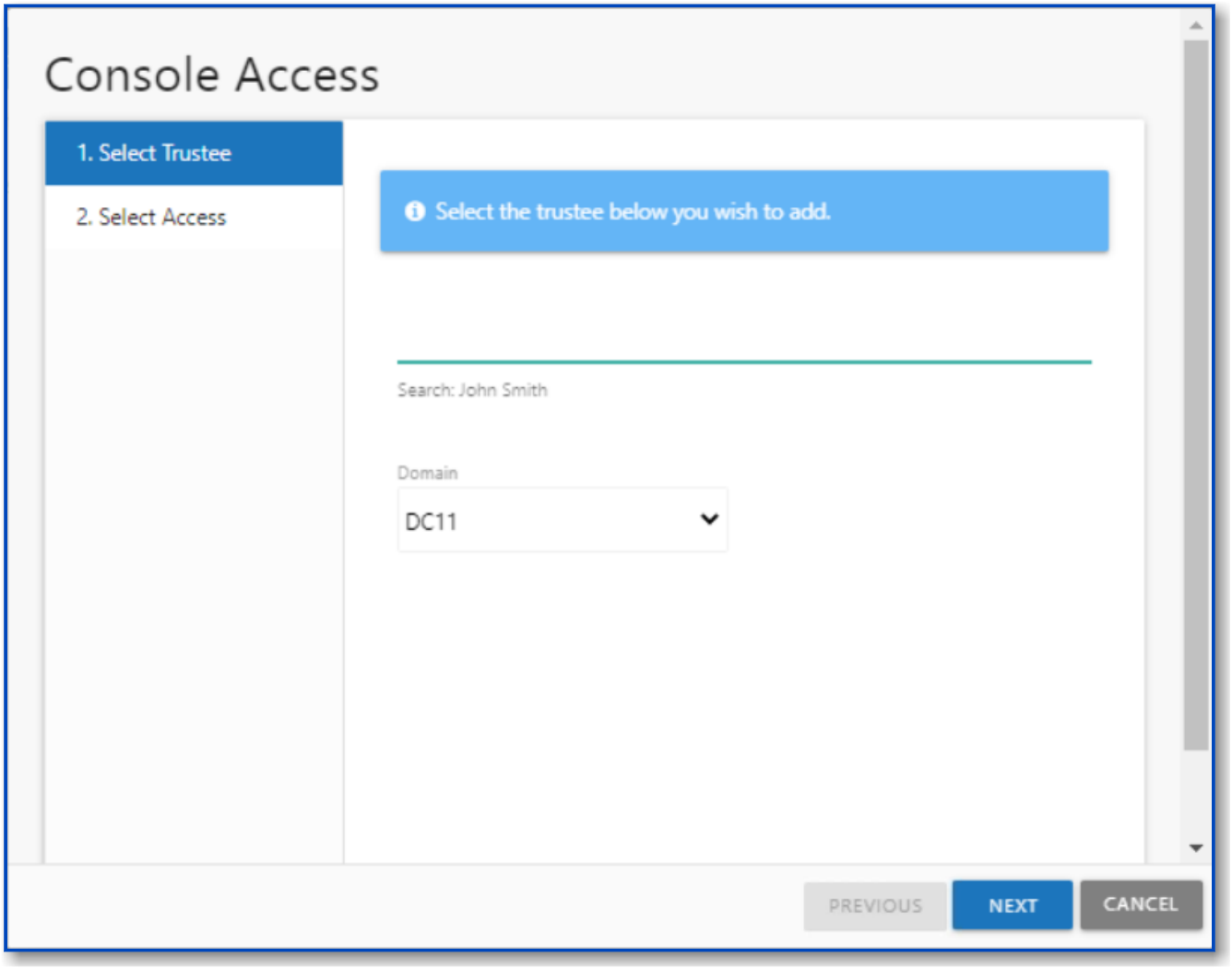
Once users have been granted console access, they can login with their domain credentials. Console access is not a requirement for owners to complete Access Reviews. See the URL & Login topic for information on how users will log in and where they are directed after login based on their assigned role or lack of role.

Add Console Users

Follow the steps to grant domain users or groups console access.

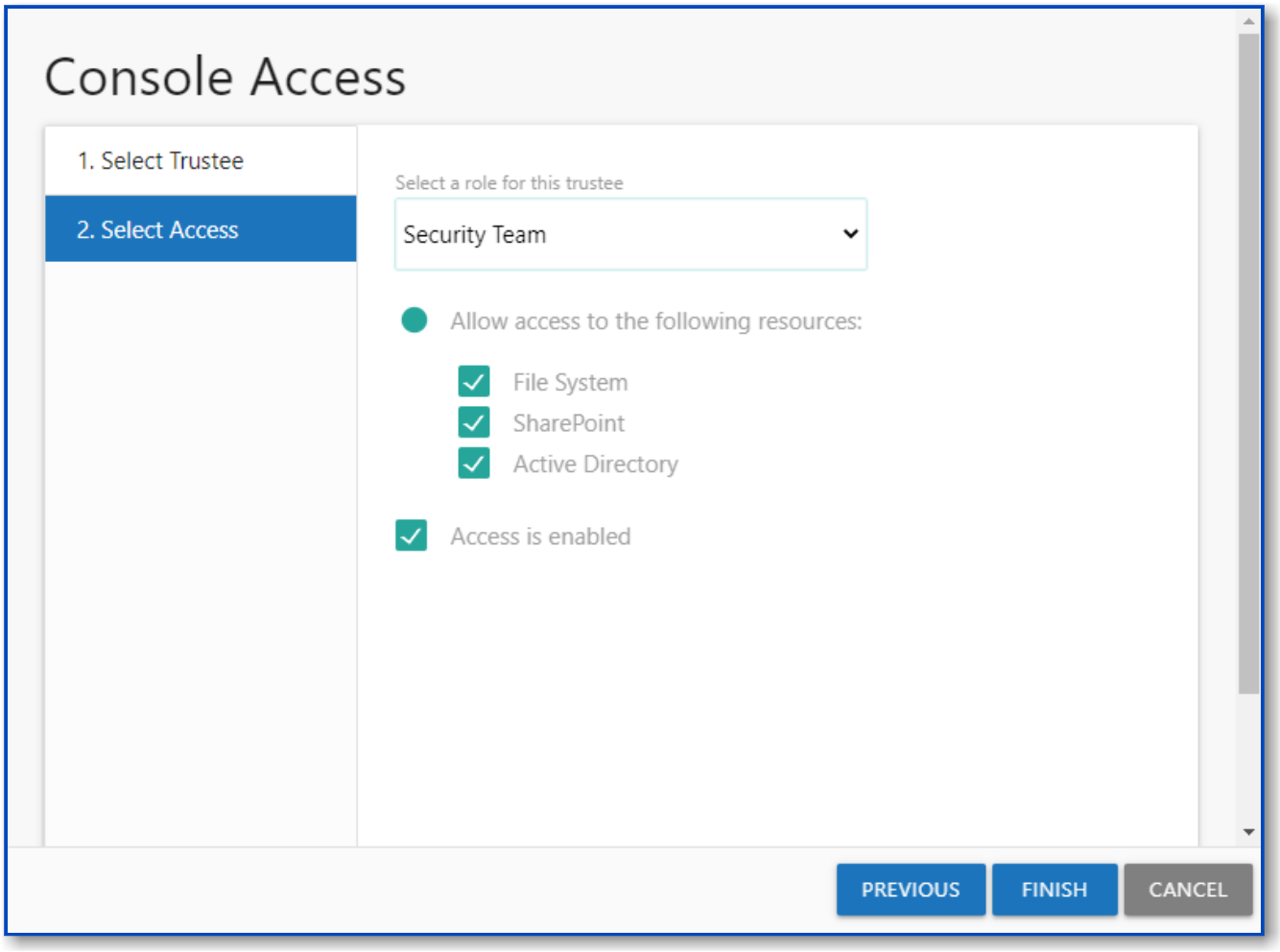


Step 1 – In the Configuration interface on the Console Access page, click Add. The Console Access wizard opens.



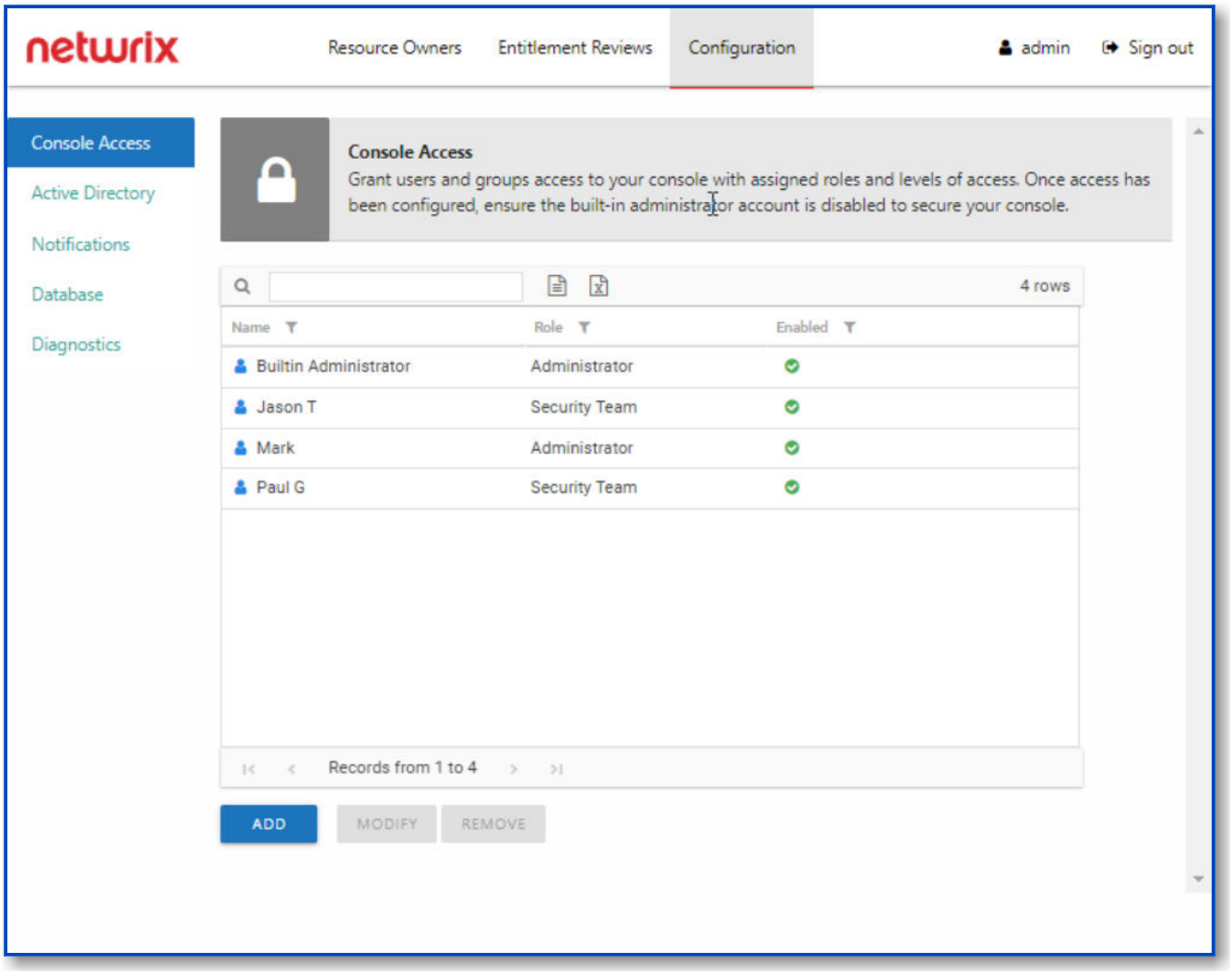
Step 2 – On the Select Trustee page, enter the following information and click Next:

- Domain — If the Access Reviews Console has been configured for multiple domains, use the drop-down menu to select the desired domain
- Search — Begin typing the sAMAccountName or display name and the field will auto-populate options from Active Directory sAMAccountName



Step 3 – On the Select Access page, enter the following information and click **Finish**:

- Select a role for this trustee – Select a role from the drop down list:
  - Unlimited Access — The Administrator role grants unlimited access
  - Limited Access — All other roles can be granted limited access
- Allow access to the following resource — When enabled, users can be limited to only having visibility into data for the selected types of resources. Check the boxes for the type of resource data to be made available to this user.
- Access is enabled – A user's account must be enabled in order to log into the console. Unchecking this option allows you to configure access to be granted at a future time.



Step 4 – The new user displays in the list on the Console Access page. Repeat these steps for each trustee to be granted console access.

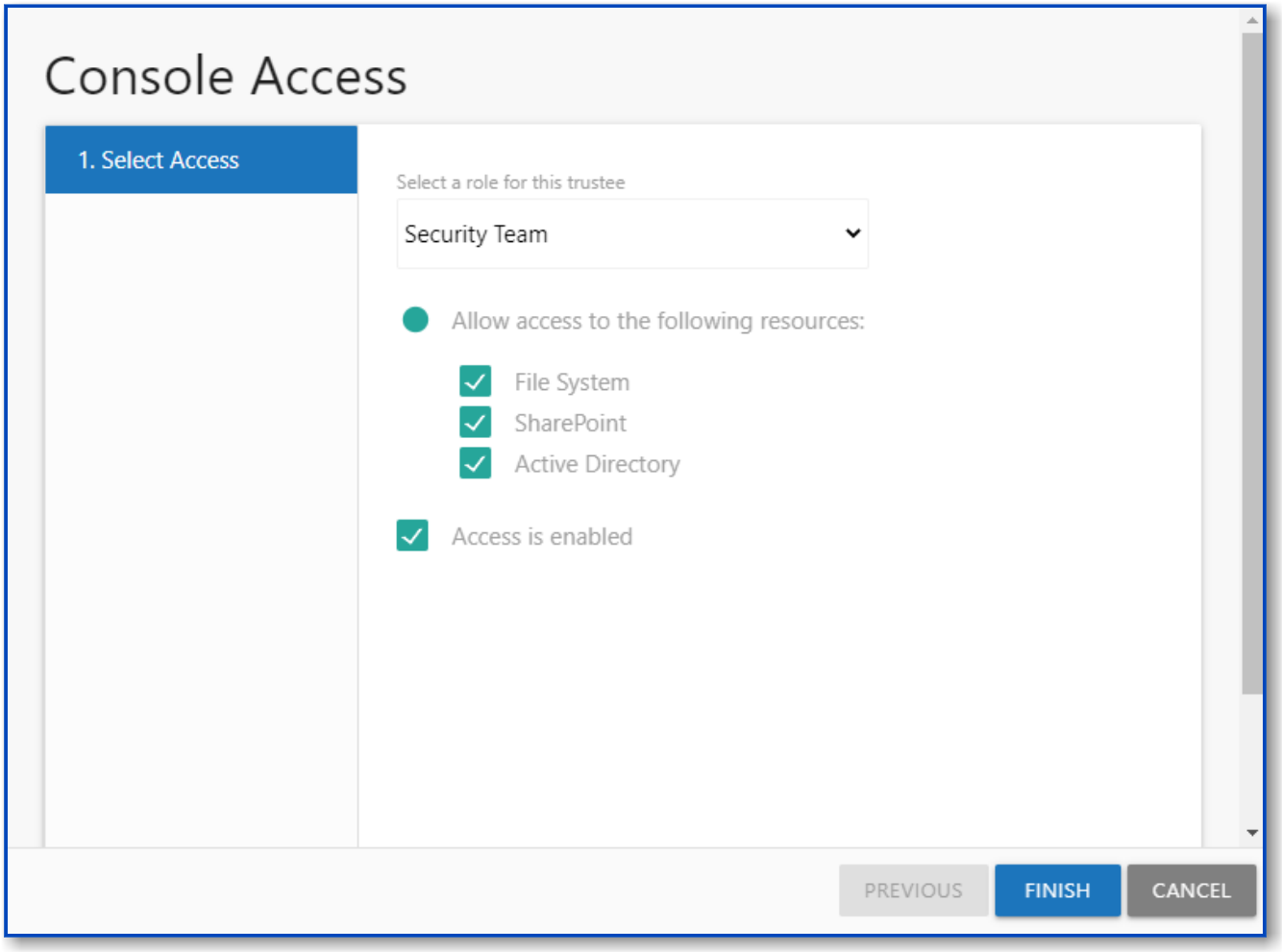
Once the first user with the role of Administrator has been added, the Builtin Administrator account can be disabled by that user. See the Modify the Builtin Administrator Account topic for additional information.

Modify Console Users

Follow the steps to modify a user's console access.

NOTE: These steps are for modifying domain users with console access roles and do not apply to the Builtin Administrator account. See the Modify the Builtin Administrator Account topic for additional information.

Step 1 – In the Configuration interface on the Console Access page, select the user to be modified and click Modify. The Console Access wizard opens to the Select Access page.



Step 2 – Modify the desired settings and click **Finish**:

- Select a role for this trustee – Select a role from the drop down list:
  - Unlimited Access — The Administrator role grants unlimited access
  - Limited Access — All other roles can be granted limited access
- Allow access to the following resource — When enabled, users can be limited to only having visibility into data for the selected types of resources. Check the boxes for the type of resource data to be made available to this user.
- Allow access to the following servers — When enabled, users can be limited to only having visibility into data for specific servers. Begin typing server names and the field will auto-populate with known servers from scanned data. A resource type appears in parentheses after the host name for quick reference.

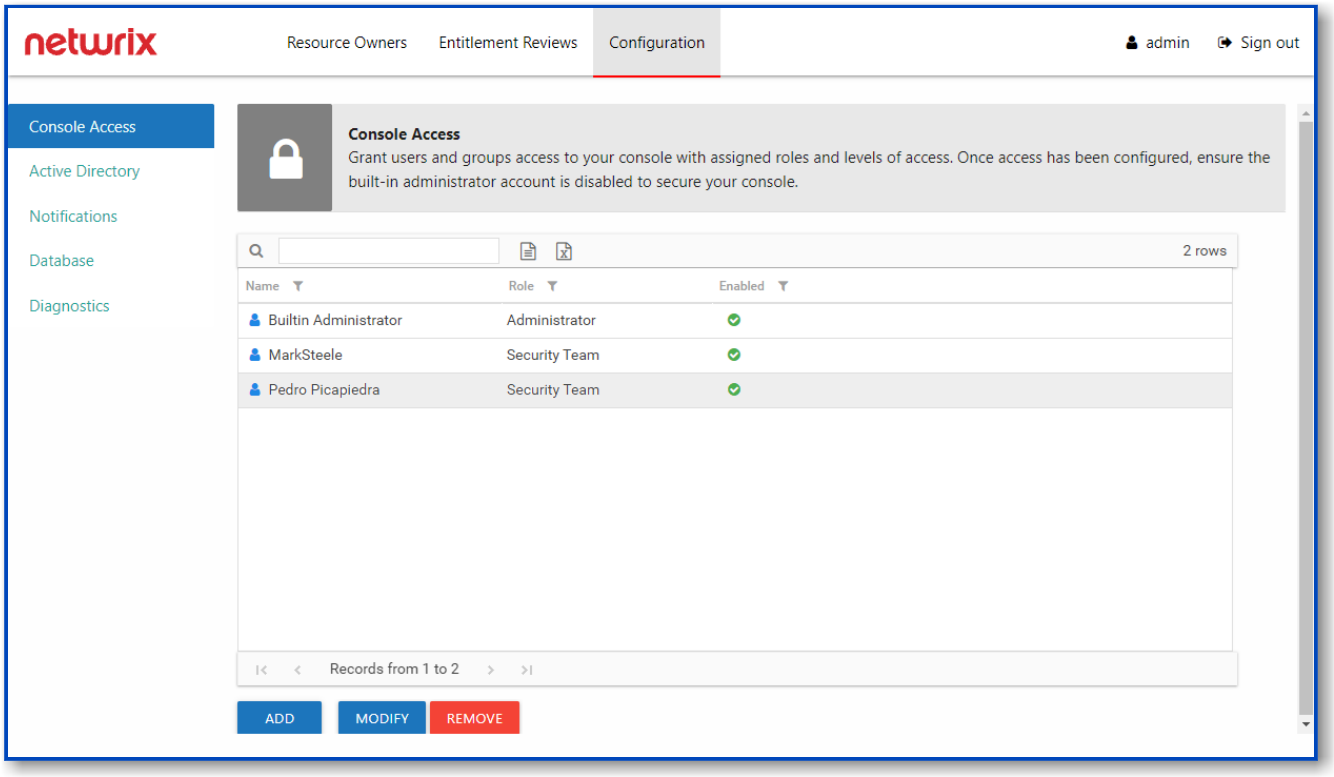
- Access is enabled – A user's account must be enabled in order to log into the console. Unchecking this option allows you to configure access to be granted at a future time.

Any modifications to the user's role are visible in the list on the Console Access page.

Delete Console Users

CAUTION: Confirmation is not requested when deleting users. An alternative to deleting a console user is to disable their access. See the Modify Console Users topic for additional information.

Follow the steps to remove a user's configured console access.



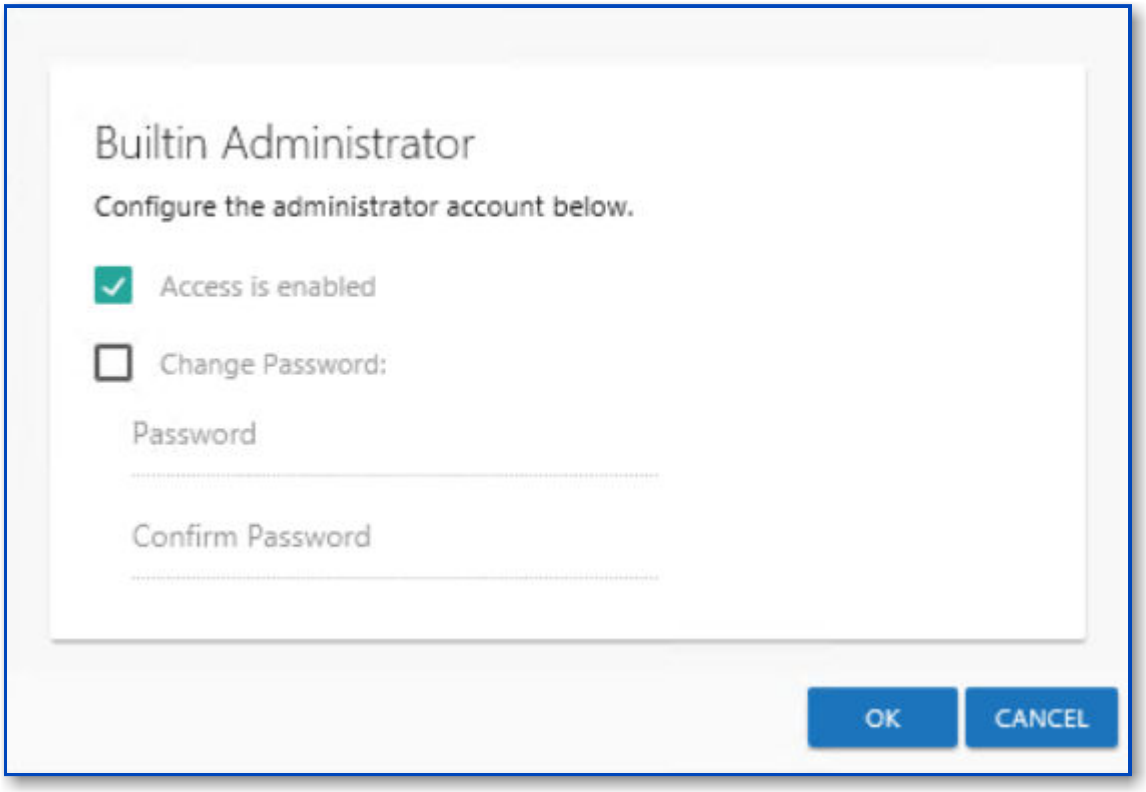
Step 1 – In the Configuration interface on the Console Access page, select the user.

Step 2 – Click Remove.

The user is removed from the list on the Console Access page.

Modify the Builtin Administrator Account

The Builtin Administrator account can be disabled or its password can be changed. Follow the steps to modify this account.



Step 1 – In the Configuration interface on the Console Access page, select the Builtin Administrator account and click **Modify**. The Builtin Administrator window opens.

Step 2 – Modify the account as desired and click **OK**:

- Access is enabled — Indicates whether the account can be used to login
- Change Password — Allows you to change the password for this Builtin Administrator account. Check the box and enter the new password in both entry fields. The password must be eight or more characters long.

The modifications to the Builtin Administrator are processed.

NOTE: The new password is encrypted in the `AccessInformationCenter.service.exe.Config` file, in the `AuthBuiltinAdminPassword` parameter. If you forget the Admin password, you can clear the `AuthBuiltinAdminPassword` value in the

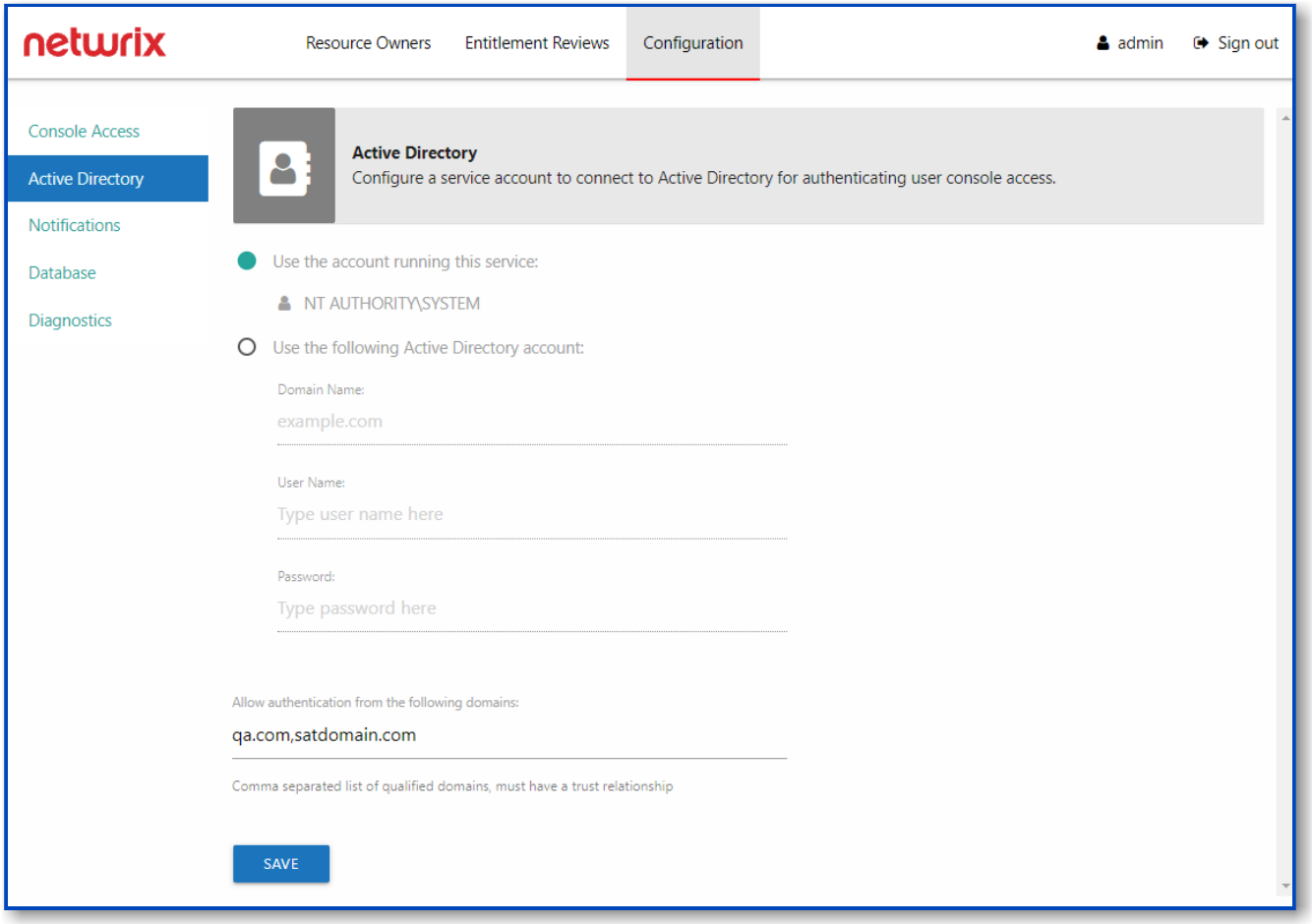
`AccessInformationCenter.Service.exe.Config` file. Then use the default first launch login credentials to set a new password.

Active Directory Page

The Access Reviews application needs to be connected to Active Directory for user authentication and to assign resource ownership in the Resource Owners interface. The Active Directory service account is configured on the Active Directory page of the Configuration interface. Read access to Active Directory is required for this purpose.

The Active Directory service account is configured during installation based on the account used for connecting to the database. If your Database service account uses:

- SQL Server authentication credentials — Active Directory service account is configured to use the Local System, or computer account, which typically has Read rights to the domain
- Windows authentication credentials — The same domain credentials are also used for the Active Directory service account



There are two options for the type of Active Directory service account:

- Use the account running this service — Local System, or computer account (NT AUTHORITY\SYSTEM)
- Use the following Active Directory account — Uses a domain account with the required permissions to Active Directory. The supplied User Name [DOMAIN\USERNAME] and Password are used as the Active Directory service account.

Multiple Domains

The **Allow authentication from the following domains** option is where additional domains can be introduced to the Access Reviews Console. By default the domain where the Access Reviews Console resides is listed. Domains that are in the same forest or have a trust can be added in a comma-separated list.

- For example: nwxtech.com,example.com

Remember, click **Save** when any changes are made to this page.

Update the Active Directory Service Account Password

Follow the steps to update the Active Directory service account password. These steps only apply for the **Use the following Active Directory account** option.

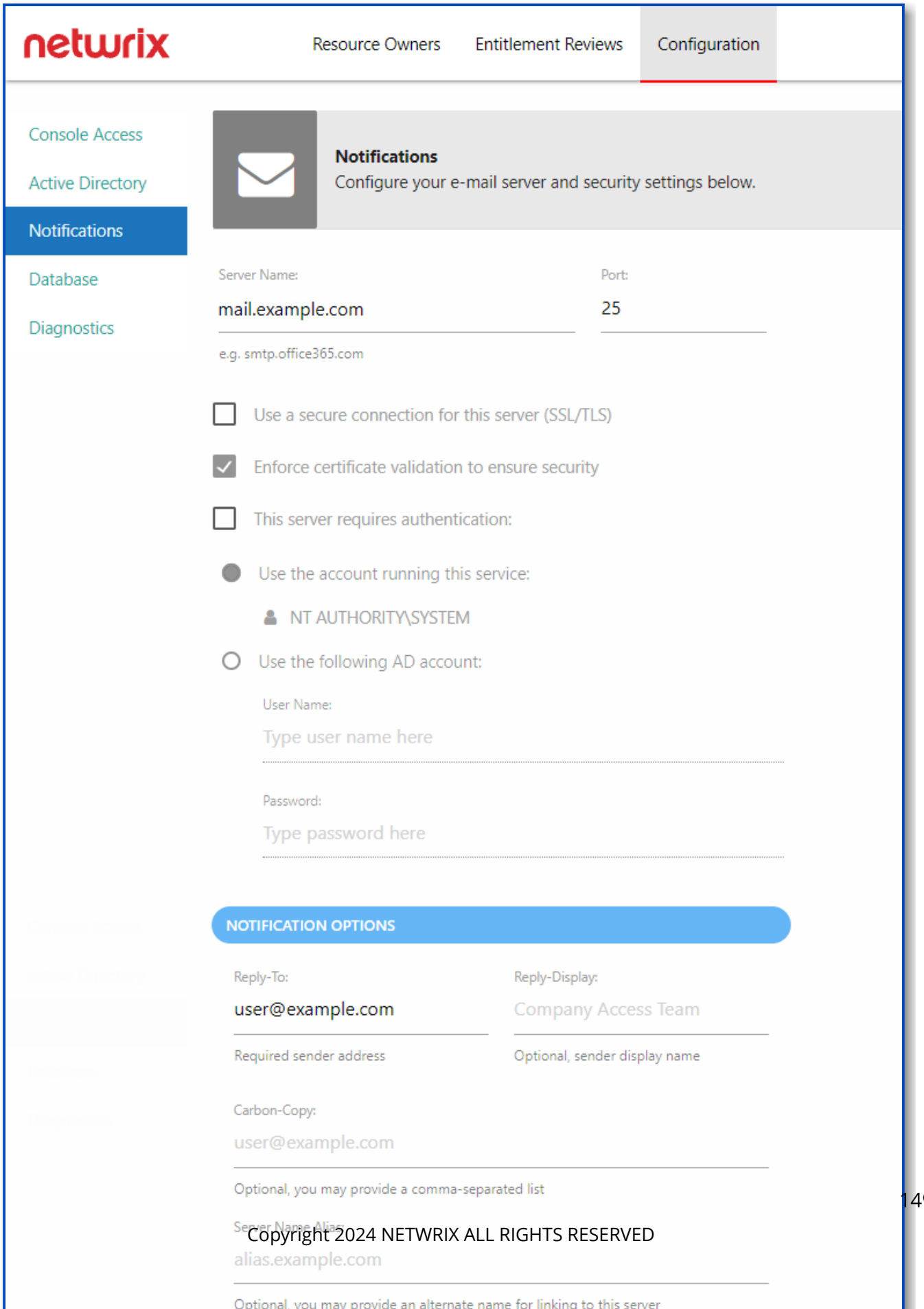
Step 1 – On the Active Directory page, enter the new password in the correct field.

Step 2 – Click **Save**. Then click **OK** to confirm.

The Active Directory service account password has been updated.

Notifications Page

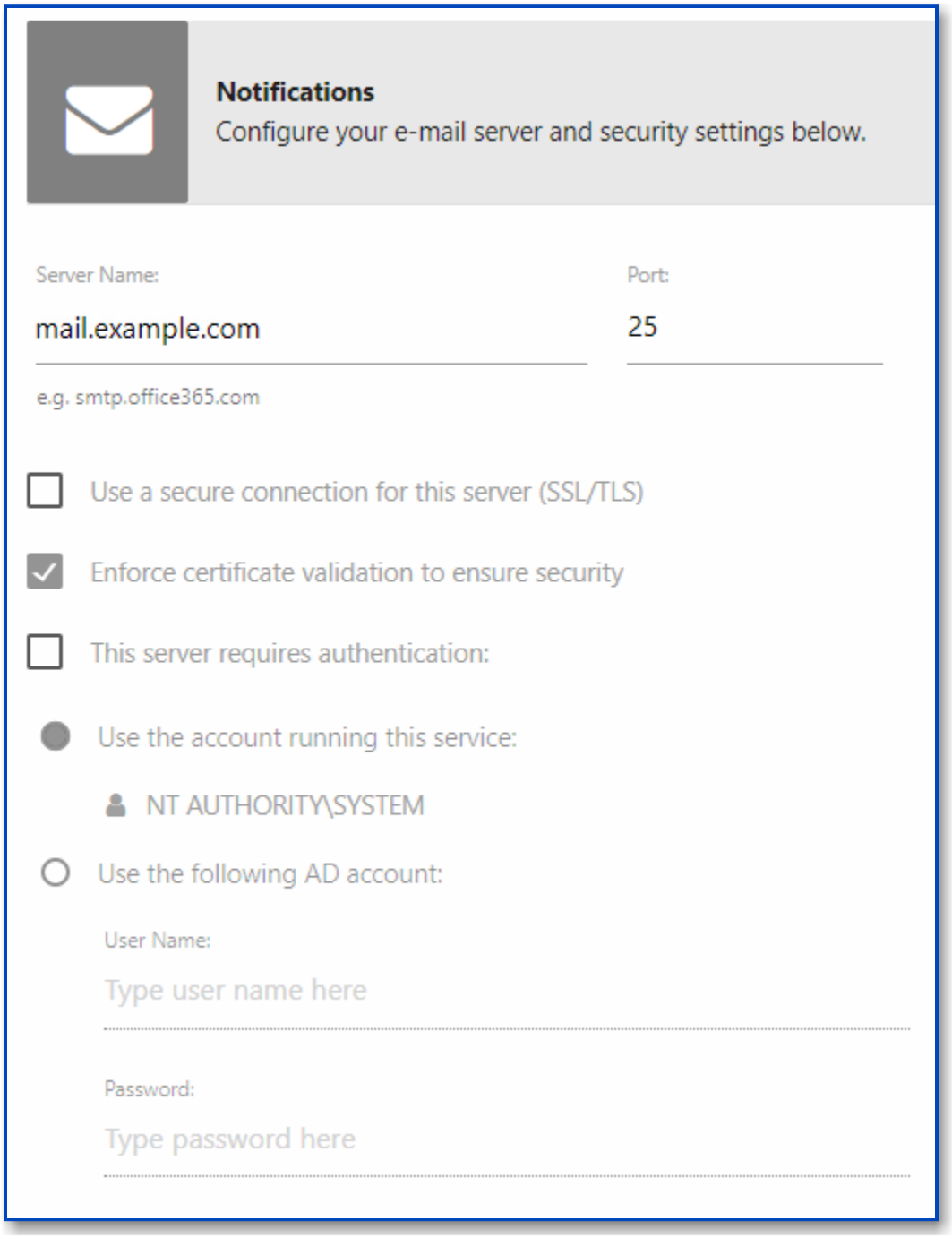
The Access Reviews application uses the Simple Mail Transfer Protocol (SMTP) to send email messages. SMTP server information and several messaging options can be set through the Configuration > Notifications page.



At the top, the SMTP server and email security settings are configured. The Notification options is where you configure the sender information, and other optional settings. The Reminders section is for configuring weekly reminders for owners with outstanding reviews.

Configure SMTP Server Settings

SMTP server information is supplied and modified on the Notifications page. Follow the steps to configure or modify the SMTP settings.



Step 1 – In the Configuration interface, select the Notifications page.

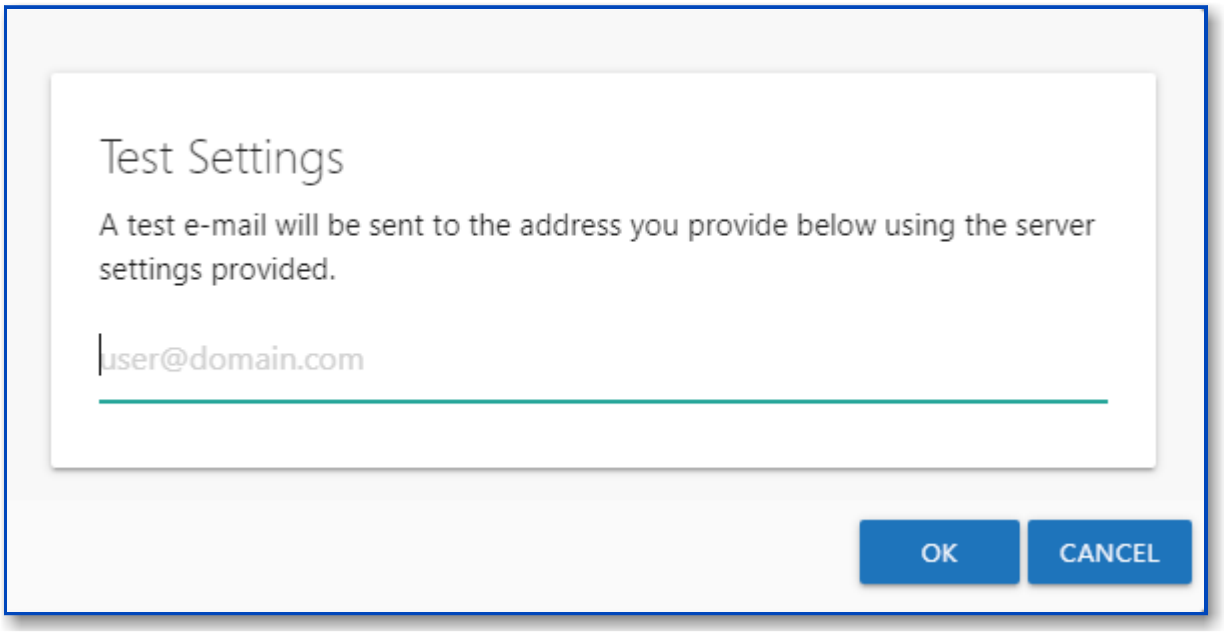
Step 2 – Enter the SMTP Server Name in the textbox. This should be the fully qualified domain name (mail.example.com) or IP Address.

Step 3 – If needed, modify the Port used by your SMTP server to listen for new messages. Historically, the default for SMTP has been port 25. However, if a secure connection is desired (SSL/TLS), the SMTPS port needs to be changed, traditionally 465. Alternately, environments

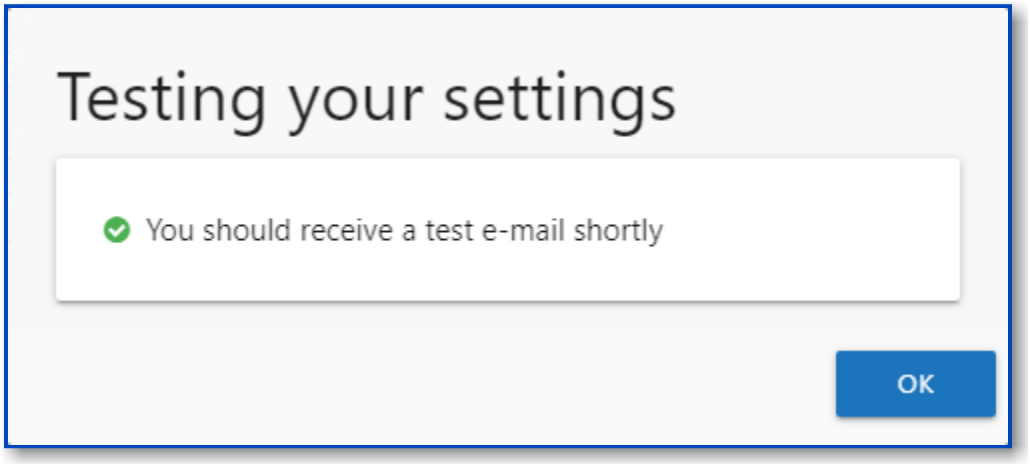
with off-premises or outsourced email service, e.g. gmail.com, hotmail.com, etc., may have to supply a different submission port, traditionally port 587. Ultimately it is an organization's email/messaging administrator who will know the proper value for the SMTP port.

Step 4 – SMTP security settings:

- Use a secure connection for this server (SSL/TLS) – Allows for the use of a secure transport layer for message relay requests (submissions) and authentication requests
- Enforce certificate validation to ensure security — Forces the use of certificate validation
- This server requires authentication – Enable if the identified SMTP server requires authentication. Some SMTP servers traditionally have been configured to deny all but anonymous relay requests, i.e. an attempt to authenticate results in a denial, while an anonymous request is not denied. Select this checkbox, and then select one of the following radio buttons if authentication is required:
    - Use the account running this service
        - To use this option, the SMTP server must be configured to use Integrated Windows Authentication (IWA).
        - Select this radio button if the configured Active Directory service account will also be used to authenticate to the SMTP server.
    - Use the following AD Account
        - To use this option, the SMTP server must be configured to use Integrated Windows Authentication (IWA).
        - Select this radio button to specify either domain account or a traditional SMTP account and password to authenticate to the SMTP server.



Step 5 – Click **Test Settings** to ensure a connection to the SMTP server. The Test Settings window opens. Enter a valid email address and click **OK**.



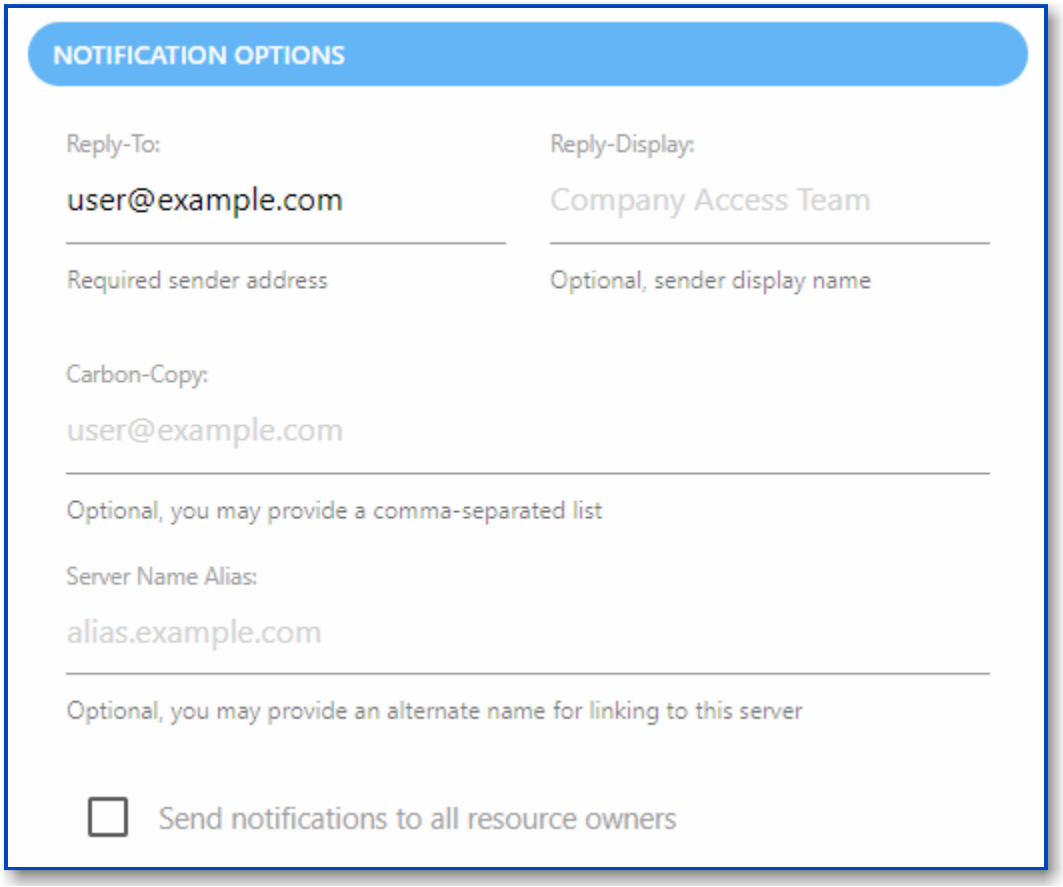
Step 6 – If the SMTP settings are configured correctly, you receive a successful message. Click **OK** to close the Testing your settings window. The test recipient should have recieved a test email.

Step 7 – Click **Save**. Then click **OK** to confirm.

The Access Reviews Console is now configured to send email. See the following topics for additional Notification options.

Notification Options

Once the SMTP server is configured, there are additional options. Only the Reply-To field must be populated:

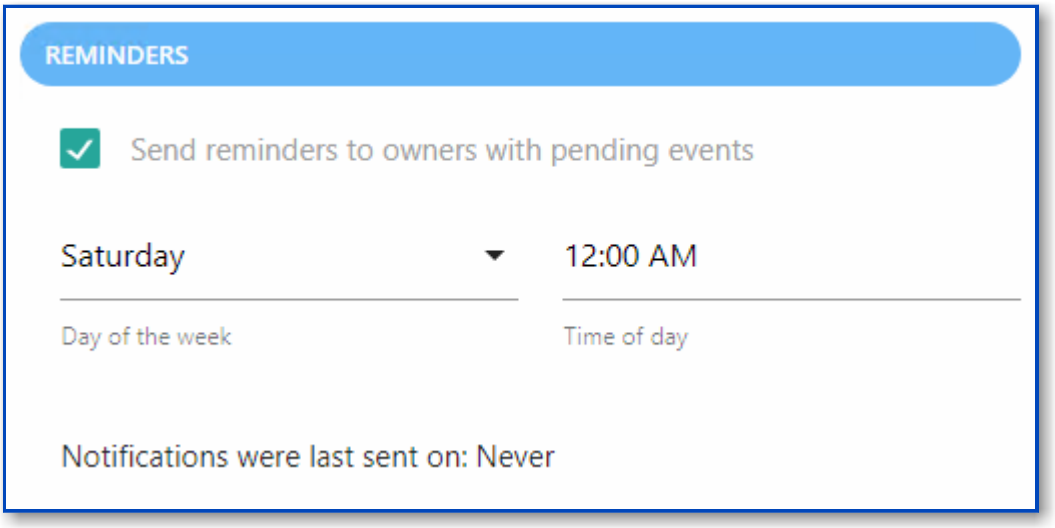


- Reply-To — The email address that receives responses to notifications sent by the application. This can be a “no reply” address.
- Reply-Display — Optionally enter a display name for the sender
- Carbon-Copy — Optionally set additional email addresses to be CC’d on all email messages sent
- Server Name Alias — Optionally provide an alternate name for the URL link to the Access Reviews Console. By default, the URL is the hosting server name and port, e.g. NEWYORKSRV10:81. If you do not want the server name visible in the URL, provide an alias here, e.g. AIC.NWXTECH.com.
- Send notifications to all resource owners — This option applies only to resources with multiple assigned owners. When unchecked, notifications are only sent to the Primary Owner. Check this option to send owner notifications to all assigned owners.

Remember, click **Save** after making modifications to the Notification settings.

Reminders

Resource Owners receive notification email when there are new pending tasks associated to their resources. You can also set up automated weekly reminders for outstanding pending tasks. Follow the steps to configure weekly reminders to resource owners.



Step 1 – In the Configuration interface, select the Notifications page and scroll down to the Reminders section.

Step 2 – Check the Send reminders to owners with pending events option.

Step 3 – Set the date and time for when the reminder will be sent:

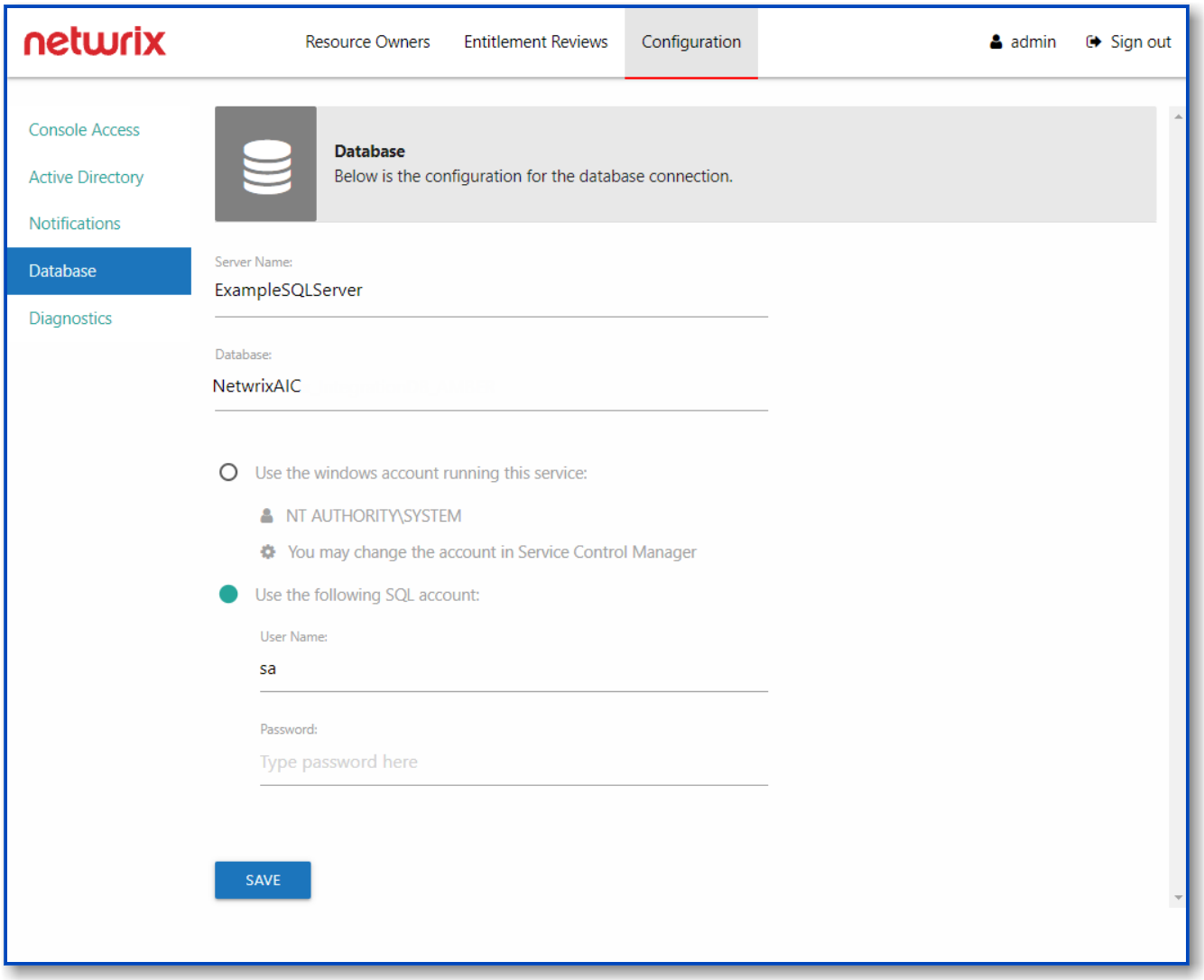
- Day of the week – Select the day of the week from the drop-down menu
- Time of day – Click on the field to open a clock window. Set the time of day reminders will be sent, e.g. 12:00 AM

Step 4 – Click **Save**. Then click **OK** to confirm.

Assigned resource owners now receive weekly reminders of pending events. The **Notifications were last sent on** field will populate with the date timestamp for when the last set of reminders were sent.

Database Page

The Access Reviews application must have access to the SQL Server hosting the database. It is configured during installation. If it is necessary to modify these setting after installation, that is done on the Database Page of the Configuration interface.



SQL Server database information:

- Server Name – Host name of the SQL Server serving the database in one of the following formats:
  - No named instance: [SQLHostName]
    - Example: NT-SQL02
  - Named instance: [SQLHostName]\[SQLInstanceName]

        - Example: NT-SQL02\Netwrix
    - No named instance with non-standard port: [SQLHostName],[PortNumber]
        - Example: NT-SQL02,1392
    - Named instance with non-standard port: [SQLHostName]\[SQLInstanceName], [PortNumber]
        - Example: NT-SQL02\Netwrix,1392
- Database – Name of the SQL database

Database service account information:

- Use the windows account running this service — Local System, or computer account (NT AUTHORITY\SYSTEM)
- Use the following SQL account – Uses SQL Authentication to the database. Provide the properly provisioned SQL credentials for the database

Remember, click **Save** when any changes are made to this page.

Update the Database Service Account Password

Follow the steps to update the Database service account password. These steps only apply for the SQL Authentication option.

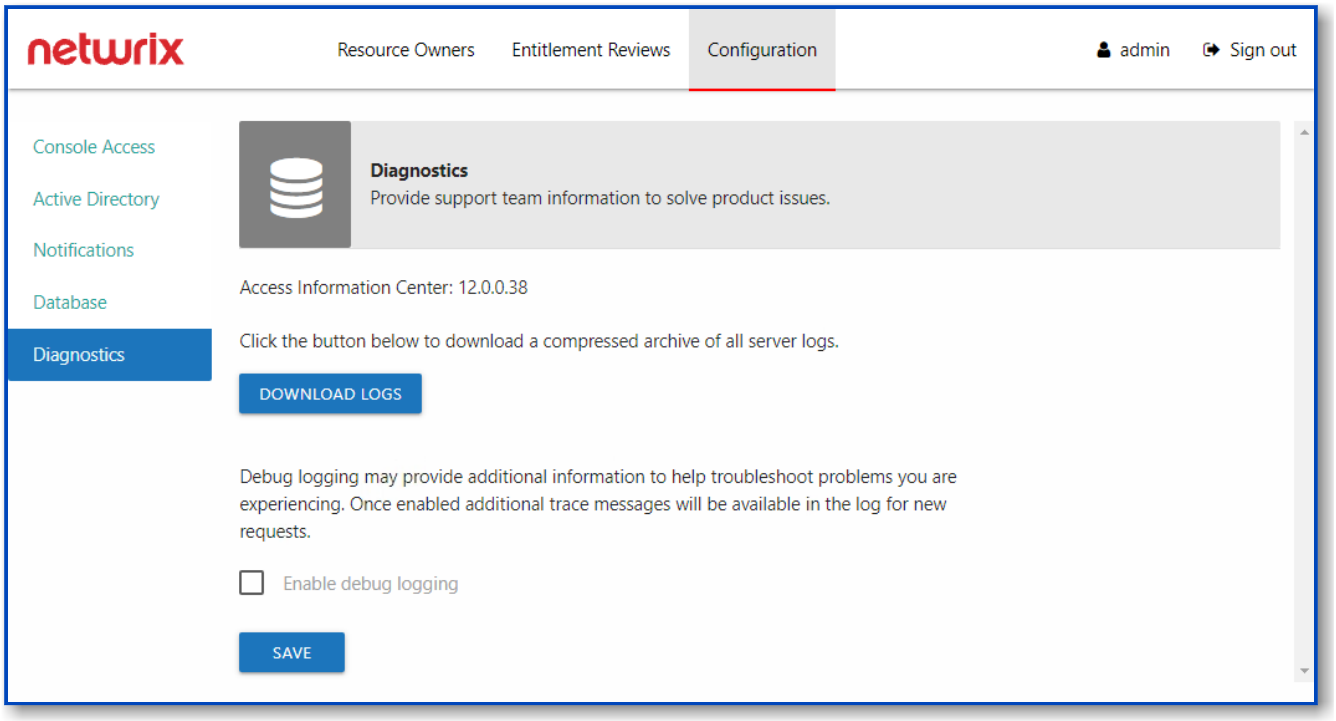
Step 1 – On the Database page, enter the new password in the correct field.

Step 2 – Click **Save**. Then click **OK** to confirm.

The Database service account password has been updated.

Diagnostics Page

Download logs and enable debug log level for troubleshooting with Netwrix Support on the Diagnostics page of the Configuration interface.



When requested by Netwrix Support, click Download Logs to download the archive of all application logs.

Debug Logs

When requested by Netwrix Support , follow the steps to provide debug logs.

Step 1 – On the Diagnostics page, check the Enable debug logging box.

Step 2 – Click **Save**.

Step 3 – Reproduce the issue you are having.

Step 4 – On the Diagnostics page, click **Download Logs**.

The downloaded logs have the debug logging information and can be sent to Netwrix Support. When your issue is resolved, do not forget to turn off Debug logs.

Additional Configuration Options

In addition to the settings that are available on the Configuration interface, the following configurations and customizations can be done by Administrators:

- Email Templates
- Timeout Parameter

Email Templates

The HTML templates used to format notification email can be customized. These templates are designed to make the message viewable within an email client. It is recommended to edit text and layout as desired, but NOT to embed new images or logos. The following table shows the notification email templates and describes the purpose of each.

Template Name	Message Type Description
EntitlementReviewReminder	Reminds owners of pending reviews; manually sent by a Review Administrator from the Entitlement Reviews interface
OwnershipChangeNotification	Sent to owners when assigned ownership is changed for a resource which already has pending reviews
OwnershipConfirm	Sent to owners to confirm or decline ownership of a given resource; manually sent by an Ownership Administrator from the Resource Owners interface
ReminderDigest	Weekly reminder configured by Administrators on the Notifications page of the Configuration interface to owners with pending reviews

While customizing the template content, take note of the inline Substitution Tokens. These exist to provide the message with dynamic content, i.e. inserting values and strings from data in line with the static portion of the message body. These Substitution Tokens begin and end with the "@" symbol, e.g. @UserName@.

Substitution Tokens are only valid for certain Notification message templates. Below is a table of the Substitution Tokens, the value or string they represent, and the message templates in which they may be used.

Substitution Token	Description	Applicable Template(s)
@LoginUrl@	URL that allows a user to access the default (login) page	OwnershipChangeNotification ReminderDigest
@ResourceDescription@	Description of resource • To use the resource's description in emails instead of the path, replace @ResourcePath@ with @ResourceDescription@	OwnershipConfirm ReminderDigest
@ResourcePath@	Path of the current resource • To use the resources' description in emails instead of the path, replace @ResourcePath@ with @ResourceDescription@	OwnershipConfirm ReminderDigest
@ResourceType@	Type of resource	OwnershipConfirm ReminderDigest
@ResourceUrl@	URL specifically created to respond to a request	EntitlementReviewReminder

Substitution Token	Description	Applicable Template(s)
		OwnershipConfirm
@ResponseCount@	Numerically formatted count of pending reviews	ReminderDigest
@ReviewCount@	Numerically formatted count of pending reviews	ReminderDigest

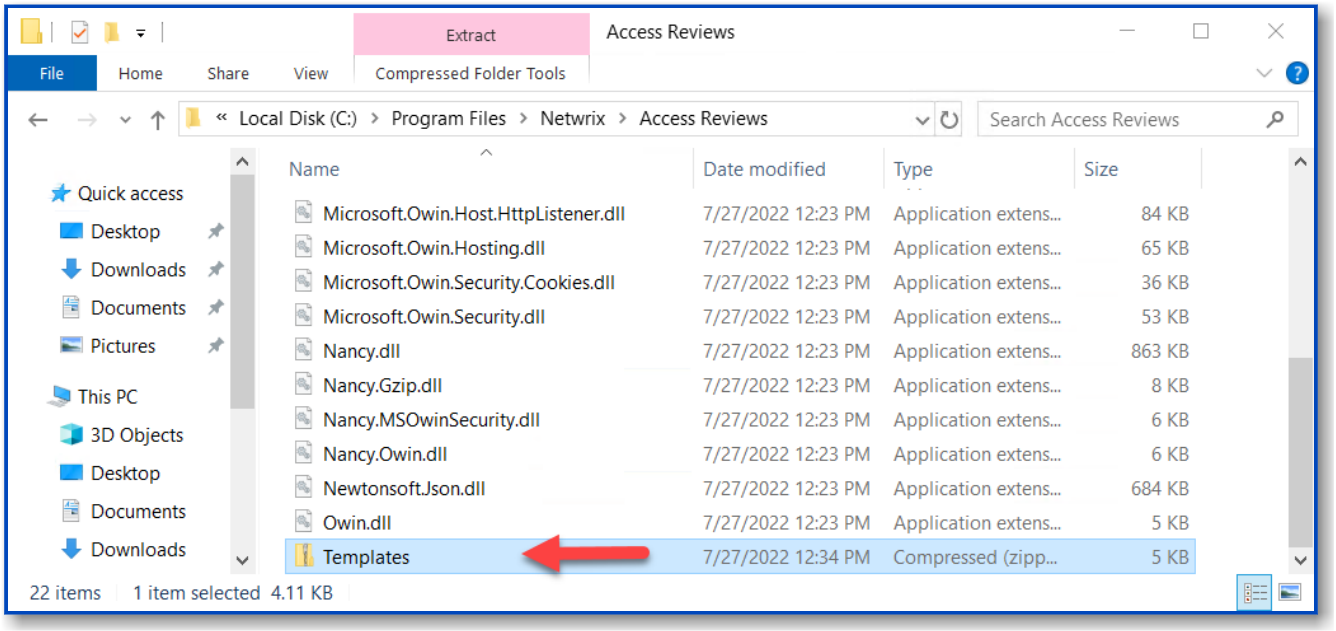
Customize Email Templates

Email templates are shipped in a ZIP file and stored in the Access Reviews installation directory:

```
...\Netwrix\Access Reviews
```

Follow the steps to customize the email templates.

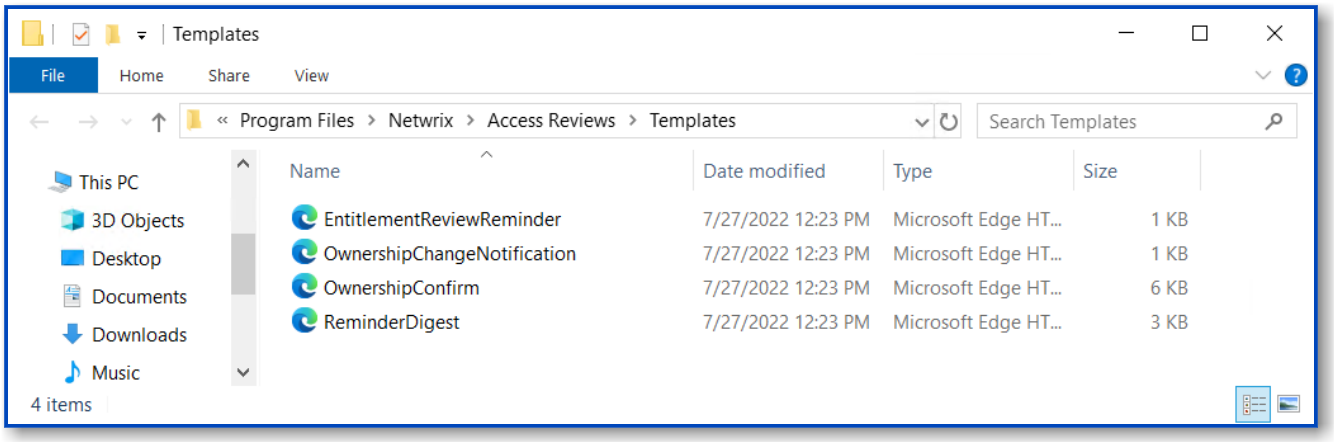
NOTE: To successfully modify these Notifications email templates, a familiarity with basic HTML is necessary.



Step 1 – Navigate to the Access Reviews installation directory.

Step 2 – Unzip the `Templates.zip` file and save the contents to a folder within this directory named `Templates`.

CAUTION: The customized email templates must be in the `Templates` folder within the installation directory to be preserved during future application upgrades.



Step 3 – Locate the desired HTML message template.

Step 4 – Open the file with a text editor, e.g. Notepad, and customize the email body.

NOTE: Using a tool other than a text editor to edit HTML files, such as a WYSIWYG web page editor which may drastically alter the underlying HTML code, is not supported.

Step 5 – Email subject lines can be edited by changing the text between the opening `<title>` tag and the closing `</title>` tag.

Step 6 – After making changes, save the file and view it within a web browser to see what the changes will look like. The Substitution Tokens will display without supplied values.

Step 7 – After making the desired changes, save and close the text editor. Then re-launch the application.

The modifications to the HTML email templates are in use by the notification emails.

Timeout Parameter

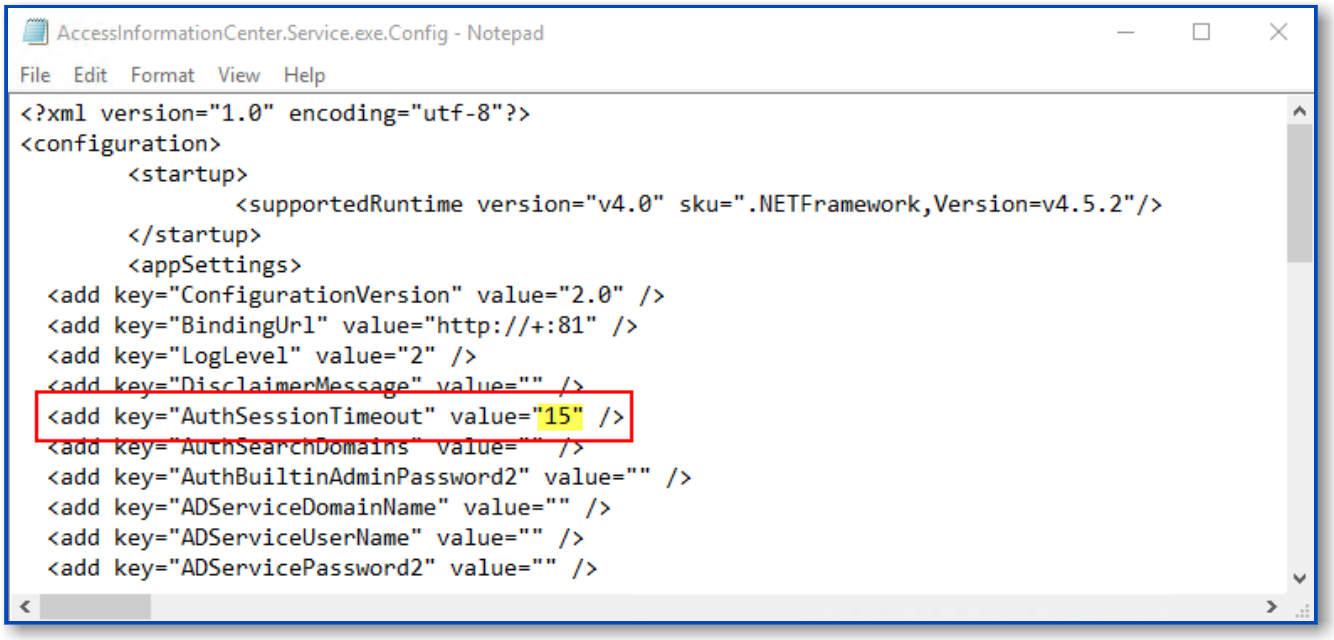
A user session will end when the timeout parameter for inactivity has been reached, and the user will be logged out. By default this is set to 15 minutes.

The timeout parameter is configured within the AccessInformationCenter.Service.exe.Config file in the Access Reviews installation directory:

```
...\Netwrix\Access Reviews
```

Follow the steps to modify the timeout parameter.

Step 1 – Open the AccessInformationCenter.Service.exe.Config file with a text editor, e.g. Notepad.



Step 2 – Change the value for the AuthSessionTimeout parameter to the desired number of minutes. For example:

```
<add key="AuthSessionTimeout" value="20"/>
```

Step 3 – Save and close the file.

A user session times out after the number of minutes specified for inactivity, for example after 20 minutes.

URL & Login

The Access Reviews Console can be accessed through a supported browser from a machine within your company's network. The URL is the hosting machine's name and the port, http://[HOSTNAME.DOMAIN.COM]:81. For example, if the application was installed on a server named

NEWYORKSRV10.NWXTech.com with the default port of 81, the URL would be http://NEWYORKSRV10.NWXTech.com:81.

Administrators

Administrators with access to the server hosting the application can use the desktop icon to launch the application in their default browser. Alternatively, the localhost URL can be used:

- HTTP URL
  - http://localhost:81
- HTTPS URL
  - https://localhost:481

Remote Access

Since Access Reviews is a browser-based application, it is possible to access the web interface remotely. It is up to the Administrator to provide users with the correct URL for access.

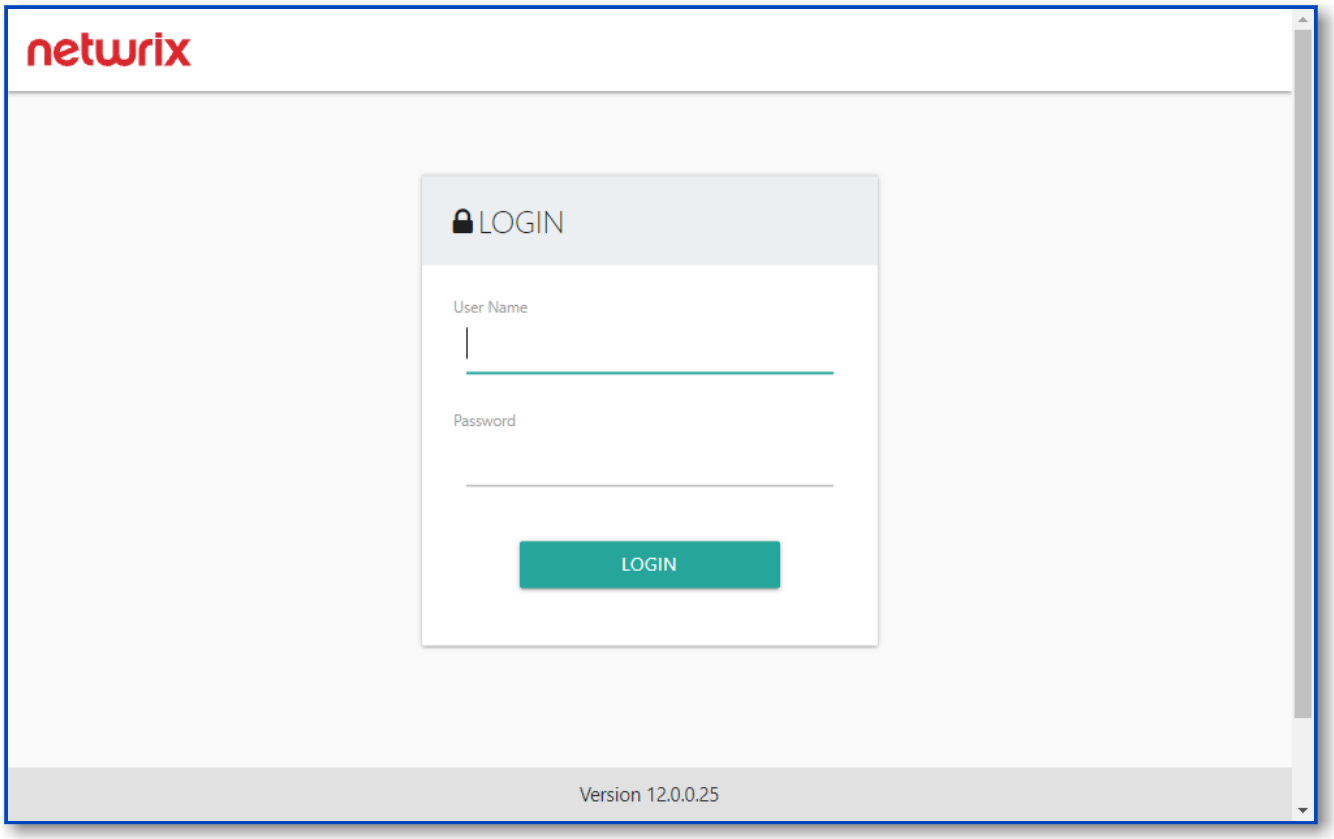
Depending on your network environment, you may need to use the NetBIOS name, FQDN, or IP Address of the hosting server in the browser. Also, additional configurations by network and system administrators may be necessary to make the web server accessible to remote users (firewall configurations, DNS settings, etc.).

The server name in the URL can be replaced with an alias. See the Notification Options topic for additional information.

Login Page

Users login with their domain credentials. If only one domain is known to the Access Reviews Console, the credentials need only be username and password. If multiple domains are known, then the username needs to be entered in the `domain\username` format.

NOTE: The URL may need to be added to the browser's list of trusted sites.



The interface a user arrives at depends upon the assigned role or lack of assigned role.

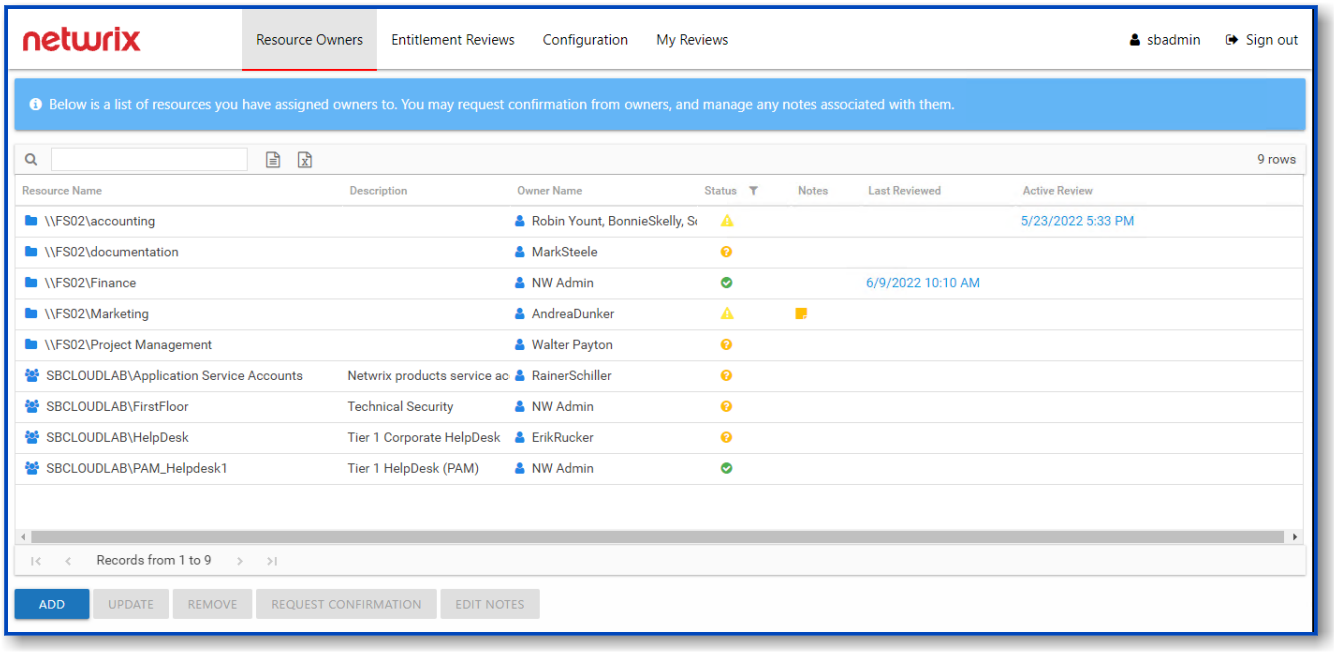
User Landing Page

Role based access controls what interfaces users can see and where each user is directed upon login.

RECOMMENDED: Send an email to your users. Let them know why you are implementing use of the application, provide the URL, and explain how to login with their domain credentials and the username format. See the Enable Console Users topic for additional information.

Administrator Role

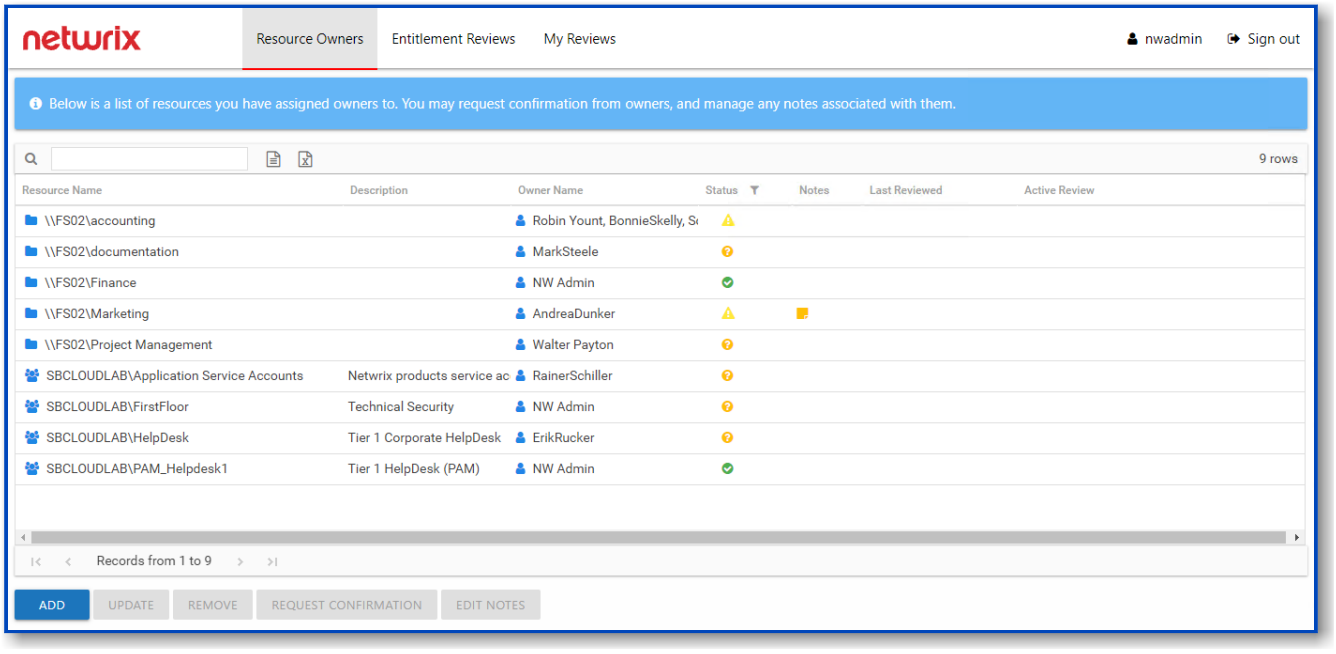
Users granted the Administrator role are directed to the Resource Owners interface upon login.



Administrators are the only ones with access to the Configuration interface. The My Reviews interface is available if the logged in user is also assigned ownership of a resource.

Security Team Role

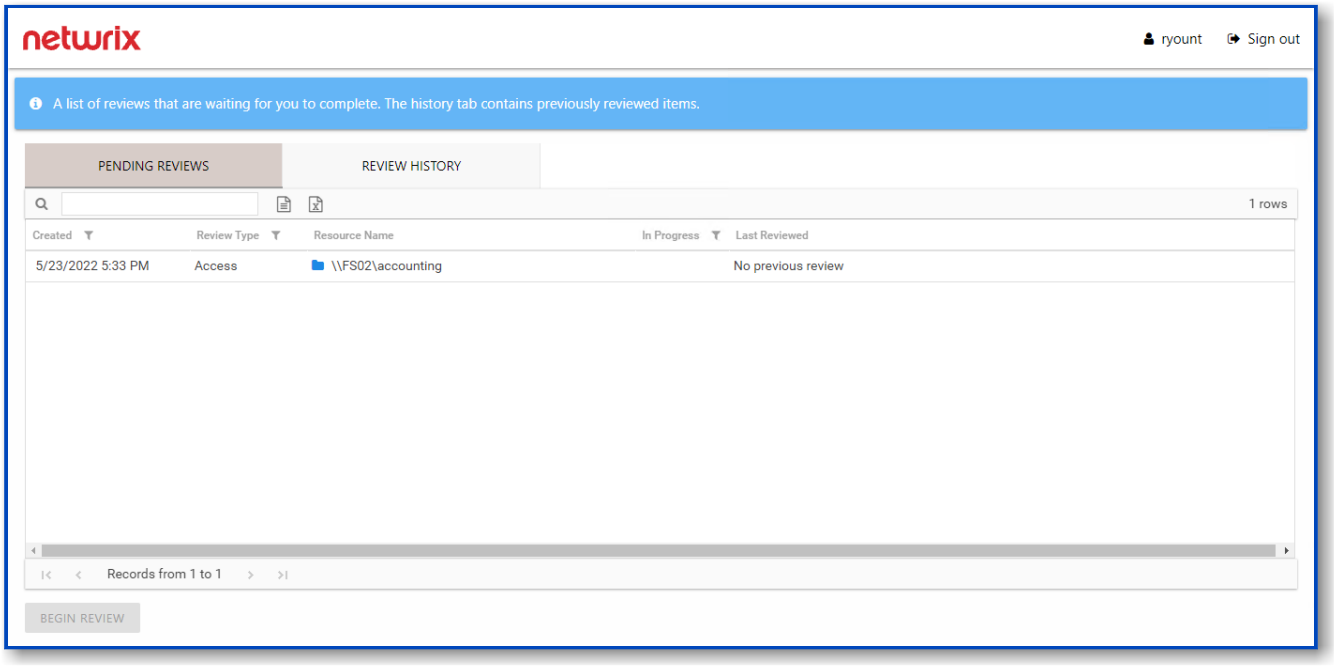
Users granted the Security Team role are directed to the Resource Owners interface upon login.



Security Team members only lack access to the Configuration interface, which is only available to Administrators. The My Reviews interface is available if the logged in user is also assigned ownership of a resource.

Owners Without Role

Users assigned ownership of a resource but not granted a user role are directed to the My Reviews interface upon login.



Owners can view pending reviews and view historical reviews.

Troubleshooting

The following are several troubleshooting tips that can assist with diagnosing trouble with the Access Reviews application. If engaging with Netwrix Support, it will be useful to be aware of these.

Configuration of Permissions on the Installation Directory:

The Windows service account running the Netwrix Auditor Access Reviews service may be used as the Database service account, the Active Directory service account, and/or the SMTP authentication account. Check the Database, Active Directory, and Notification pages in the Configuration interface to confirm where the account is in use before modifying it to ensure

these functionality are not impaired. If this account is changed, a new account must have the **Full Control** permission to files and folders in the Access Reviews installation directory. See the Application Service Account topic for additional information.

Log File:

By default the Access Reviews application is configured to log at the Info level. When requested by Netwrix Support, you can enable Debug level from the Diagnostics page of the Configuration interface. See the Diagnostics Page topic for additional information.

If a different log level is needed or desired, the `aic.log` file can be modified. See the Change Log Level topic for additional information.

Credential Password Changes:

The Access Reviews application uses several different types of service accounts. If a credential password for one of these accounts is no longer valid, it will impact application functionality. Additionally, if the Builtin Administrator account remains enabled, it may be necessary to reset the password. See the Update Credential Passwords topic for additional information.

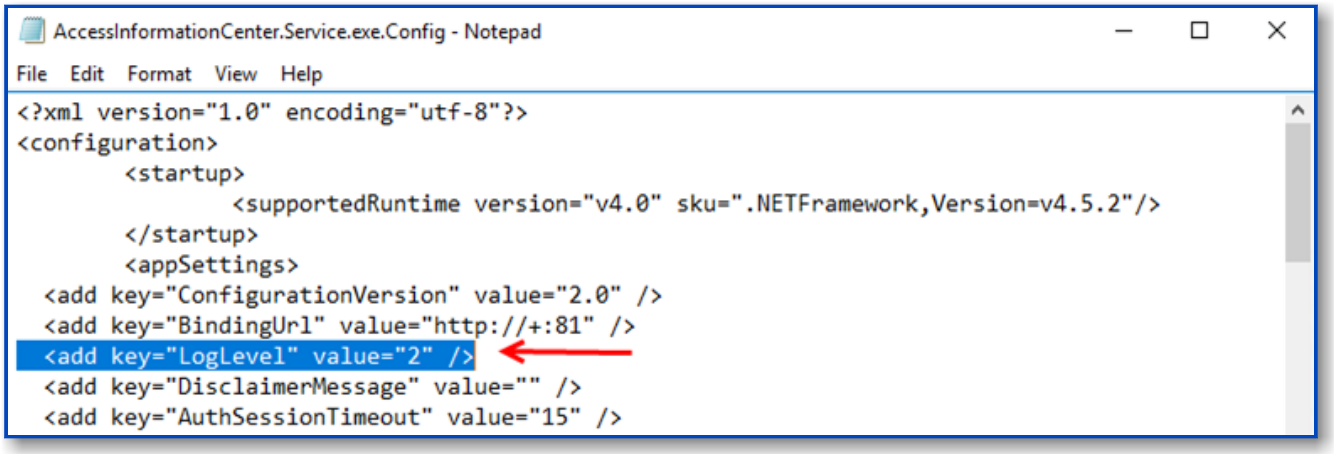
Change Log Level

The `AccessInformationCenter.Service.exe.Config` file is located in the Logs folder of the Access Reviews installation directory:

```
...\Netwrix\Access Reviews
```

Follow the steps to modify the log level.

Step 1 – Open the `AccessInformationCenter.Service.exe.Config` file in a text editor, e.g. Notepad.



Step 2 – The level value is set in the `LogLevel` parameter, where "2" is the default level. As the logging level increases from 0 to 3, the types of information and level of detail included within the log file also increase. Change to the desired log level:

```
<add key="LogLevel" value="2" />
```

- Error level is when `value="0"`
- Warning level is when `value="1"`
- Info level is when `value="2"`
- Debug level is when `value="3"`
    - Debug logging can be enabled from the Diagnostics page of the Configuration interface

Step 3 – Save and close the `AccessInformationCenter.Service.exe.Config` file.

Once troubleshooting has finished, it is recommended to return the log level to the default level, Info = 2, to prevent the log file from growing too large.

Application Service Account

The Windows service account running the Netwrix Auditor Access Reviews service may be used as the Database service account, the Active Directory service account, and/or the SMTP authentication account. Check the Database, Active Directory, and Notification pages in the Configuration interface to confirm where the account is in use before modifying it to ensure these functionality are not impaired. If the same account is being used for multiple purposes, it will require the proper permissions for each purpose.

It may become necessary (for testing purposes, infrastructure changes, etc.) to change the Windows account set to run the Netwrix Auditor Access Reviews service. The following step-by-step instructions are for modifying this account within the Services Control Manager console.

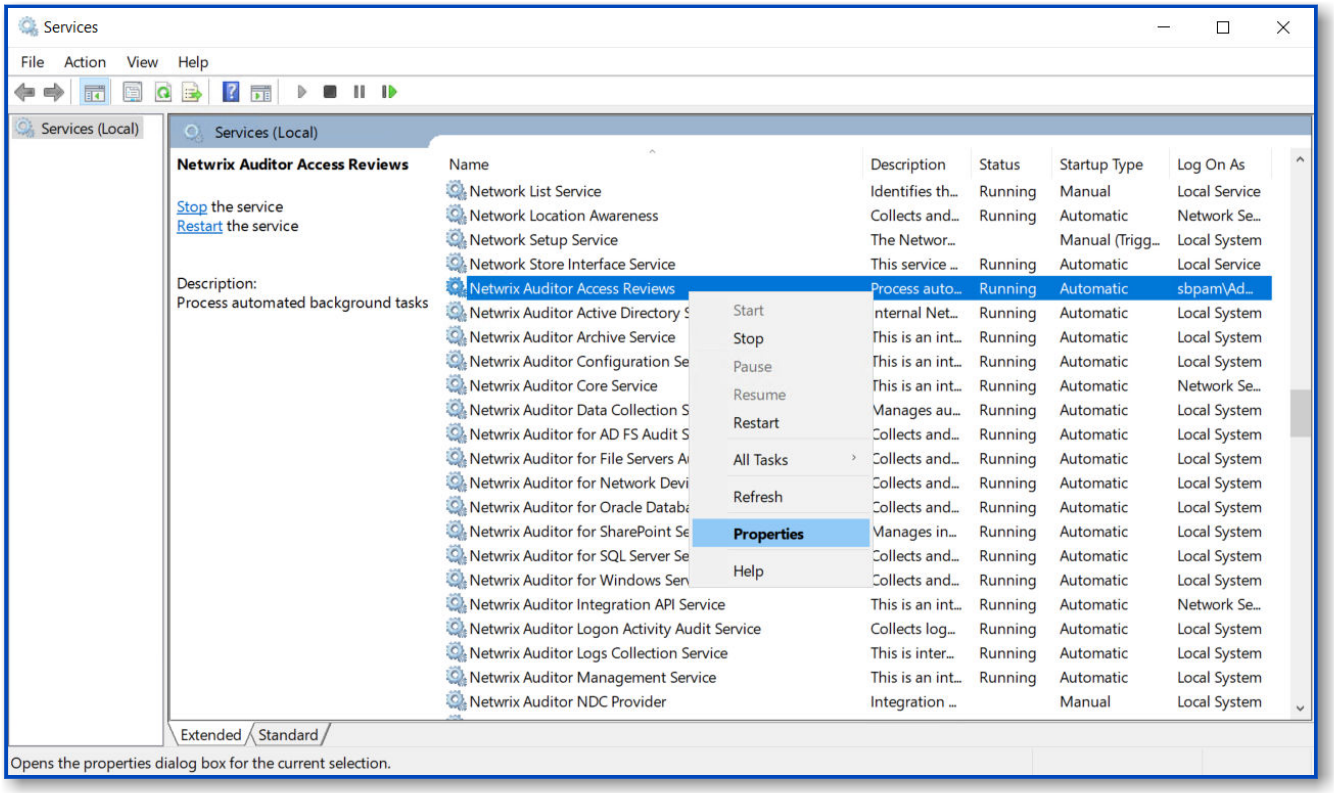
CAUTION: The account assigned to run the NETWRIX AUDITOR ACCESS REVIEWS service must have Full Control over the installation directory:

```
...\Netwrix\Access Reviews
```

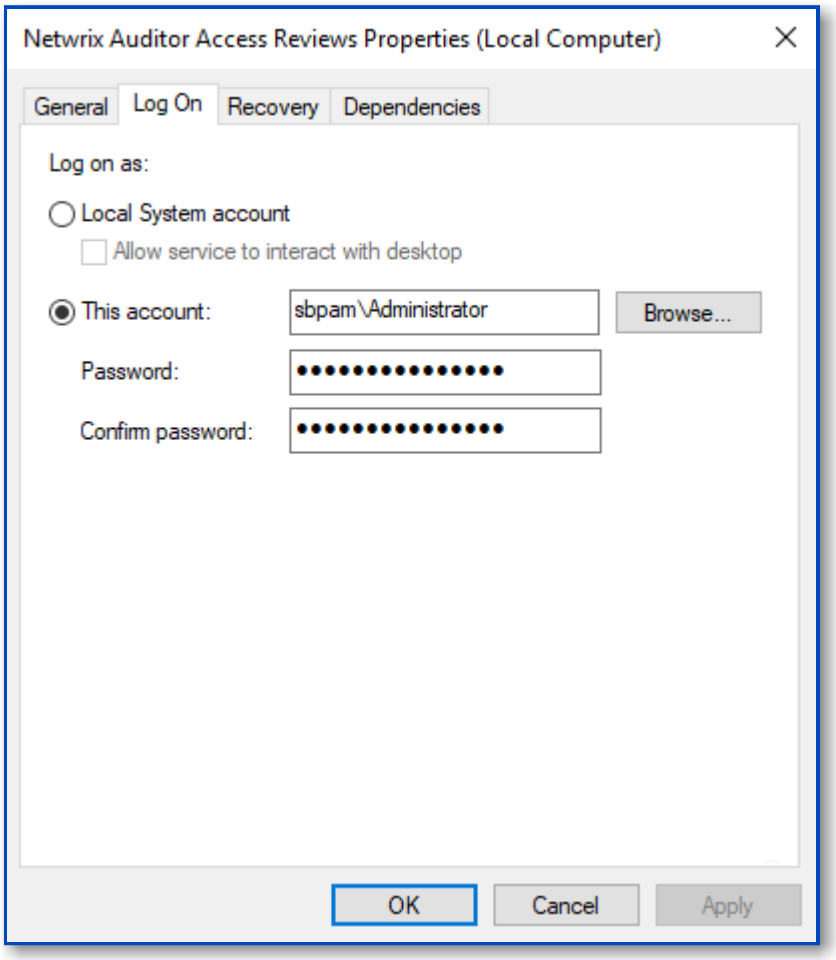
Modify the Service Account via Service Control Manager

Follow the steps to enable and/or modify the Windows service account running the Netwrix Auditor Access Reviews service.

Step 1 – Navigate to Service Control Manager (`services.msc`). The Services Control Manager opens.



Step 2 – Right-click on the Netwrix Auditor Access Reviews service and select **Properties**. The service Properties window opens.



Step 3 – On the **Log On** tab, select the **This account** radio button. Enter the account name using NTAccount format [`DOMAIN\username`]. Optionally, use the **Browse** button to search for the account. Enter the account's password in both the **Password** and **Confirm password** fields. Then click **OK**. The Properties window closes.

Step 4 – The selected account is displayed in the Log On As column for the service. Either Restart or Stop and Start the service for this change to take affect.

The Netwrix Auditor Access Reviews service is now running with the supplied Windows account.

Update Credential Passwords

Credential passwords occasionally need to be updated due to various reasons, such as security policies that require passwords to be reset on a regular basis. The following types of credentials may be impacted by password changes or security policies:

- Database service account

- Active Directory service account
- SMTP authentication service account
- Application Service Account
- Bultin Administrator account

Database Service Account

The Database service account grants access to the SQL Server database. It can be updated on the Database page of the Configuration interface. See the Update the Database Service Account Password topic for instructions.

Active Directory Service Account

The Active Directory service account handles user authentication to the Access Reviews Console. It can be updated on the Active Directory page of the Configuration interface. See the Update the Active Directory Service Account Password topic for instructions.

SMTP Authentication Service Account

An SMTP server is required for the application to send notifications. If the SMTP server requires authentication, the service account can be updated on the Notifications page of the Configuration interface. See the Configure SMTP Server Settings topic for instructions.

Application Service Account

The account used to run the Netwrix Auditor Access Reviews service can be updated using Services Control Manager console. See the Modify the Service Account via Service Control Manager topic for instructions.

Builtin Administrator Account

The Builtin Administrator account is an application account that is created during the first launch. It is used to complete the initial configuration steps and to grant console access to domain users. This account can be disabled after Administrator users are added. However, if it is enabled and a security policy requires the password to be reset, it can be updated on the Console Access page of the Configuration interface. See the Modify the Builtin Administrator Account topic for modification instructions.

Resource Owners Overview

The Resource Owners interface is where Access Reviews Console users with either the Security Team or Administrator role (to be referred to as Ownership Administrators) can assign ownership of resources to be managed through the application. Assigned owners do not require a console user role. Resources to be included in the Access Reviews workflow must first be assigned owners within the Resource Owners interface.

RECOMMENDED: The Access Reviews application is configured to send Notifications.

Remember, a "resource" refers to the file system shared folders, SharePoint Online site collections, and Active Directory (AD) groups. All data available within the *Access Reviews* application is collected by *Netwrix Auditor* according to the synchronized monitoring plans.

"Owners" are the users who are responsible for reviewing access to the resources to which they are assigned.

The My Reviews interface provides owners with access to historical and pending reviews. The My Reviews interface is only accessible to users who have been assigned ownership of at least one resource. Owners without a console user role are directed to the My Reviews interface at login. Owners with a console user role access the pending and historical reviews for their resources by clicking the My Reviews tab. See the Pending Reviews topic for additional information.

Who Can Assign Ownership (Ownership Administrators)?

- Console Users with Administrator role
    - Can complete the Review Administrator's approval process without impacting the visibility into the review created by a Review Administrator with the Security Team role

CAUTION: Visibility into a review created by a Review Administrator with the Security Team role is blocked if a Review Administrator with the Administrator role starts a new instance.

- Console Users with Security Team role
  - Visibility into only those reviews personally created

What Can Resource Owners Do?

- Perform an access review (when there is a pending review)
- View historical information on access reviews

See the Resource Owners Interface topic for additional information.

Workflow of Ownership Assignment

Prerequisite:

- Optional: The Access Reviews application is configured to send Notifications. See the Notifications Page topic for additional information.

  NOTE: By default, the application is configured to send notifications only to the primary owner. However, this can be customized on the Configuration > Notifications page to send notifications to all assigned owners.

- Owners assigned to resources must have:
  - Email address to receive notifications
  - Credentials for a domain known to the application
- Resources and groups must be known to the application

Workflow:

NOTE: This workflow is not numbered because the Notification piece can occur at any time in the workflow.

- Add resources to be managed by associating a business data owner with a resource. See the Add New Resource Wizard topic for additional information.
- Confirm resource ownership. See the Ownership Confirmation topic for additional information.

- Notify owners of their responsibilities. See the Notification to Owners topic for additional information.

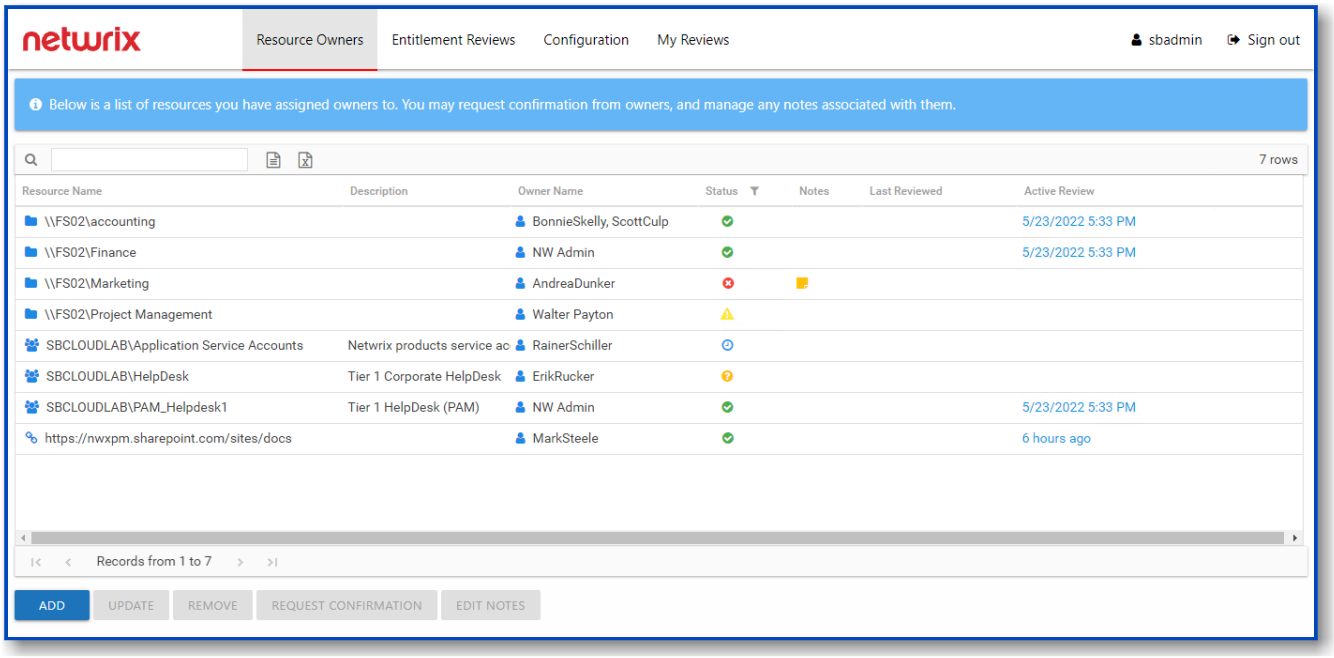
Notification to Owners

Let your owners know what their responsibilities are by notifying them with the following information:

- An explanation of what a review is and why your organization is conducting them through the Netwrix Auditor Access Reviews application.
- How owners should log into the application console, specifically what URL and credentials to use.
- Expectation on response times
- How to access instructions on how to complete a review. You can link to the Owners & Access Reviews topic or download that topic and its subtopics as a PDF and make it available within your corporate resources.

Resource Owners Interface

The Resource Owners interface opened by the Resource Owners tab is where Ownership Administrators perform many operations around assigning and managing ownership.



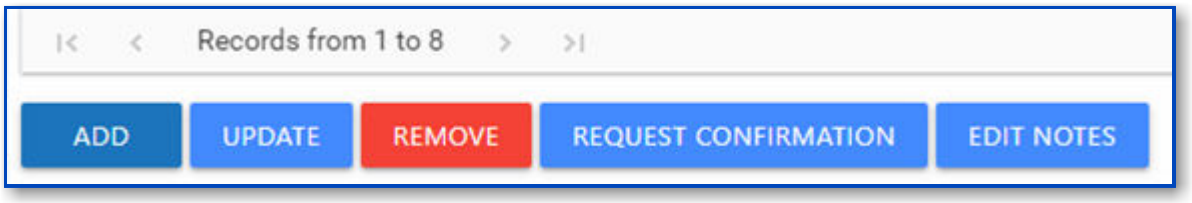
The information displayed in the table includes:

- Resource Name – The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
- Description – Description or explanation of the resource as supplied by either the Ownership Administrator or the assigned owner. See the Notes & Descriptions topic for additional information.
- Owner Name – Name of the assigned owner. If there are several owners of a resource, the list is comma-separated.
- Status – Indicates whether or not the assigned owner has confirmed ownership of that resource. Tool-tips display when hovering over the icons indicating whether the resource ownership has been confirmed, declined, pending response, or that a confirmation has not been requested. See the Ownership Confirmation topic for additional information.
- Notes – Icon indicates a Note has been added. Click on the icon to read the attached note(s). Notes can be added by Ownership Administrators or populated with alternative owners by individuals who declined ownership. See the Edit Notes Window and the Notes & Descriptions topics for additional information.
- Last Reviewed – Date timestamp when the last review took place for the resource. The hyperlink will open the Entitlement Reviews interface to that Review Details page displaying the historical review instance. See the Review Details Page topic for additional information.

- Active Review – Indicates whether or not there is a pending review. The hyperlink will open the Entitlement Reviews interface to that Review Details page displaying the active review instance. See the Review Details Page topic for additional information.

The table data grid functions the same way as other table grids. See the Data Grid Features topic for additional information.

The buttons at the bottom enable you to conduct the following actions:



Button	Function
Add	Launches the Add new resource wizard to add a new resource to the list. This allows you to add one resource at a time and assign an owner. See the Add New Resource Wizard topic for additional information.
Update	Launches the Update resource wizard for the selected resource. This allows you to make changes to the assigned owners or add/edit the resource description. See the Update Resource Wizard topic for additional information.
Remove	Opens the Confirm removal window to removes the selected resource from being managed through the application. *Remember,* only resources with an assigned owner will be visible in the table. Removing a resource from this table does not delete the resource from the application database.

Button	Function
	See the Confirm Removal Window topic for additional information.
Request Confirmation	Opens the Confirm Ownership wizard. Sends an email to the assigned owner(s) for the selected resource requesting ownership confirmation. See theConfirm Ownership Wizard topic for additional information.
Edit Notes	Opens the Edit Notes window for the selected resource and allows free-text editing of the notes. See the Edit Notes Window topic for additional information.

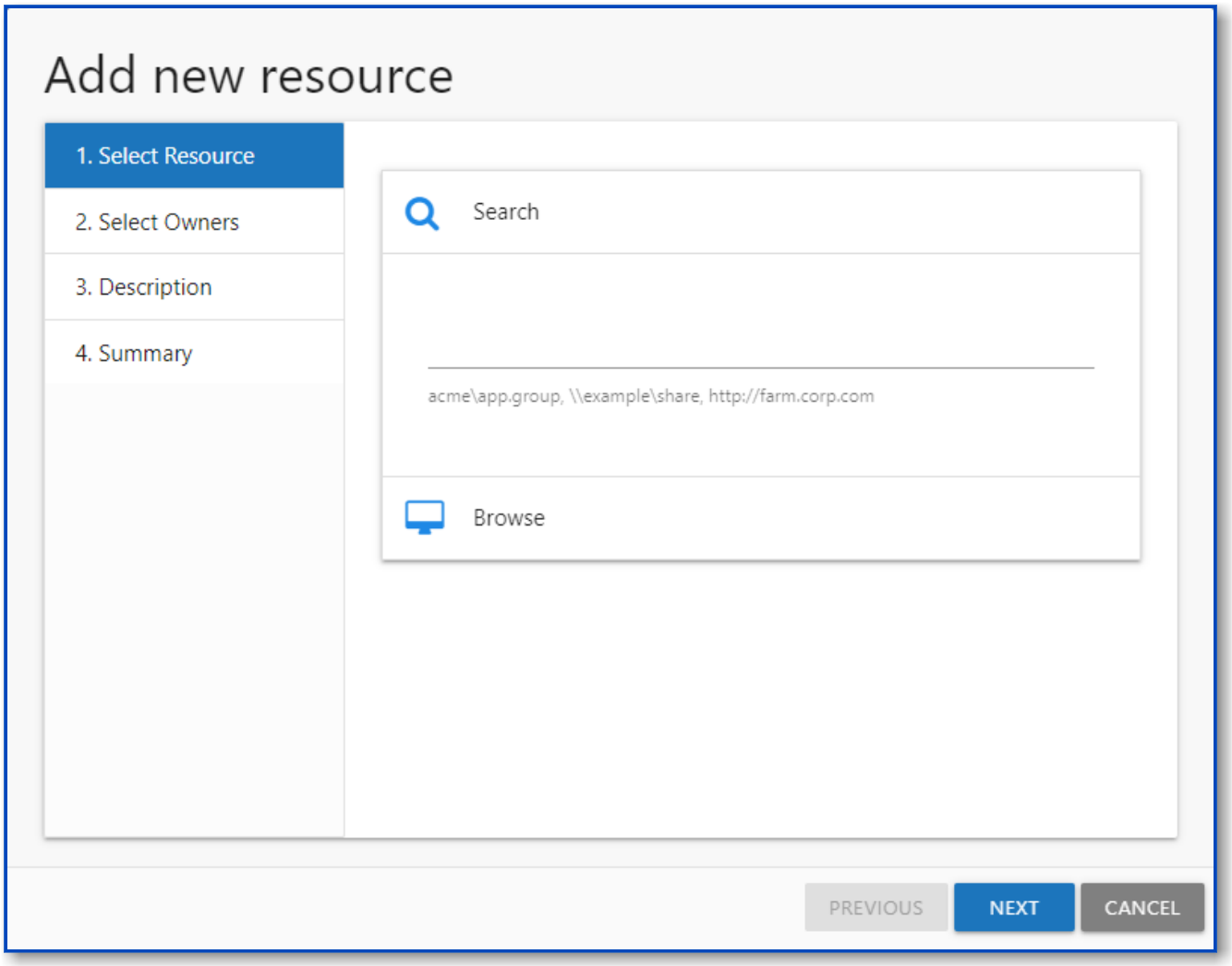
Notes & Descriptions

A note entered by an Ownership Administrator in the Resource Owners interface is only visible to those with access to this interface. This note can also be populated with alternative owners suggested by an individual who declined ownership.

A resource description can be supplied by either the Ownership Administrator or the assigned owner, and is visible during Resource Review creation.

Add New Resource Wizard

The Add new resource wizard is opened with the **Add** button in the Resource Owners interface.



It contains four pages:

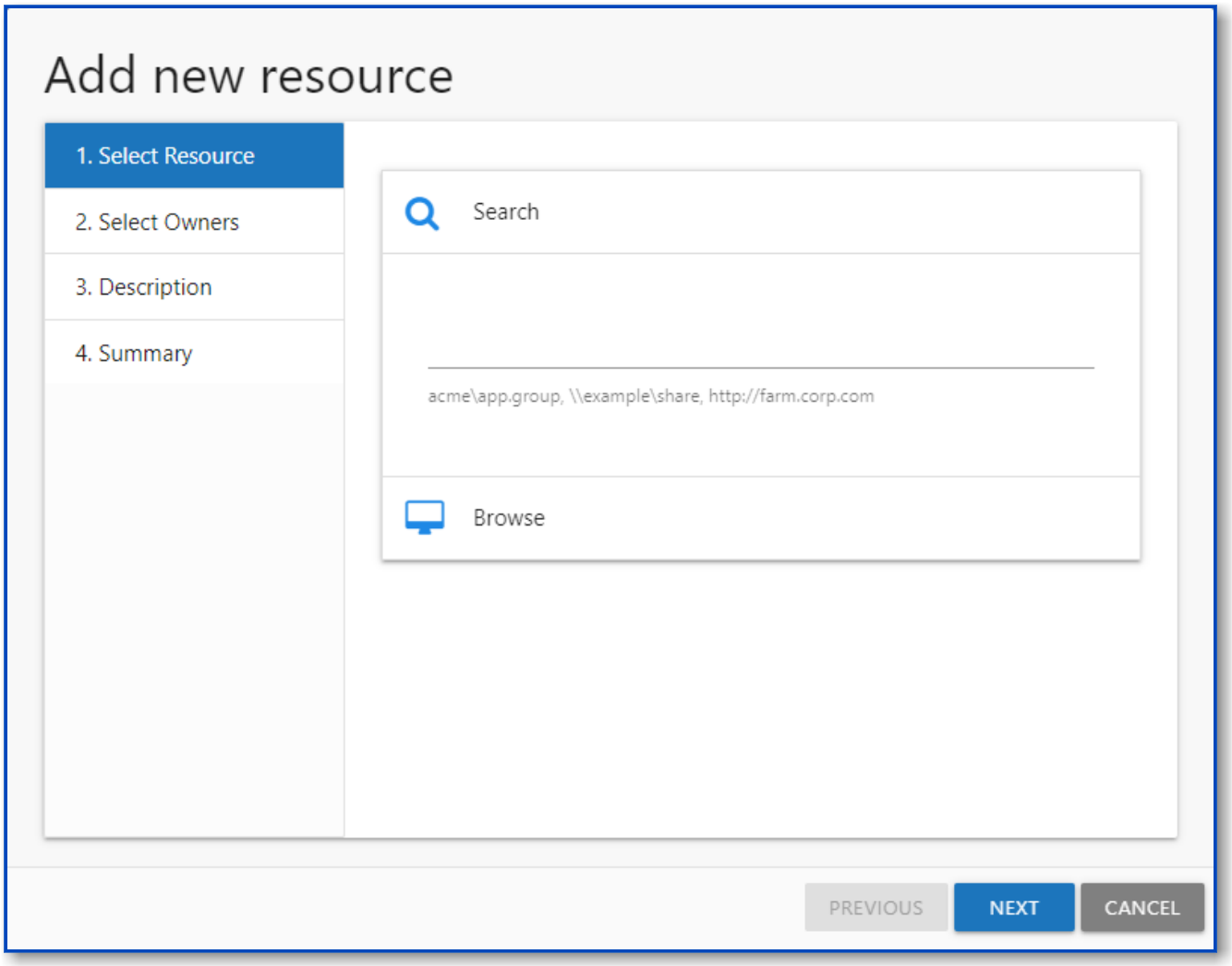
- 1. Select Resource — Select the resource or group to be managed by the owner
- 2. Select Owners — Select Owners from Active Directory
- 3. Description — Optionally enter a note describing the resource
- 4. Summary — This page provides a preview of the settings selected within the wizard

See the Add a Resource topic for additional information.

Add a Resource

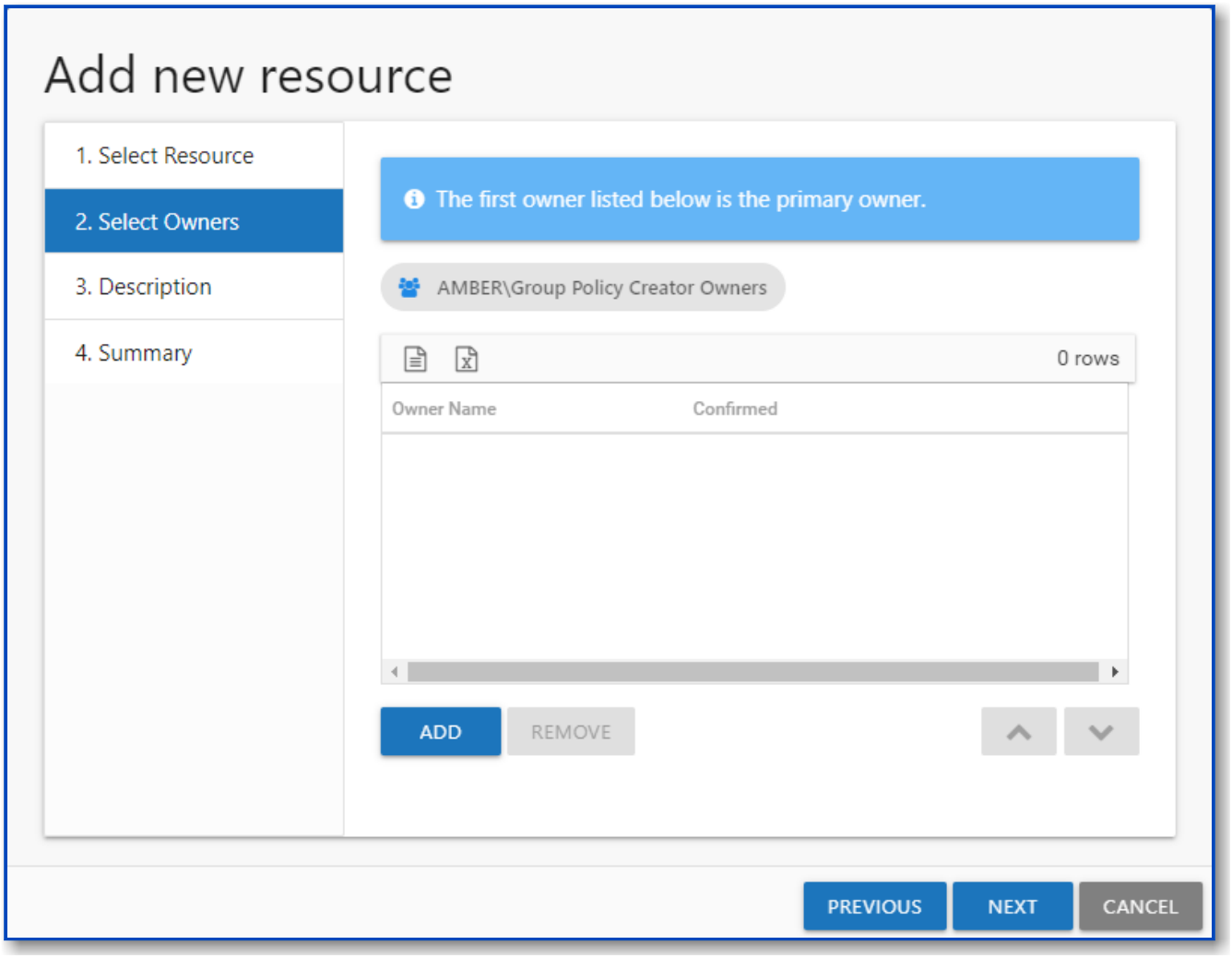
Follow the steps to add resources one at a time and assign owners.

Step 1 – In the Resource Owners interface, click **Add**. The Add new resource wizard opens.

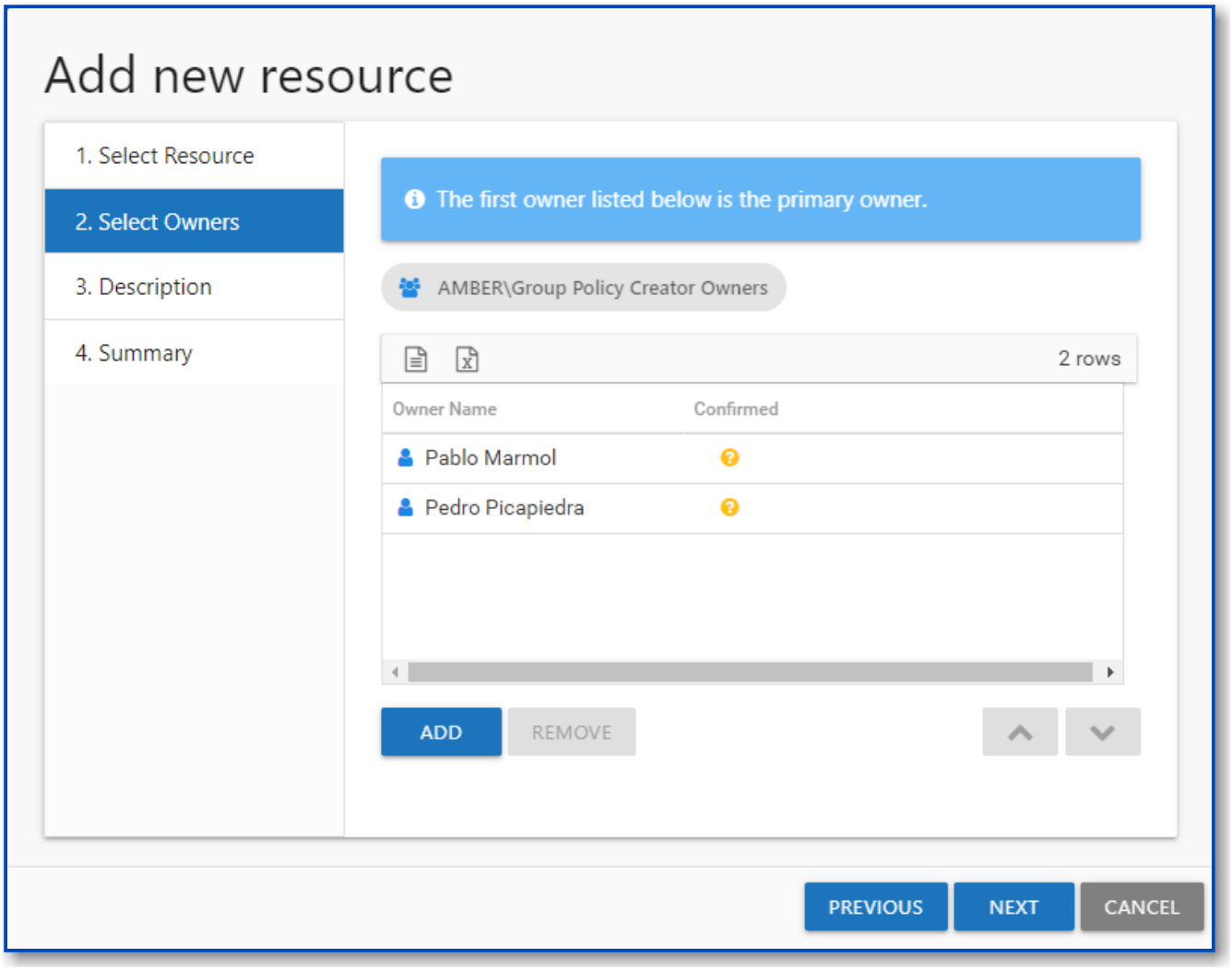


Step 2 – On the Select Resource page, select the resource to be managed. Then click **Next**.

- Search field – Begin typing the name of the resource:
  - For File System, enter a share UNC path starting with "\\"
    - For example, \\example\share
  - For SharePoint, enter the site URL starting with "http://"
    - For example, http://farm.corp.com
  - For groups, enter the group name in NTAccount format [DOMAIN\GROUP]
    - For example, acme\app.group
- Browse option – Navigate through the resource tree to select the desired File System or SharePoint resource.



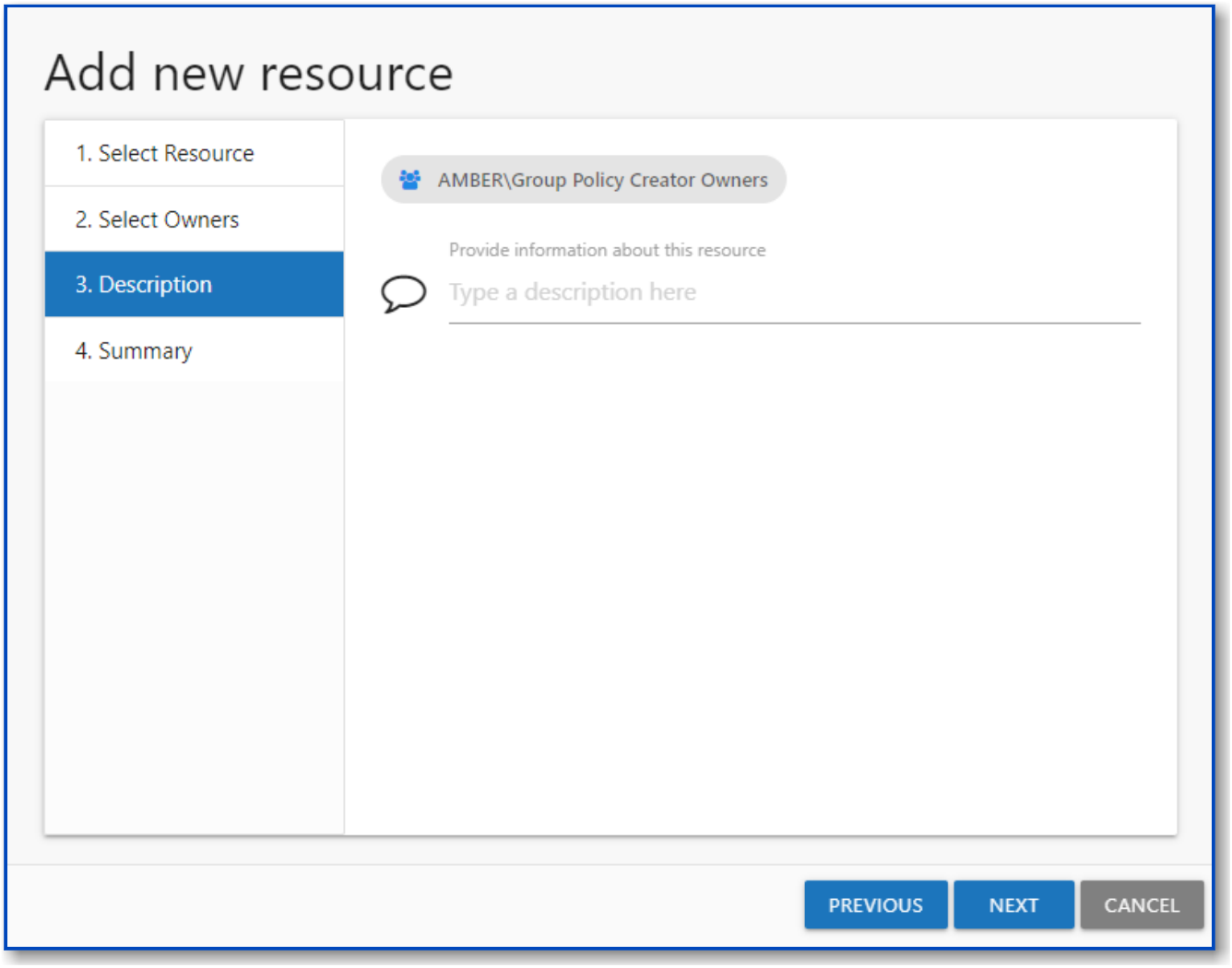
Step 3 – On the Select Owners page, click **Add** to browse for an owner. Repeat this Step to add multiple owners. See the Add Owner Window topic for additional information.



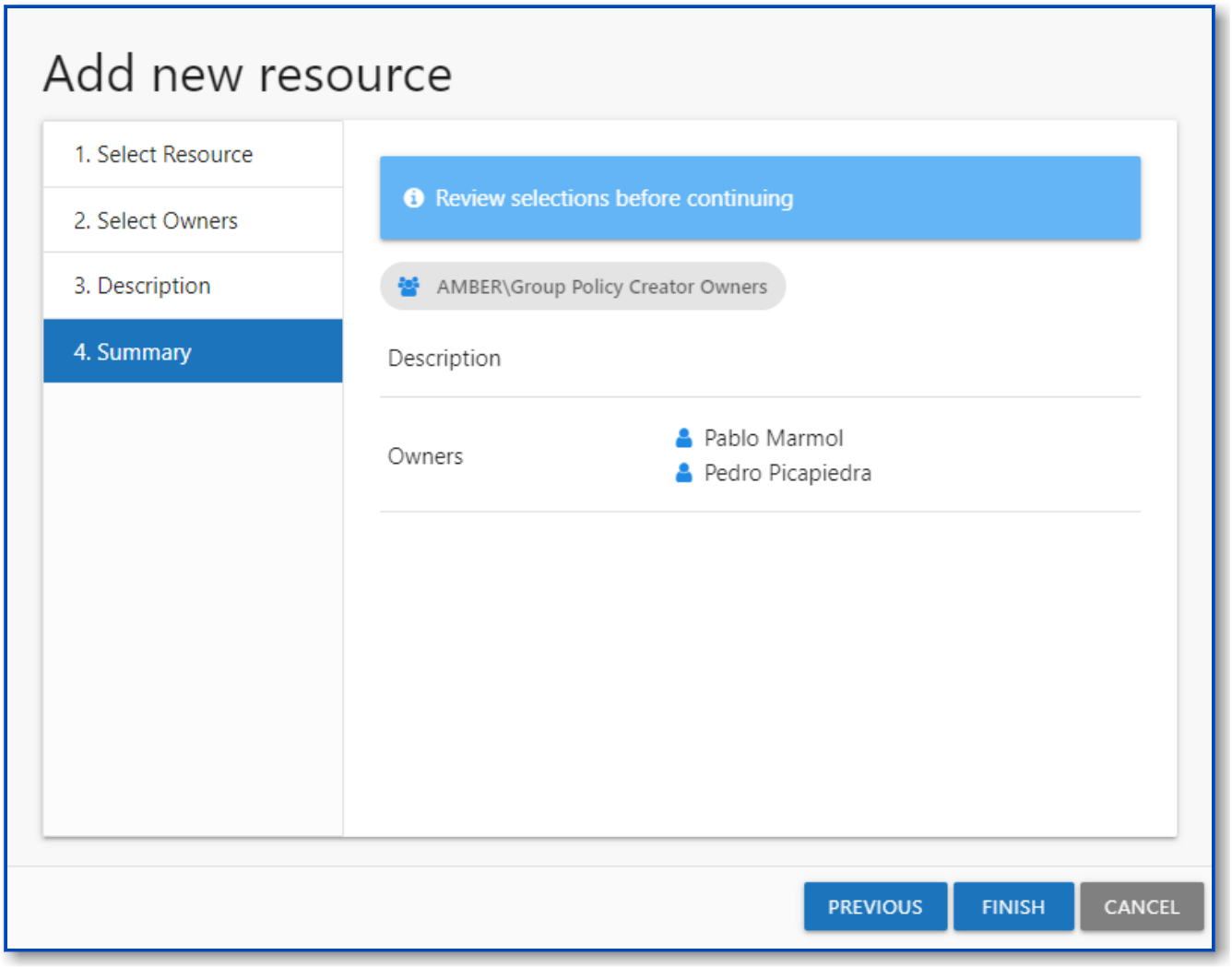
Step 4 – When only one owner is assigned, the owner will be the Primary by default. When multiple owners are assigned, the first owner in the list is the Primary owner. Use the arrow buttons to order the owners. Use the **Add** and **Remove** buttons to modify the list of owners. When the owners list is complete, click **Next**.The table has several columns with information on the owners:

- Owner Name — Name of the assigned owner
- Owner Account — sAMAccountName associated with the owner, as read from Active Directory
- Owner Mail — Trustee's email address as read from Active Directory
- Owner Title — Trustee's title as read from Active Directory
- Owner Department — Trustee's department as read from Active Directory

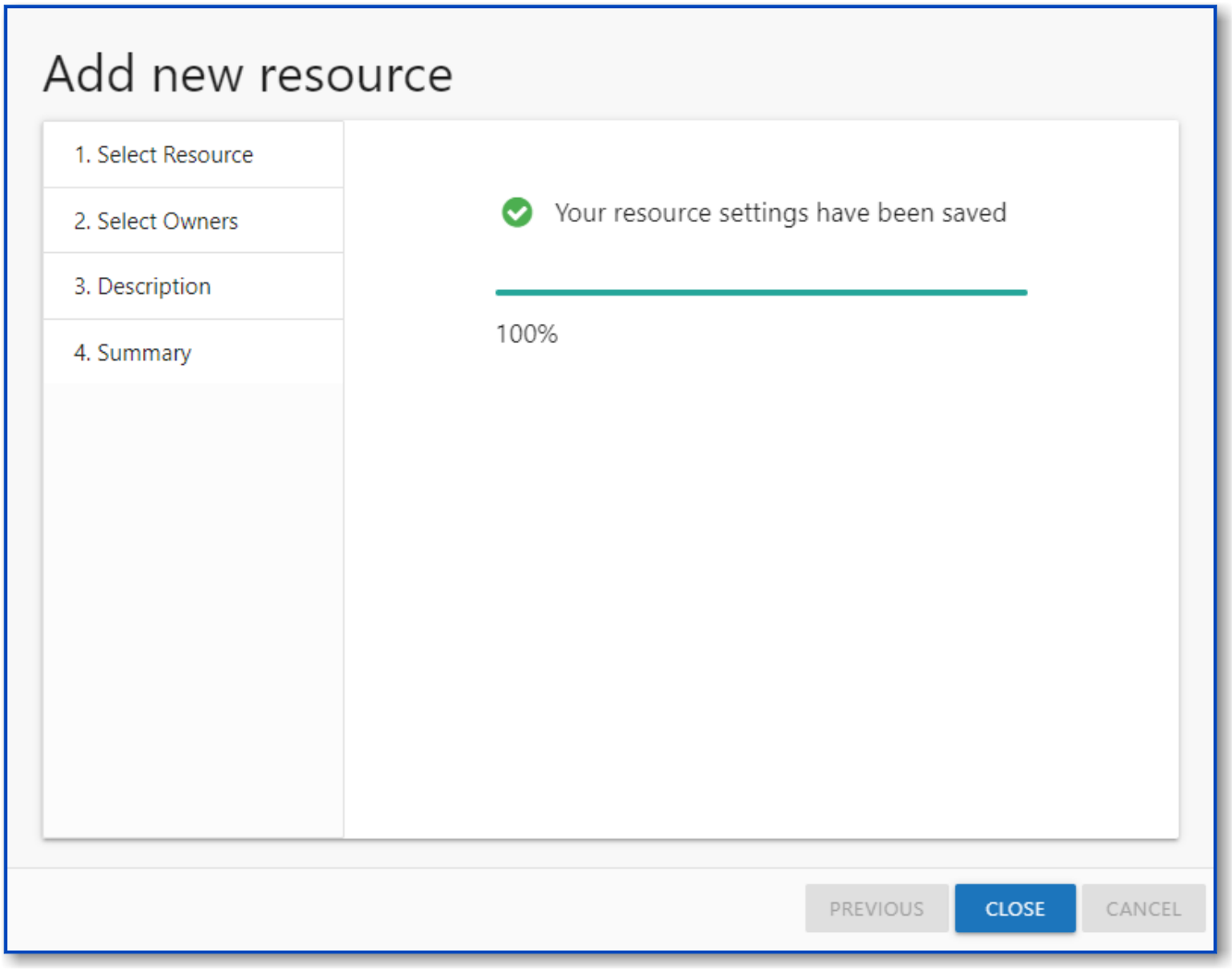
- Confirmed — Indicates whether or not the assigned owner has confirmed ownership of that resource. Tool-tips display when hovering over the icons indicating whether the resource ownership has been confirmed, declined, pending response, or that a confirmation has not been requested.



Step 5 – On the Description page, optionally add a description for the resource in the textbox. Then click **Next**.



Step 6 – On the Summary page, review the settings and click Finish. The Access Reviews application begins to process the ownership configuration.

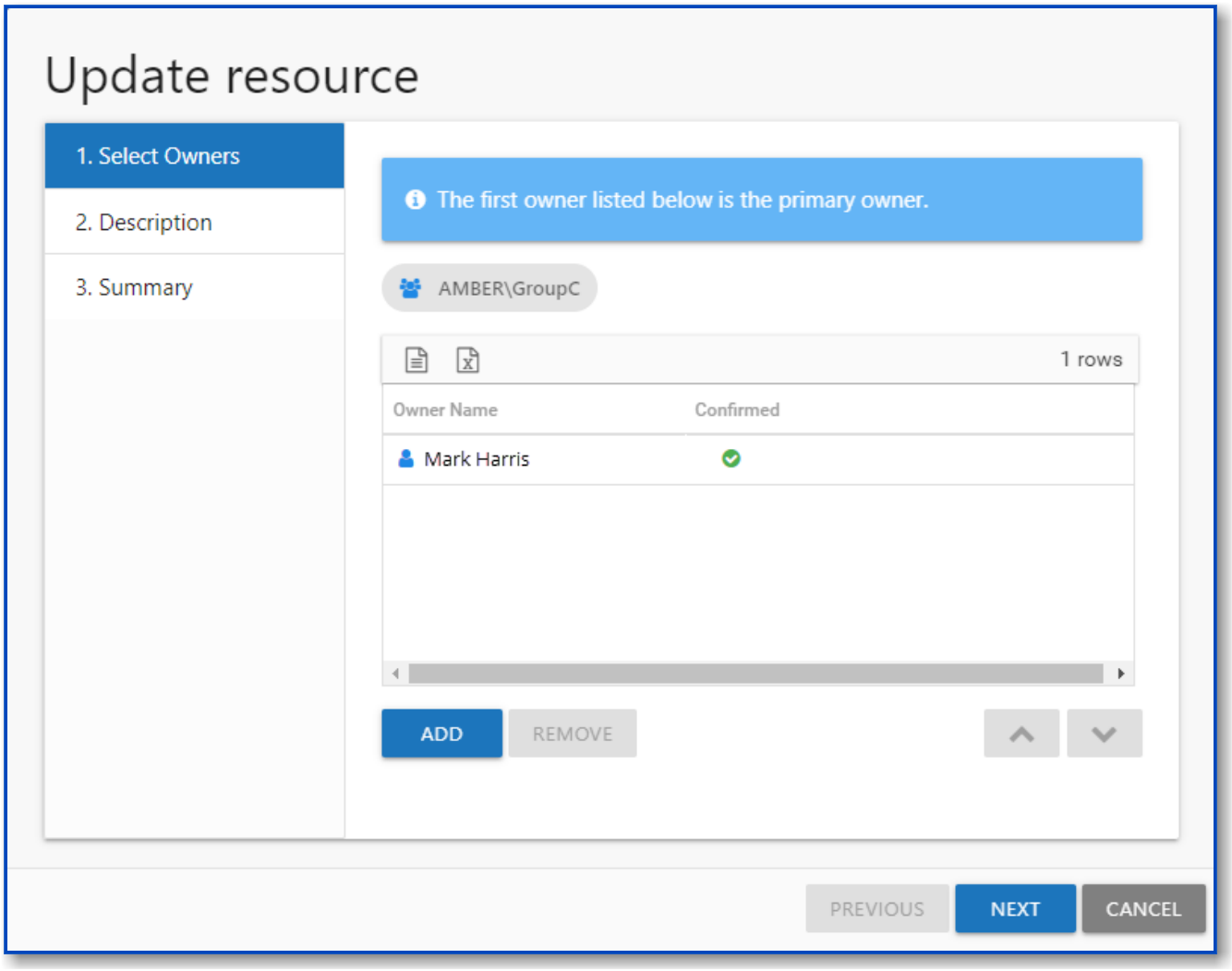


Step 7 – The action status displays on the page. When the task has completed (100%), click **Close**. The Add new resource wizard closes.

This resource is now being managed through the Access Reviews application.

Update Resource Wizard

The Update resource wizard is opened with the **Update** button in the Resource Owners interface.



It contains three pages:

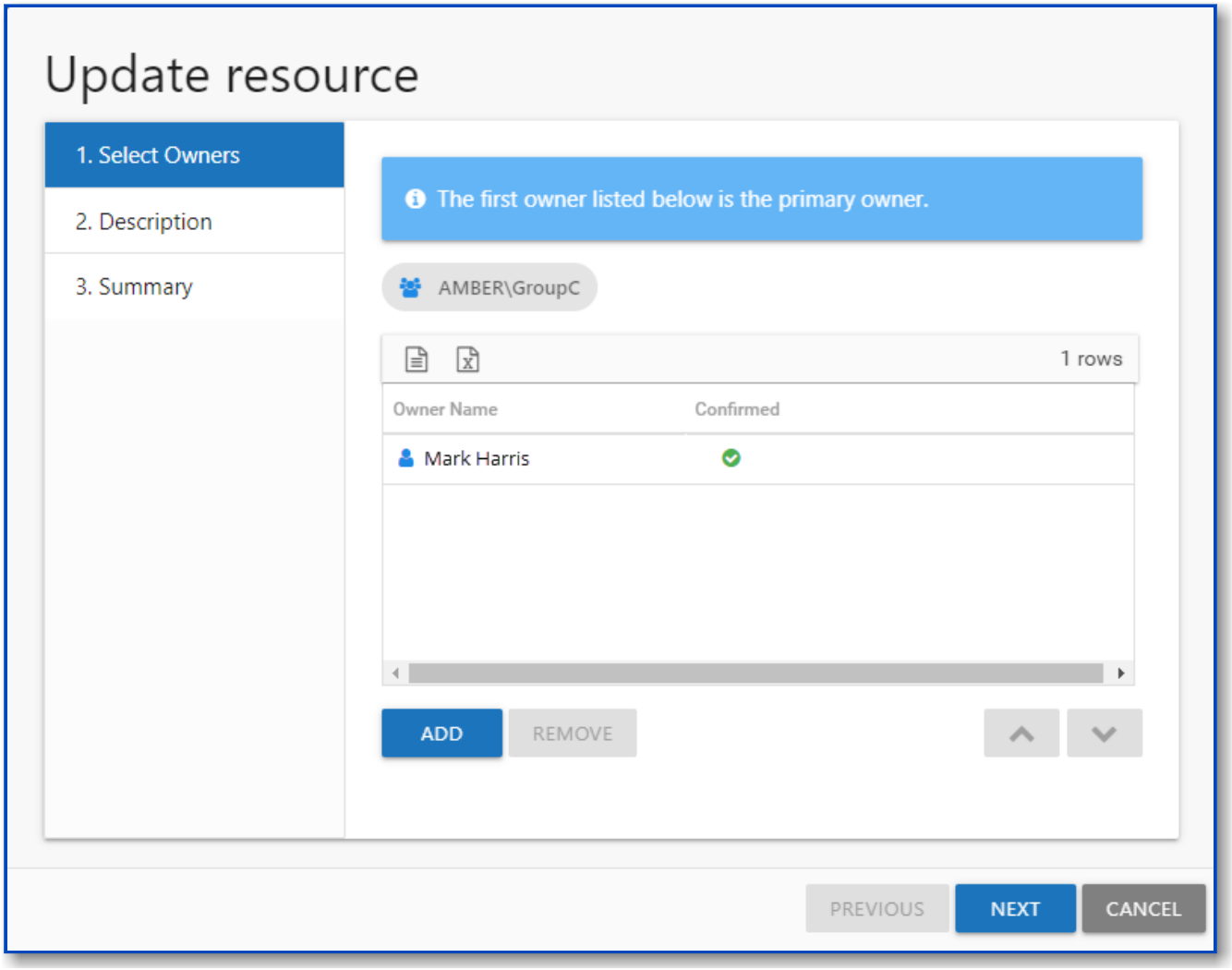
- 1. Select Owners — Lists the current owner(s). Modify by adding new owners, removing owners, or changing owner priority order (primary, secondary, etc.)
- 2. Description — Enter or modify a note describing the resource
- 3. Summary — Provides a preview of the settings selected within the wizard

See the Update a Resource topic for additional information.

Update a Resource

Follow the steps to update ownership configuration for a resource.

Step 1 – In the Resource Owners interface, select the desired resource and click **Update**. The Update resource wizard opens.

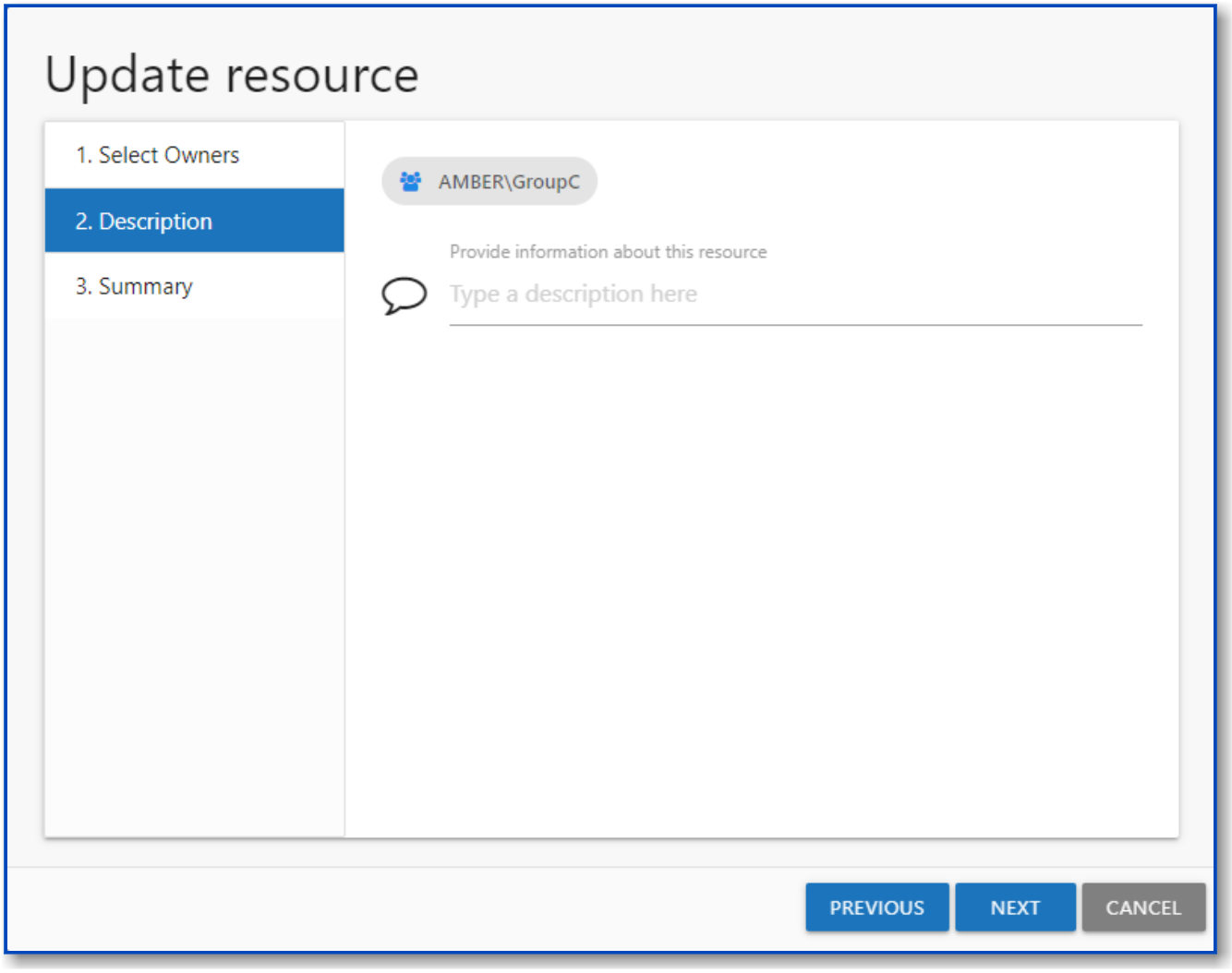


Step 2 – The Select Owners page lists the currently assigned owner(s). Modify as desired and click **Next** to continue.

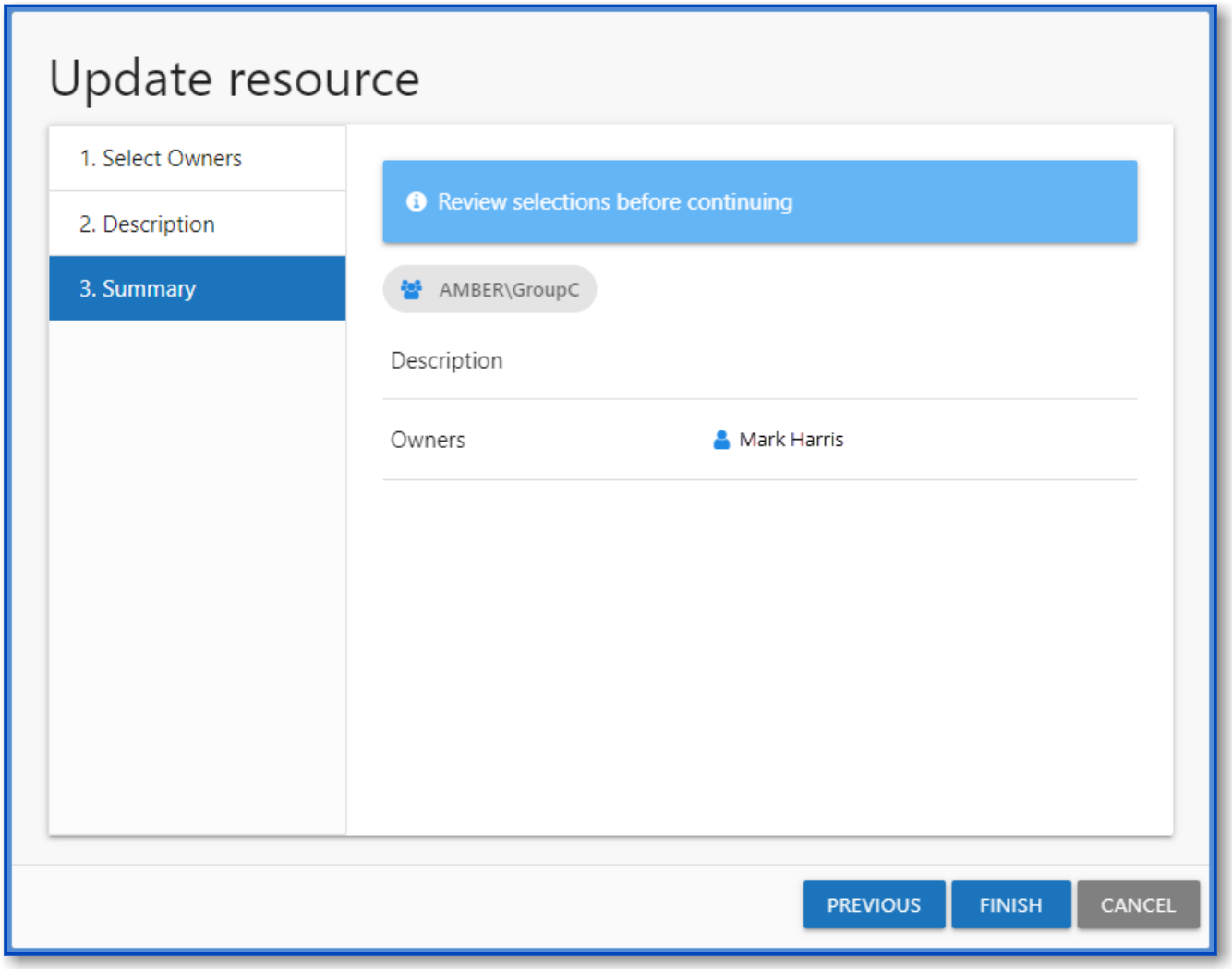
- Add new owners — Click **Add** to browse for a new owner. See the Add Owner Window topic for additional information.
- Remove an owner — Select an owner and click **Remove**
- Change owner priority — Select an owner and use the arrow buttons to change the order

Remember, the first owner in the list is the primary owner. The table has several columns with information on the owners:

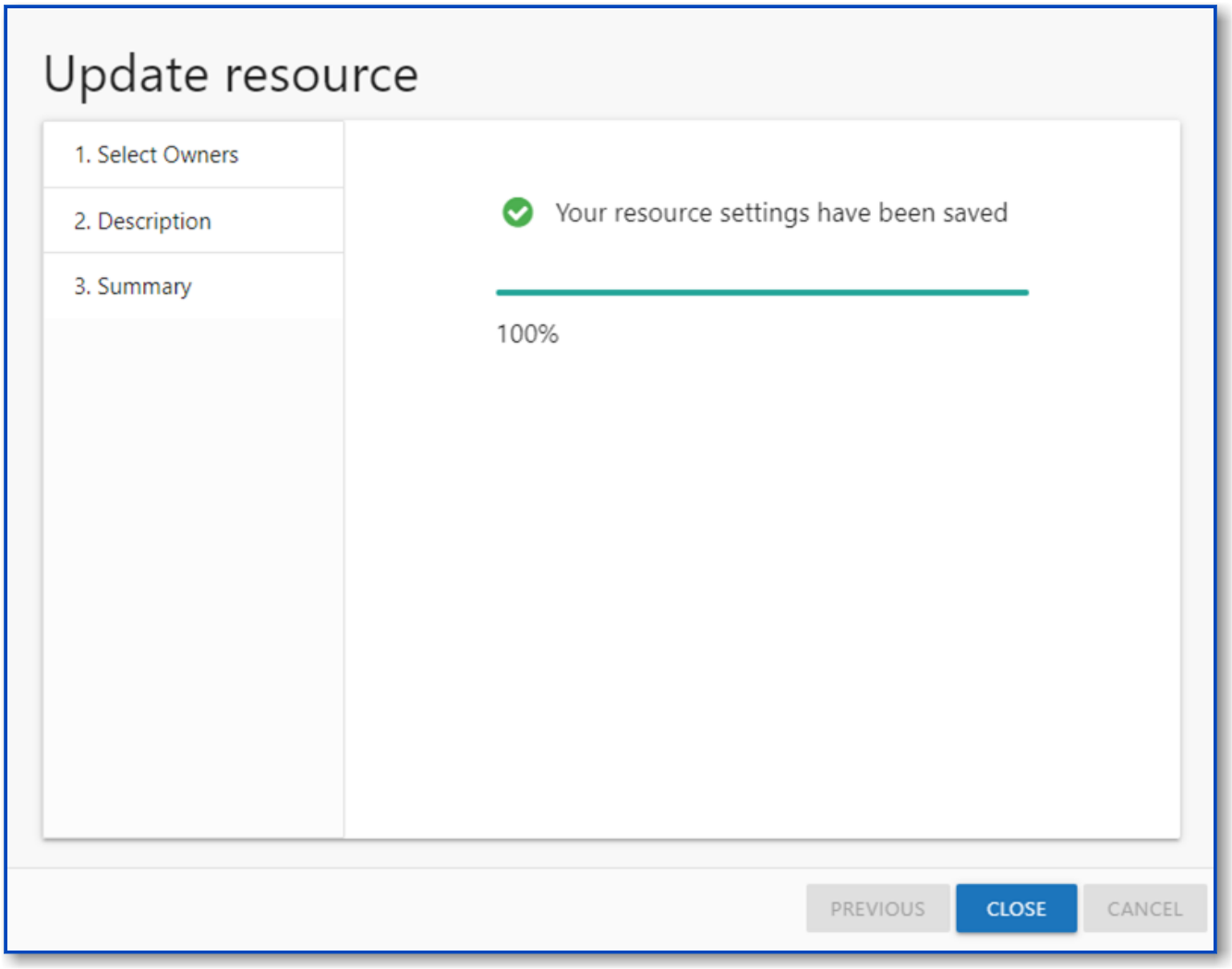
- Owner Name — Name of the assigned owner
- Owner Account — sAMAccountName associated with the owner, as read from Active Directory
- Owner Mail — Trustee's email address as read from Active Directory
- Owner Title — Trustee's title as read from Active Directory
- Owner Department — Trustee's department as read from Active Directory
- Confirmed — Indicates whether or not the assigned owner has confirmed ownership of that resource. Tool-tips display when hovering over the icons indicating whether the resource ownership has been confirmed, declined, pending response, or that a confirmation has not been requested.



Step 3 – The Description page displays any description that has been provided by either the Ownership Administrator or the assigned owner(s) for the resource. Modify as desired by typing in the textbox. Then click **Next** to continue.



Step 4 – On the Summary page, review the settings and click Finish. The Access Reviews application begins to process the ownership changes.

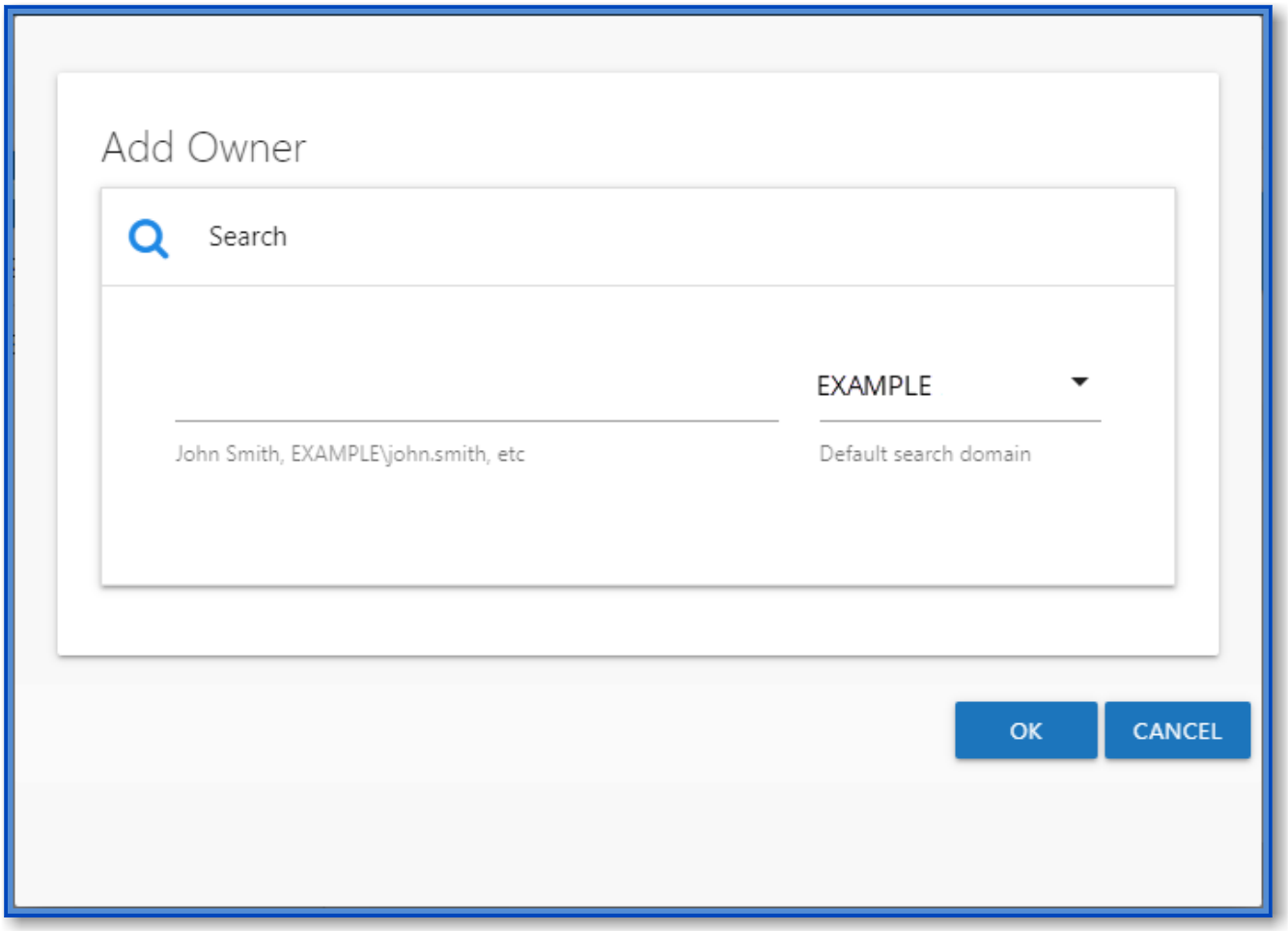


Step 5 – The action status displays on the page. When the update has completed (100%), click **Close**. The Update resource wizard closes.

This updates to ownership configuration have been processed.

Add Owner Window

The Add Owner window opens from either the Add New Resource Wizard of the Update Resource Wizard. This window is used to search for a user account by browsing Active Directory.



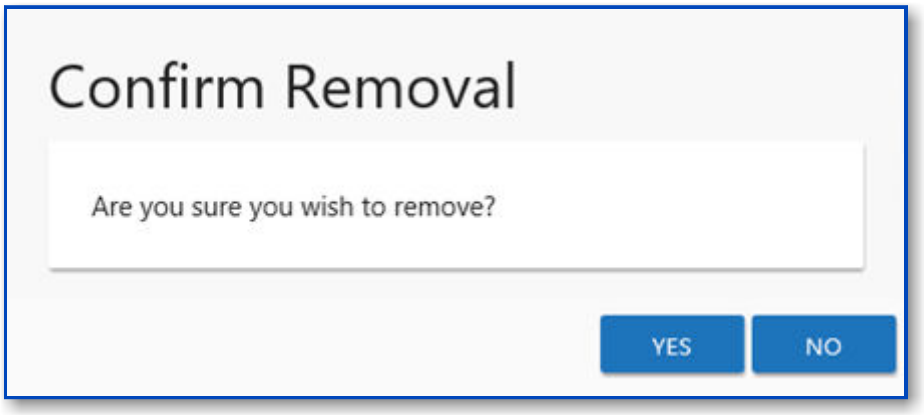
Enter a name in the search field to find and select users from Active Directory, which populates in a drop-down menu as you type. If multiple domains are known to the application, ensure the correct domain is selected from the drop-down menu. Click **OK** and the Add Owner window closes. The selected user appears in the Owner list.

Confirm Removal Window

The process of removing a resource from the Resource Owners interface disassociates the owner(s) from the resource, it does not remove the resource from the database or from the available reports. Any history of actions performed by the owner for that resource will be maintained, but pending actions will be canceled. Pending actions may include s outstanding reviews.

Follow the steps to remove a resource from being managed through the application.

Step 1 – In the Resource Owners interface, select the resource and click Remove. The Confirm Removal window opens.



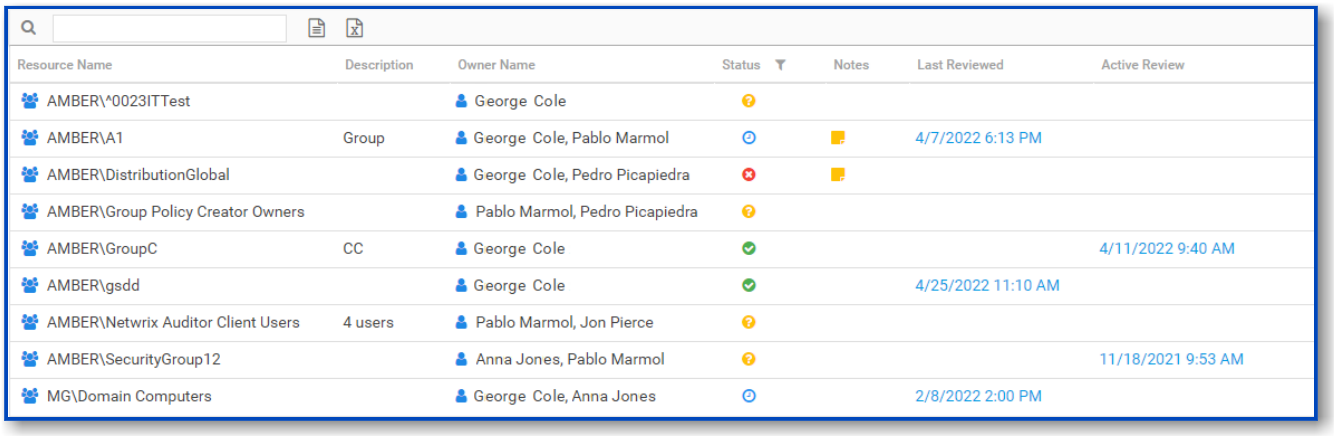
Step 2 – Click Yes to complete the removal process or **No** to cancel it.

The resource no longer appears in the Resource Owners interface.

Ownership Confirmation

The reason for assigning owners to resources is to enable those resources to be included in reviews, or attestations, conducted through the application. In order for this to work, the assigned owner needs to claim that ownership responsibility. Resources that do not have confirmed owners may fall through the cracks.

NOTE: This does require the Notification settings to be configured for the Access Reviews application. See the Notifications Page topic for additional information.



Resource Name	Description	Owner Name	Status	Notes	Last Reviewed	Active Review
AMBER*0023ITTest		George Cole				
AMBER\A1	Group	George Cole, Pablo Marmol			4/7/2022 6:13 PM	
AMBER\DistributionGlobal		George Cole, Pedro Picapiedra				
AMBER\Group Policy Creator Owners		Pablo Marmol, Pedro Picapiedra				
AMBER\GroupC	CC	George Cole				4/11/2022 9:40 AM
AMBER\gsdd		George Cole			4/25/2022 11:10 AM	
AMBER\Netwrix Auditor Client Users	4 users	Pablo Marmol, Jon Pierce				
AMBER\SecurityGroup12		Anna Jones, Pablo Marmol				11/18/2021 9:53 AM
MG\Domain Computers		George Cole, Anna Jones			2/8/2022 2:00 PM	

The table in the Resource Owners interface includes a Status column. The following icons appear in this column to indicate the owner confirmation status:

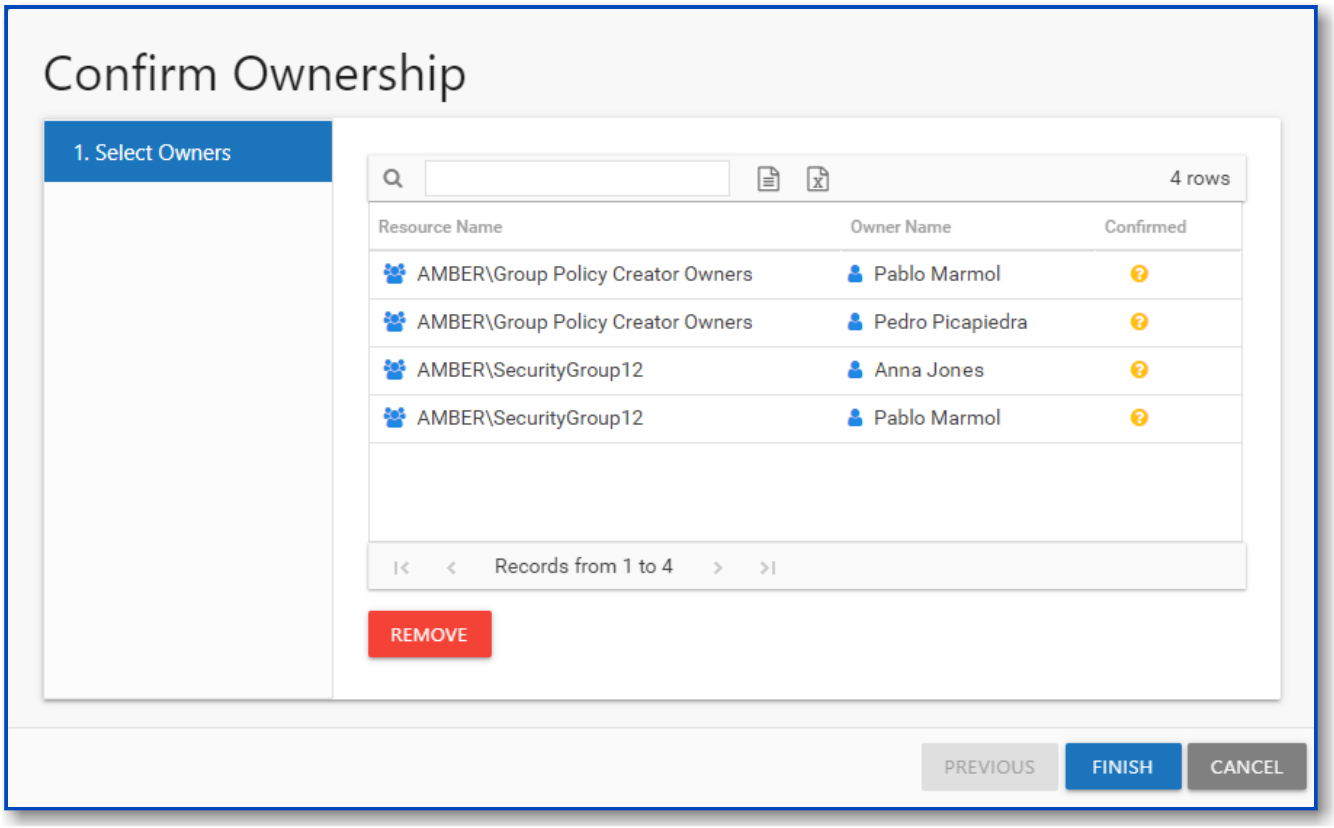
Icon	Meaning	Description
	No Status	Indicates ownership confirmation has not been requested, and there is no ownership status at this time
	Waiting	Indicates a request for confirmation has been sent, and you are waiting for a response from the assigned owner. Hover over the icon to view the date timestamp of the request.
	Confirmed	Indicates the assigned owner confirmed ownership of the resource. Hover over the icon to view the date timestamp of the confirmation.
	Declined	Indicates the assigned owner declined ownership of the resource. These individuals would have been asked to suggest an alternative owner. Check the Notes for the resource to view this information. Hover over the icon to view the date timestamp of the decline. *Remember,* a resource with declined ownership needs to be updated to assign a new owner. See the Update Resource Wizard topic for additional information.

If multiple owners have been assigned, there is a choice for which assigned owner(s) should receive the confirmation. If multiple owners were sent the request, the column remains as a waiting symbol until the assigned Primary owner replies.

See the Confirm Ownership Wizard topic for additional information.

Confirm Ownership Wizard

The Confirm Ownership wizard is opened with the **Request Confirmation** button in the Resource Owners interface. It can be opened for one or multiple resources.



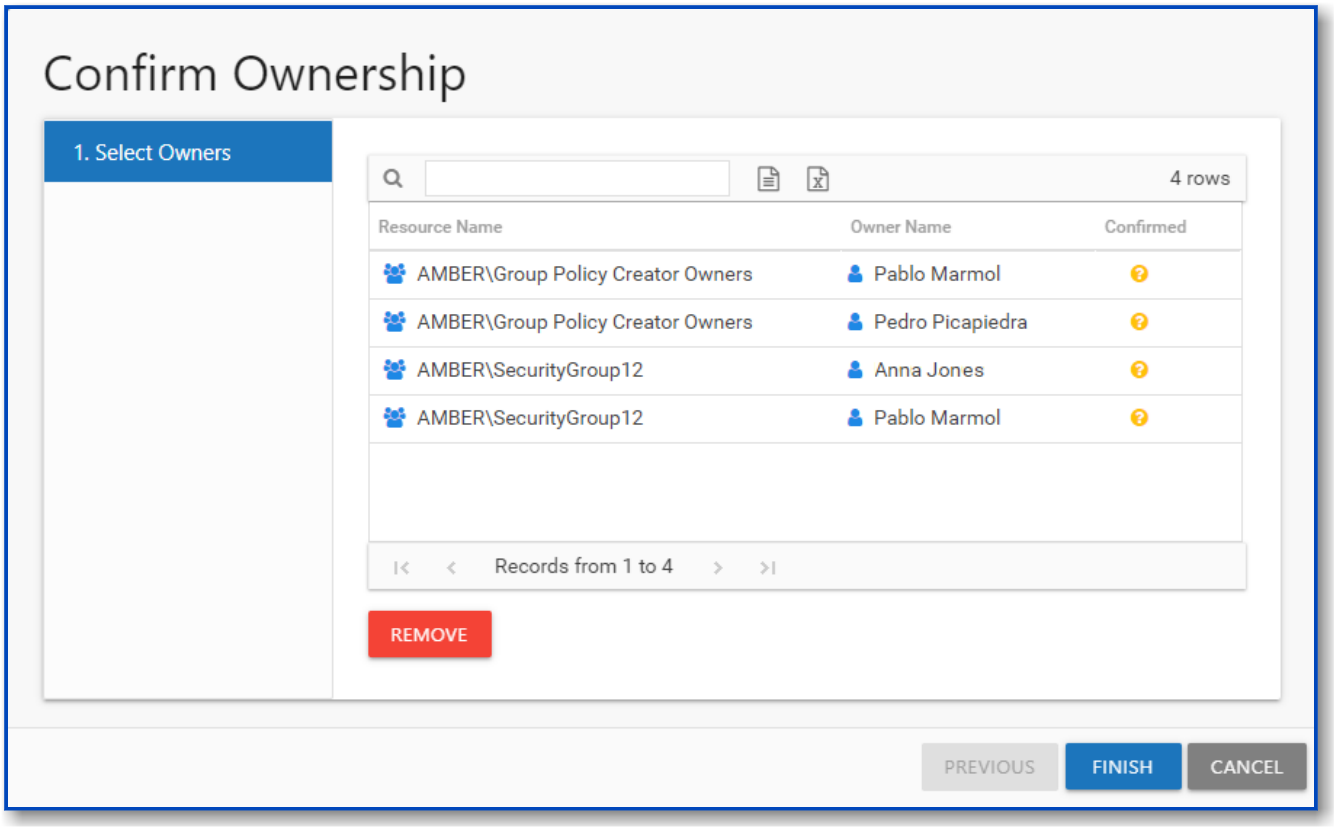
It contains one page:

- 1. Select Owners — Lists the current owner(s) for each selected resource and confirmation status

Request Ownership Confirmation

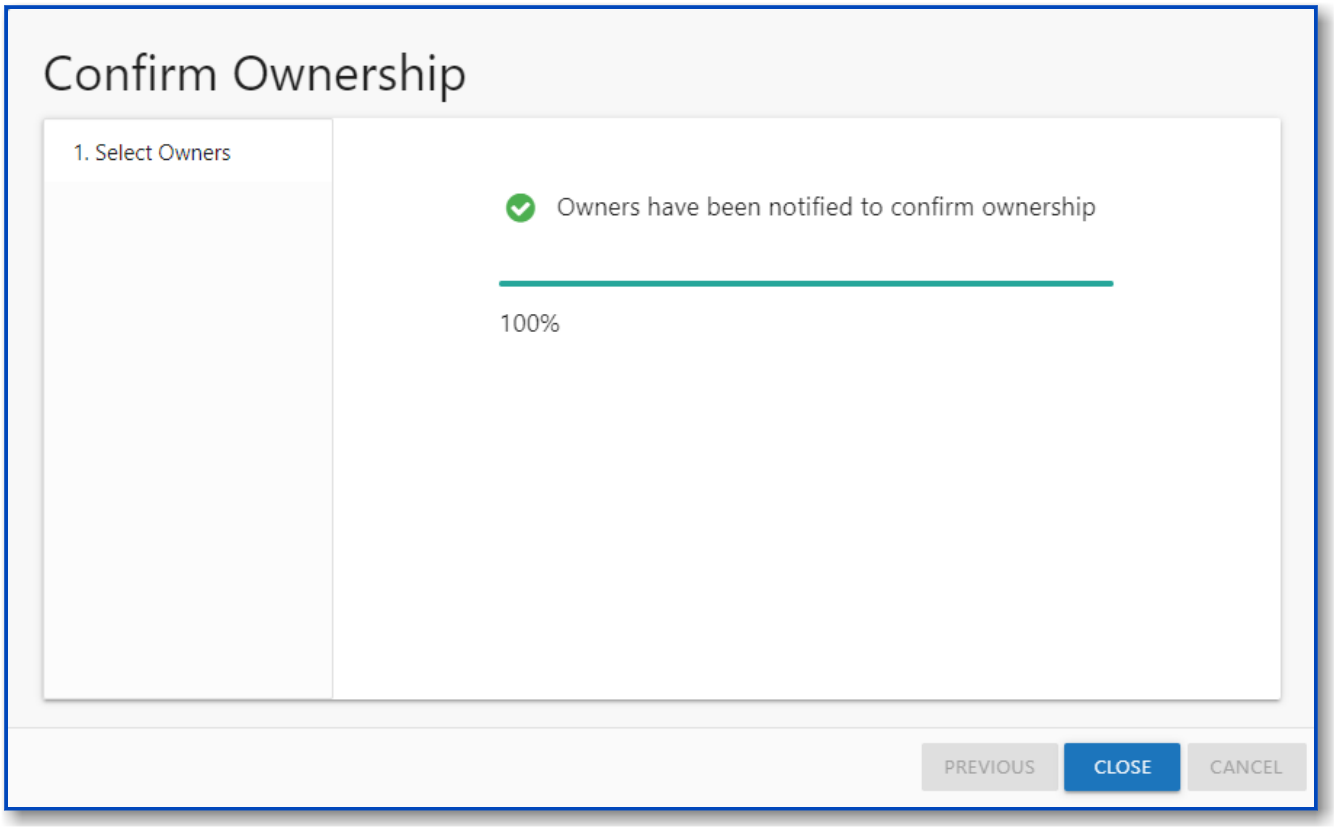
Follow the steps to request ownership confirmation.

Step 1 – In the Resource Owners interface, select the desired resource or resources and click Request Confirmation. The Confirm Ownership wizard opens.



Step 2 – On the Select Owners page, you can optionally remove owners you do not want or need ownership confirmation from. Select those owners and click **Remove**. Those owners will not receive the confirmation email. Once the list is set as desired, click **Finish**. The Access Reviews application begins to send the confirmation email. The table provides the following information:

- Resource Name — The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
- Owner Name — Name of the assigned owner
- Confirmed — Indicates whether or not the assigned owner has confirmed ownership of that resource. Tool-tips display when hovering over the icons indicating whether the resource ownership has been confirmed, declined, pending response, or that a confirmation has not been requested.



Step 3 – The action status displays on the page. When the owner confirmation notification has completed (100%), click Close. The Confirm Ownership wizard closes.

The selected owners receive an email from the Access Reviews application asking if they are the owner of the assigned resource. See the Ownership Confirmation Request Email topic for additional information.

Reviews Overview

The Entitlement Reviews interface is where users with either the Security Team or Administrator role (to be referred to as Review Administrators) can manage reviews. The workflow provides a way for business users or data custodians (to be referred to as Owners) to attest to the access and privileges users have to their resources.

For the purpose of the Access Reviewsapplication, a “resource” refers to the file system shared folders, SharePoint Online site collections, and Active Directory (AD) groups. All data available within the Access Reviews application is collected by Netwrix Auditor according to the synchronized monitoring plans.

Remember, Owners are assigned to resources in the Resource Owners interface. Only resources with assigned Owners can be included in a reviews.

Who Can Run Reviews (Review Administrators)?

- Console Users with Administrator role
  - Can complete the Review Administrator's approval process without impacting the visibility into the review created by a Review Administrator with the Security Team role

    CAUTION: Visibility into a review created by a Review Administrator with the Security Team role is blocked if a Review Administrator with the Administrator role starts a new instance.
- Console Users with Security Team role
  - Visibility into only those reviews personally created

Who Participates in Reviews?

- Review Administrators — Create / start reviews and approve / process owner recommended changes
- Owners — Perform reviews and recommend changes

Types of Reviews

There are two types of reviews:

- Access – Review user access rights to resources
- Membership – Review group membership

See the Entitlement Reviews Interface topic for additional information.

Workflow of Reviews

Prerequisite:

- The Access Reviews application is configured to send Notifications. See the Notifications Page topic for additional information.

  NOTE: By default, the application is configured to send notifications only to the primary owner. However, this can be customized on the Configuration > Notifications page to send notifications to all assigned owners.

- Owners assigned to resources within the Resource Owners interface. See the Resource Owners Overview topic for additional information.

Workflow:

RECOMMENDED: When deploying the Access Reviews application in an organization to process reviews, owners should be notified prior to launching the first set of reviews. See the Notification to Owners topic for additional information.

1. Review Administrator creates a review or starts a new review instance. See the Create Review Wizard topic for additional information.
2. Owner performs a review. See the Pending Reviews topic for additional information.
3. Review Administrator approves owner recommendations. See the Approval Process topic for additional information.
4. Implement approved changes in your organization. Manually, export a list of approved changes and deliver it to your IT department.

When desired, the Review Administrator runs another instance of the review and the workflow starts again. See the Review Instances topic for additional information.

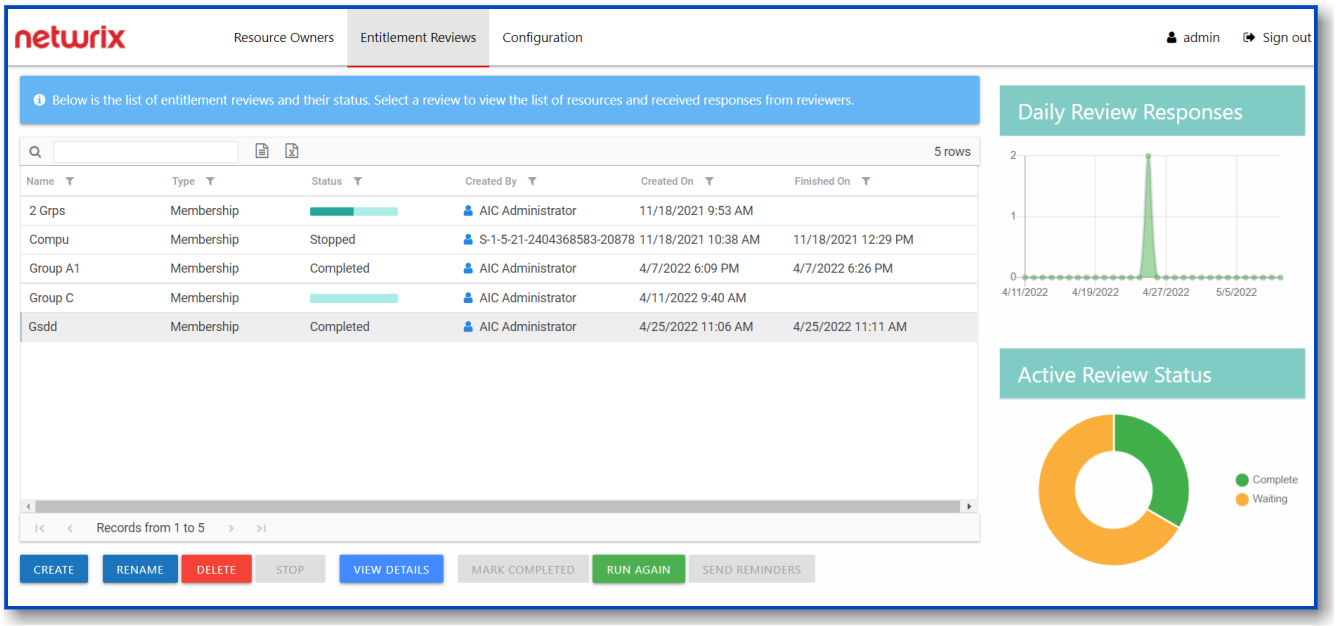
Entitlement Reviews Interface

The Entitlement Reviews interface opened by the Entitlement Reviews tab is where Review Administrators perform many operations around managing reviews. This interface has multiple pages:

- Manage Reviews Page — Create and manage all reviews
- Review Details Page — Manage and view all instances for a specific review

Manage Reviews Page

The Manage Reviews page is the first page in the Entitlement Reviews interface. It displays high-level information for reviews.



The interface includes:

- Table of reviews
- Daily Review Responses line graph
- Active Review Status donut graph

The information displayed in the table includes:

- Name — Name of the review, as provided by the Review Administrator
- Type — Type of review:
  - Access – Review user access rights to resources
  - Membership – Review group membership
- Status — Status of the review:
  - Status bar with specified percentage completed
    - [Empty bar] 0% – Indicates not started. Hovering over the bar will display the number of items included.
    - [Partially filled bar] with a non-zero% – Indicates the specific percentage of items completed. Hovering over the bar displays the number of items completed out of the total number of items.

    - Responses awaiting review — Owner(s) completed reviews. Waiting on Review Administrator's approval.
    - All responses processed — Reviews have been approved by Review Administrators. The review can be marked as completed.
    - Stopped — Indicates that the review was stopped and is considered complete even if all of the responses have not been received or processed. The review remains static until it is run again.
    - Completed — Indicates the Review Administrator has processed the owners' responses. The review remains static until it is run again. This status can appear by accepting the review as-is with the Mark Completed button.
- Created By — Name of the Review Administrator who create the review
- Created On — Date timestamp for when the review was creation. If it has been run multiple times, this is the date timestamp of the last instance.
- Finished On — Date timestamp when the review is marked complete by the Review Administrator. If it has been run multiple times, this is the date timestamp of the last instance.

The table data grid functions the same way as other table grids. See the Data Grid Features topic for additional information.

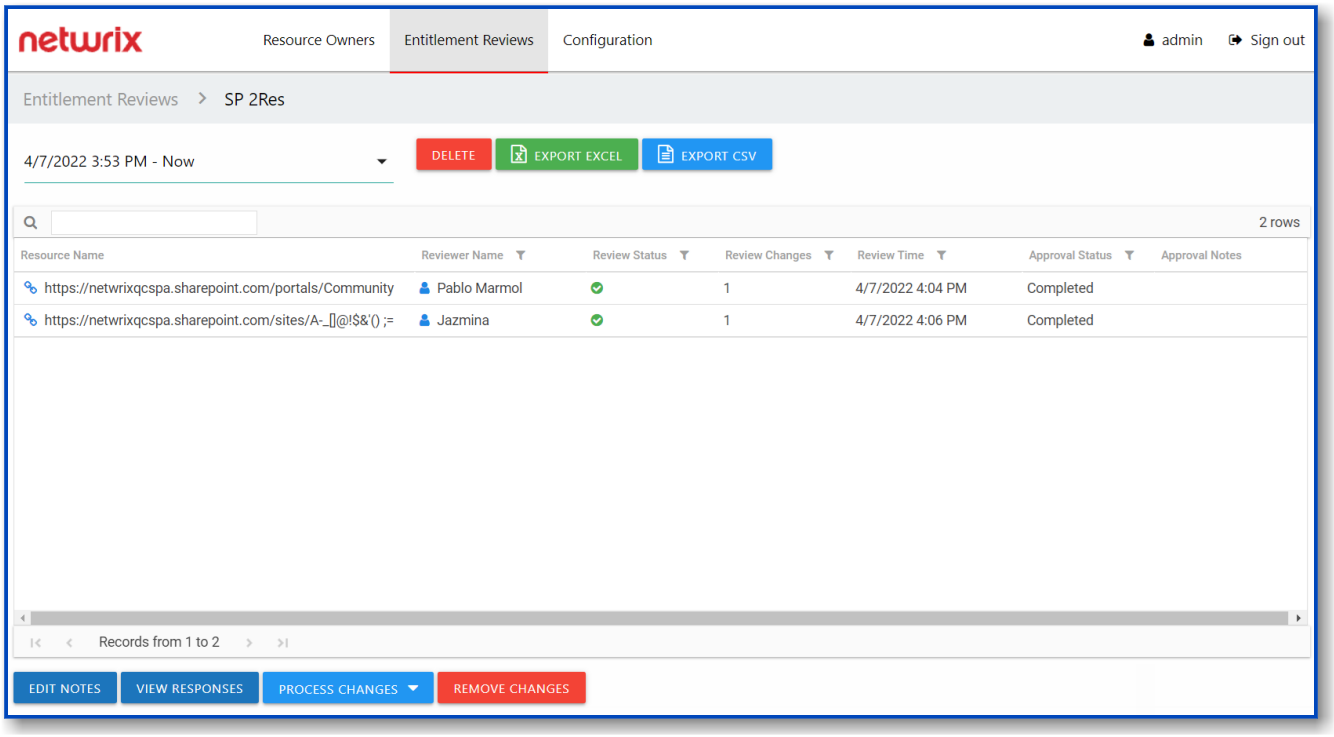
The buttons at the bottom enable you to conduct the following actions:

Button	Description
Create	Launches the Create Review wizard for creating a new review. See the Create Review Wizard topic for additional information.
Rename	Opens the Rename Review window for modifying the review name. See the Rename Review Window topic for additional information.
Delete	Opens the Delete Review window to delete review and its instance history, which asks for confirmation of

Button	Description
	the action. See the Delete Review Window topic for additional information.
Stop	Opens the Stop Review window, which asks for confirmation of the action. See the Stop Review Window topic for additional information.
View Details	Opens the Review Details page for the selected review. See the Review Details Page topic for additional information.
Mark Completed	Closes the selected review as-is and marks it as completed. Requires the owner(s) to have responded. **CAUTION:** No confirmation is requested for this action.
Run Again	Opens the Create Review wizard for the selected review without the option to change the review type. Modify as desired and relaunch the review. See the Review Instances topic for additional information.
Send Reminders	Sends a notification email to the assigned owner(s), reminding of the pending review. Opens the Send Reminders window, which indicates an action status. See the Send Reminders Window topic for additional information.

Review Details Page

The Review Details page displays information for all instances of the selected review, which is named in the page breadcrumb. This page is opened by selecting a review on the Manage Reviews page and clicking **View Details**.



Instances are selected from the drop-down menu. By default the most current instance will be displayed. Instances are named with date timestamps indicating the start and end times for the review instance.

The information displayed in the table includes:

- Resource Name — The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
- Reviewer Name — Primary owner assigned to the resource
- Review Status — Indicates whether or not the assigned owner has submitted the review. Tool-tips display when hovering over the icons.
- Review Changes — Displays a count of items that have recommended changes for the resource
- Review Time — Date timestamp for when the owner submitted the review

- Approval Status — Status of the Review Administrator's approval:
  - Blank — Indicates the owner has not completed the review for the resource
  - Status bar with specified percentage completed
    - [Empty bar] 0% – Indicates not started. Hovering over the bar will display the number of items included.
    - [Partially filled bar] with a non-zero% – Indicates the specific percentage of items completed. Hovering over the bar displays the number of items completed out of the total number of items.
  - Completed — Indicates the Review Administrator has processed the owners' responses. The review remains static until it is run again.
- Approval Notes – Icon indicates a Note has been added. Click on the icon to read the attached note(s). Notes displayed here can only be added or viewed by the Review Administrator. See the Edit Notes Window topic for additional information.

The table data grid functions the same way as other table grids. See the Data Grid Features topic for additional information.

The buttons at the top and bottom enable you to conduct the following actions:

Button	Description
Delete	Opens the Delete Review window to delete selected review instance, which asks for confirmation of the action. See the Delete Review Window topic for additional information.
Export Excel	Exports the selected review instance information to an Excel spreadsheet. This automatically downloads the spreadsheet. See the Data Grid Features topic for additional information.

Button	Description
Export CSV	Exports the selected review instance information to a CSV file. This automatically downloads the file. See the Data Grid Features topic for additional information.
Edit Notes	Opens the Edit Notes window for the selected resource and allows free-text editing of the notes. See the Edit Notes Window topic for additional information.
View Responses	Opens the View Responses window, which is only available if the owner has recommended changes for the resource. This window displays all recommended changes, notes provided by the owner for the recommended change, and action buttons to Accept, Decline, or Defer the recommended change. See the View Responses Window topic for additional information.
Process Changes	Opens a drop-down menu to Accept, Decline, or Defer all owner-recommended changes for the selected resource. This option allows the Review Administrator to process responses in batches, so all owner-recommended changes for the selected resource will be processed with the same action.
Remove Changes	Opens the Remove changes window. Clears all requested changes for the selected resource. The resource is returned to a 'Waiting' status, requiring the owner to review the resource again. See the Remove Changes Window topic for additional information.

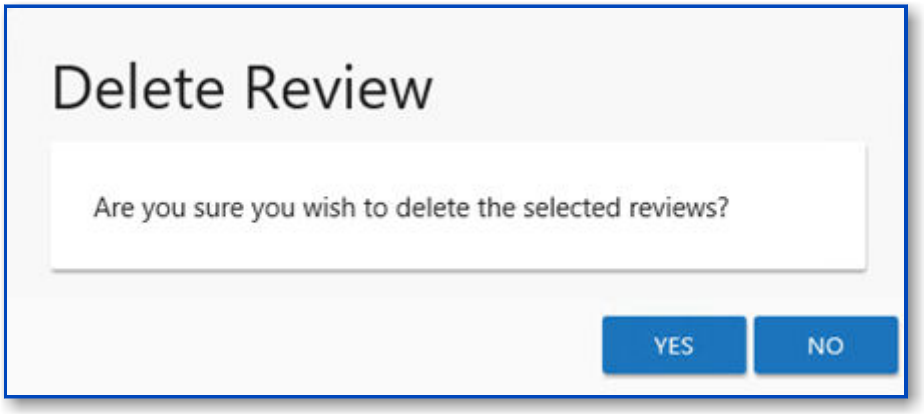
Delete Review Window

The Delete Review window opens from either the Manage Reviews Page or the Review Details Page of the Entitlement Reviews interface:

- Delete Entire Review — Deleting a review from the Manage Reviews page will delete all instances of the selected review
- Delete Review Instance — Deleting a review from the Review Details page will delete the selected review instance

Delete Entire Review

Select the desired review on the Manage Reviews page and click **Delete**. The Delete Review window opens to confirm the action.

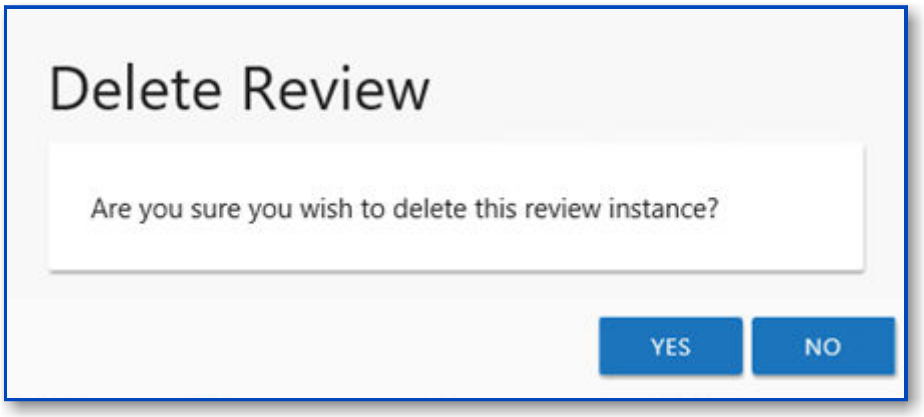


CAUTION: This will delete all instances of the selected review and all historical data associated with it.

Click **Yes** to complete the deletion. Click **No** to cancel it. The Delete Review window closes.

Delete Review Instance

Select the desired review instance from the drop-down menu on the Review Details page and click **Delete**. The Delete Review window opens to confirm the action.



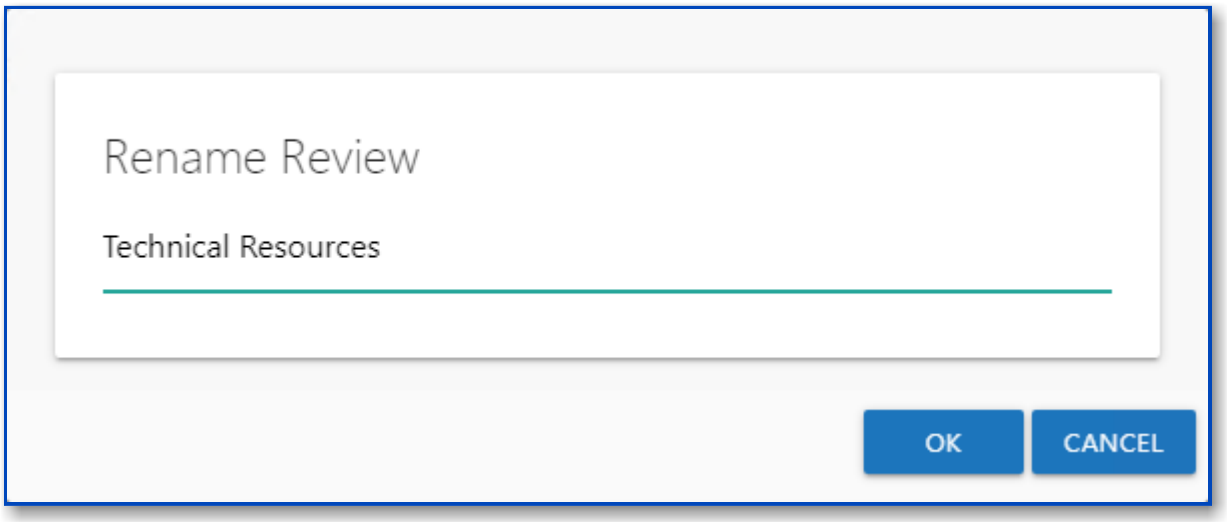
CAUTION: This will delete all historical data associated to the selected review instance.

Click **Yes** to complete the deletion. Click **No** to cancel it. The Delete Review window closes.

Rename Review Window

The Rename Review window opens from the Manage Reviews Page of the Entitlement Reviews interface. Follow the steps to rename a review.

Step 1 – Select the review and click **Rename**. The Rename Review window opens.



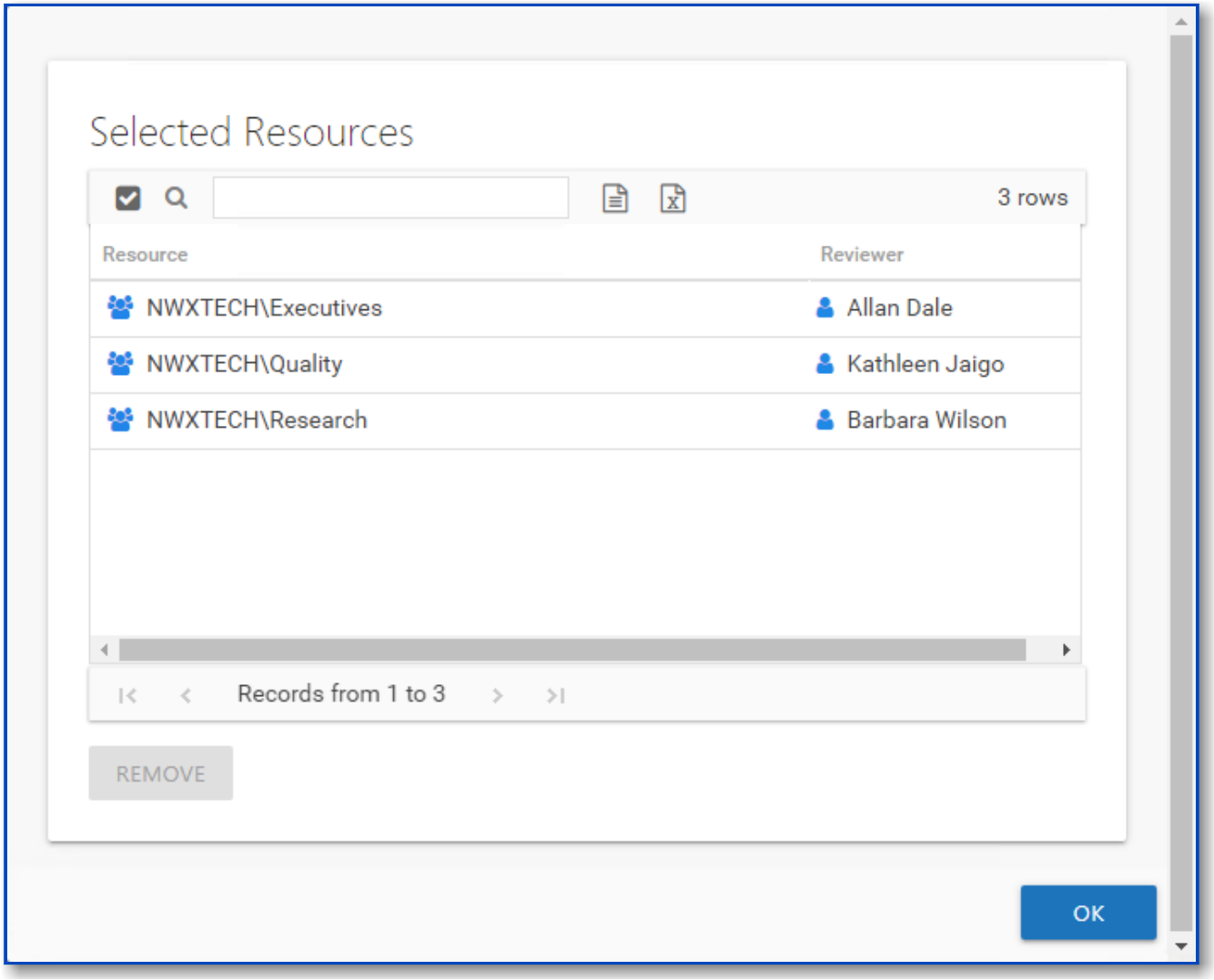
Step 2 – Edit the review name in the textbox.

Step 3 – Click **OK** when finished. The Rename Review window closes.

The renamed review will display in the table on the Manage Reviews page.

Selected Resources Window

The Selected Resources window opens from the **View Selections** button in the Create Review Wizard.



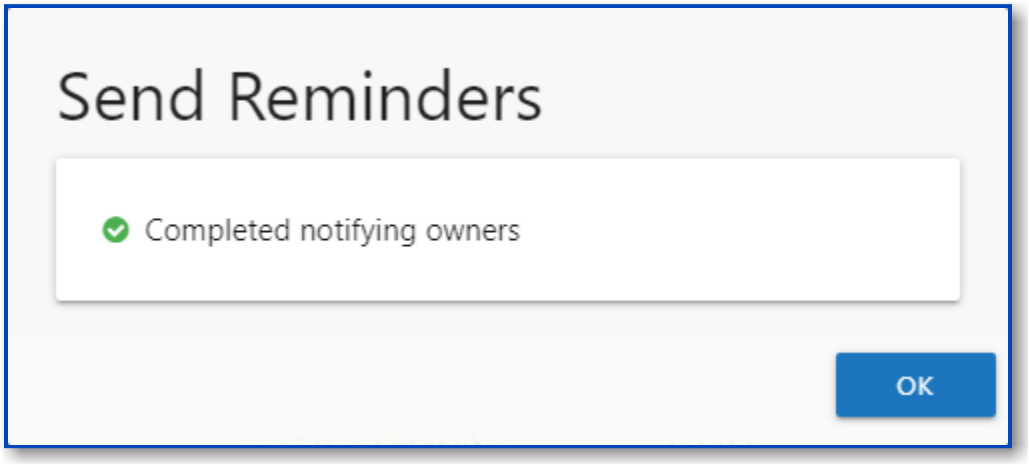
The table displays:

- Resource — The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
- Reviewer — Primary owner assigned to the resource

Use the **Remove** button to remove a resource from this review. Click **OK** to close the window and complete the review creation.

Send Reminders Window

The Send Reminders window opens from the Manage Reviews Page of the Entitlement Reviews interface. Select the desired active review(s) and click **Send Reminders** to send immediate reminder notifications. The Send Reminders window opens to display an action status.

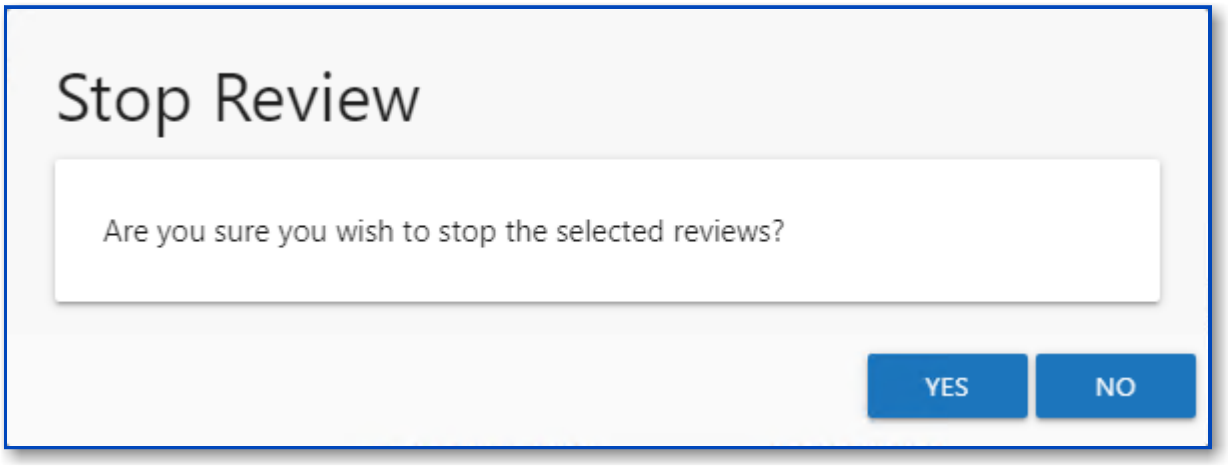


The window displays the action status. When a successful status is indicated, assigned owners were sent a reminder email. Click **OK** to close the Send Reminders window.

Remember, automatic weekly reminders can be configured on the Notifications Page of the Configuration interface.

Stop Review Window

The Stop Review window opens from the Manage Reviews Page of the Entitlement Reviews interface. Select the desired active review(s) and click **Stop**. The Stop Review window opens to confirm the action.

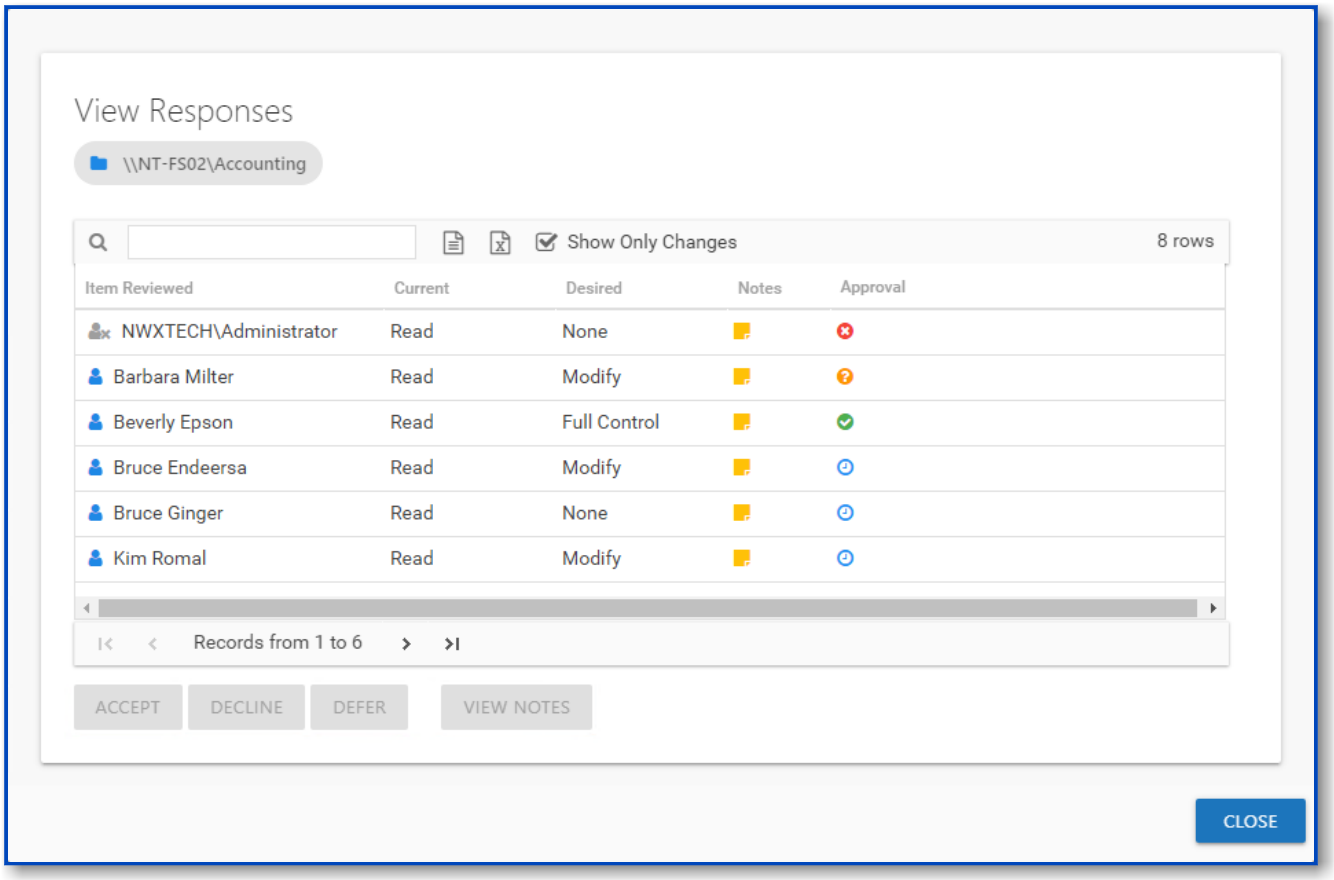


CAUTION: This will prevent owners from completing the review, removing associated resources from their Pending Reviews list.

Click **Yes** to stop the review. Click **No** to cancel the action. The Stop Review window closes.

View Responses Window

The View Responses window opens from the **View Response** button on the Review Details Page of the Entitlement Reviews interface. It displays all owner-recommended changes and notes for the selected resource.



The information displayed in the table includes:

- Item Reviewed — Item upon which changes were suggested by the owner
- Current — Current state of the item at the time of the review
- Desired — Change suggested by the owner
- Notes — Icon indicates a Note has been added. Click on the icon to read the attached note(s).
- Approval — Status of the Review Administrator's approval
    - Clock — Indicates waiting on the Review Administrator to make an official decision
    - Green Checkmark — Indicates the Review Administrator has approved the request
    - Red X — Indicates the Review Administrator has declined the request
    - Yellow Question mark — Indicates the Review Administrator has deferred taking action until a later time

The **Show Only Changes** checkbox is selected by default to show only the items with owner-recommended changes. If deselected, all items included in the review are displayed. When selecting the items with no changes in the grid, the change buttons at the bottom of the page are disabled.

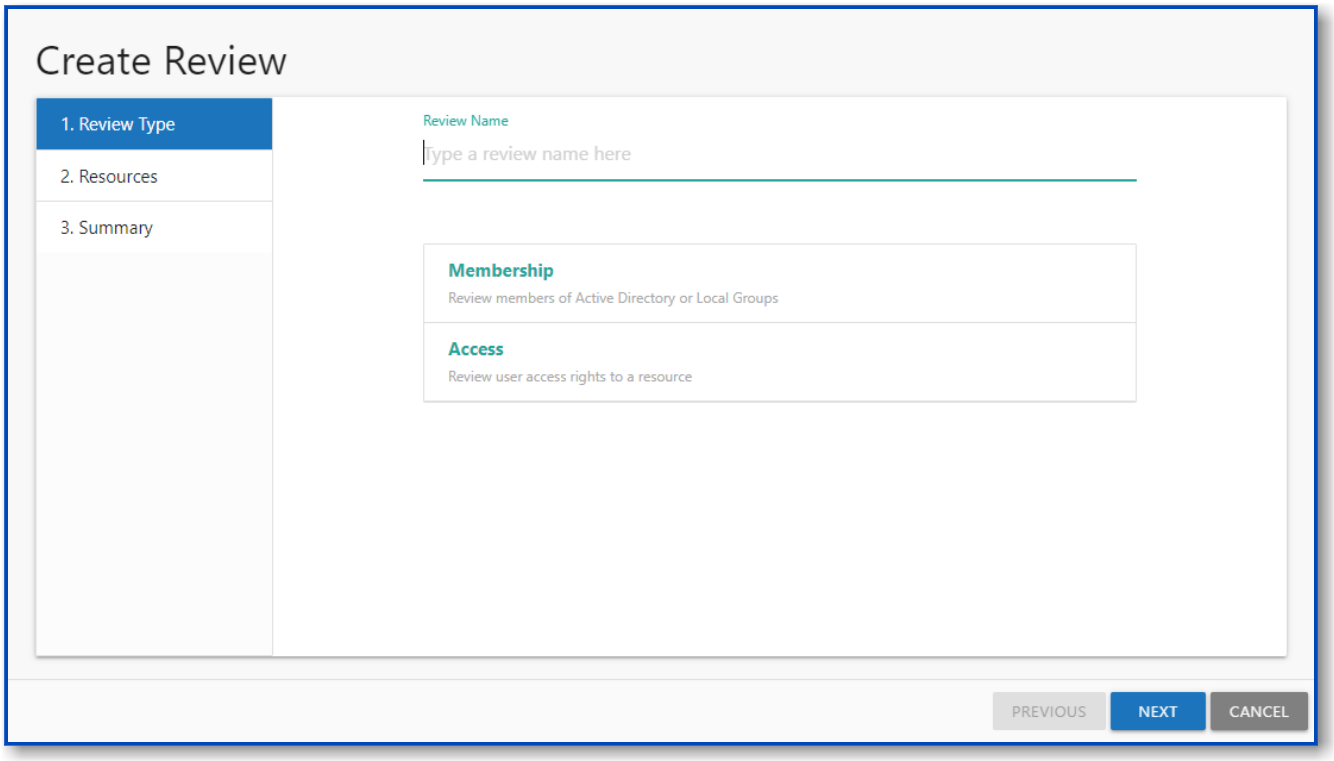
The table data grid functions the same way as other table grids. See the Data Grid Features topic for additional information.

Select an item in the table, and use the action buttons at the bottom to identify the decision:

Button	Description
Accept	Accepts the selected owner-recommended change.
Decline	Declines, or rejects, the owner-recommended change.
Defer	Defers the owner-recommended change to a later time.
View Notes	Opens the Notes window for the selected item.

Create Review Wizard

The Create Review wizard is opened with the **Create** button on the Entitlement Reviews interface. See the Manage Reviews Page topic for additional information.



It contains three pages:

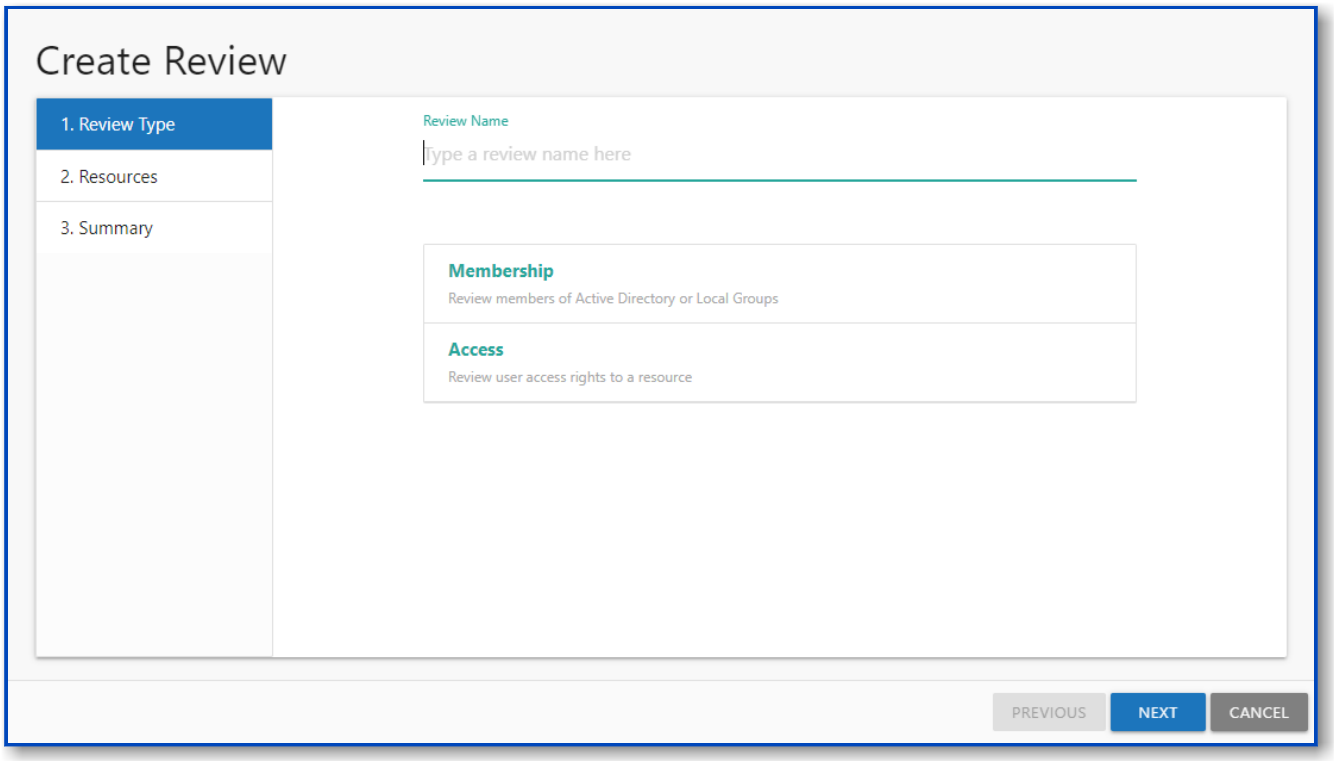
- 1. Review Type
  - Review Name — Visible only to Review Administrators
  - Select the type of review to be created:
    - Membership – Review group membership
    - Access – Review user access rights to resources
- 2. Resources — Select resources to be included in the review
- 3. Summary
  - Preview of the review selections
  - Provides a status of the action being committed. Action includes creating the review and sending notifications to owners.

See the Create a Review topic for additional information.

Create a Review

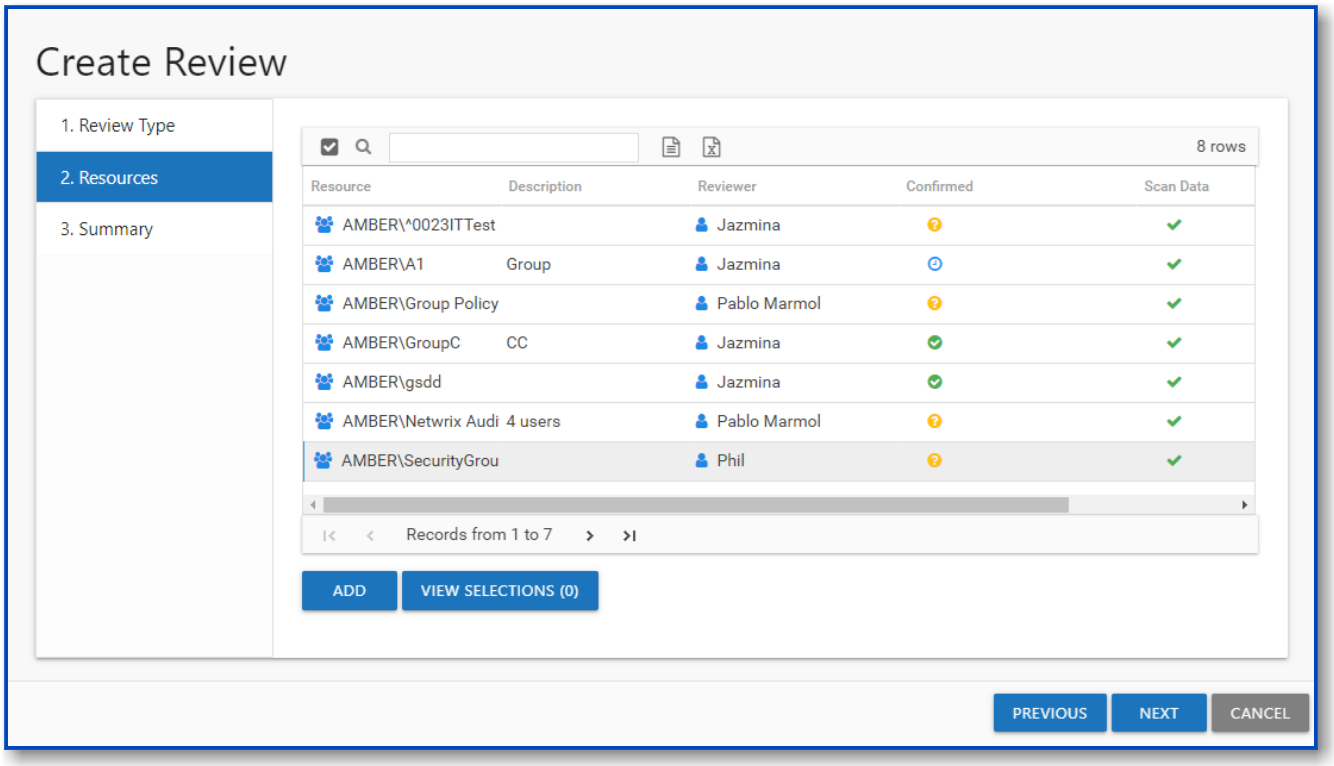
Follow the steps to create a review.

Step 1 – On the Manage Reviews page, click Create. The Create Review wizard opens.



Step 2 – On the Review Type page, provide the following information and click **Next**:

- Review Name — Enter a unique, descriptive name for the review. The review name is only visible to Review Administrators.
- Select Type — Reviews are limited to one type. Select the type of review from the buttons provided:
  - Membership – Review group membership
  - Access – Review user access rights to resources

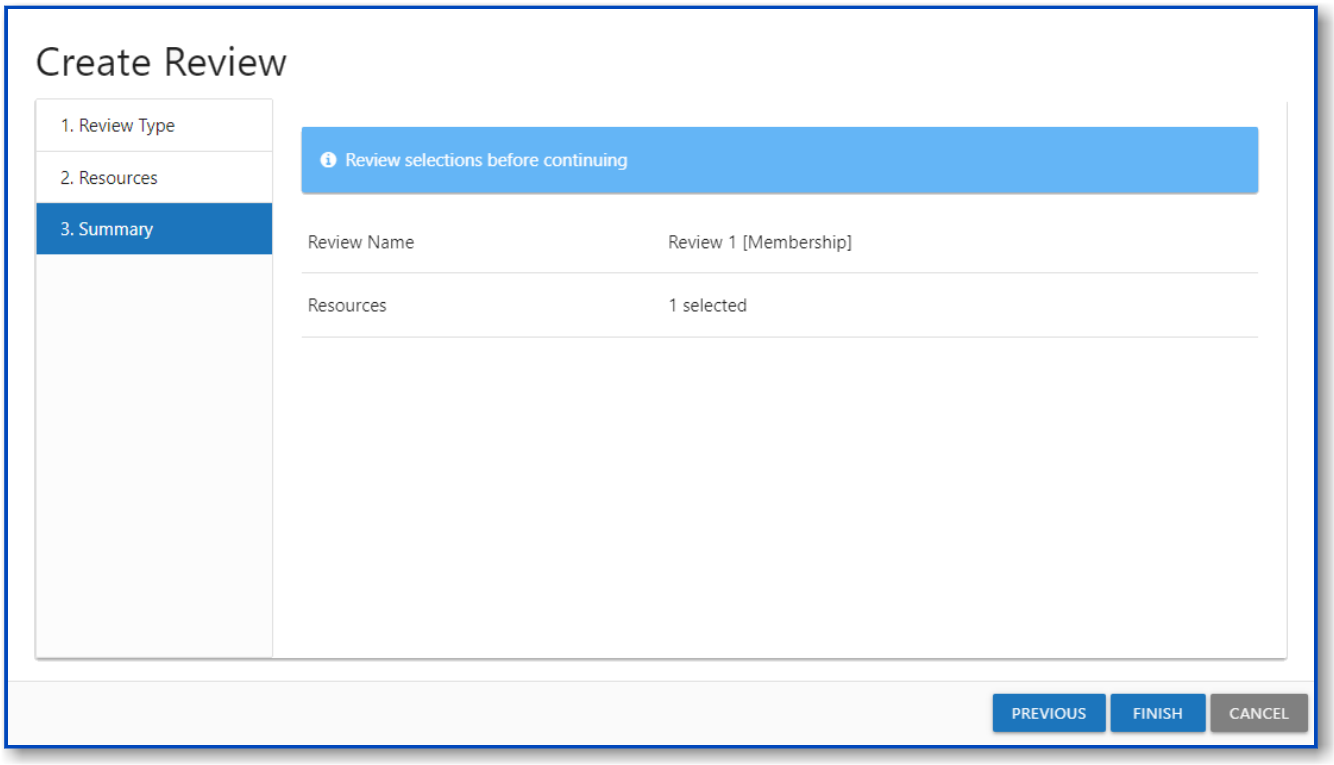


Step 3 – On the Resources page, select the resources to be included in the review. The Search feature is available to filter the list of available resource that match the type of review being created.

- The table displays the following information:
  - Resources — The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
  - Description — Description or explanation of the resource as supplied by either the Ownership Administrator or the assigned owner
  - Reviewer — Primary owner assigned to the resource
  - Confirmed — Indicates whether or not the assigned owner has confirmed ownership of that resource. Tool-tips display when hovering over the icons indicating whether the resource ownership has been confirmed, declined, pending response, or that a confirmation has not been requested.
  - Scan Data — A checkmark indicates the resource has been scanned. Only resources with scan data can be included in a review.
- Select the desired resource(s) and click **Add**. The **View Selections** button indicates how many resources have been selected. Click the button to open the Selected Resources

window, where you can view and modify the selections. See the Selected Resources Window topic for additional information.

- Once the desired resources have been selected, click **Next**.



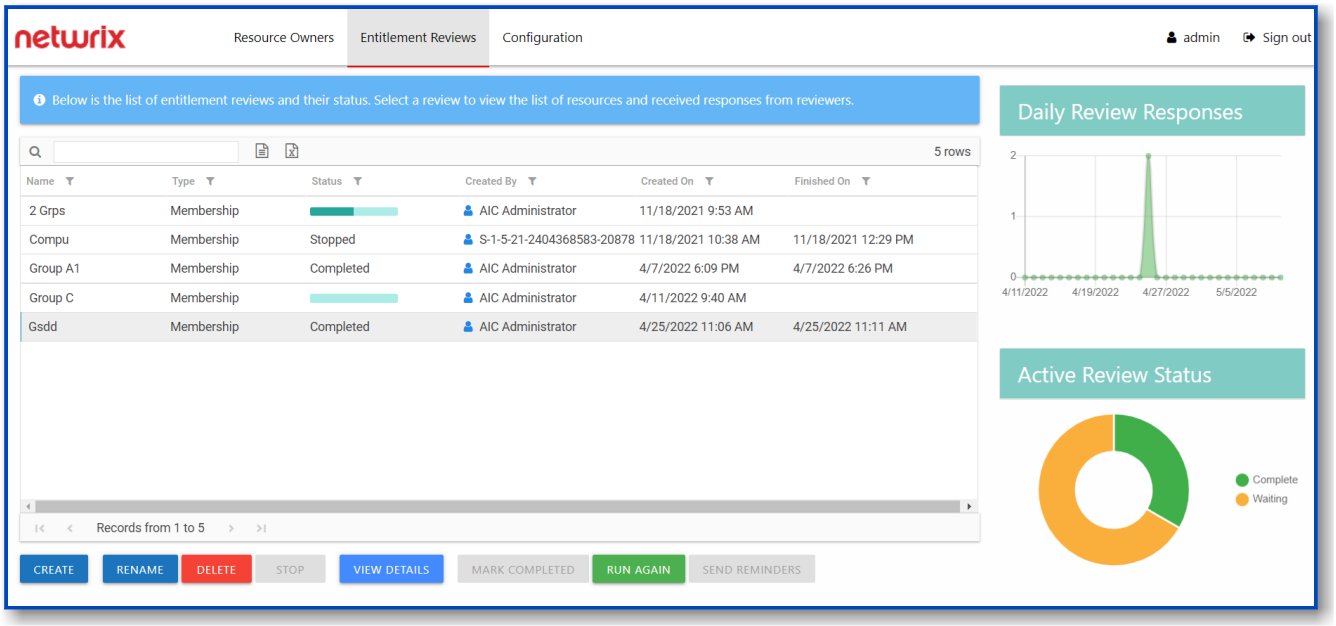
Step 4 – On the Summary page, review the settings and click Finish. The Access Reviews begins to create the review. Action status displays on the page. When the update has completed (100%), click Close. The Create Review wizard closes.

The new review displays in the table on the Manage Reviews page. An email was sent to the primary owner assigned to the resource(s) in this review. By default, the application is configured to send notifications only to the primary owner. However, this can be customized on the Configuration > Notifications page to send notifications to all assigned owners. See the Notifications Page topic for additional information.

Review Instances

After a review has been completed, it can be run again, which creates multiple instances of the review. Each instance is identified by date timestamps indicating its start and end times.

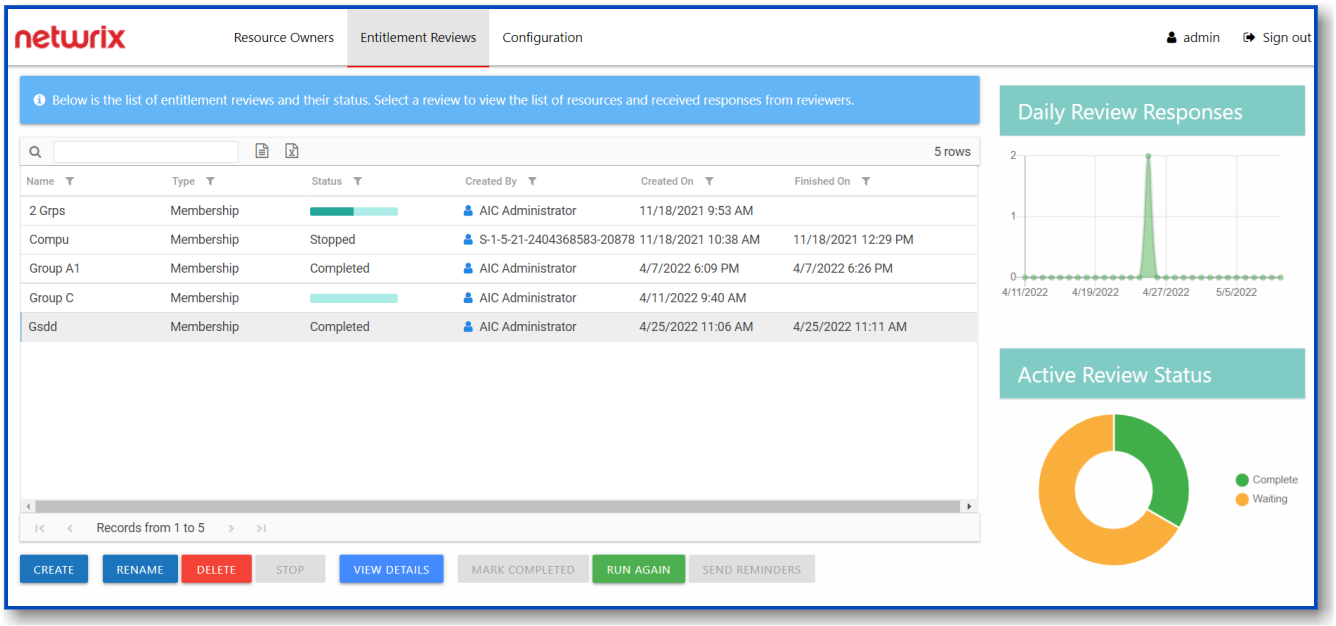
RECOMMENDED: Prior to running another review instance, ensure the most up to date information is available to owners for review.



On the Manage Reviews page in the Entitlement Reviews interface, a review with a Completed status can be started again. Select the review and click **Run Again**. The Create Review wizard opens without the Review Type page. The review can be run as-is by navigating through the wizard with the **Next** buttons, or you can modify as desired. Completing the wizard process restarts the review. See the Create Review Wizard topic for additional information.

Approval Process

After all owners assigned to a specific review have submitted their review, its status on the Manage Reviews page of the Entitlement Reviews interface changes to Responses awaiting review.



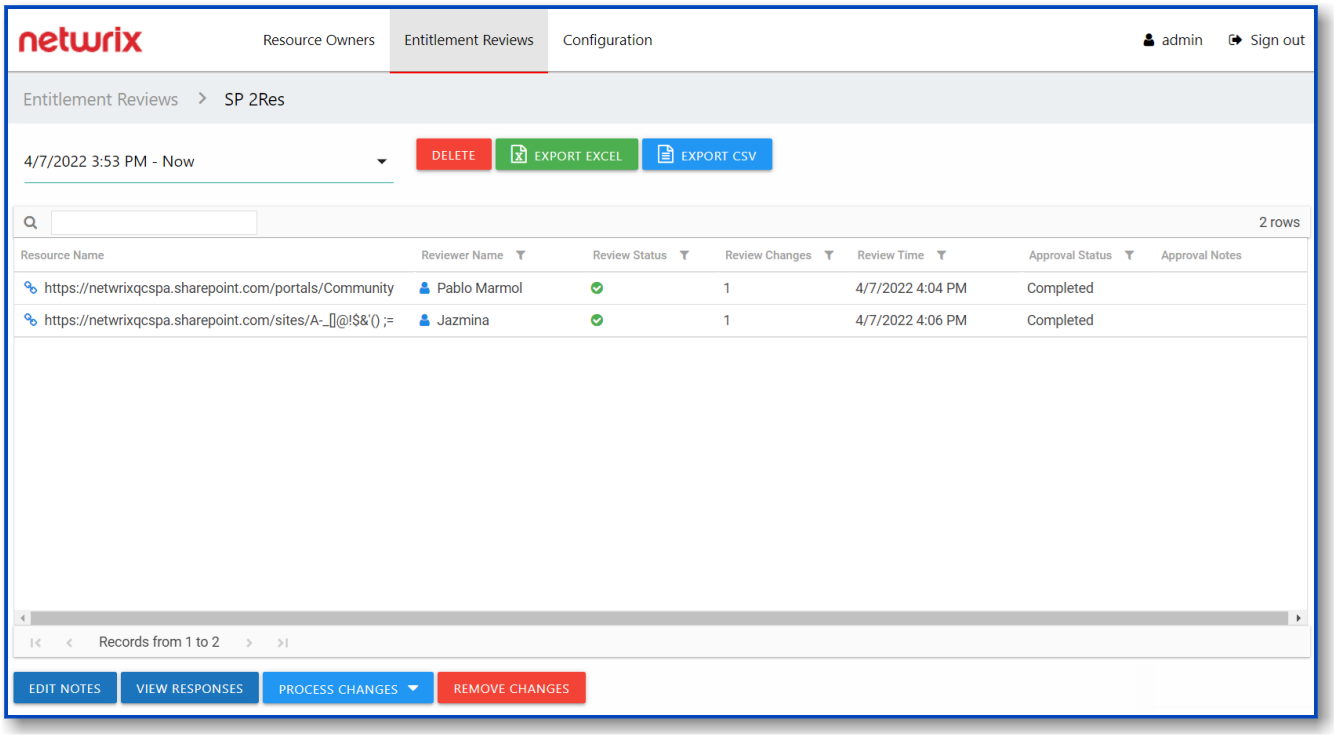
In the approval process, the Review Administrator looks at the owner-recommended changes and chooses to approve, deny, or defer the changes.

See the Process Owner Responses topic for instructions on how to perform a granular review of owner-recommended changes. See the Batch Processing topic for instructions on how to approve, decline, or defer all owner-recommended changes for a review.

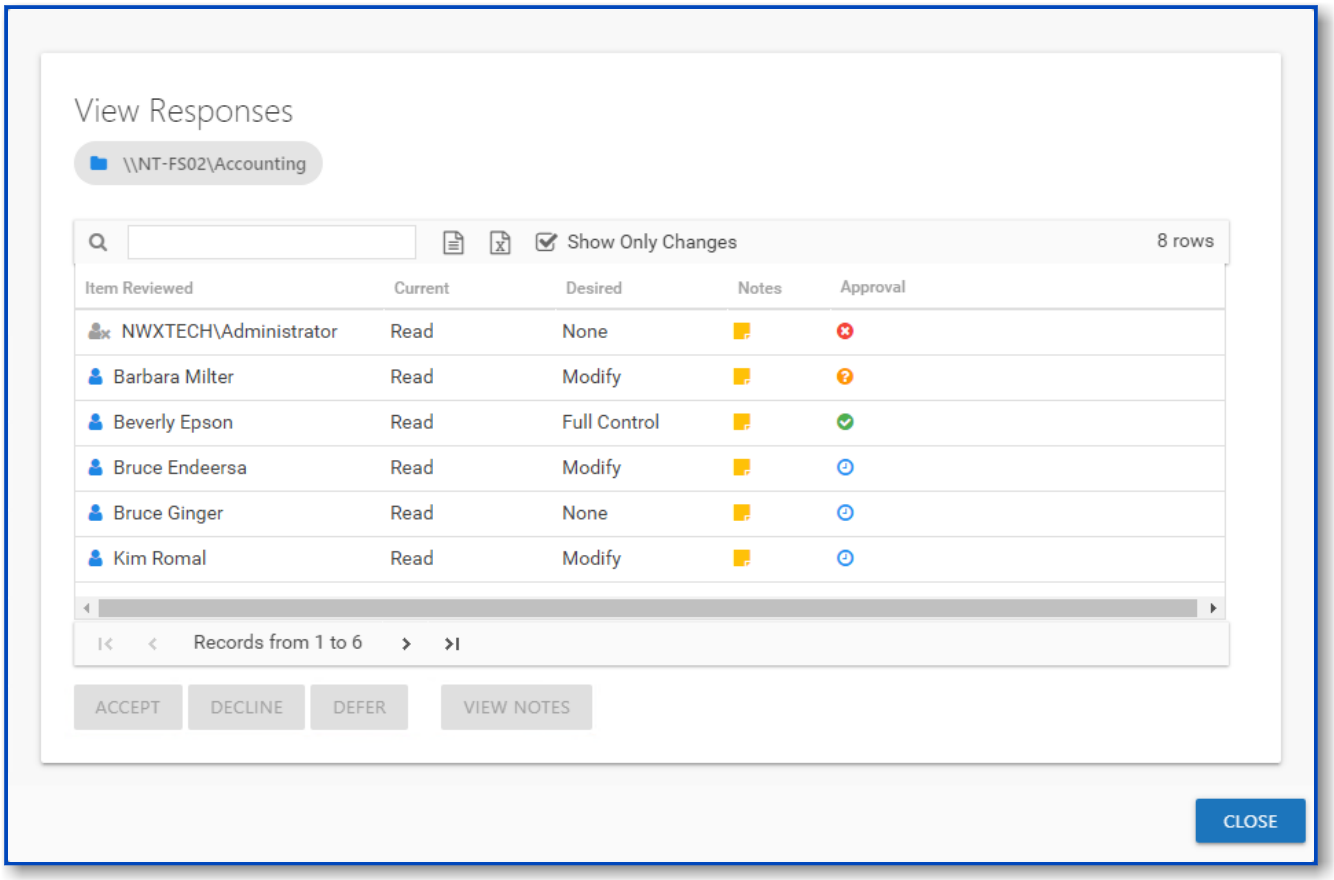
Process Owner Responses

Follow the steps to perform a granular review of a resource owner's recommended changes.

Step 1 – On the Manage Reviews page, select a review and click **View Details**. The Review Details page opens.



Step 2 – Select a resource in the list and click **View Responses**. The View Responses window opens.



Step 3 – By default, the table displays only the recommended changes. Select an item and click the desired action button: Accept, Decline, or Defer. The Approval column icon updates. See the View Responses Window topic for additional information.

Step 4 – Repeat Step 3 until all changes have been processed. Then click **Close**. The View Responses window closes.

Step 5 – Repeat Steps 2-4 for each resource included in the review.

Step 6 – Remediation of the accepted changes must be done manually. Accepted changes must be implemented outside of the application by your IT department. Use the **Export Excel** or **Export CSV** buttons to generate and download an export of accepted changes.

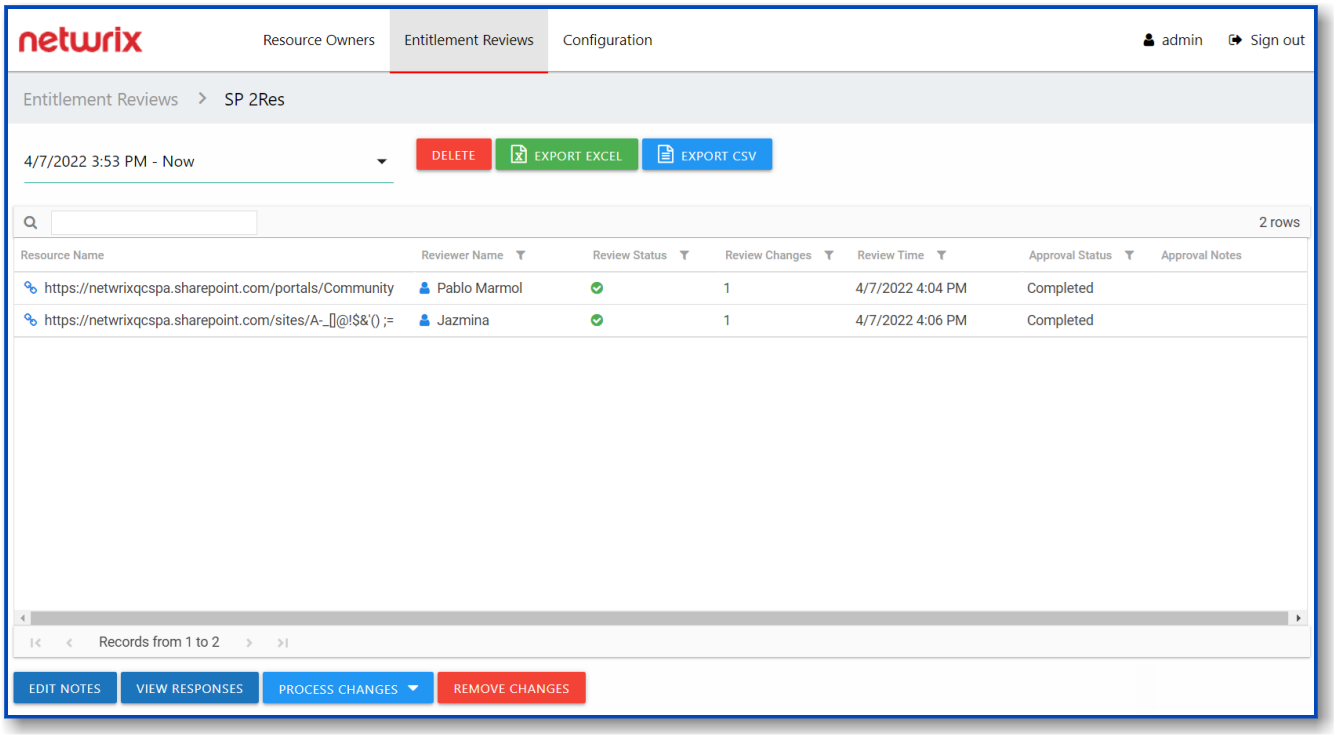
Step 7 – When remediation is complete, return to the Mange Reviews page (click on the breadcrumb). Select the review in the list and click **Mark Completed**.

The review remains marked as Completed until the next instance is started.

Batch Processing

Follow the steps to perform a batch processing of a resource owner's recommended changes.

Step 1 – On the Manage Reviews page, select a review and click **View Details**. The Review Details page opens. .



Step 2 – Select a resource in the list and open the **Process Changes** drop-down menu.

Step 3 – Select the desired action for all recommended changes: Accept, Decline, or Defer.

Remember, all recommended changes for the selected resource will be processed with the same resolution.

Step 4 – Repeat Steps 2-3 for each resource included in the review.

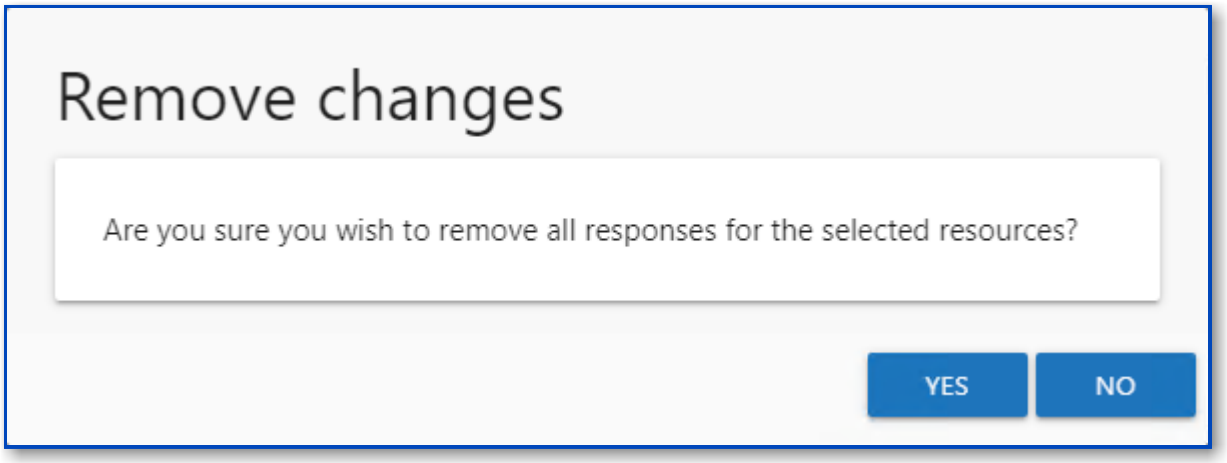
Step 5 – Remediation of the accepted changes must be done manually. Accepted changes must be implemented outside of the application by your IT department. Use the **Export Excel** or **Export CSV** buttons to generate and download an export of accepted changes.

Step 6 – When remediation is complete, return to the Mange Reviews page (click on the breadcrumb). Select the review in the list and click **Mark Completed**.

The review remains marked as Completed until the next instance is started.

Remove Changes Window

Select the desired resource on a Review Details page and click **Remove Changes**. The Remove changes window opens to confirm the action.



CAUTION: This will clear all owner-recommended changes and notes for the resource. The owner will be required to complete the review again.

Click Yes to clear owner-recommended changes. Click No to cancel it. The Remove changes window closes.

Owners & Access Reviews

This topic and its subtopics are written for users who have been assigned resource ownership.

When your organization performs an access review on a resource for which you are the assigned owner, it means you, the business user or data custodian, need to attest to the access and privileges users have to your resource.

NOTE: For the Netwrix Auditor Access Reviews application, a “resource” refers to the file system shared folders, SharePoint Online site collections, and Active Directory (AD) groups.

Your organization's Ownership Administrator and/or Review Administrator will let you know what URL to use for logging in as well as what credentials to use. The URL will require you to be connected to your organization's network. Upon login, you will be directed to the My Reviews page where you can view pending and historical reviews for your resources.

You may receive email notifications requesting ownership confirmation from your organization's Ownership Administrators. You will receive email notifications when you have a pending access review to perform.

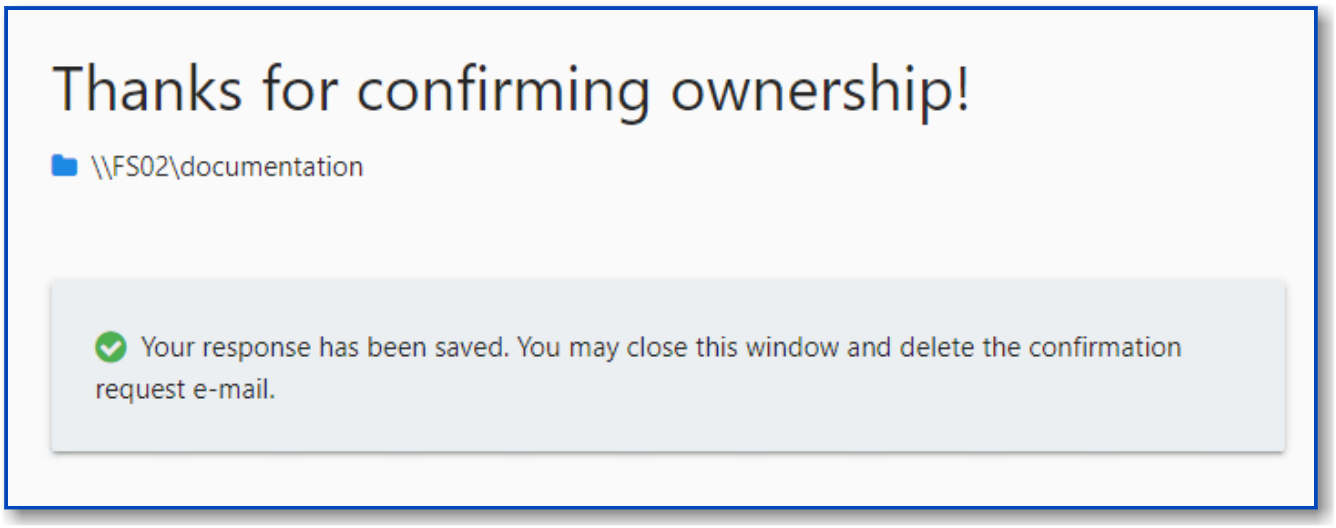
Ownership Confirmation Request Email

The Ownership Administrator may request ownership confirmation for a resource being managed through the Access Reviews application. As an assigned owner, you will receive the following email.

The Ownership Confirmation Request email provides buttons for confirming (Yes) or declining (No) ownership of the listed resource. You will be asked to authenticate for your response to be processed. The application will launch in your default browser. Enter your domain credentials to complete the process. One of two messages will appear according to if you confirmed or declined.

Confirmed Ownership Message

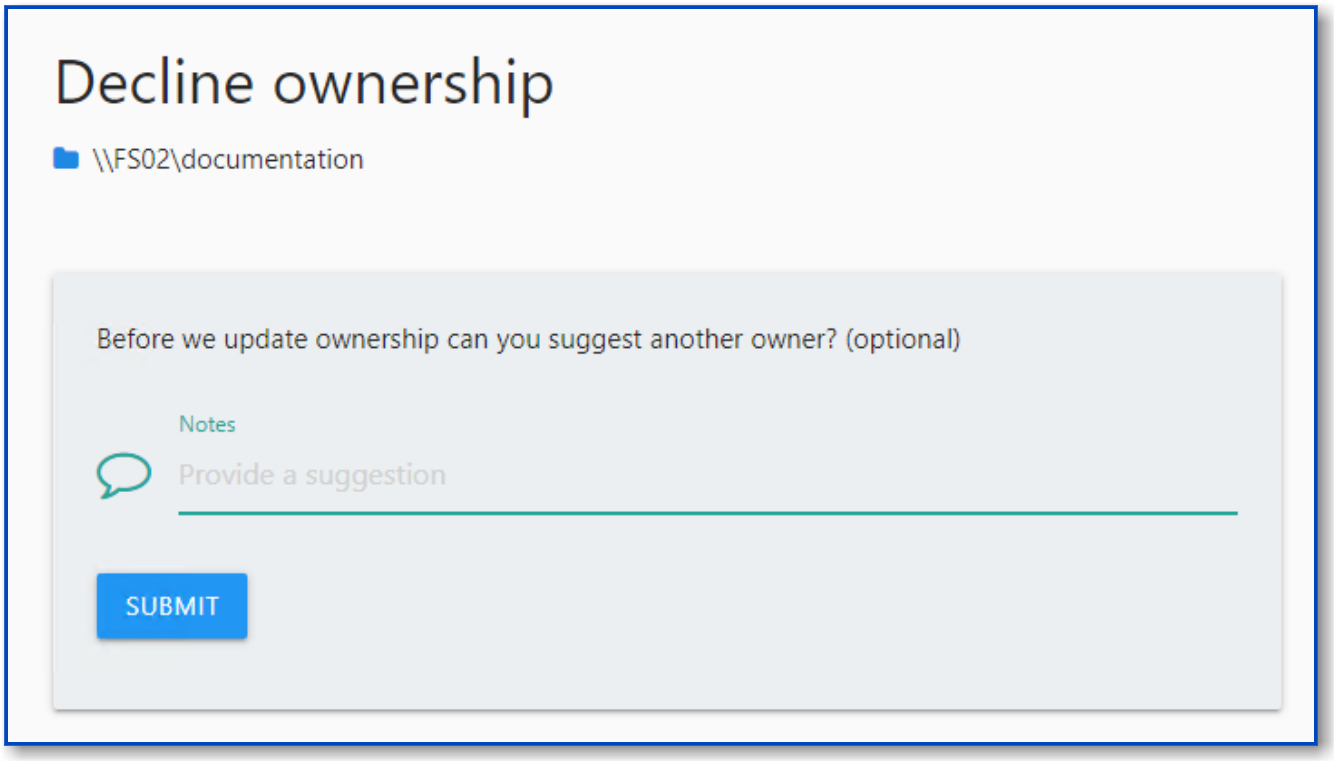
If you have accepted ownership for the assigned resource, the browser will display the following message after authentication:



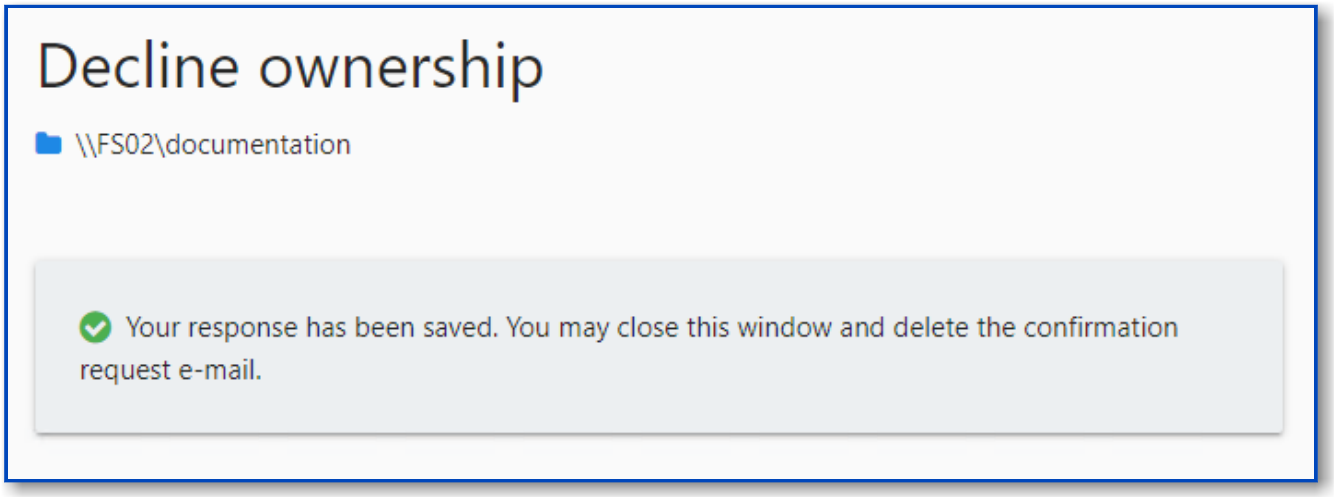
"Your response has been saved. You may close this window and delete the confirmation request e-mail."

Declined Ownership Message

If you have declined ownership for the assigned resource, the browser will display the following message after authentication:



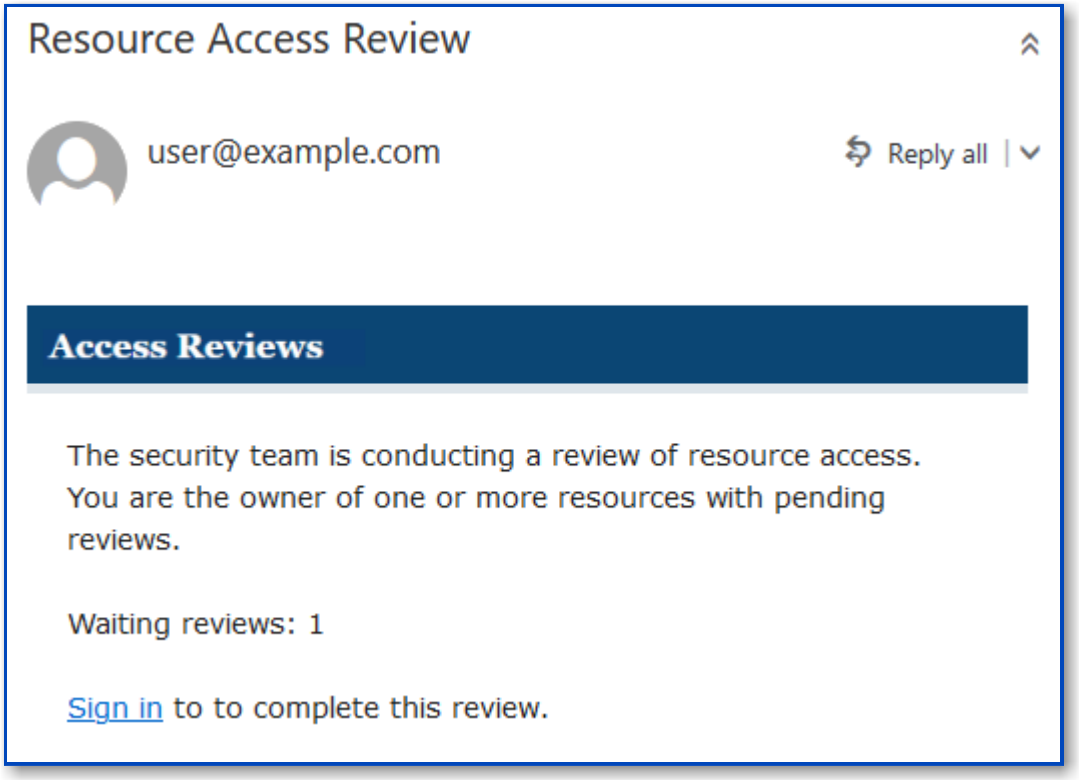
"Before we update ownership can you suggest another owner?" Enter possible owners in the textbox. Click **Submit** to complete the process.



"Your response has been saved. You may close this window and delete the confirmation request e-mail."

Pending Reviews

When your organization performs a review on a resource for which you are the assigned owner, it means you, the business user or data custodian, need to attest to the access and privileges users have to your resource. When the Review Administrator creates a new review or starts a new instance of an existing review, you receive an email notification that includes a link to the your pending reviews.



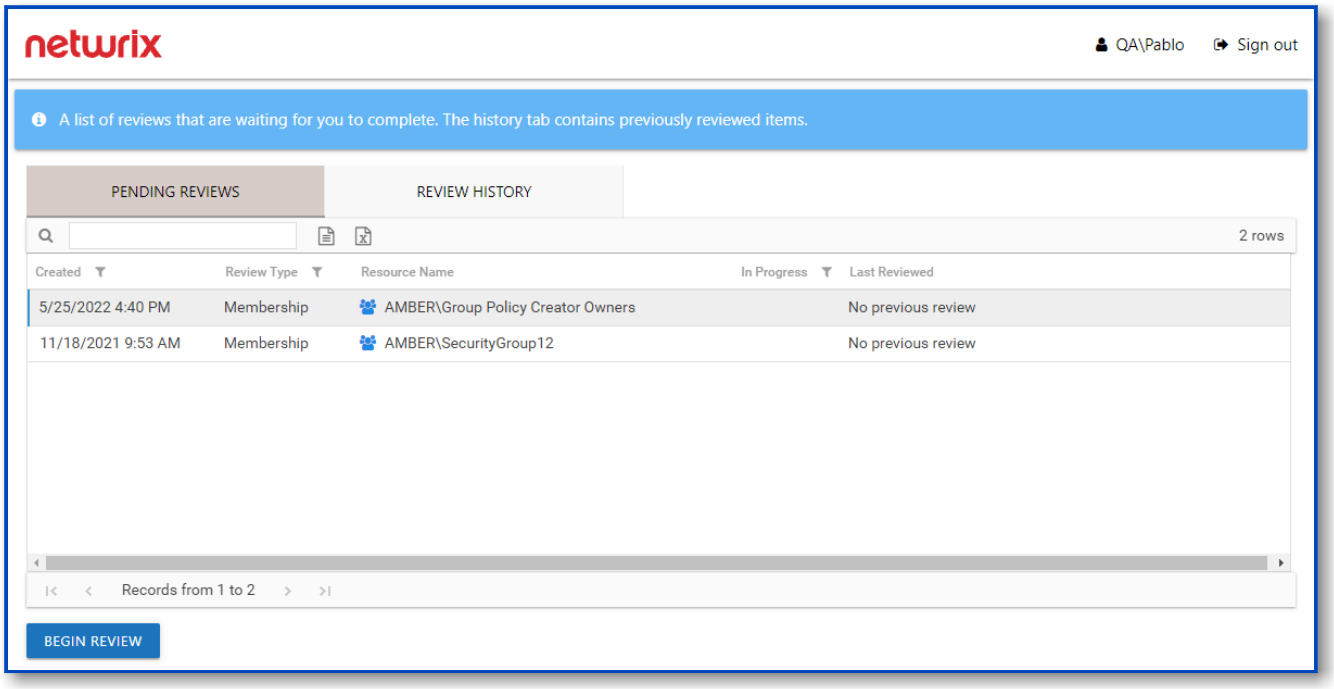
Use the **Sign in** link at the bottom to open the My Reviews interface in the Access Reviews Console.

Remember, your company domain credentials are used to log in.

The My Reviews interface has two pages: Pending Reviews and Review History. See the Review History Page topic for additional information.

Pending Reviews Page

The Pending Reviews page lists all of your resources included in pending reviews.



The information displayed in the table includes:

- Created — Date timestamp for when the review was creation. If it has been run multiple times, this is the date timestamp of the last instance.
- Review Type – Type of review:
  - Access – Review user access rights to resources
  - Membership – Review group membership
- Resource Name — The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
- In Progress — Displays a clock icon for an in-progress review
- Last Reviewed — Date timestamp when the last review took place for the resource.

The table data grid functions the same way as other table grids. See the Data Grid Features topic for additional information.

Performing a review means you are evaluating the resources. You can leave the resource unchanged or make recommendations for changes. Consider the following examples:

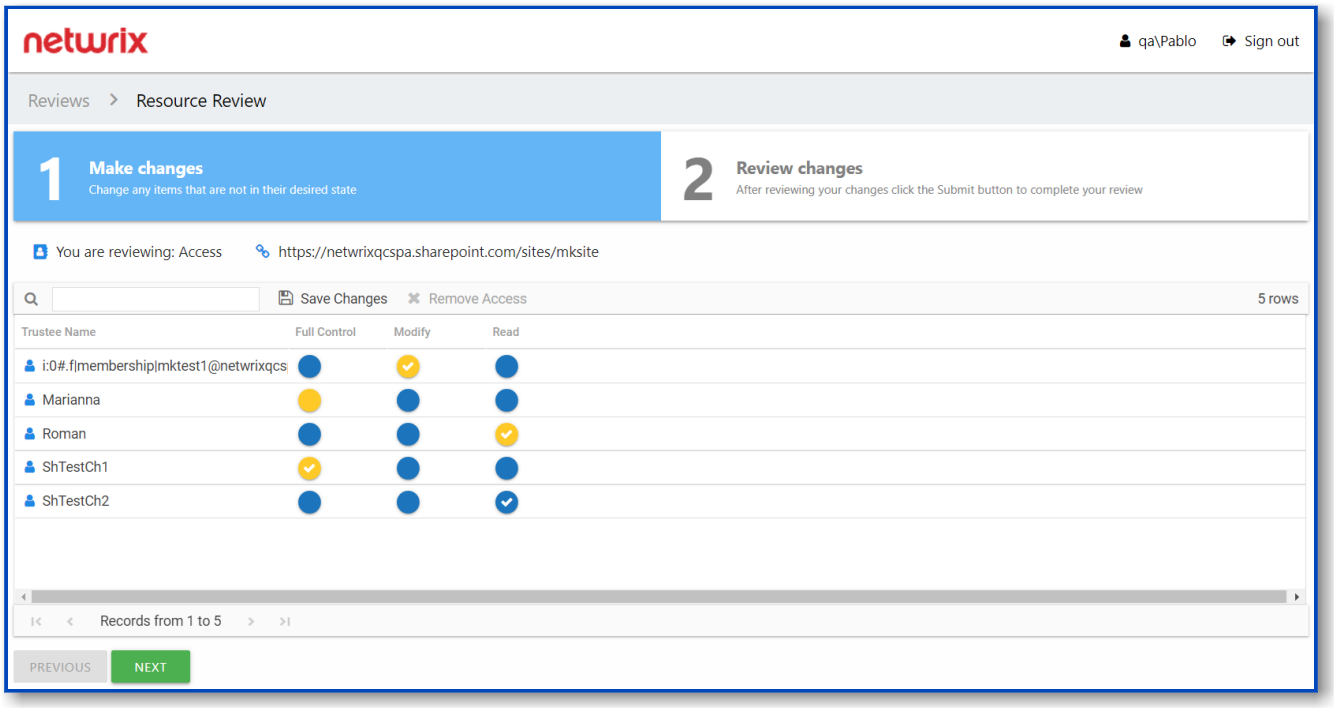
- In an Access review, you can recommend changes to the type of access granted to the resource.

- In a Membership Review, you can recommend removing group membership from specific users.

Remember, any proposed changes are not committed until the Review Administrator approves the recommendation and processes those changes.

Resource Review Page

The Begin Review button opens the Resource Review page to start the review.



The Resource Review page varies based on the type of review; however, there are several common features:

- Tabs — This page has two tabs:
  - 1 Make changes — Displays current access for the resource.
  - 2 Review changes — Displays changes you recommend making for your review prior to submission
- You are reviewing — Indicates the type of review, the resource being reviewed, and the date timestamp for when the review instance was started

- Search — Filters the table for matches to the typed value
- Save Changes — Saves all recommended changes, enabling you to leave the review in progress and return at a later time to complete it. It opens the Saving review window, which displays a status for the action.
- Remove Access — On the 1 Make changes tab, removes access from the selected trustee(s). Ctrl-click can be used for multi-select. Current access blue icon with a checkmark will turn to an empty yellow icon.
- Only show changes since last review — Scopes the table to only display those items that have been modified since the last review instance
- Previous / Next buttons — Moves between the two tabs
- Submit button — On the 2 Review changes tab, the **Next** button becomes a **Submit** button. This submits your review to the Review Administrator.

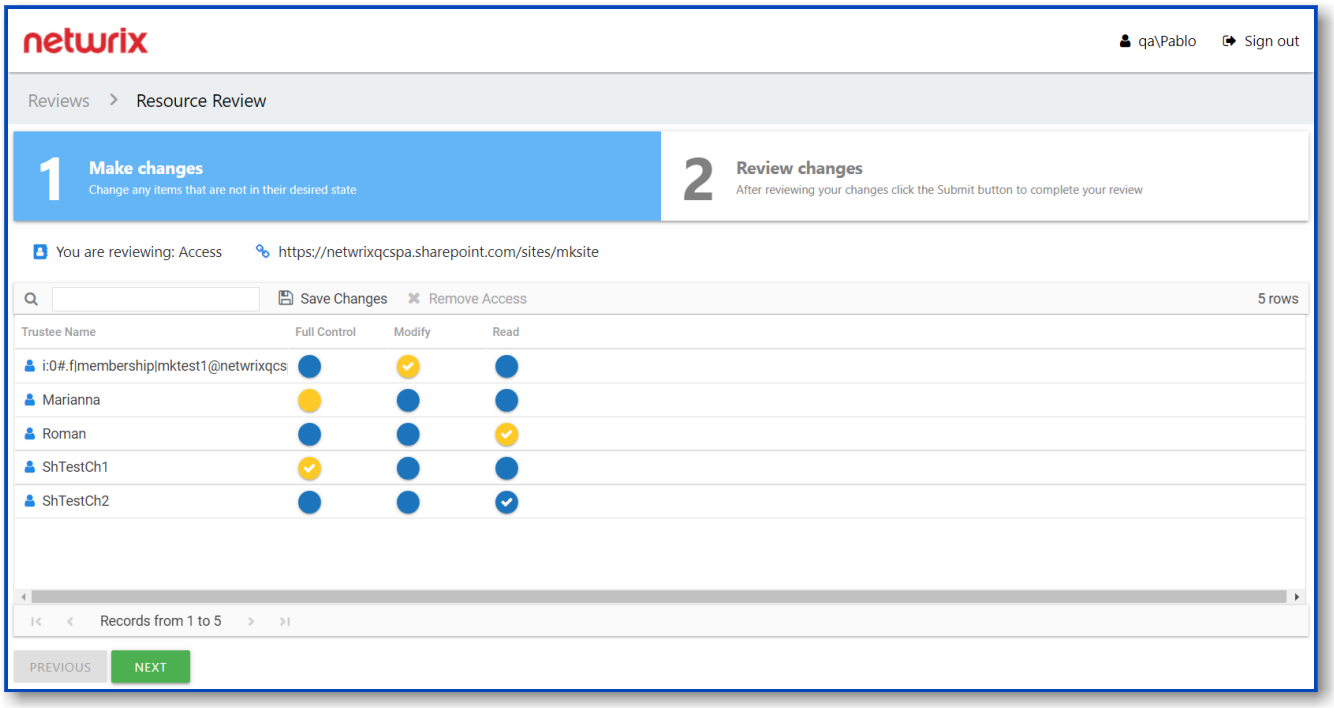
The content within the table varies, and additional options may appear depending on the type of review being conducted. See the following sections for step by step instructions:

- Perform an Access Review
- Perform a Membership Review

Perform an Access Review

An Access review can be conducted for various types of data repository resources. Follow the steps to perform an Access review.

Step 1 – On the Pending Reviews page, select the resource with a pending Access review and click **Begin Review**. The Resource Review page opens to the 1 Make changes tab.



The table displays access information for the resource being reviewed:

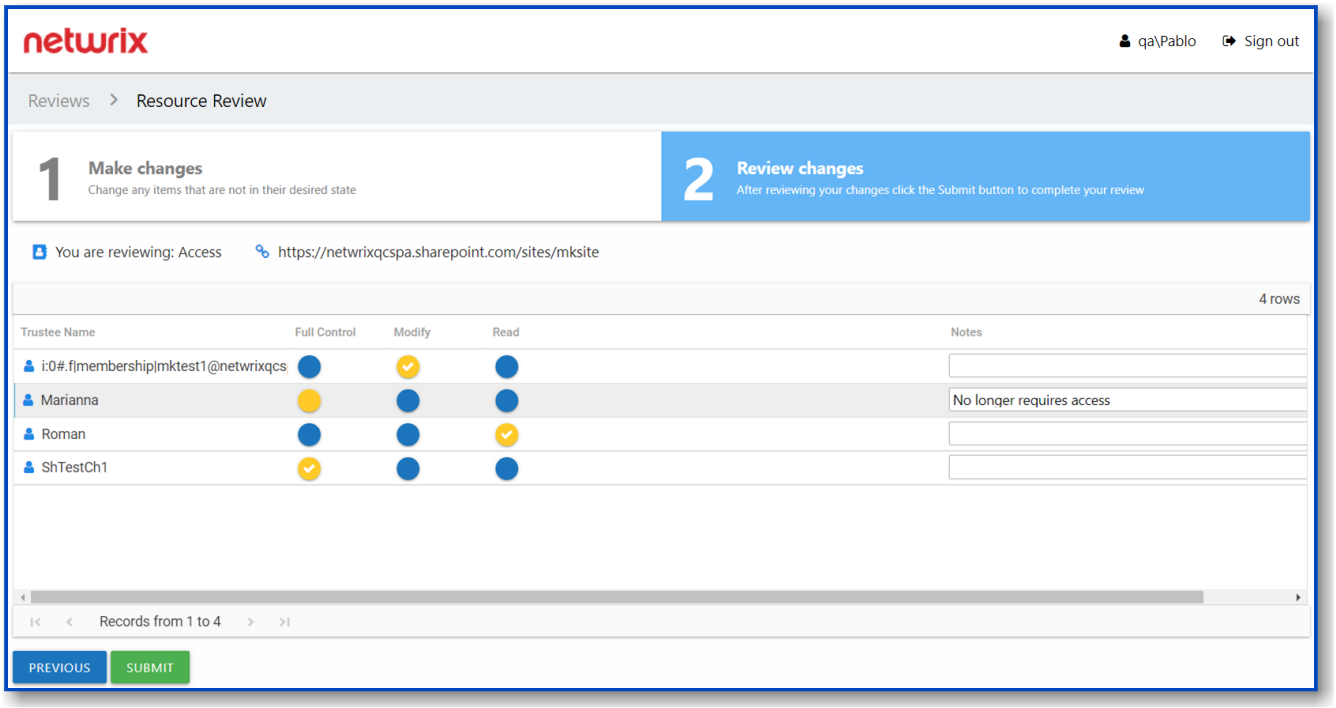
- Trustee Name — Name of the trustee with access to this resource. If the trustee is a group, click the hyperlink to open the Group Membership window. See the Group Membership Window topic for additional information.
- Access Level (Full Control, Modify, and Read) columns — Blue checkmark icon indicates current access level

Step 2 – Recommend access changes for a trustee by clicking the icon for the desired access level (Full Control, Modify, or Read columns). A yellow checkmark icon indicates the new level of access you are recommending.

Step 3 – Recommend removing access by selecting one or more trustees and clicking the **Remove Access** button or by clicking on a checkmark icon. A blank yellow icon indicates you are recommending all access be removed; it appears in the column for the current level of access.

Remember, at any time you can save your recommendations and exit the review. It will remain pending until you submit all recommendations for this resource.

Step 4 – When the recommended changes are set as desired, click **Next**. The 2 Review changes tab opens in the Resource Review page.



Step 5 – This tab displays a filtered table of trustees with recommended changes. Confirm your recommendations and optionally add notes to the Review Administrator. Owners are encouraged to leave notes explaining why the change is recommended.

NOTE: To make changes to your recommendations, you must return to the first tab. Click **Previous**.

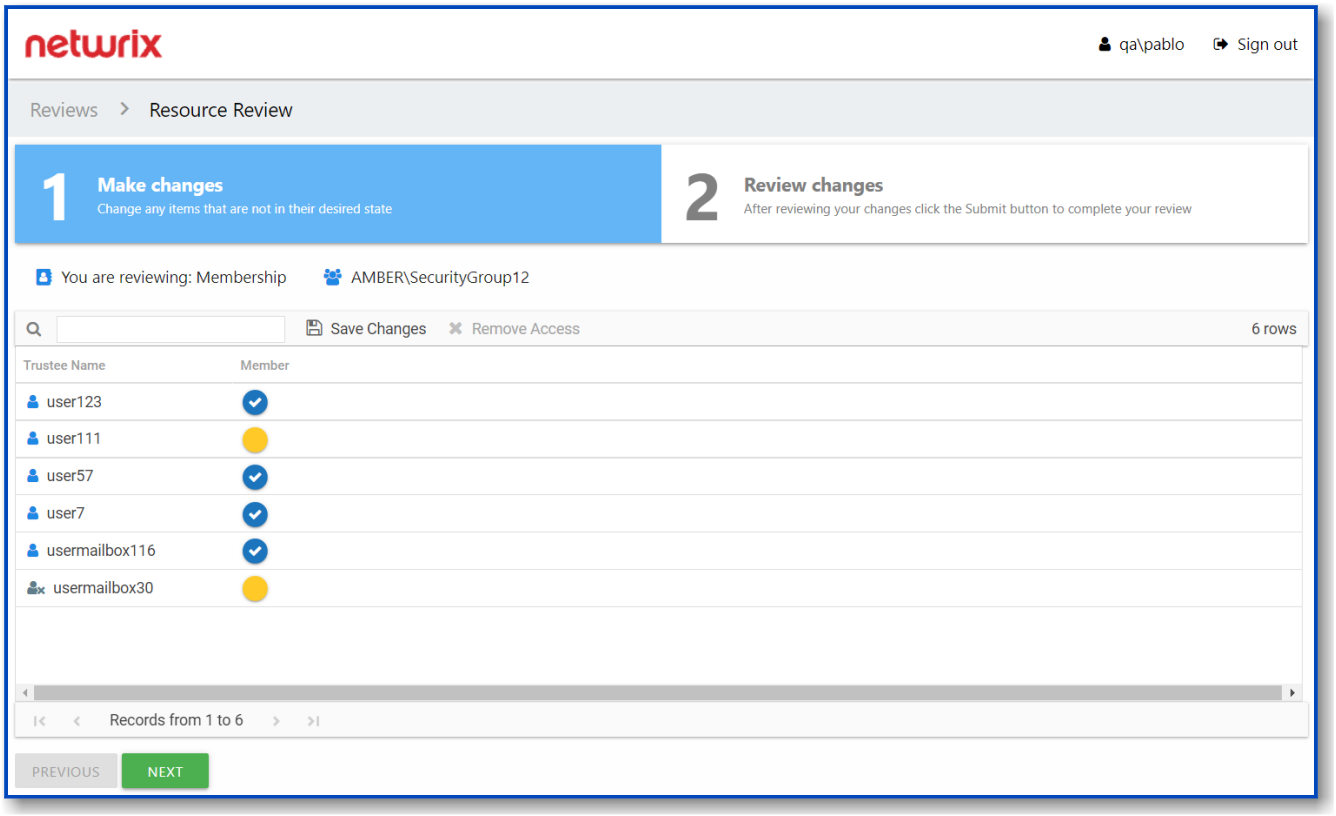
Step 6 – When all recommendations are confirmed and the desire notes added, click **Submit**. A message displays stating that the review is complete. Click **OK** to close the message window.

The review for this resource is now complete. You will be redirected to the Pending Reviews page. Your recommended changes have been sent to the Review Administrator for approval and processing.

Perform a Membership Review

A Membership review is an evaluation of group membership. Follow the steps to perform a Membership review.

Step 1 – On the Pending Reviews page, select the resource with a pending Membership review and click **Begin Review**. The Resource Review page opens to the 1 Make changes tab.



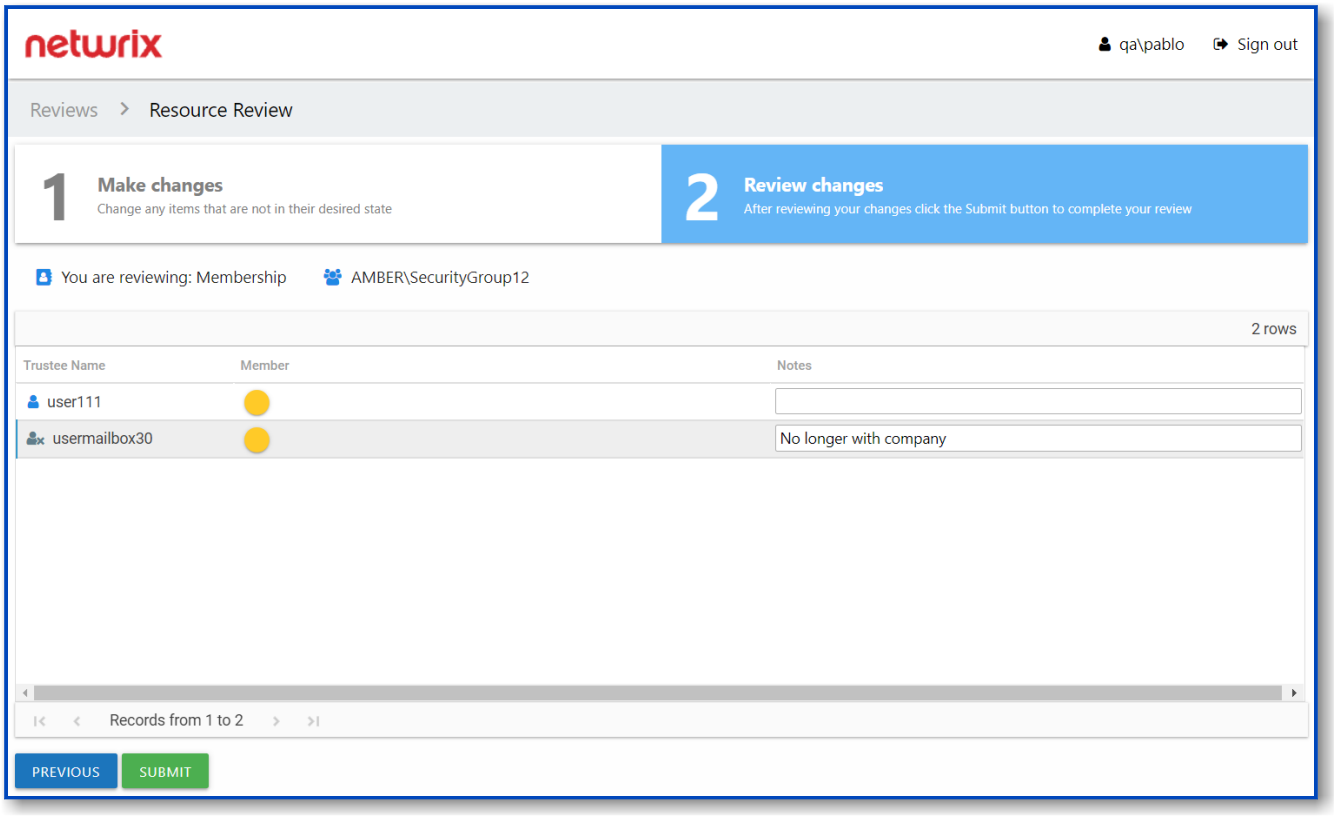
The table displays membership information for the group being reviewed:

- Trustee Name — Name of the trustee with group membership. If the trustee is a group, click the hyperlink to open the Group Membership window. See the Group Membership Window topic for additional information.
- Member — Blue checkmark icon indicates current membership

Step 2 – Recommend removing membership by selecting one or more trustees and clicking the **Remove Access** button or by clicking on a checkmark icon. A blank yellow icon indicates you are recommending the trustee be removed from the group.

Remember, at any time you can save your recommendations and exit the review. It will remain pending until you submit all recommendations for this resource.

Step 3 – When the recommended changes are set as desired, click **Next**. The 2 Review changes tab opens in the Resource Review page.



Step 4 – This tab displays a filtered table of trustees with recommended changes. Confirm your recommendations and optionally add notes to the Review Administrator. Owners are encouraged to leave notes explaining why the change is recommended.

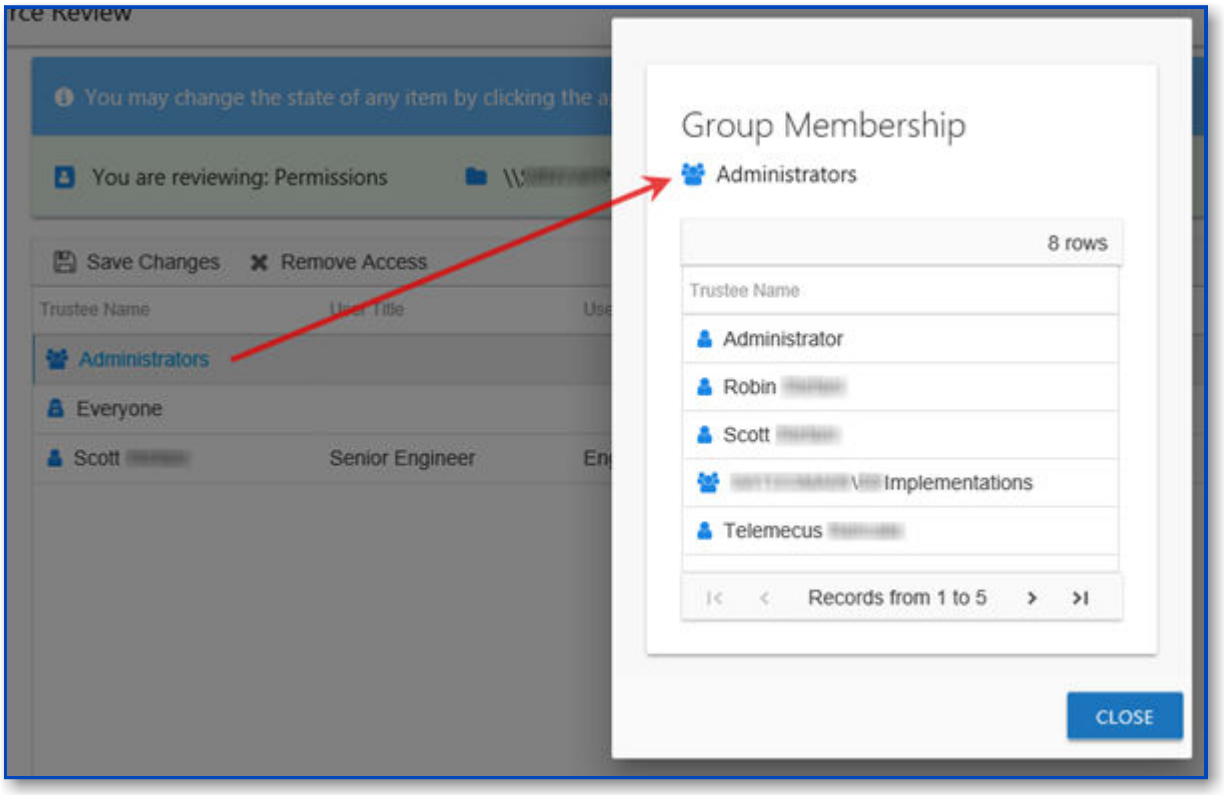
NOTE: To make changes to your recommendations, you must return to the first tab. Click **Previous**.

Step 5 – When all recommendations are confirmed and the desire notes added, click **Submit**. A message displays stating that the review is complete. Click **OK** to close the message window.

The review for this resource is now complete. You will be redirected to the Pending Reviews page. Your recommended changes have been sent to the Review Administrator for approval and processing.

Group Membership Window

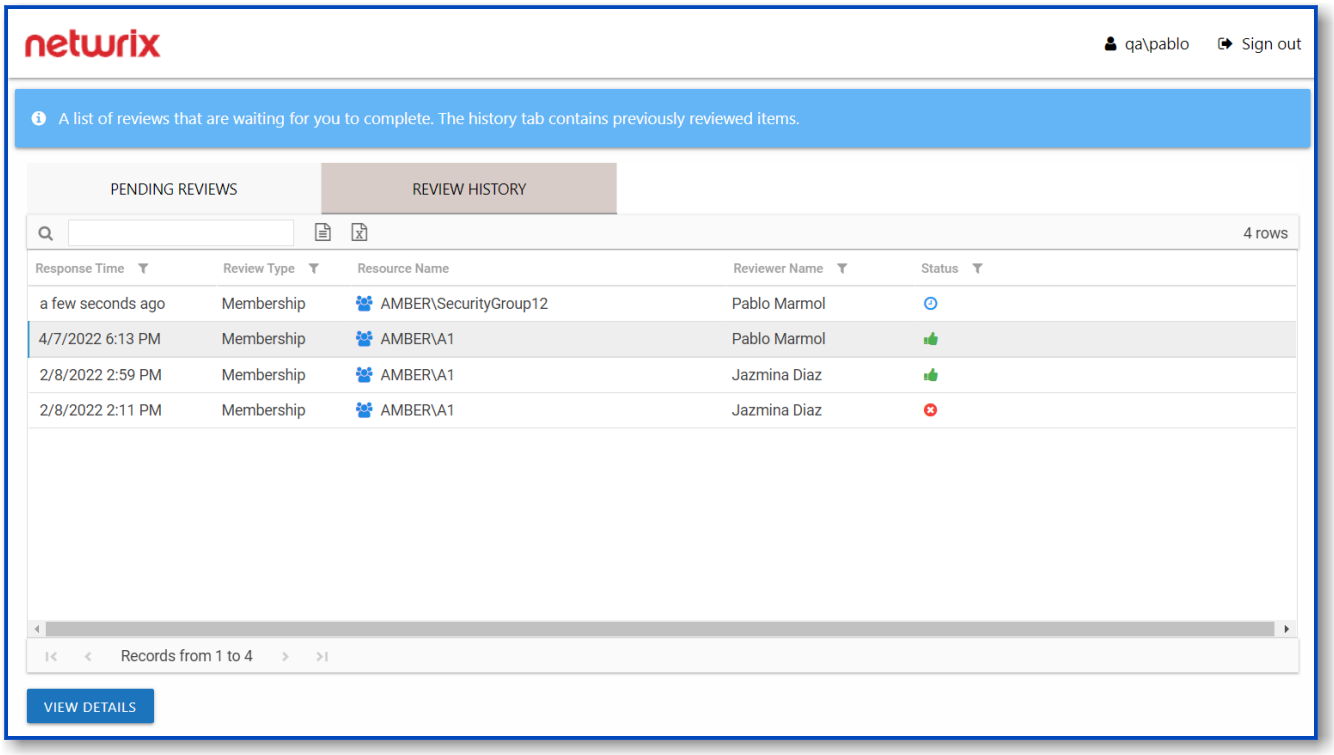
When a group trustee appears in the Trustee Name column of a review, it appears as a blue hyperlink in addition to the group icon displayed in front of the name.



Click the hyperlink to open the Group Membership window. The group's direct membership is listed for review. Click **Close** to return to the review.

Review History Page

The Review History page lists all completed review instances for your resources.



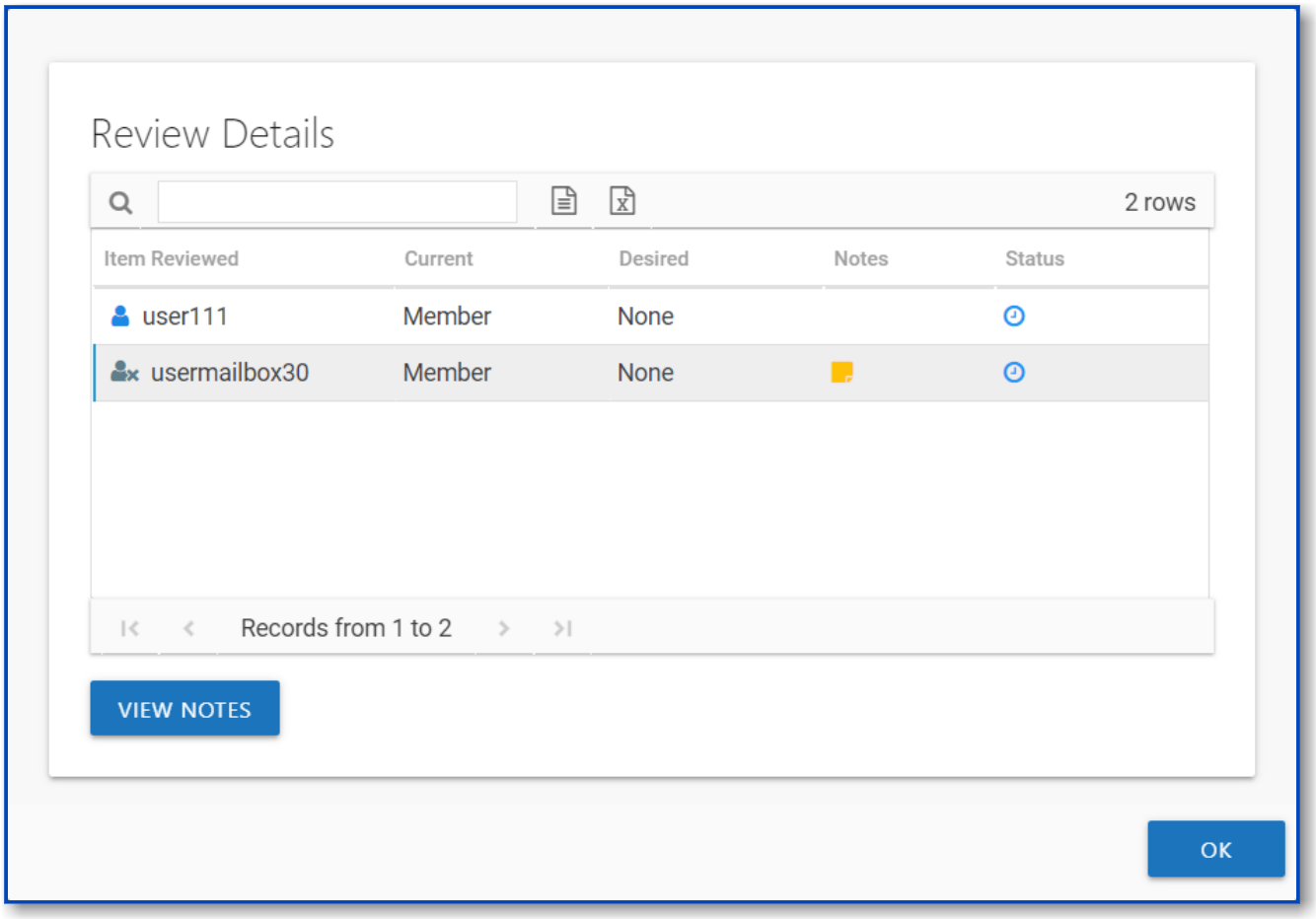
The information displayed in the table includes:

- Response Time – Date timestamp when the last review took place for the resource.
- Review Type – Type of review
- Resource Name – The icon indicates the type of resource. The resource name includes its location, such as the UNC path for a file system resource, the URL for SharePoint resource, or Group name (e.g., [Domain]\[Group]).
- Reviewer Name – Name of the assigned owner who performed the review
- Status – Icon indicates the decision provided by the Review Administrator: Accept, Decline, Defer, or Waiting. Hover over a status icon to display its tooltip.

The table data grid functions the same way as other table grids. See the Data Grid Features topic for additional information.

Review Details Window

The View Details button at the bottom of the Review History page opens the Review Details window for a resource where changes were recommended.



The information displayed in the table includes:

- Item Reviewed – Item upon which changes were suggested by the owner
- Current – Current state of the item at the time of the review. It could be the type of access (for Access reviews) or being a member (for Membership reviews).
- Desired – Change suggested by the owner. It could be the new type of access (for Access reviews) or removing membership (for Membership reviews).
- Notes – An icon here indicates notes were entered by the owner. Select the item and click the **View Notes** button to open the View Notes window.
- Status – Icon indicates the decision provided by the Review Administrator: Accept, Decline, Defer, or Waiting. Hover over a status icon to display its tooltip.

Click **OK** to close the window.