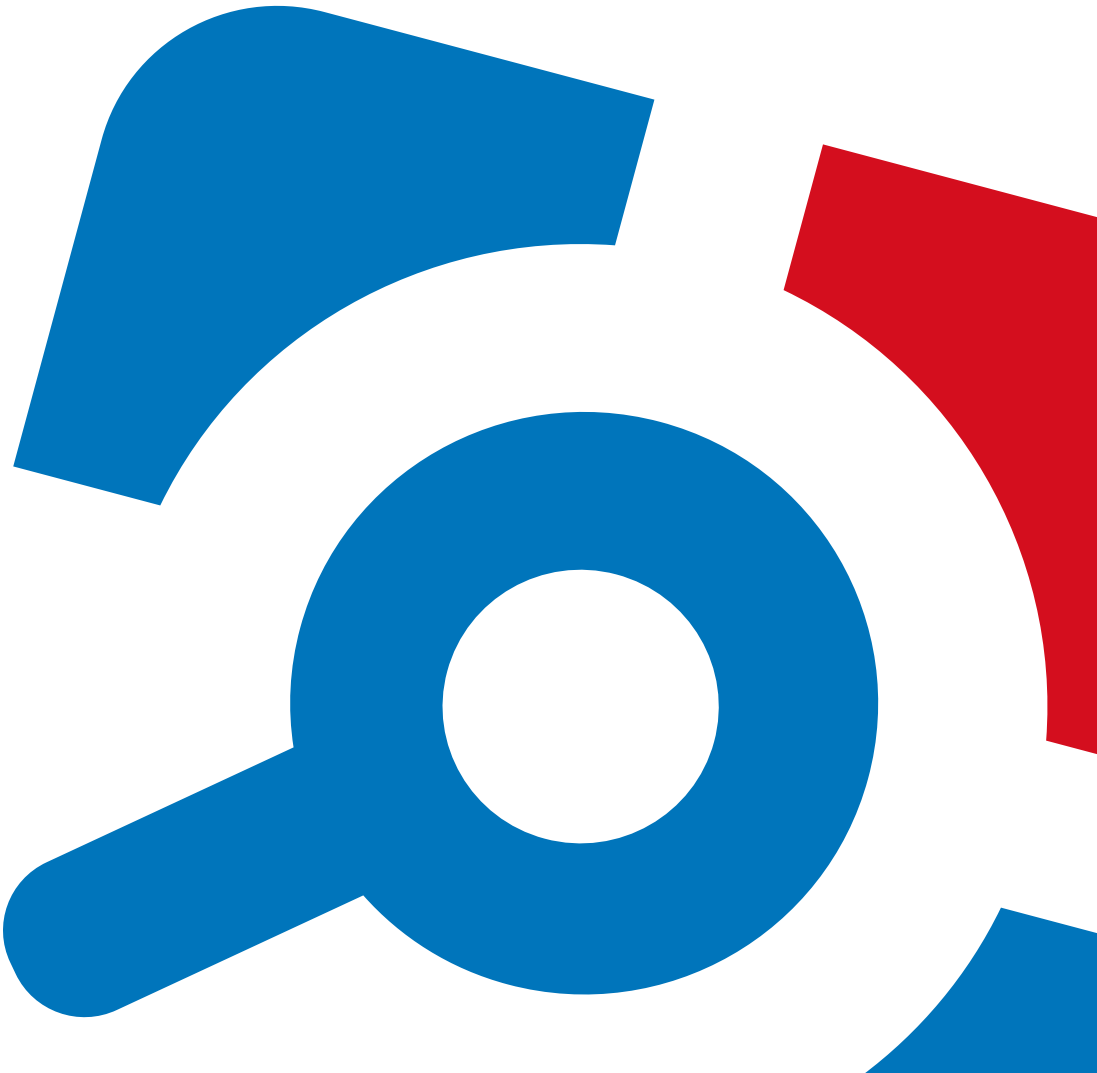
netwrix

Netwrix Auditor

Administration Guide

Version: 9.0
7/19/2017



Legal Notice

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

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. Introduction

This guide is intended for Netwrix Auditor global administrators and configurators, provides step–by–step instructions on how to start monitoring your environments, create monitoring plans, configure Audit Database settings and email notifications. It also provides information on fine-tuning the product, additional configuration, etc.

The product functionality described in this guide applies to Netwrix Auditor Standard Edition. Note that Free Community Edition provides limited functionality. See Product Editions for more information.

1.1. Netwrix Auditor Overview

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

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

Major benefits:

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

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

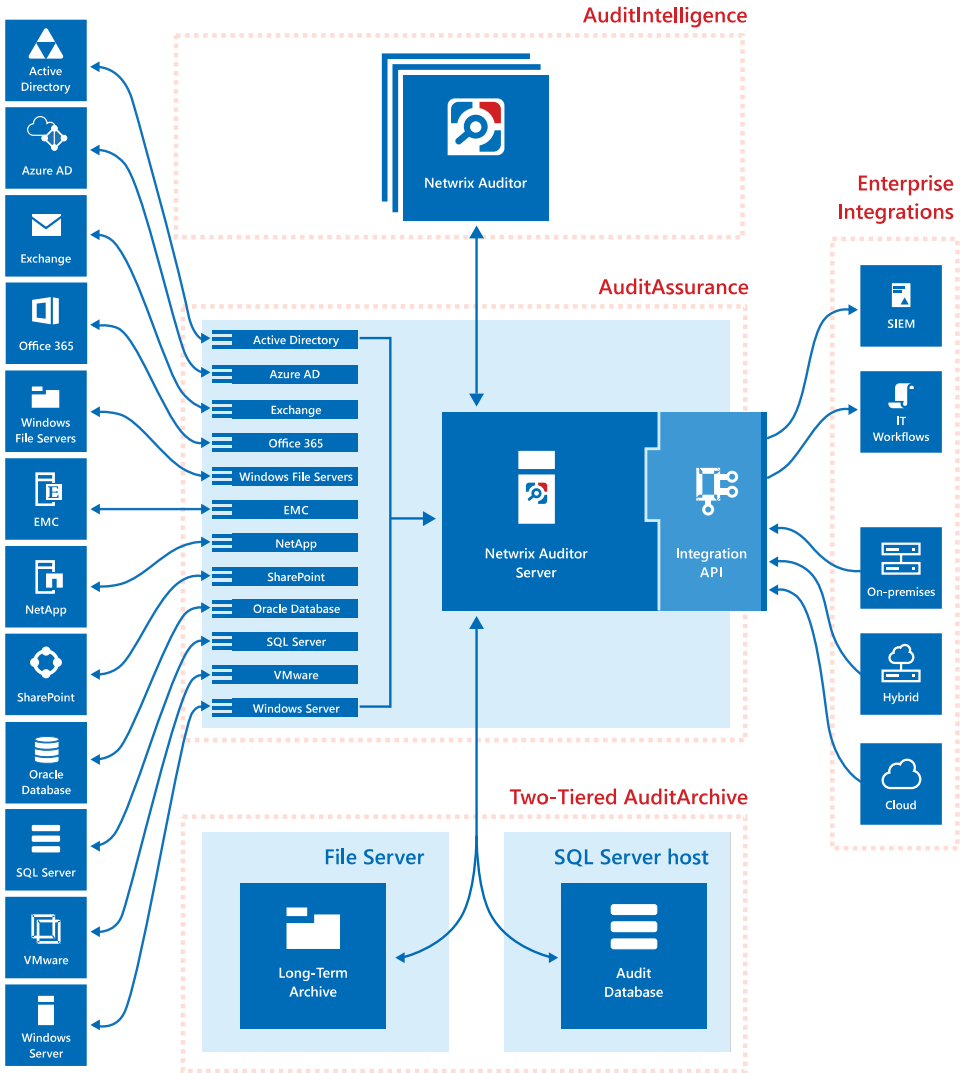
Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain structure that can be used to assess its state at present or at any moment in the past. The product provides logon activity summary, reports on interactive and non-interactive logons including failed logon attempts. Also, Netwrix Auditor for Active Directory helps address specific tasks—detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a stand-alone

Application	Features
	Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.
Netwrix Auditor for Azure AD	Netwrix Auditor for Azure AD detects and reports on all changes made to Azure AD configuration and permissions, including Azure AD objects, user accounts, passwords, group membership, and more. The products also reports on successful and failed logon attempts.
Netwrix Auditor for Exchange	Netwrix Auditor for Exchange detects and reports on all changes made to Microsoft Exchange configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange organization, and notifies the users whose mailboxes have been accessed by non–owners.
Netwrix Auditor for Office 365	Netwrix Auditor for Office 365 detects and reports on all changes made to Microsoft Exchange Online and SharePoint Online. For Exchange Online, the product provides auditing of configuration and permissions changes. In addition, it tracks mailbox access events in the managed Exchange Online organization, and notifies the users whose mailboxes have been accessed by non–owners. For SharePoint Online, the product reports on read access and changes made to SharePoint Online sites, including modifications of content, security settings, and sharing permissions. In addition to SharePoint Online, OneDrive for Business changes are reported too.
Netwrix Auditor for Windows File Servers	Netwrix Auditor for Windows File Servers detects and reports on all changes made to Windows–based file servers, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for EMC	Netwrix Auditor for EMC detects and reports on all changes made to EMC VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for Oracle	Netwrix Auditor for Oracle Database detects and reports on all

Application	Features
Database	changes made to your Oracle Database instance configuration, privileges and security settings, including database objects and directories, user accounts, audit policies, sensitive data, and triggers. The product also reports on failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on read access and changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration, database content, and logon activity.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. With a stand-alone Event Log Manager tool, Netwrix Auditor collects Windows event logs from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

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



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

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

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

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

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

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

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

1.3. Product Editions

Netwrix Auditor is available in two editions: full-featured Standard Edition activated with a license key and limited Free Community Edition that is distributed free of charge.

Netwrix Auditor Standard Edition 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. 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 Standard Edition, simply by supplying a commercial license in **Settings** → **Licenses**.

Refer to a table below to compare product editions.

Feature	Free Community Edition	Standard Edition
Deployment options	One Netwrix Auditor client instance per one Netwrix Auditor Server	Multiple Netwrix Auditor clients for Netwrix Auditor Server
Role–based access and delegation	–	+

Feature	Free Community Edition	Standard Edition
Support plan	Forum support only	Full
Automatic audit configuration	+	+
Data sources		
Active Directory (including Group Policy and Logon Activity)	One domain	Unlimited
Azure AD	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
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	–	+

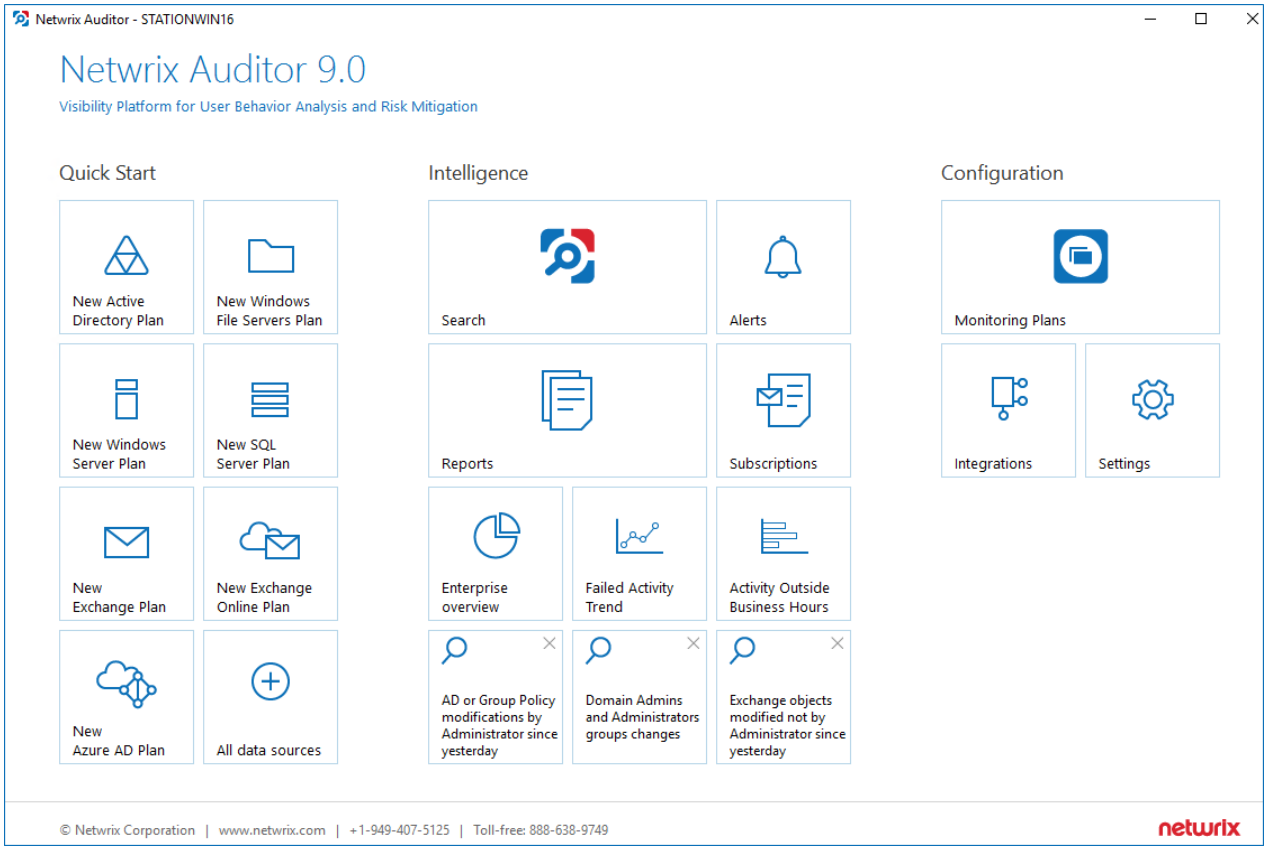
Feature	Free Community Edition	Standard Edition
Netwrix Auditor Event Log Manager	–	+
Netwrix Auditor Inactive User Tracker	–	+
Netwrix Auditor Password Expiration Notifier	–	+
Data collection details		
Who	–	+
What	+	+
When	+	+
Where	+	+
Workstation	+	+
User Activity video recording	–	+
Intelligence		
Activity Summary	A single recipient	Multiple recipients
AuditArchive	–	Both Long-Term Archive and Audit Database
Search	–	+
Reports (including organization–level reports, overview diagrams, change and activity reports, reports with video and review status) and special report packs	–	+
State–in–time reports	–	+
Subscriptions	–	+
Saved searches	–	+
Alerts	–	+
Netwrix Auditor Integration API		

Feature	Free Community Edition	Standard Edition
Data in	–	+
Data out	–	+

2. Launch Netwrix Auditor

To start using Netwrix Auditor

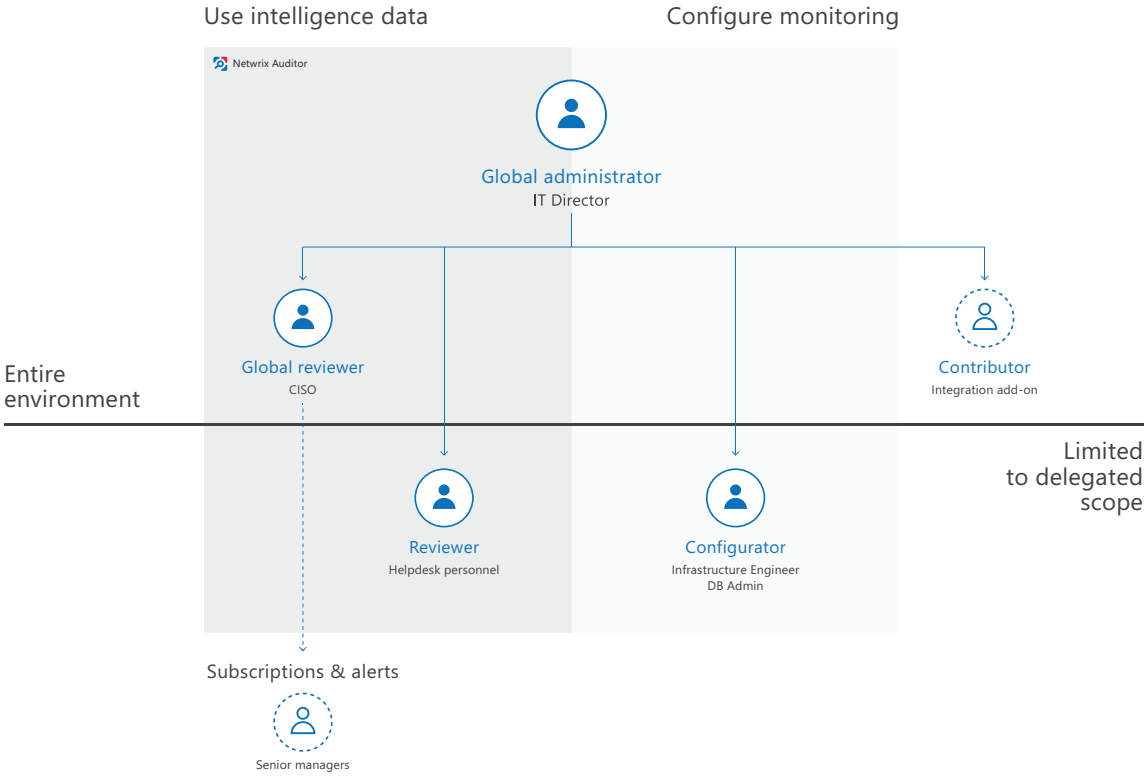
- Navigate to **Start** → **Netwrix Auditor** → **Netwrix Auditor**. You will see the **Welcome** page:



3. 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 the further 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 Netwrix Auditor Server host in your environment.

Role	Access level	Recommended use
		By default, the user who installed Netwrix 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 Netwrix 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 Netwrix 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 Netwrix Auditor Integration API to retrieve data from the Audit Database.
Contributor	Write access to Netwrix Auditor Server and Audit Database.	This service role is granted to specialists who use Netwrix Auditor Integration API to write data to the Audit Database. This role is also granted to service accounts or any accounts used for interaction with Netwrix Auditor Server (e.g., add-on scripts).

3.1. Compare Roles

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Launch Netwrix Auditor client	+	+	+	+	+
Delegate control, grant and revoke	+	–	–	–	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
permissions					
View global settings	+	Some	Some	Some	Some
Modify global settings (including default Audit Database, 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 Add and	Some Add and	Some Restricted to	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
		remove Activity Summary recipients	remove Activity Summary recipients within the delegated scope	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	+	+	+	+	+
Generate reports	+	+	Some Restricted to the delegated scope (folder or monitoring	–	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
			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 saved searches	+	+	+	+	+
List alerts	+	+	+	+	+
Create, modify, delete alerts	+	+	–	–	–
Import investigation data from the Long-Term Archive	+	–	–	–	–
View investigation data	+	+	–	–	–
Netwrix Auditor Integration API					
Write Activity Records	+	–	–	–	+
Retrieve Activity Records	+	+	+ Restricted to the delegated	–	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
			scope (folder or monitoring plan)		

3.2. Assign Roles

3.2.1. Understand Scopes and Assign Roles Correctly

NOTE: Only Global administrator can delegate control, grant and revoke permissions.

Netwrix Auditor allows assigning roles not only on the product as a whole but also on a specific scope that can be limited to a single monitoring plan or to the contents of a folder. This is helpful when you want to achieve more granular separation of duties with the product. For example, to ensure that database administrators (DBAs) have no access to Active Directory management data, domain administrators have no permissions to view database schema changes or update data collection settings.

Global administrator, Global reviewer, and Contributor roles are assigned on the global scope only. On folder and plan levels, you may leverage role separation capabilities too: designate Configurators and Reviewers. The roles are inherited from a higher level and cannot be revoked locally, i.e., Global reviewer has access to all collected data while local Reviewer can generate reports and run search on data limited to his or her scope.

Scope	Roles
Global (All monitoring plans)	Global administrator Global reviewer Contributor
Folder level	Configurator Reviewer Contributor
Plan level	Configurator Reviewer Contributor

To delegate control to some scope, review, or revoke assigned roles

1. On the main Netwrix Auditor page, navigate to the **Monitoring Plans** section.
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).
3. Click **Delegate**.
4. Review roles that are already defined for this scope.
5. 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.
Revoke a role assignment	• Click ✕ next to the user.

6. Click **Save** or **Save&Close**.

Along with adding a new **Global administrator**, **Global reviewer**, or **Reviewer**, Netwrix Auditor will automatically assign this user the **Browser** role on the Report Server. The **Browser** role is required to generate reports and is granted on all reports or within a delegated scope. If for some reason, Netwrix Auditor is unable to grant the **Browser** role, configure it manually. See Netwrix Auditor Installation and Configuration Guide for more information.

3.2.2. Review Default Role Assignments

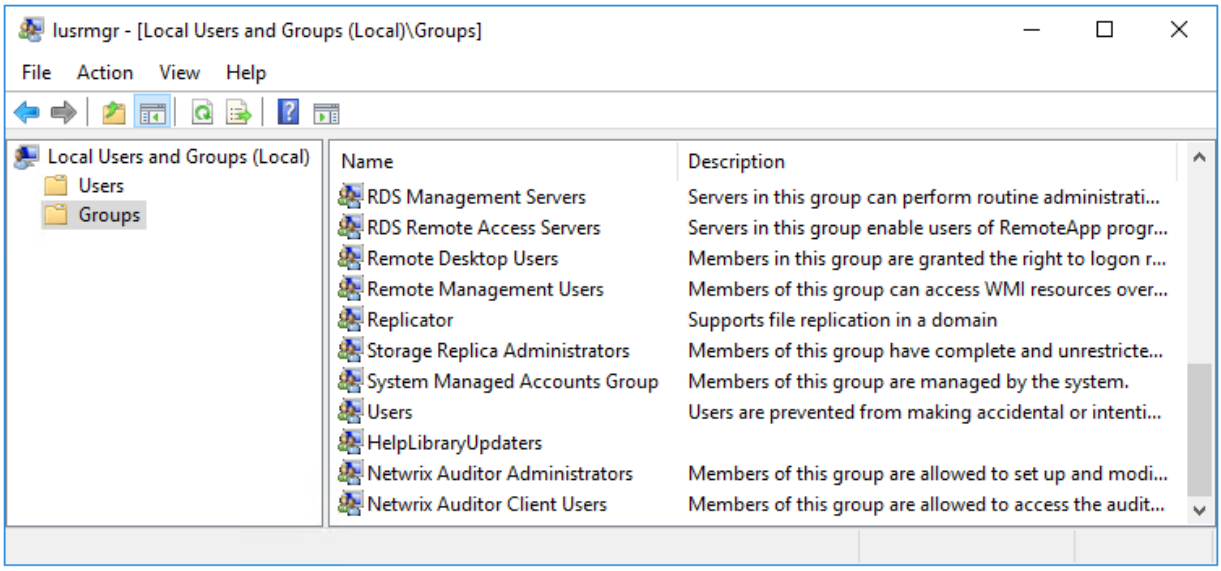
By default, some accounts and local groups are assigned the following roles:

Account or group name	Role
Local Administrators	Global administrator
Local service accounts	Global administrator **NOTE:** Netwrix Auditor uses system accounts for data processing and interaction between product components.
Netwrix Auditor Administrators	Global administrator
Netwrix Auditor Client Users	Global reviewer

During the Netwrix Auditor Server installation, **Netwrix Auditor Administrators** and **Netwrix Auditor Client Users** groups are created automatically. To delegate control through group membership, add users to these groups on the computer where Netwrix Auditor Server resides. Keep in mind that users will be granted roles with extended permissions while it may be reasonable to limit their scope to a specific monitoring plan.

To add an account to a group

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



3.3. Provide Access to a Limited Set of Data

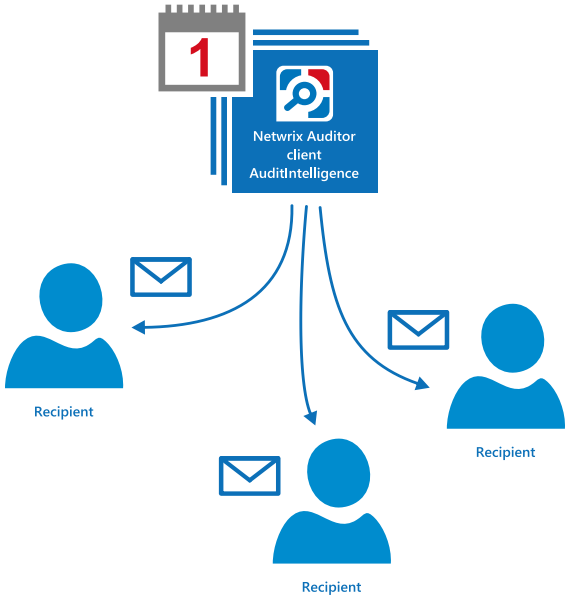
By default, only users designated in Netwrix Auditor are allowed to view its configuration and collected data. This policy ensures that only authorized and trustworthy users access sensitive data and make changes.

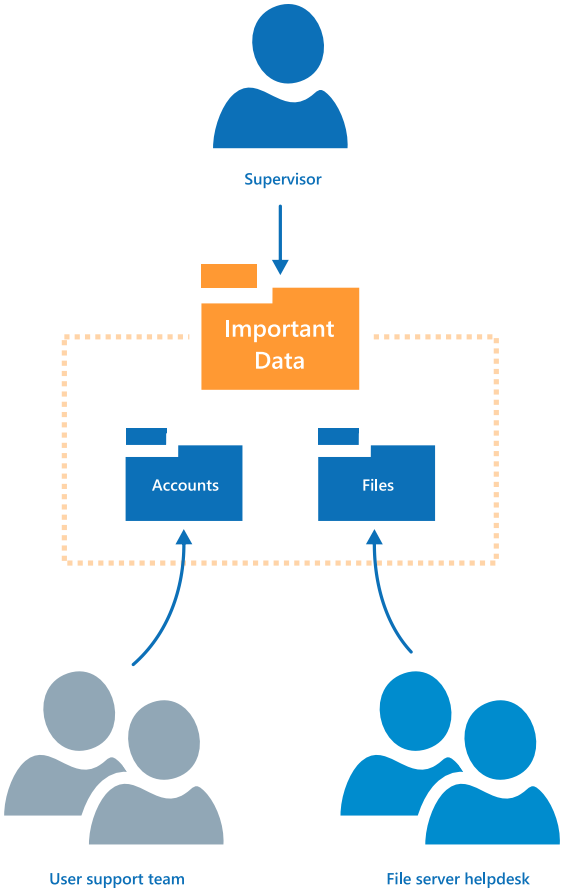
However, in some cases, organizations need to provide certain employees with access to a limited set of audit data. For example, an auditor might need to review particular access reports once or twice a year. You can provide these users (recipients) with means to review the data they need without actually running Netwrix 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 information to other departments. You can configure Netwrix 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.

Do..	Recommended use
	
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.

4. Monitoring Plans

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan. All your monitoring plans are listed in the **Monitoring Plans** section.

A monitoring plan defines your data sources and general data collection, notification, and storage settings. To start collecting data, choose a data source, such as Active Directory or SharePoint, and add items to its scope. Item is a specific object you want to audit, e.g., a server, SharePoint farm. All data sources and items in your plan share common settings so that you can supervise and manage several data collections as one.

On a high level, you should perform the following steps to start monitoring your environment:

1. Create a monitoring plan with a wizard. See Create a New Plan for more information.
2. Add data sources. Although you are prompted to select the first data source in the wizard, you can specify more data sources later. See Manage Data Sources for more information.
3. Add items for monitoring. Netwrix Auditor does not collect data until you specify an item. See Add Items for Monitoring for more information.

Once you create a plan, it becomes available in the **Monitoring Plans** section. To review your plan, navigate to the **Monitoring Plans** section and expand the **All Monitoring Plans** tree.

To..	Do..
See plan overview	Click on a plan name to see data sources included in the plan and data collection status for each data source.
Update data collection status and generate Activity Summary with latest changes	Select a plan and click **Edit**. On the page that opens, click **Update**.
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 in details. Review the following for additional information: • Manage Data Sources • 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 of 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 Role-Based Access and Delegation for more information.

To..	Do..
Review data collected for the monitoring plan	Select a plan and click **Edit**. On the page that opens, click **Search** in the **Intelligence** section. The interactive search page will appear with a monitoring plan filter set to your plan name. Netwrix Auditor provides quick access to reports as well. To see the reports list, click **View reports**.

4.1. Create a New Plan

NOTE: You must assigned the Global administrator role if you want to create plans. Configurator can create plans only within a delegated folder. See Role-Based Access and Delegation for more information.

To start creating a plan, do one of the following:

- On the main Netwrix Auditor page, in the **Quick Start** section, click the tile with a data source of your choice, e.g., Active Directory. Click **All data sources** to specify data source that is not listed on the main page.
- On the main Netwrix Auditor page, in the **Configuration** section, click the **Monitoring Plans** tile. On the **Monitoring Plans** page, select **Add Plan**.

The wizard that appears will help you set up a new plan in a few easy steps:

- Choose a data source for monitoring
- Specify an account for collecting data
- Specify default SQL Server instance and configure the Audit Database to store your data
- Configure notification settings
- Specify the recipients who will receive daily activity summaries
- Specify a plan name

4.1.1. New Monitoring Plan (Data Source)

Specify the first data source or pick a specific area of interest. Once you complete the wizard, you will be able to add more data sources to your plan and customize data source's scope and settings.

4.1.2. New Monitoring Plan

Option	Description
Specify the account for collecting data	Provide a user name and a password for the account that Netwrix Auditor will use to collect data. By default, the user name is prepopulated with your account name. 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 Netwrix Auditor Installation and Configuration Guide. 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.
Configure audit settings	For most data sources, Netwrix Auditor can configure audit settings in your environment automatically. Select **Adjust audit settings automatically**. In this case, Netwrix Auditor will continually check and enforce the relevant audit policies. **NOTE:** Netwrix Auditor has certain limitations when configuring audit settings for NetApp and EMC. See File Servers for more information. For a full list of audit settings and instructions on how to configure them manually, refer to Netwrix Auditor Installation and Configuration Guide.

4.1.3. Default SQL Server Instance

To provide search, alerting, and report capabilities, Netwrix Auditor has to store security intelligence data in the Audit Database hosted on a SQL Server instance. Define the default SQL Server instance on this step or disable security intelligence. Netwrix Auditor skips this step if have already configured Audit Database settings for other monitoring plans.

Specify one of the following options:

- **Disable security intelligence and make data available only in activity summaries**—Select only if you do not want to generate reports and run data searches. Audit data will not be written to the Audit Database and will be available only in Activity Summary emails.

  Even if you 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. Refer to Audit Database for detailed instructions on how to configure the **Audit Database** settings.

- **Install a new instance of Microsoft SQL Server Express automatically**—Select if you want

Netwrix Auditor to download and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance**—Select to continue using an installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and prepopulates the fields. Complete the following fields:

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data. **NOTE:** If you have more than one Netwrix Auditor Server running in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Netwrix Auditor Servers.
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. **NOTE:** This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role. See Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password.

4.1.4. Audit Database

Specify a database name to store security intelligence data for your monitoring plan or disable this functionality. 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 Audit Database for more information.

NOTE: Make sure to store data on the same SQL Server instance. Otherwise some data may become unavailable for search and reporting.

Netwrix Auditor will create a database on the SQL Server instance you specify.

4.1.5. Notifications

Specify the email settings that will be used for activity summaries, reports and alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. 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. **NOTE:** It is recommended to 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 the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL authentication	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. **NOTE:** The option is not available for auditing User Activity as well Netwrix Auditor tools.

NOTE: You can always configure SMTP settings later if you do not want to receive email notifications. See Notifications for more information.

4.1.6. Recipients

Specify the users who will receive daily activity summaries that list changes that occurred for a given time period. Click **Add Recipient** and provide email address.

NOTE: It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

4.1.7. Monitoring Plan Summary

Your plan is almost complete. Provide a name and description for your monitoring plan. Make sure the **Add item now** checkbox is selected. In this case, on the next step, you will be prompted to add an item for monitoring.

NOTE: 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, Netwrix 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.

4.2. Manage Data Sources

Netwrix Auditor allows you to combine different data sources in a single monitoring plan. Basically, you specify the first data source when you create a new plan. Later, you can add more data sources to this plan. This can be helpful if these data sources have common settings (e.g., same account for data collection and Activity Summary recipients). In this case, you will be able to supervise and manage data collection for these data sources as one.

NOTE: 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 Role-Based Access and Delegation for more information.

To add a new data source to existing plan

1. Specify a plan in the **Monitoring Plans** and click **Edit**.
2. In the right pane, select **Add data source**.
3. Specify a data source.
4. Configure settings specific to your data source.

You can fine-tune data collection for each data source. To do it, select a data source within your monitoring plan and click **Edit data source**. For all items included in a data source, you can:

- Enable or disable monitoring
- Depending on the data source, customize the monitoring scope (e.g., enable read access auditing, monitoring of failed attempts)

Review the following for additional information:

- Active Directory
- Azure AD
- Exchange
- Exchange Online
- File Servers
- Group Policy
- Logon Activity
- Oracle Database
- SharePoint
- SharePoint Online
- SQL Server
- User Activity
- Windows Server
- VMware
- Netwrix API

4.2.1. Active Directory

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.
Monitoring Active Directory partitions	Select which of your Active Directory environment partitions you want to audit. 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, 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 objects. Updates to this partition are replicated to all domain controllers in the forest. **NOTE:** You cannot disable auditing the Domain partition for changes.
Detect additional details	Specify additional information to include in reports and activity summaries. Configure the following: • **Originating workstation** — Workstation from which the change was made. • **Group membership** — 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.

Option	Description
	NOTE: This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. 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 Netwrix Auditor Installation and Configuration Guide.
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. In the **Manage historical snapshots** section, 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. Move the selected snapshots to the **Snapshots available for reporting** list using the arrow button. You must be assigned the **Global administrator** or the **Global reviewer** role to import snapshots. **NOTE:** By default, snapshots are uploaded once a day and 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.

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 Add Items for Monitoring for more information.

4.2.2. Azure AD

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.
Monitor Azure AD logon activity	Specify what types of logon events you want to monitor: • Failed logons • Successful logons

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 Add Items for Monitoring for more information.

4.2.3. Exchange

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.
Detect additional details	Specify additional information to include in reports and activity summaries. Configure the following: • **Originating workstation** — Workstation from which the change was made. • **Group membership** — 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. **NOTE:** This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. 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 Netwrix Auditor Installation and Configuration Guide.
Collect data on non-owner access to mailboxes	Enable monitoring of unauthorized access to mailboxes within your Exchange organization. Configure the following: • **Enable automatic audit configuration** — If you select to

Option	Description
	automatically configure audit in the target environment, 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. 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 Netwrix Auditor Installation and Configuration Guide. If you want to configure audit manually, refer to Netwrix Auditor Installation and Configuration Guide for a full list of audit settings, and instructions on how to configure them. • **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 Add Items for Monitoring for more information.

4.2.4. Exchange Online

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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. **NOTE:** This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed.

Option	Description
	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 Netwrix Auditor Installation and Configuration Guide.
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 Add Items for Monitoring for more information.

4.2.5. Group Policy

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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 Netwrix Auditor Installation and Configuration Guide for more information on software requirements.
Detect additional details	Specify additional information to include in reports and activity summaries. Configure the following: • **Originating workstation** — Workstation from which the change was made.

Option	Description
	• **Group membership** — 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. **NOTE:** This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. 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 Netwrix Auditor Installation and Configuration Guide.
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. In the **Manage historical snapshots** section, 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. Move the selected snapshots to the **Snapshots available for reporting** list using the arrow button. You must be assigned the **Global administrator** or the **Global reviewer** role to import snapshots. **NOTE:** By default, snapshots are uploaded once a day and 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.

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 Add Items for Monitoring for more information.

4.2.6. File Servers

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.
Specify actions for monitoring	Specify actions you want to track and auditing mode. Review the following for additional information: **Changes** **Successful** — Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion. **Failed** — Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it. **Read access** **Successful** — Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive. **Failed** — Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive. **NOTE:** Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share). The changes include creation, modification, deletion, moving, etc. To track the copy action, enable successful read access and change auditing. See Monitored Object Types, Actions, and Attributes for

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>more information.</td></tr>
<tr><td>Specify data collection method</td><td>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.</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.

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

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 Netwrix Auditor Installation and Configuration Guide.

Some settings cannot be configured automatically. Netwrix Auditor 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>EMC Celerra</td><td>+</td><td>+</td><td>+</td><td>—</td><td>+</td><td>—</td></tr>
<tr><td>EMC Isilon</td><td>n/a</td><td>n/a</td><td>+</td><td>—</td><td>n/a</td><td>n/a</td></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>
</table>
</td></tr>
<tr><td>Collect data for state-in-time reports</td><td>Configure Netwrix Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation.</td></tr>
</table>

Option	Description
	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, select all checkboxes under **Include details on effective permissions**. In the **Manage historical snapshots** section, 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. Move the selected snapshots to the **Snapshots available for reporting** list using the arrow button. You must be assigned the **Global administrator** or the **Global reviewer** role to import snapshots. **NOTE:** By default, snapshots are uploaded once a day and 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.

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 Add Items for Monitoring for more information.

NOTE: Netwrix Auditor supports auditing of DFS and clustered file servers provided that **Object Access Auditing** is enabled on DFS file shares or every node belonging to the cluster correspondingly.

- When adding a clustered file server for auditing, it is recommended to specify a Computer item and provide FQDN name.
- When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path. For example: "\\domain\dfsnamespace\" (domain-based namespace) or "\\server\dfsnamespace\" (in case of stand-alone namespace).

4.2.7. Logon Activity

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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. **NOTE:** This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. 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 Netwrix Auditor Installation and Configuration Guide.

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 Add Items for Monitoring for more information.

4.2.8. Oracle Database

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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

Option	Description
	case all required components have been already installed, this section will be omitted. See Netwrix Auditor Installation and Configuration Guide for more information on software requirements.
Monitor Oracle Database logon activity	Specify what types of logon events you want to monitor: • Failed logons • Successful logons • Logoffs
Include or exclude specific users from monitoring	Click **Specify Users** and configure the following: • **Specify users for monitoring**—Add users to be included in the auditing scope by specifying their names and type (OS or database user). • **Exclude**—Add users to be excluded from the auditing scope by specifying their names and type (OS or database user). **NOTE:** User names are case sensitive.
Audit data access and changes	Create rules for objects and actions that you want to audit. Click **Add rule**, specify a name of Oracle database object or schema and check actions (successful or failed reads, successful or failed changes). **NOTE:** 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 Add Items for Monitoring for more information.

4.2.9. SharePoint

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.
Detect additional details	Specify additional information to include in reports and activity summaries. Configure the following:

Option	Description
	• **Originating workstation** — Workstation from which the change was made. • **Group membership** — 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. **NOTE:** This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. 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 Netwrix Auditor Installation and Configuration Guide.

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 Add Items for Monitoring for more information.

4.2.10. SharePoint Online

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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 Netwrix Auditor to monitor SharePoint Online read access.

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 Add Items for Monitoring for more information.

4.2.11. SQL Server

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.
Audit SQL Server configuration changes	SQL Server configuration changes are always audited.
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 SQL and Windows logons • Successful SQL logons • Successful Windows logons
Audit data changes	Create rules for the data to be audited and therefore to receive change reports on the selected data only. Set the number of data changes per SQL transaction to be included in reports. In this case Netwrix Auditor-specific data will be written to the audited tables. Click **Add Rule** to create columns auditing rules and configure the following: • **Type**—Select rule type: inclusive or exclusive. • **Server**—Specify a name of the SQL Server instance where the database resides. • **Database**—Specify database name. • **Table**—Specify table name. • **Column**—Specify column name. **NOTE:** The following column types are currently not supported: `text`, `ntext`, `image`, `binary`, `varbinary`, `timestamp`, `sql_variant`. **NOTE:** Wildcard (*) is supported.

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 Add Items for Monitoring for more information.

4.2.12. User Activity

Complete the following fields:

Option	Description
	General
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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.
	Video Recording
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. • **User has been idle for <...> minutes**—Video recording will be stopped if a user is considered inactive during the selected time period. • **Free disk space is less than <...> MB**—Video recording will be stopped when upon reaching selected disk space limit.
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.
	Applications
Specify applications you want to	Select the applications that you want to monitor. You can select

Option	Description
track	**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 Monitoring for more information. The list contains computer name, its current status and last activity time.	

4.2.13. VMware

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.

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 Add Items for Monitoring for more information.

4.2.14. Windows Server

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix 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. • **Hardware** — Enables auditing of hardware devices configuration. For example, your network adapter configuration changes.

Option	Description
	• **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 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

Option	Description
	necessary. **NOTE:** This method is recommended for evaluation purposes in test environments. If any conflicts are detected with your current audit settings, automatic audit configuration will not be performed. 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 Netwrix Auditor Installation and Configuration Guide.

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 Add Items for Monitoring for more information.

4.2.15. Netwrix API

Netwrix API is a special data source for the data received through Netwrix Auditor Integration API. 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.

If you want to associate data from your custom data source or SIEM solution with a certain plan, add a **Netwrix API** data source to your plan and mark the plan name in activity records before import. In this case, data will be written to the database linked to your monitoring plan. This can be helpful:

- If you need to restrict access to imported data. In this case only the users who are granted permissions to see the plan data will get access to imported activity records.
- If you want to simplify your search. In this case, you will be able to specify filters, such as **Monitoring plan** and **Data source**, and find the imported activity records faster.
- If you want to use Netwrix Auditor as intermediate solution in your monitoring routine. In this case, you will be able to export previously imported data.

NOTE: The account used to import activity records must be assigned a special Contributor role. See Role-Based Access and Delegation for more information.

Complete the following fields:

Option	Description
Monitor this data source and collect activity data	Enable monitoring of the selected data source and configure Netwrix Auditor to collect and store audit data.

Option	Description
	NOTE: If monitoring is disabled, you will not be able to import activity records to database linked to your monitoring plan.

To further diversify your data, add **Integration** items to your **Netwrix API** data source. See Integration for more information.

NOTE: 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 in activity records before importing data. See Netwrix Auditor Integration API Guide for detailed instructions on API commands and Activity Record structure.

4.3. Add Items for Monitoring

Once you completed monitoring plan wizard and specified data sources, add items for monitoring. You can 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. For example, select the **Computer** item. For example, select the **EMC VNX/VNXe** item. Select the **NetApp** item.

Data Source	Item
Active Directory Group Policy Exchange Logon Activity	Domain
Azure AD Exchange Online SharePoint Online	Office 365 Tenant
File Servers (including Windows file server, EMC, and NetApp)	AD Container Computer EMC Isilon EMC VNX/VNXe

Data Source	Item
	IP Range NetApp Windows File Share
Oracle Database	Oracle Database Instance
SharePoint	SharePoint Farm
SQL Server	SQL Server Instance
VMware	VMware ESX/ESXi/vCenter
Windows Server User Activity	Computer AD Container IP Range
Netwrix API	Integration

NOTE: 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 Role-Based Access and Delegation for more information.

To add a new item to a data source

1. Navigate to your plan settings.
2. Click **Add item** under the data source.
3. 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)

4.3.1. AD Container

Complete the following fields:

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. **NOTE:** 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. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.2. Computer

Complete the following fields:

Option	Description
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 **Custom account** and enter credentials. The credentials are case sensitive. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data

Option	Description
	collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.3. 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 **Custom account** and enter credentials. The credentials are case sensitive. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.4. EMC Isilon

Complete the following fields:

Option	Description
	General
Specify EMC Isilon 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.
Access Zone	Enter the name of access zone on your file server (e.g., zone1).
OneFS web administration interface URL	Enter EMC Isilon web administration URL (e.g., *https://172.28.15.126:8080/*).
File Share UNC path to audit logs	Path to the file share located on a EMC Isilon with event log files (e.g., *srv**netwrix_audit$**logs*\).

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. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.
	Scope
Monitor the following shares	If you want to limit your auditing scope by several shares, click **Add** under the **Specific file shares** and select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.

4.3.5. EMC VNX/VNXe

Complete the following fields:

Option	Description
	General
Specify EMC VNX or VNXe 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. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.
	Scope
Monitor the following shares	If you want to limit your auditing scope by several shares, click **Add** under the **Specific file shares** and select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.

4.3.6. IP Range

Complete the following fields:

Option	Description
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. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.7. 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.

Option	Description
	NOTE: A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.
	ONTAPI
Specify protocol for accessing ONTAPI	Select one of the following: • **Detect automatically**—If selected, a connection protocol will be detected automatically. • **HTTP** • **HTTPS** **NOTE:** Refer to Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to enable HTTP or HTTPS admin access.
Specify management interface	Select management interface to connect to ONTAPI. If you want to use custom management interface for ONTAPI, select **Custom** and provide a server name by entering its FQDN, NETBIOS or IP address.
Specify account for connecting to ONTAPI	Select an account to connect to NetApp and collect data through ONTAPI. 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. **NOTE:** See Netwrix Auditor Installation and Configuration Guide for more information on required rights and permissions.
	Scope
Monitor the following shares	If you want to limit your auditing scope by several shares, click **Add** under the **Specific file shares** and select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.

4.3.8. Office 365 Tenant

Complete the following fields:

Option	Description
Specify Office 365 Account	Specify email address and password of your Microsoft account that will be used to connect to Office 365.

4.3.9. Oracle Database Instance

Complete the following fields:

Option	Description
Specify Oracle Database instance	Provide connection details in the following format: *host:port/service_name*. Make sure audit settings are configured for your Oracle Database 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 than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.10. 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

Option	Description
	credentials. The credentials are case sensitive. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.
	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 Netwrix Auditor Installation and Configuration Guide 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 Netwrix Auditor Installation and Configuration Guide for more information. • **Manually**—See Netwrix Auditor Installation and Configuration Guide for more information.

Option	Description
	NOTE: 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. **NOTE:** 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.
	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. **NOTE:** Read access auditing significantly increases the number of

Option	Description
	events generated on your SharePoint and the amount of data written to the AuditArchive.

4.3.11. 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 than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.12. VMware ESX/ESXi/vCenter

Complete the following fields:

Option	Description
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 than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.13. Windows File Share

Complete the following fields:

Option	Description
Specify Windows file share	Provide UNC path to a shared resource.
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. **NOTE:** A custom account must be granted the same permissions and access rights as the default account used for data collection. See Netwrix Auditor Installation and Configuration Guide for more information.

4.3.14. Integration

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.

NOTE: 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. See Netwrix Auditor Integration API Guide for detailed instructions on API commands and Activity Record structure.

4.4. 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.

NOTE: 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 Role-Based Access and Delegation for more information.

To edit your plan settings

1. Select a plan in the **All Monitoring Plans** list and click **Edit**.
2. In the right pane, select **Edit settings**.
3. In the **Plan Settings** page, review the tabs and modify settings.

Option	Description
	General
Name Description	Update a plan name or its description.
	Data Collection
Specify the account for collecting data • User name • Password	Specify a new user name and a password for the account that Netwrix Auditor will use to collect data. 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 Netwrix Auditor Installation and Configuration Guide.
	Audit Database
Disable security intelligence and make data available only in activity summaries	Keep this checkbox cleared if you want Netwrix 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 Audit Database for more information.
Specify custom connection parameters	Specify this option to use non-default settings (e.g., use a different authentication method or user). **NOTE:** Make sure to store data on the same SQL Server instance. Otherwise some data may become unavailable for search and reporting.

Option	Description
	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 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 Netwrix Auditor to always send emails with attachments instead of listing activity and changes in email body. • **Compress attachment before sending**—You can configure Netwrix 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. **NOTE:** It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

5. Data Collection

On a high level, the Netwrix Auditor data collection works as follows:

1. Once a monitoring plan is created, a data source is specified, and an item is added, Netwrix Auditor Server starts collecting data from the Active Directory domain or organizational unit, a server, a SharePoint farm, Office 365 tenant, or VMware Virtual Center, etc.
2. The first data collection gathers information on the data source's current configuration state. Netwrix Auditor uses this information as a benchmark to collect data on changes to the audited environment. After the first data collection has finished, an email notification is sent to the specified recipients stating that the analysis has completed.

   For monitoring SharePoint farms and User Activity, Netwrix Auditor employs a different data collection method. It requires a Core Service to be installed on the monitored computers/SharePoint server. The Core Service starts collecting data immediately and does not require to run the first data collection to gather information on the data source's current configuration state.
3. For all data sources, the latest data collection status can be reviewed in any Netwrix Auditor client, remote or installed along with Netwrix Auditor Server. To do it, navigate to the monitoring plan which includes the data source whose data collection status you want to check. Review data collection status in the **Status** column. The status is updated automatically every time you navigate to the monitoring plan page.
4. For most data sources, collected data is uploaded to the Audit Database every 10-30 minutes. After this, it becomes available for search and reporting.
5. If a critical action is detected or a threshold is reached, an email notification—an alert—is sent to the specified recipients. Make sure you enabled one of the predefined alerts or configured your custom alert.
6. Typically, the product generates and sends an Activity Summary once a day (by default, 3 AM). The notification lists all activity that occurred during this period.
7. If the state-in-time functionality is enabled, Netwrix Auditor also writes a state-in-time snapshot of the data source's current state to the Audit Database. Typically, the full snapshot is written once a day, along with Activity Summary delivery.

   NOTE: This functionality is currently available for the following data sources:

   - Active Directory
   - File Servers
   - Group Policy

5.1. Launch Data Collection Manually and Update Status

If you do not want to wait until a scheduled data collection, you can launch it manually. Along with data collection, the following actions will be performed:

- An Activity Summary email will be generated and sent to the specified recipients. It will list all changes that occurred since the last scheduled or on-demand Activity Summary delivery.
- Changes that occurred between data collections will be written to the Long-Term Archive and the Audit Database, and become available in the Netwrix Auditor client.
- A state-in-time data will be updated.

To launch data collection manually

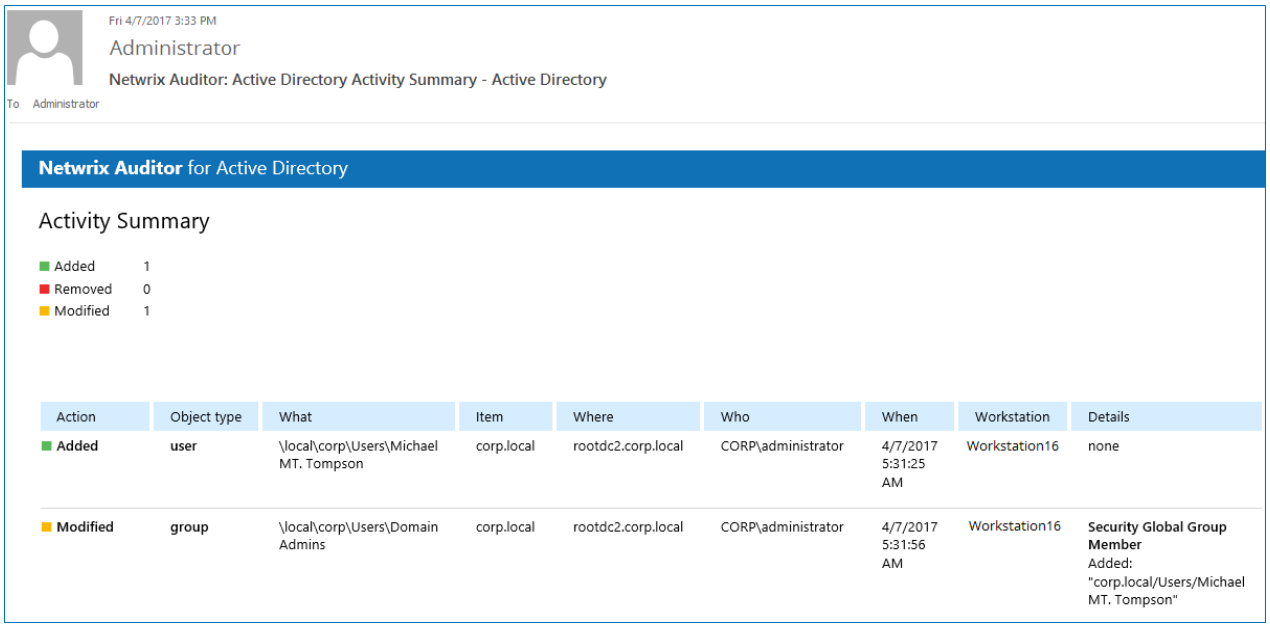
1. Navigate to **All monitoring plans** → your monitoring plan, select **Edit**.
2. In the right pane, click **Update**.

NOTE: Depending on the size of the monitored environment and the number of changes, data collection may take a while.

6. Activity Summary

An Activity Summary is email that lists all changes / recorded user sessions that occurred since the last Activity Summary delivery. Notifications on user activity and event log collection (Event Log Collection Status) are a bit different and do not show changes. 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 an Activity Summary generation manually.

NOTE: The Activity Summary example applies to Active Directory. Other Activity Summaries generated and delivered by Netwrix Auditor may vary slightly depending on the data source.



Fri 4/7/2017 3:33 PM

Administrator

Netwrix Auditor: Active Directory Activity Summary - Active Directory

To Administrator

Netwrix Auditor for Active Directory

Activity Summary

Added 1
Removed 0
Modified 1

Action	Object type	What	Item	Where	Who	When	Workstation	Details
Added	**user**	\local\corp\Users\Michael MT. Tompson	corp.local	rootdc2.corp.local	CORP\administrator	4/7/2017 5:31:25 AM	Workstation16	none
Modified	**group**	\local\corp\Users\Domain Admins	corp.local	rootdc2.corp.local	CORP\administrator	4/7/2017 5:31:56 AM	Workstation16	**Security Global Group Member** Added: "corp.local/Users/Michael MT. Tompson"

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
Object Type	Shows the type of the modified AD object, for example, 'user'.
What	Shows the path to the modified AD object.
Item	Shows the item associated with the selected monitoring plan.

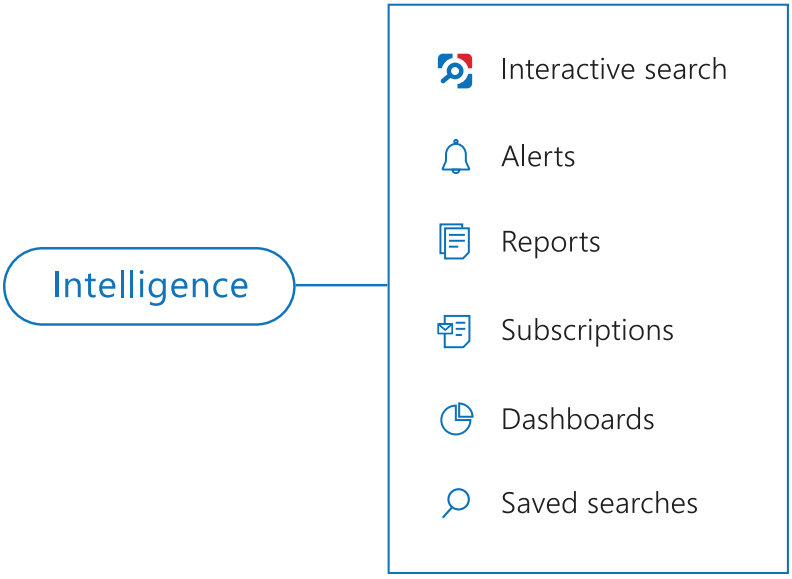
Column	Description
Where	Shows the name of the domain controller where the change was made.
Who	Shows the name of the account under which the change was made.
When	Shows the exact time when the change occurred.
Workstation	Shows the name / IP address of the computer where the user was logged on when 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 sent listing all activity occurring since the last data collection.

7. Intelligence

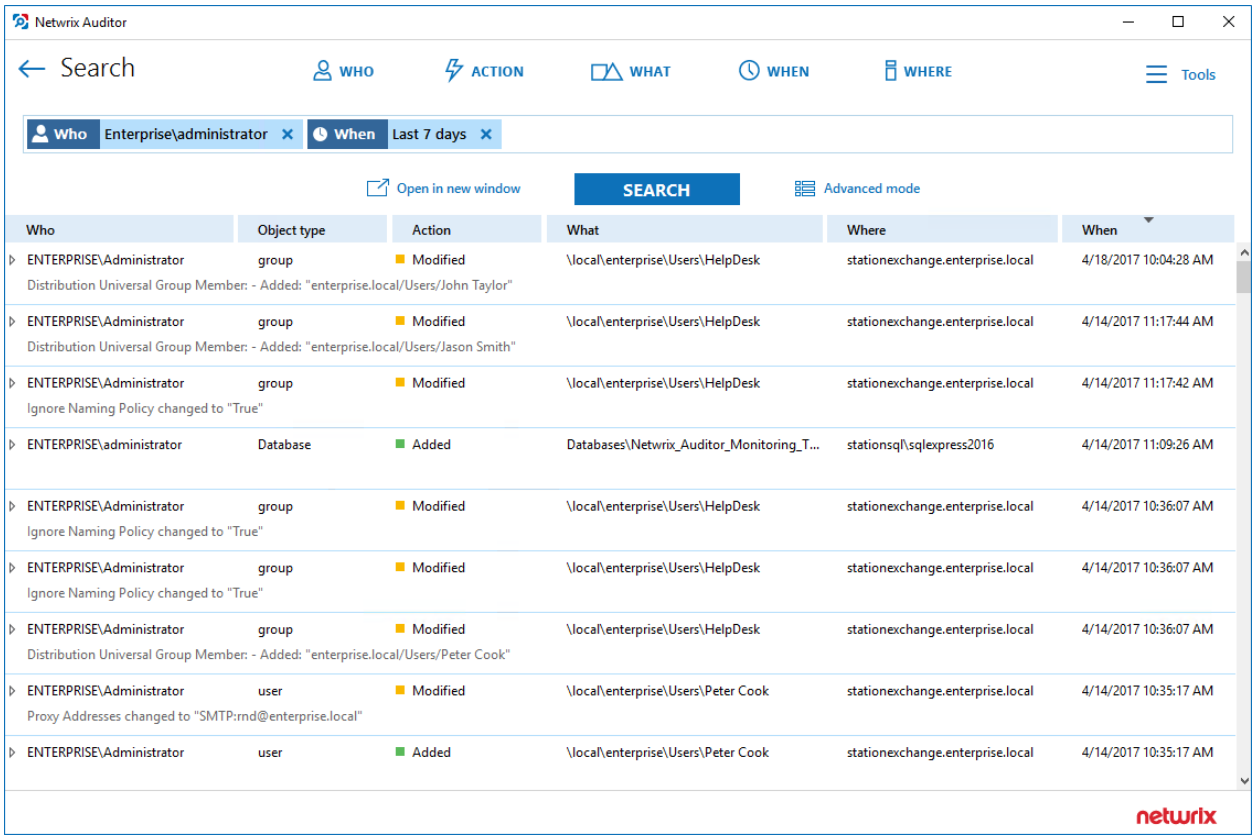
Besides notifying on changes a daily basis, Netwrix Auditor brings security intelligence into your IT infrastructure and enables complete visibility.

The technology works as follows: Netwrix Auditor can be configured to write collected audit trails to the SQL-based Audit Database and the file-based Long-Term Archive. Netwrix Auditor uses data stored in the Audit Database to generate reports, trigger alerts, and run data searches.



The product provides a variety of predefined reports for each data source that help you keep track of all changes in your IT infrastructure and validate compliance with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.). A straight-forward and interactive search interface allows a user to run custom searches, while alerts keep you notified on critical changes.

To review intelligence data, you must be assigned the Global administrator or Global reviewer role in the product, or the Reviewer role on the plan. See Role-Based Access and Delegation for more information.



NOTE: To employ reports, alerts, and interactive search capabilities, you must configure Audit Database settings for each monitoring plan. Also, make sure all databases that store audit data reside on the same default SQL Server instance. Otherwise, this data will not be available in the search results and reports.

Review the following for additional information:

- Investigations
- Netwrix Auditor Intelligence Guide

8. Settings

In the **Settings** section, you can configure general 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. Review the following for additional information:

- Audit Database
- Long-Term Archive
- Investigations
- Notifications
- Integrations
- Licenses

NOTE: You must be assigned the Global administrator role to modify Netwrix Auditor settings. See Role-Based Access and Delegation for more information.

8.1. Audit Database

If you want to leverage your security intelligence data, generate reports, and run the interactive searches, Audit Database settings must be properly configured. The Audit Database settings include default SQL Server, SSRS, and retention settings, and settings specific to each monitoring plan.

Normally, Audit Database settings are configured when you create a first monitoring plan. The SQL Server instance you specified is set as default and settings are listed on the **Settings** → **Audit Database** tab. Later, when you create other monitoring plans these settings prepopulate fields on the **Audit Database** step of the wizard.

To review and update default Audit Database settings (including SQL Server, SSRS, retention settings), navigate to **Settings** → **Audit Database**. If you have not specified the default settings before, click **Configure**.

Review the following for additional information:

Option	Description
Default SQL Server settings	Define the default Audit Database location and connection information, etc. See To configure default SQL Server settings for more information. **NOTE:** Netwrix Auditor allows you to specify settings for each monitoring plan individually. To specify custom settings (e.g., use a different account or authentication type), navigate to the monitoring plan's settings. See

Option	Description
	Fine-Tune Your Plan and Edit Settings for more information.
Database retention	Can be configured if you want audit data to be deleted automatically from your Audit Database after a certain period of time. These settings are common and cannot be modified for a certain plan. See To configure database retention for more information.
SQL Server Reporting Services settings	Define the Report Server URL and account used to upload data to Report Server. These settings are common and cannot be modified for a certain plan. See To configure SSRS settings for more information.

To 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. **NOTE:** If you have more than one Netwrix Auditor Server running in your network, make sure to configure them to use different SQL Server instances. The same SQL Server instance cannot be used to store audit data collected by several Netwrix Auditor Servers.
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. **NOTE:** This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role. See Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password.

To configure database retention

On the **Settings** → **Audit Database** tab, review settings and click **Modify** under the **Database retention** section.

Option	Description
Clear stale data when a database retention period is exceeded / Set a database retention period to clear stale data	Select if you want audit data to be deleted automatically from your Audit Database after a certain period of time.
Store audit data in database for	Specify the number of months for which audit data will be stored. Data is deleted automatically when its retention period is over. By default, it is set to 180 days.

To 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 be used to connect to SSRS. Make sure this account is granted the **Content Manager** role on the Report Server.
Password	Enter a password.

8.2. 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**.

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.

Option	Description
	Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Long-Term Archive service account as well. **NOTE:** 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. Additional procedures are required if you upgraded Netwrix Auditor from 8.0. See the article for details.
Keep audit data for (in months)	Specify how long data will be stored. By default, it is set to 120 months. Data will be deleted automatically when its retention period is over. If the retention period is set to *0*, data will be automatically stored for the last 4 data collections for most of the data sources (event if the retention period is set to *0* data on SQL Server, file servers and Windows Server changes will be stored for the last 2 data collections, and 7 data collections for user activity).
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. **NOTE:** 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: • The **List folder / read data**, **Read attributes**, **Read extended attributes**, **Create files / write data**, **Create folders / append data**, **Write attributes**, **Write extended attributes**, **Delete subfolders and files**, and **Read permissions** advanced permissions on the folder where the Long-Term Archive is stored • The **Change** share permission and the **Create files / write data** folder permission on file shares where report subscriptions are saved **NOTE:** Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Long-Term Archive service account as well.

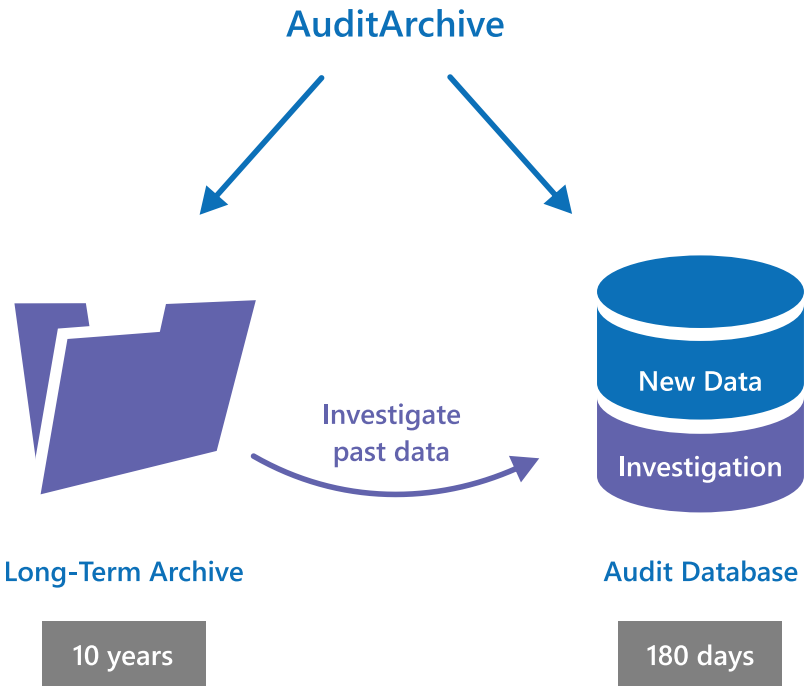
NOTE: Netwrix Auditor informs you if you are running out of space on a system disk where the Long-Term Archive is stored by default. You will see events in the **Netwrix Auditor System Health** log once the free disk space starts approaching minimum level. When the free disk space is less than 3 GB all

Netwrix services will be stopped (except for services responsible for user activity, SharePoint and syslog auditing).

8.3. 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.

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.

Option	Description
	NOTE: 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 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. **NOTE:** 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. **NOTE:** This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role. See Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password.
Clear imported data	Select to delete all previously imported data. **NOTE:** 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

Option	Description
	Audit Database. Netwrix Auditor lists monitoring plans that are currently available in the product configuration. **NOTE:** 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**.

8.4. Notifications

Basically, the SMTP 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**. Review the following for additional information:

- To modify SMTP Settings
- To configure the product to notify you about critical events

To modify SMTP Settings

Navigate to **Default SMTP settings** 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. **NOTE:** It is recommended to 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 the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL authentication	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. **NOTE:** The option is not available for auditing User Activity as well Netwrix Auditor tools.

NOTE: You can configure Activity Summary frequency, format and delivery time for each monitoring plan individually. See Fine-Tune Your Plan and Edit Settings for more information.

To configure the product to notify you about critical events

1. Navigate to the **Product health notice settings** and click **Modify**.
2. Specify emails where notifications on critical system state will be sent.

To learn more about product heath, review Netwrix Auditor System Health event log—a proprietary log that contains information on the product activity and data collection status. See Monitor Netwrix Auditor System Health for more information.

8.5. 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**: Centralize auditing and reporting by feeding Netwrix Auditor with audit data from any existing on-premises or cloud applications. All of your audit data will be centrally stored and ready for reporting.
- **Data out**: Get the most from your SIEM investment by feeding more granular audit data into your HPE ArcSight, Splunk, IBM QRadar or other solution, thus increasing the signal-to-noise ratio. Moreover, you can also feed the granular audit data from Netwrix Auditor into critical IT processes, such as change management or ticketing, to further automate and streamline operations.

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. See Netwrix API for more information.

NOTE: In Netwrix Auditor 9.0, Netwrix has updated API schemas. Make sure to check and update your custom scripts and add-ons.

To learn more about Integration API capabilities, refer to Netwrix Auditor Integration API Guide.

8.6. Licenses

The **Licenses** tab allows you to review the status of your current licenses, update them and add new licenses.

To update or add a license

1. Click **Update**.
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.

8.6.1. 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. To ensure that licenses are calculated correctly (per heartbeat) by Netwrix, perform the following steps:

1. Create organizational units within audited domains and add there service accounts you want to exclude from license count.
2. On the computer where Netwrix Auditor Server resides, navigate to *Netwrix Auditor installation folder\Netwrix Auditor\Administrative Console* and locate **MSP.xml**.
3. In **MSP.xml**, provide the following:

   - **CustomInstanceIdentificator**—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).

     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.

     NOTE: Netwrix gathers the following information about MSP licenses: identifier, license key and license count.

   - **ServiceAccount Path**—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.

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
"	**"**

Symbol	XML entity
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

5. Navigate to *Netwrix Auditor installation folder\Netwrix Auditor\Administrative Console* and start **Netwrix.NAC.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.NAC.MSPTool.exe** every time you update **MSP.xml**.

9. Address Specific Tasks with Netwrix Auditor Tools

9.1. Manage Users with Netwrix Auditor Inactive User Tracker

Netwrix 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.

Review the following for additional information:

- To create monitoring plan to audit inactive users
- To review report on inactive users

To create monitoring plan to audit inactive users

1. Navigate to **Start** → **Netwrix Auditor** → **Netwrix Auditor Inactive Users Tracker**.
2. On the main page, you will be prompted to select a monitoring plan. Click **Add** to add a new monitoring plan.
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 users whose accounts/passwords are going to expire in the specified number of days. Use semicolon to separate several addresses.

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 Netwrix Auditor Installation and Configuration Guide.
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.

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.
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.

Option	Description
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.

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.
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.

7. Navigate to the **Notifications** tab and complete the following fields:

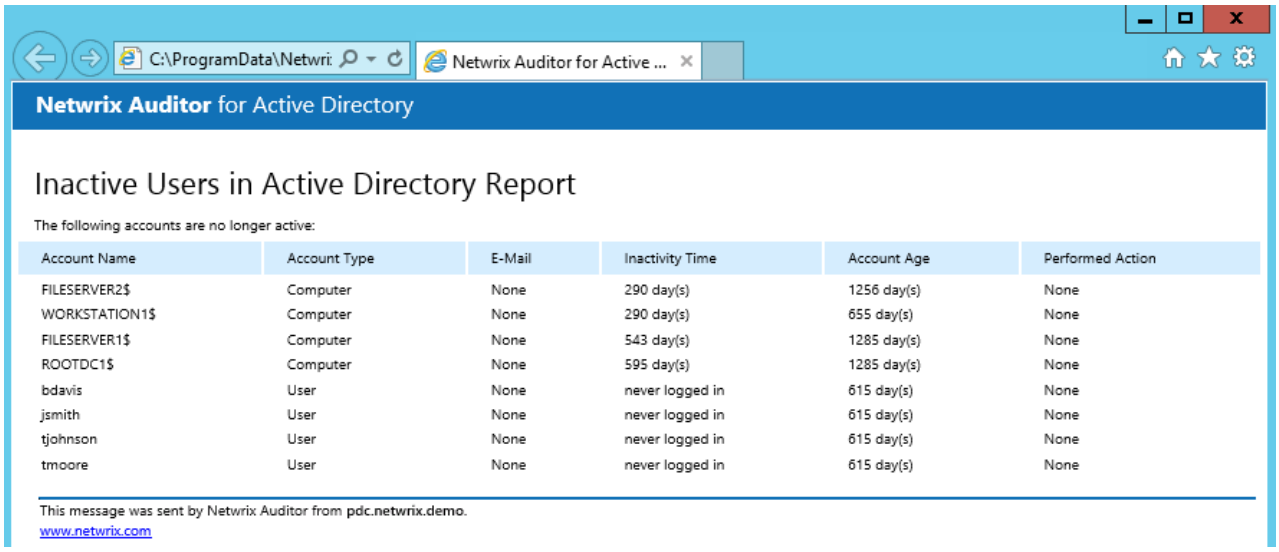
Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.

Option	Description
Sender address	Enter the address that will appear in the **From** field. **NOTE:** It is recommended to click **Verify**. 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 the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

8. If you want to save your current configuration, click **Save**.

To review report on inactive users

1. Click **Generate** next to **Generate report on inactive users** to view report immediately.



9.2. Alert on Passwords with Netwrix Auditor 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.

Review the following for additional information:

- To configure password expiration alerting
- To review Password Expiration Report

To configure password expiration alerting

1. Navigate to **Start** → **Netwrix Auditor** → **Netwrix Auditor Password Expiration Notifier**.
2. On the main page, you will be prompted to select a monitoring plan. Click **Add** to add a new monitoring plan.
3. Configure basic parameters as follows:

Option	Description
Enable password expiration alerting	Select the checkbox to discover expiring passwords 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 users whose accounts/passwords are going to expire in the specified number of days. Use semicolon to separate several addresses.

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 Netwrix Auditor Installation and Configuration Guide.

Option	Description
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.
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.

5. Navigate to the **Actions** tab and complete the following fields:

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 **<group> 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.
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.
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.
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.
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.

  NOTE: If the **Pager** property of an AD User contains a full email address, Provider Name will be ignored.

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. **NOTE:** It is recommended to click **Verify**. 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 the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Display the following **From address** in email notifications	Enter the address that will appear in the "*From*" field in email notifications.

Option	Description
	NOTE: 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.

7. Navigate to the **Advanced** tab and complete the following fields:

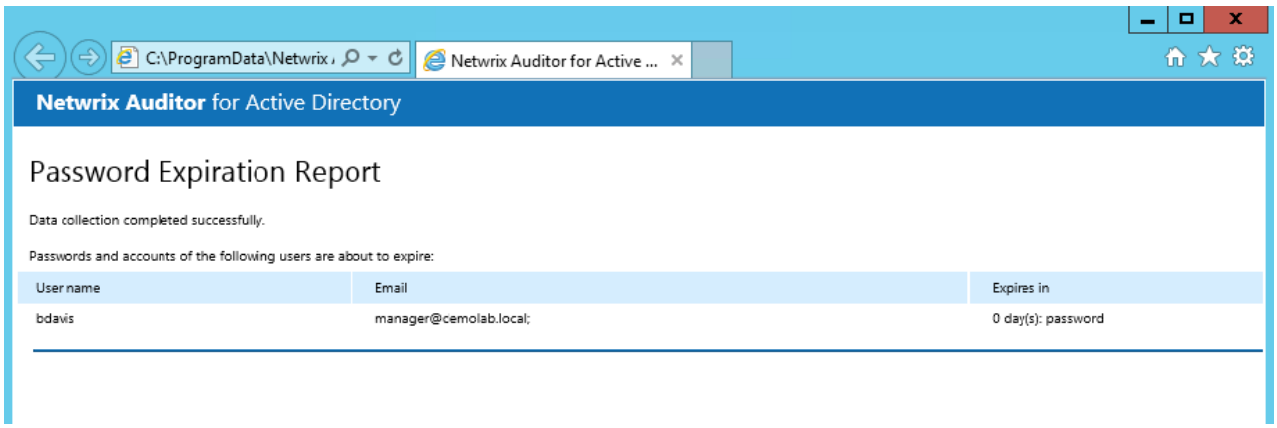
Option	Description
Modify scheduled task start time	The default start time of the scheduled task is 3.00 AM every day. Click **Modify** to configure custom schedule.
Customize the report template	Click **Customize** to edit the notification template, for example, modify the text of the message. You can use HTML tags when editing a template.
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.

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.



9.3. Monitor Events with Netwrix Auditor 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 Netwrix Auditor.

Review the following for additional information:

- Create Monitoring Plans to Audit Event Logs
- Configure Audit Archiving Filters for Event Log
- Create Alerts for Event Log
- Create Alerts for Non-Owner Mailbox Access Events
- Review Past Event Log Entries
- Import Audit Data with the Database Importer

9.3.1. Create Monitoring Plans to Audit Event Logs

Review the following for additional information:

- To configure monitoring plan for auditing event logs
- To review the Event Log Collection Status email

To configure monitoring plan for auditing event logs

1. Navigate to **Start** → **Netwrix Auditor** → **Netwrix Auditor Event Log Manager**.
2. On the main page, you will be prompted to select a monitoring plan. Click **Add** to add new plan.

   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**. • Click **Exclude** to specify domains, OUs, and containers you do not want to audit. **NOTE:** 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**.

NOTE: 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.

3. 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 Netwrix Auditor Installation and Configuration Guide.
Audit archiving filters	Define what events will be saved to the Long-Term Archive or the Audit Database. Refer to Configure Audit Archiving Filters for Event Log 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 detailed instructions on how to configure Netwrix Auditor Event Log Manager alerts.

4. 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. **NOTE:** It is recommended to click **Verify**. 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 the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

5. 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.

   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. **NOTE:** 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.

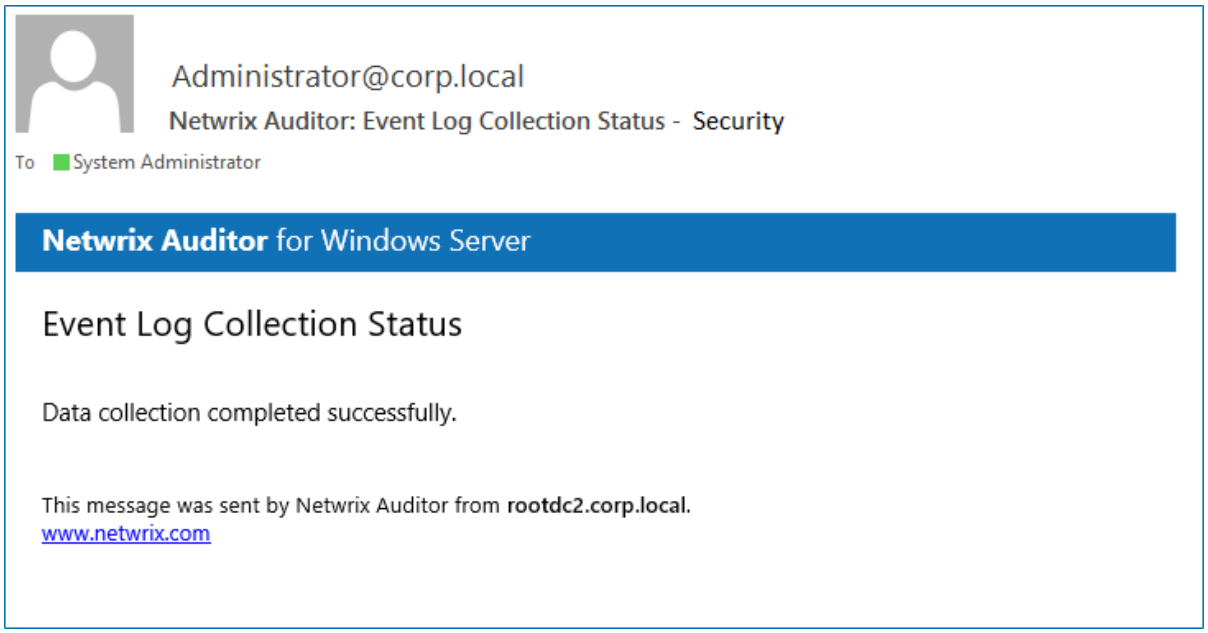
   NOTE: You cannot edit SQL Server settings for **Netwrix Auditor Event Log Manager**.

6. 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.

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.



9.3.2. 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.

To configure audit archiving filters, perform the following:

- To create or modify an audit archiving filter, see To create or edit an audit archiving filter.
- 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.

To create or edit an audit archiving filter

1. On the **Audit archiving filters** page, click **Add** or select a filter and click **Edit**.
2. Complete the fields. Review the following for additional information:

Option	Description
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) or **Administrative Tools** (Windows 2012 R2 and below) → **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. **NOTE:** 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). **NOTE:** 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. **NOTE:** 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

Option	Description
	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. **NOTE:** 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. **NOTE:** 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. **NOTE:** 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**.

9.3.3. 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**.

To create new alert

1. In the **Alerts** window, click **Add** to start new alert.
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.
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.

   NOTE: The **%ManagedObjectName%** variable will be replaced with your monitoring plan name.
4. On the **Event filters** step, specify an event that will trigger the alert.

   Complete the **Event Filters** wizard. Complete the following fields:

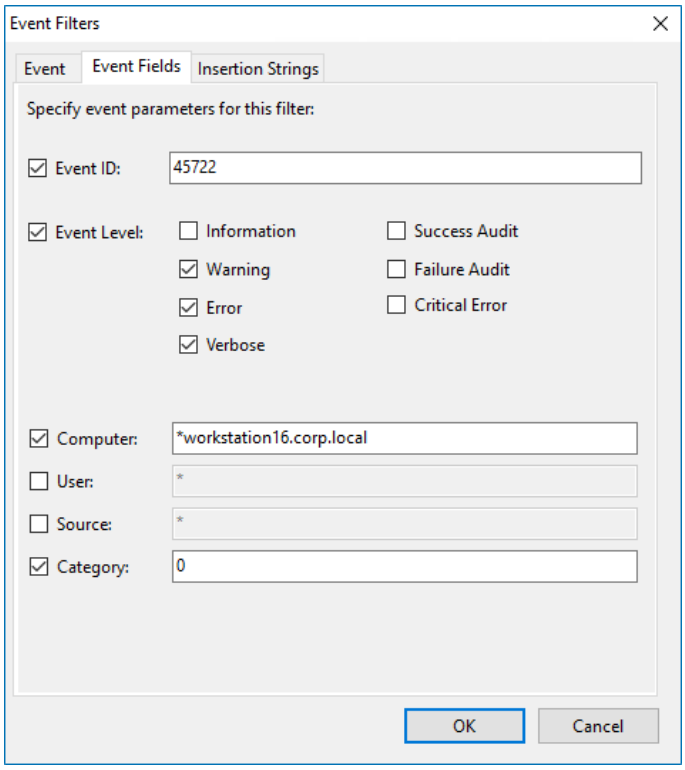
- In the **Event** tab:

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) or **Administrative Tools** (Windows 2012 R2 and below) → **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 does not collect the **Analytic** and **Debug** logs, so you cannot configure alerts for these logs. **NOTE:** 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. **NOTE:** If you want to specify several computers, you can define a mask for this parameter. Below is an example of a mask:

Option	Description
	• * - 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. **NOTE:** 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. **NOTE:** 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**.

5. Click **OK** to save the changes and close the **Event Filters** dialog.

9.3.4. 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.

Review the following for additional information:

- To create alerts for non-owner mailbox access events
- To review event description

To create alerts for non-owner mailbox access events

NOTE: 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 Create Monitoring Plans to Audit Event Logs for more information.

1. Create a monitoring plan in Netwrix Auditor Event Log Manager.
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*".
3. Navigate to the **Monitored computers** list and add a server where your Exchange organization resides.
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.
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.

   NOTE: Specify alert recipient if you want the alert to be delivered to a non-default email.
6. Navigate to **Event Filters** and click **Add** to specify an event that will trigger the alert.
7. 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

ID	Description	Access Type (as displayed in XML view of event details)
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

See To review event description for more information.

- 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 **Insertion String**.

Click **OK** to save the changes and close the **Event Filters** dialog.

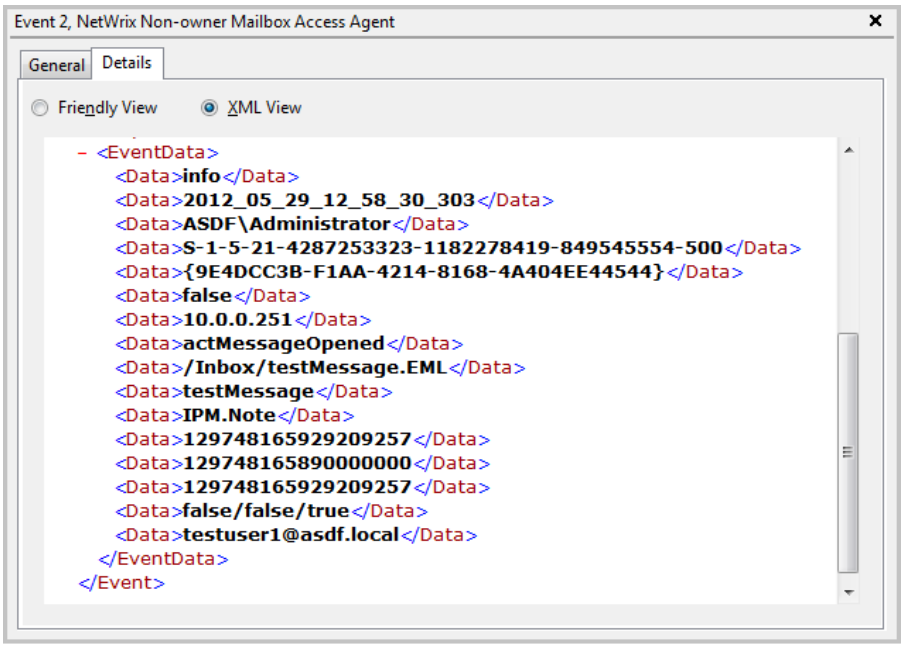
8. In the **Netwrix Auditor Event Log Manager** wizard, navigate to **Notifications** section and specify the email address where notifications will be delivered.

   NOTE: It is recommended to click **Verify**. The system will send a test message to the specified email address and inform you if any problems are detected.

9. 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.
10. Click **Save** to save your changes. If an event occurs that triggers an alert, an email notification will be sent immediately to the specified recipients.

To 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
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

Event ID	Access type (String 8)	Strings	Description
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.
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

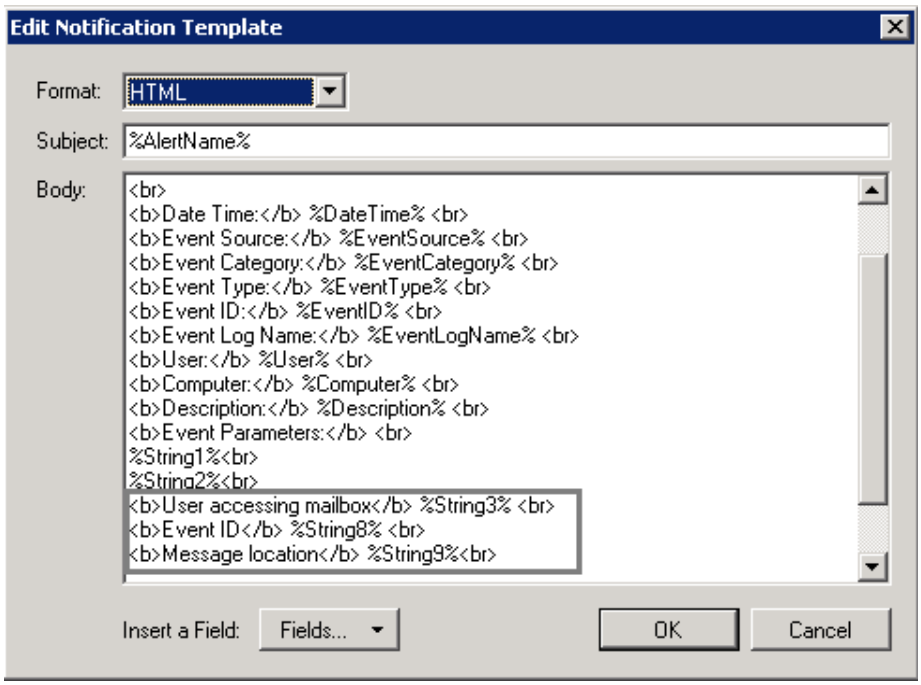
Event ID	Access type (String 8)	Strings	Description
		String12	The destination folder URL
		String13	The message type: IPM.Note— Email, IPM.Contact – contact, etc.
10	actFolderMoveCopy	Strings 9 -13	The string descriptions for the folder are similar to those for messages.
14	actFolderCreated	String9	The new folder URL

NOTE: 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



9.3.5. Review Past Event Log Entries

Netwrix Auditor Event Log Manager collects event log entries and stores them to the Audit Archive. To review past events, do the following:

1. On the main Netwrix Auditor Event Log Manager page, click **View** next to **View collected events**.
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.

9.3.6. Import Audit Data with the Database Importer

1. On the main Netwrix Auditor Event Log Manager page, click **Import Data**.
2. Select a monitoring plan and the time range for which you want to import data.
3. Click **Import**.

9.4. Roll Back Changes with Netwrix Auditor 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. Perform the following procedures:

- Modify Schema Container Settings
- Roll Back Unwanted Changes

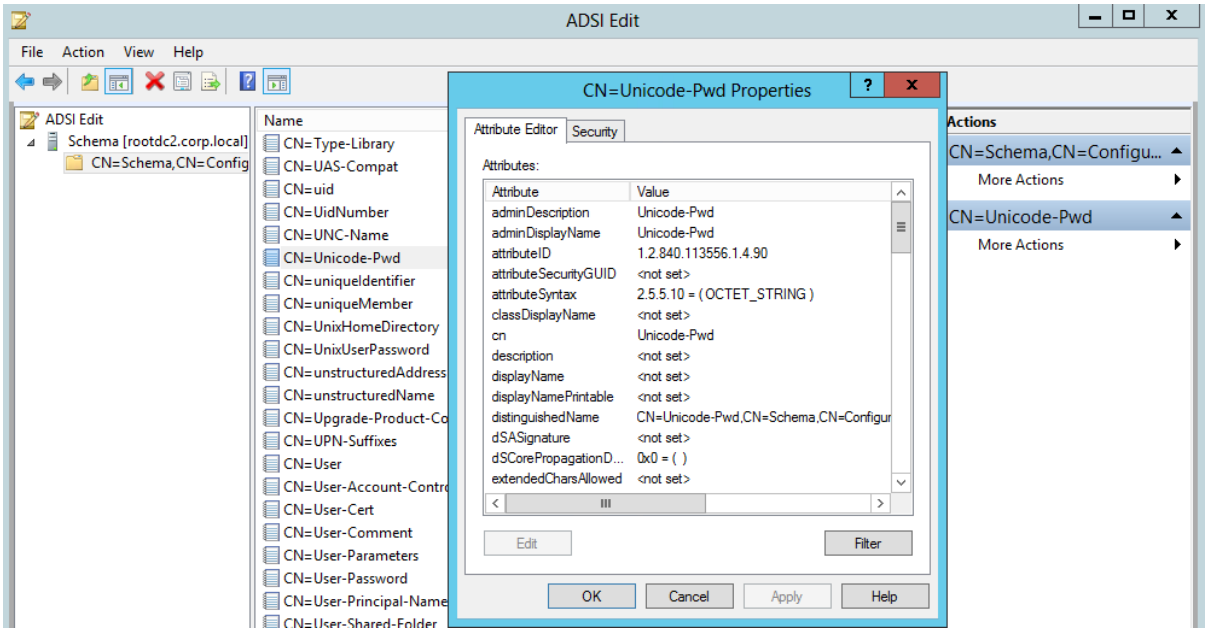
9.4.1. Modify Schema Container Settings

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.

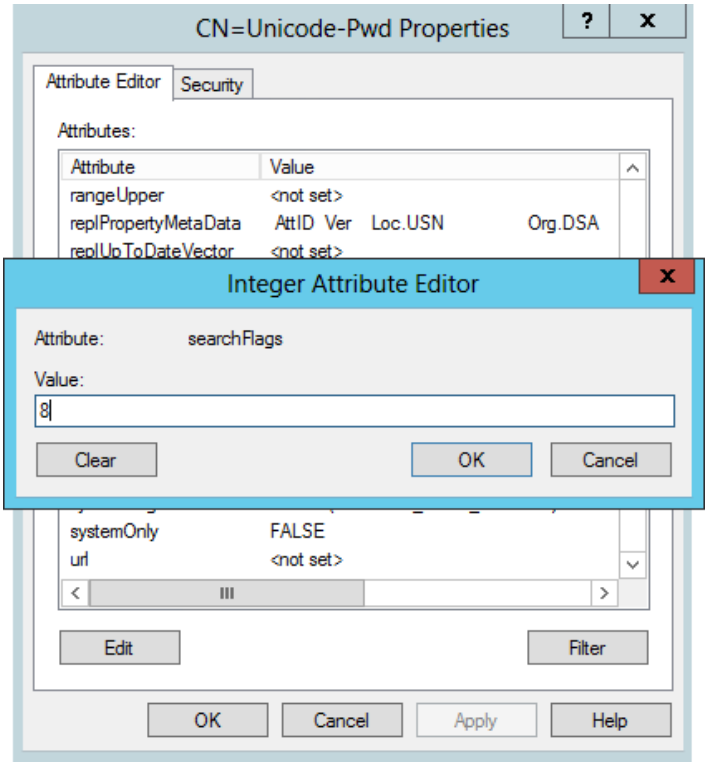
To modify schema container settings

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

1. Navigate to **Start** → **Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **ADSI Edit**.
2. Right-click the **ADSI Edit** node and select **Connect To**. In the **Connection Settings** dialog, enable **Select a well-known Naming Context** and select **Schema** from the drop-down list.
3. Expand the **Schema your_Root_Domain_name** node. Right-click the **CN=Unicode-Pwd** attribute and select **Properties**.



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.

9.4.2. Roll Back Unwanted Changes

1. Navigate to **Start** → **Netwrix Auditor** → **Netwrix Auditor Object Restore for Active Directory**.
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.
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

Option	Description
	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.

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.
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.
6. Wait until the tool has finished restoring the selected objects. On the last step, review the results and click **Finish** to exit the wizard.

10. Additional Configuration

This chapter provides instructions on how to fine–tune Netwrix Auditor using the additional configuration options. Review the following for additional information:

- Monitor Netwrix Auditor System Health
- Exclude Objects From Auditing Scope
- Fine–tune Netwrix Auditor Using Registry Keys
- Automate Sign-in to Netwrix Auditor Client
- Customize Branding

10.1. Monitor Netwrix Auditor System Health

When an error occurs, a system administrator or support engineer must determine what caused this error and prevent it from recurring. For your convenience, Netwrix Auditor records important events in the proprietary **Netwrix Auditor System Health** log. The log can be viewed in two ways:

- When issues encountered during data collection. Click **Details...** in the **Status** column and select **View Health Log**.

  OR

- Open Health Log manually:

  1. On the computer where Netwrix Auditor Server resides, navigate to **Start** → **All Programs** → **Event Viewer**.
  2. In the **Event Viewer** dialog, navigate to **Event Viewer (local)** → **Applications and Services Logs** → **Netwrix Auditor System Health** log.

There are three types of events that can be logged:

Event Type	Description
Information	An event that describes the successful operation beginning and/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

Event Type	Description
	data source.

Review the following for additional information:

- Start Auditing the Netwrix Auditor System Health Log
- Alert on Netwrix Auditor Server Health Status
- Review the Netwrix Auditor System Health Report

10.1.1. Start Auditing the Netwrix Auditor System Health Log

To enable monitoring of Netwrix Auditor events, you need to create a monitoring plan for auditing event logs in **Netwrix Auditor Event Log Manager** standalone tool.

To configure the Netwrix Auditor System Health log auditing

NOTE: The procedure below describes the basic steps, required for creation of the monitoring plan that will be used to collect data on Netwrix Auditor health status events. See Create Monitoring Plans to Audit Event Logs for more information.

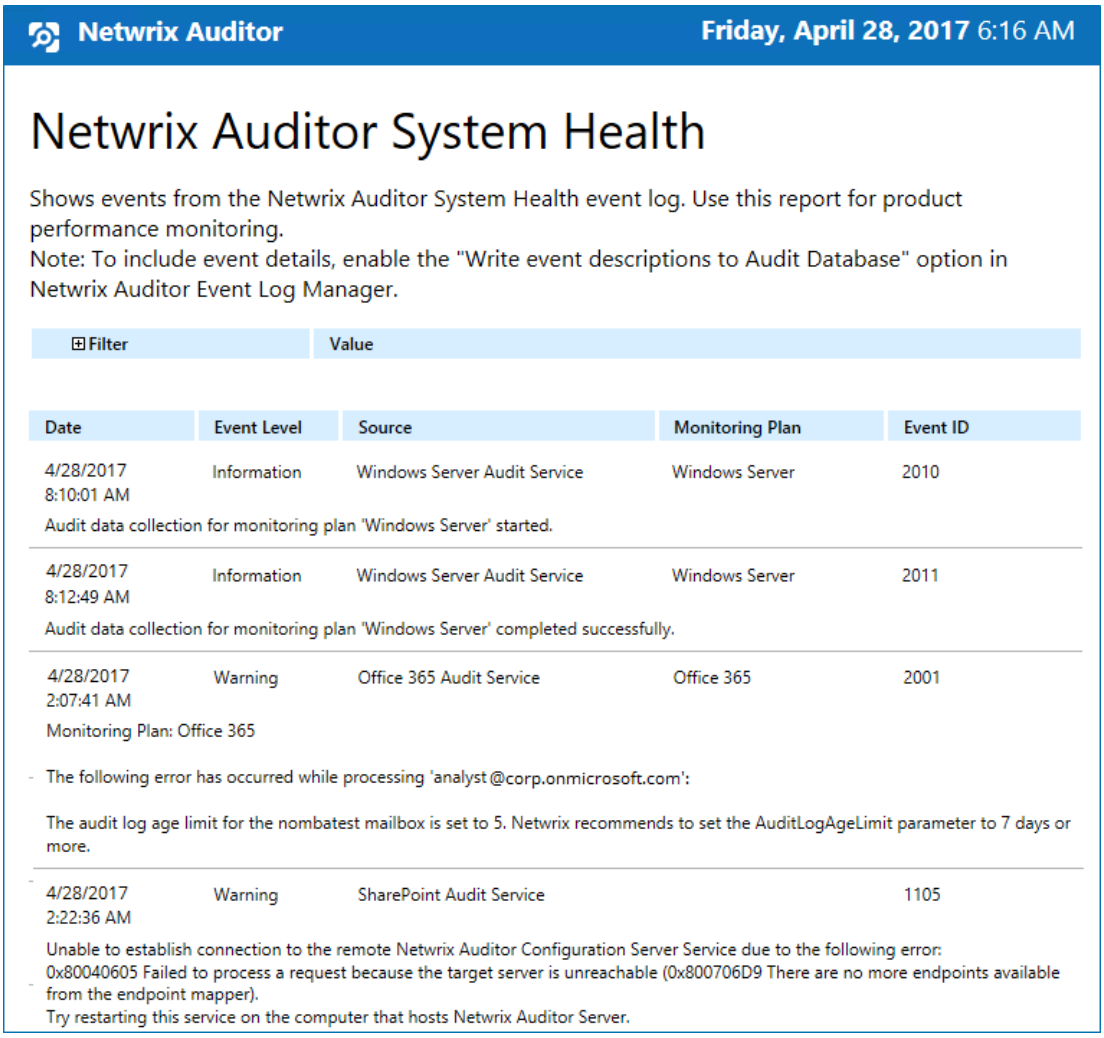
1. Start Netwrix Auditor Event Log Manager and create the new monitoring plan.
2. Make sure that the **Enable event log collection** checkbox is selected. Specify the name for the new monitoring plan, for example, *"Netwrix Auditor Health Status"*.
3. Navigate to the **Monitored computers** list and add a server where the Netwrix Auditor Server resides.

   NOTE: 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. See Audit Database for more information.
4. Click **Configure** next to **Audit archiving filters** and select the **Netwrix Auditor System Health Log** filter in the **Inclusive Filters** list.

10.1.2. Review the Netwrix Auditor System Health Report

Netwrix Auditor provides a special report designed for reviewing Netwrix Auditor health status (successful and failed data collections, warnings, errors, etc.). Do the following to review the **Netwrix Auditor System Health** report:

1. In Netwrix Auditor client, navigate to **Reports** → **Windows Server** → **Event Log**.
2. Select the **Netwrix Auditor System Health** report and click **View**.



Netwrix Auditor Friday, April 28, 2017 6:16 AM

Netwrix Auditor System Health

Shows events from the Netwrix Auditor System Health event log. Use this report for product performance monitoring.
Note: To include event details, enable the "Write event descriptions to Audit Database" option in Netwrix Auditor Event Log Manager.

Filter	Value

Date	Event Level	Source	Monitoring Plan	Event ID
4/28/2017 8:10:01 AM	Information	Windows Server Audit Service	Windows Server	2010
Audit data collection for monitoring plan 'Windows Server' started.				
4/28/2017 8:12:49 AM	Information	Windows Server Audit Service	Windows Server	2011
Audit data collection for monitoring plan 'Windows Server' completed successfully.				
4/28/2017 2:07:41 AM	Warning	Office 365 Audit Service	Office 365	2001
Monitoring Plan: Office 365 The following error has occurred while processing 'analyst@corp.onmicrosoft.com': The audit log age limit for the nombatest mailbox is set to 5. Netwrix recommends to set the AuditLogAgeLimit parameter to 7 days or more.				
4/28/2017 2:22:36 AM	Warning	SharePoint Audit Service		1105
Unable to establish connection to the remote Netwrix Auditor Configuration Server Service due to the following error: 0x80040605 Failed to process a request because the target server is unreachable (0x800706D9 There are no more endpoints available from the endpoint mapper). Try restarting this service on the computer that hosts Netwrix Auditor Server.				

10.1.3. Alert on Netwrix Auditor Server Health Status

You can configure alerts to be triggered by important events in the **Netwrix Auditor System Health** log.

To create alerts to be notified on Netwrix Auditor Health Status

NOTE: The procedure below describes the basic steps, required for creation of the monitoring plan that will be used to collect data on Netwrix Auditor health status events. See Create Monitoring Plans to Audit Event Logs for more information.

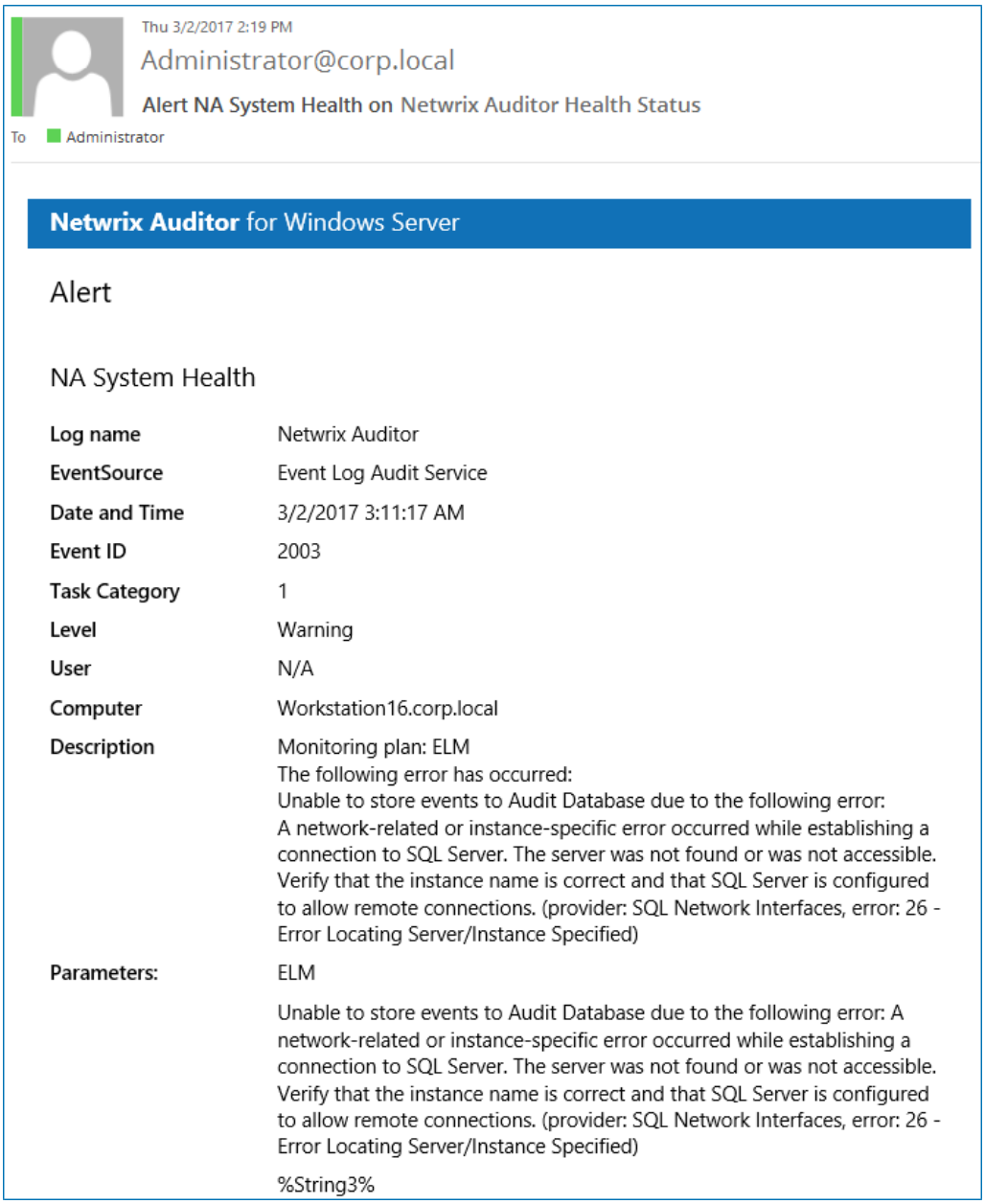
1. Start Netwrix Auditor Event Log Manager and create the new monitoring plan.
2. Make sure that the **Enable event log collection** checkbox is selected. Specify the name for the new plan, for example, *"Netwrix Auditor Health Status"*.
3. Navigate to the **Monitored computers** list and add a server where the Netwrix Auditor Server resides.

4. On the **General** tab, click **Configure** next to **Alerts**. Make sure the predefined alerts are disabled. Click **Add** to create anew alert.
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.

   NOTE: Specify alert recipient if you want the alert to be delivered to a non-default email.
6. Navigate to **Event Filters** and click **Add** to specify an event that will trigger the alert.
7. Complete the **Event Filter** dialog.
   - In the **Event** tab, specify the filter name and description. In the **Event Log** field select the **Netwrix Auditor** log.
   - In the **Event Fields** tab, select event levels that will trigger the alert.

   Click **OK** to save the changes and close the **Event Filters** dialog.
8. In the **Netwrix Auditor Event Log Manager** wizard, navigate to **Notifications** section and specify the email address where notifications will be delivered.

   NOTE: It is recommended to click **Verify**. The system will send a test message to the specified email address and inform you if any problems are detected.
9. In the **Audit Archiving filters**, select the **Netwrix Auditor System Health** as the inclusive filter.
10. Click **Save** to save your changes. If an event occurs that triggers an alert, an email notification will be sent immediately to the specified recipients.



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%

10.2. Exclude Objects from Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the auditing scope. This can be helpful if you want to reduce time required for the data collection, reduce the disk space, required to store the collected data and customize your reports and data searches.

To exclude data from the auditing scope, perform the following procedures:

- Exclude Data from Active Directory Auditing Scope
- Exclude Data from Azure AD Auditing Scope
- Exclude Data from Exchange Auditing Scope

- Exclude Data from Exchange Online Auditing Scope
- Exclude Data from File Servers Auditing Scope
- Exclude Data from SharePoint Auditing Scope
- Exclude Data from SharePoint Online Auditing Scope
- Exclude Data from SQL Server Auditing Scope
- Exclude Data from VMware Auditing Scope
- Exclude Data from Windows Server Auditing Scope
- Exclude Data from Event Log Auditing Scope
- Exclude Data from Group Policy Auditing Scope
- Exclude Data from Inactive Users Auditing Scope
- Exclude Data from Logon Activity Auditing Scope
- Exclude Data from Password Expiration Auditing Scope

10.2.1. Exclude Data from Active Directory Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Active Directory auditing scope.

To exclude data from the Active Directory auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - 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, Netwrix Auditor does not show any data in the **Details** column in the Activity	`Object type:property:` For example, to show a group description on this group's creation, add the following line: `group:description:`

File	Description	Syntax
	Summary emails. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.	

allowedpathlist.txt	Contains a list of AD paths to be included in Activity Summaries, reports, and search results.
	
	This file can be used, for example, if you only want to monitor specific OU(s) inside your AD domain, but not the entire domain. In this case, 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.
		`Path`
		
		NOTE: The path must be provided in the same format as it is displayed in the **What** column.
		
		For example, to monitor only the **Users** OU in domain **CORP**, add the following line:
		
		`\local\corp\Users\*`
		
		In the omitpathlist.txt file, specify the wildcard (*)

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. In this case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, then specify the OU (s) you want to audit in the allowedpathlist.txt file, and then specify the paths you want to exclude from within them in the **omitallowedpathlist.txt** file.
		`Path`
		
		NOTE: The path must be provided in the same format as it is displayed in the **What** column.
		
		For example, to monitor the **Users** OU, but to exclude users **jsmith** and **pbrown**, do the following:
		
		1. Add the wildcard (*) to the **omitpathlist.txt** file.
		2. Add the following line to the **allowedpathlist.txt** file: `*\Users\*`
		3. Add the following lines to the **omitallowedpathlist.txt** file:
		
		`*\pbrown`
		
		`*\jsmith`

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` **NOTE:** 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` **NOTE:** 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 Activity Summaries, reports, and search results.	`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:
		
		`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

File	Description	Syntax
		Summary emails.
omitsnapshotpathlist.txt	Contains a list of AD paths to be excluded from AD snapshots.	`Path` **NOTE:** 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` **NOTE:** 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`.
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, Netwrix 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	`object type:property:`

File	Description	Syntax
	deleted AD objects. When an object is deleted, Netwrix 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.	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`

10.2.2. Exclude Data from Azure AD Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Azure AD auditing scope or modify the way it will be displayed.

To exclude data from the Azure AD auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Azure AD Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported.
   - 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 Azure AD search results, reports and Activity Summaries.	`user@tenant.com`

File	Description	Syntax
adomiteventuserlist.txt	Contains a list of users whose user names you want to exclude from Azure AD 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 Azure AD 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". **NOTE:** 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 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 “Azure AD object” object type.
		`operation = object type`
		
		For example:
		
		`add owner to group = Group`

omitproplist.txt	Contains a list of object classes and attributes to be excluded from Azure AD search results, reports and Activity Summaries.	`classname.attrname` **NOTE:** 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	`object=friendlyname`
		
		`object.property=friendlyname`
		
		For example:

File	Description	Syntax
	results, reports, and Activity Summaries.	`*.PasswordChanged = Password Changed`
proptypes.txt	Defines how values will be displayed in the Details columns in Azure AD search results, reports, and Activity Summaries.	For example: `*.Role.DisplayName = MultiValued`

10.2.3. Exclude Data from Exchange Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Exchange auditing scope. In addition, you can exclude data from non-owner access auditing.

- To exclude data from Exchange auditing scope
- To exclude users or mailboxes from the Mailbox Access auditing scope

To exclude data from Exchange auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - 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`

File	Description	Syntax

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:
		`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`
		NOTE: 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

File	Description	Syntax
		available, possible causes are that Public stores are not mounted and the Information Store service is not running. ID no: c1030af3", add `*c1030af3*` to the file.

omitexchangeserverlist.txt	Defines Exchange 2010 and above servers to be excluded from data collection.	`FQDN_server_name`
		For example:
		`mailserver01.ent.local`

omitstorelist_ecr.txt	Contains a list of classes and attributes names to be excluded from Exchange snapshots.	`object_type.property_name`
		NOTE: 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 auditing scope

Netwrix Auditor allows specifying users and mailboxes that you do not want to audit for non-owner mailbox access events. To do this, edit the **mailboxestoexclude.txt**, **userstoexclude.txt**, and **agentomitusers.txt** files.

1. Navigate to the *%Netwrix Auditor installation folder%\Non-owner Mailbox Access Reporter for Exchange* folder.
2. Edit **mailboxestoexclude.txt**, **userstoexclude.txt**, or **agentomitusers.txt** files, based on the

following guidelines:

- Each entry must be a separate line.
- Wildcards (* and ?) are supported.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description
mailboxestoexclude.txt	This file contains a list of mailboxes and folders that must be excluded from reports. You can specify a 'Mailbox_Name', a 'Mailbox_Name/Folder_Name', or use wildcards (*/Folder_Name). In the last example, the specified folder will be excluded in all mailboxes. If the Netwrix Auditor Mailbox Access Core Service is disabled, the 'Mailbox_Name/Folder_Name' lines are ignored.
userstoexclude.txt	This file contains a list of users in the *DOMAIN\username* format, who must be excluded from reports if they perform non-owner access to mailboxes (audit data on these users will still be stored in the snapshots). If a user is removed from this list, the information on this user's actions can be viewed with the Report Viewer.
agentomitusers.txt	This file contains a list of users in the *DOMAIN\username* format, 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 affect reports and snapshots only if **Use Core Service to collect detailed audit data** is enabled.

10.2.4. Exclude Data from Exchange Online Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Exchange Online auditing scope.

To exclude data from Exchange Online Auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Exchange Online Auditing* folder.
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{*}`
		`DiscoverySearchMailbox{*}`
		`FederatedEmail.*`
		NOTE: 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:

File	Description	Syntax
		`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`

10.2.5. Exclude Data from File Servers Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Windows File Server, NetApp Filer and EMC Storage auditing scope.

To exclude data from Windows File Server, NetApp Filer and EMC Storage auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\File Server Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (*, ?) are supported. For example, you can use * for a class name to specify an attribute for all classes.
   - Lines that start with the # sign are treated as comments and are ignored.
   - A backslash (\) must be put in front of (*), (?) and (,) if they are a part of an entry value.

File	Description	Syntax

omitcollectlist.txt	Contains a list of objects to be excluded from being audited.	`monitoring plan name,server name,resource path`
		NOTE: 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/warnings to be	`monitoring plan name,server name,error text`
		For example:
		`*,productionserver1.corp.local,*Access is denied*`

File	Description	Syntax
	omitted from logging to the Netwrix Auditor System Health event log.	

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`
		
		NOTE: 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 AuditArchive 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`
		
		NOTE: 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`

omitstoreprocesslist.txt	Contains a list of	`monitoring plan name,resource path,executable path`

File	Description	Syntax
	processes to be excluded from being stored to the AuditArchive and showing up in reports.	**NOTE:** Only local applications can be excluded. For example: `*,*,*notepad.exe`

10.2.6. Exclude Data from SharePoint Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the SharePoint auditing scope.

To exclude data from SharePoint auditing scope

1. Navigate to the *%ProgramData%\Netwrix Auditor\Netwrix Auditor for SharePoint\Configuration* folder and locate yourmonitoring plan.

   NOTE: If you have several monitoring plans for auditing SharePoint farms, configure omitlists for each monitoring plan separately.

2. Edit the *.txt files, based on the following guidelines:

   - Each entry must be a separate line.
   - A wildcard (*) is supported, except for **omiteventloglist.txt**.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitscstorelist.txt	Contains a list of site collections to be excluded from audit data collection.	`http(s)://URL` **NOTE:** 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.

File	Description	Syntax
		For example: `https://siteColl*`

omitwastorelist.txt	Contains a list of web applications to be excluded from audit data collection.	`http(s)://URL`
		NOTE: 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/`

omiteventloglist.txt	Contains a list of event IDs to be excluded from the Netwrix Auditor System Health event log.	`event ID`
		For example:
		`1001`
		NOTE: Only add known error or warning events, otherwise you may lose important data.

omitviewstorelist.txt	Contains lists and list items to be excluded from being audited for read access.	`URI Reference`
		NOTE: Only specify URI reference to a list or list item without `https:\\<siteCollection_name>` part.
		For example:
		`*list/document.docx`

omituserviewstorelist.txt	Contains a list of user or service accounts to be excluded from read access auditing.	`Login name` For example: SHAREPOINT\System

10.2.7. Exclude Data from SharePoint Online Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the SharePoint Online auditing scope.

To exclude data from SharePoint Online auditing scope

1. Navigate to the *%ProgramData%\Netwrix Auditor\Netwrix Auditor for SharePoint Online\Configuration* folder and locate your monitoring plan.

   NOTE: If you have several monitoring plans for auditing SharePoint Online, configure omitlists for each monitoring plan separately.

2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported, except for **omiteventloglist.txt**.
   - 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:
		`1001`
		NOTE: 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 audited 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 auditing.	Provide user name in the UPN format. For example: `account@example.*.com`

10.2.8. Exclude Data from SQL Server Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the SQL Server auditing scope.

To exclude data from the SQL Server auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\SQL Server Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitlogonlist.txt	Contains a list of logons to be excluded from being audited.	`monitoring plan name,SQL Server instance,logon type,account,workstation,application name`
		
		NOTE: 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 types to be excluded from Activity	`object_type_name` For example:

File	Description	Syntax
	Summaries and reports. **NOTE:** This .txt file has no effect on SQL logons auditing. Use the omitlogonlist.txt to exclude SQL logons from being audited.	`Database` `Column`
omitpathlist.txt	Contains a list of resource paths to the objects to be excluded from Activity Summaries and reports. In this case data is still being collected and saved to the AuditArchive.	`Server_instance:resource_path` where `resource_path` is shown in the **What** column in the reports. 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 audited and stored to the AuditArchive.	`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. • `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`.

File	Description	Syntax
omitstorelist.txt	Contains a list of objects you want to exclude from being stored to the AuditArchive. **NOTE:** This .txt file has no effect on SQL logons auditing. Use the omitlogonlist.txt to exclude SQL logons from being audited.	`server_instance.resource_path` where `resource_path` is shown in the **What** column in the reports.
omittracelist.txt	Contains a list of SQL Server instances you do not want to enable SQL tracing on. In this case the "Who", "Workstation" and "When" values will not be reported correctly (except for content changes). **NOTE:** If you enabled auditing of SQL logons, SQL trace for these logons will be created anyway.	`server\instance name`

pathtotracelogs.txt	Contains a list of SQL Server instances whose traces must be stored locally.	`SQLServer\Instance|UNC path`
		
		For example:
		
		`server\instance|C:\Program Files\Microsoft SQL Server\MSSQL\LOG\`

File	Description	Syntax

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`

10.2.9. Exclude Data from VMware Auditing Scope

You can fine-tune Netwrix Auditor by specifying various data types that you want to exclude/include from/in the VMware reports.

To exclude data from VMware auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\VMware Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - 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` **NOTE:** 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 **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	`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:*.config.cpuAllocation.shares.shares`.

File	Description	Syntax
	is set to certain value.	
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` **NOTE:** `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.`

10.2.10. Exclude Data from Windows Server Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Windows Server auditing scope.

To exclude data from the Windows Server auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Windows Server Auditing* folder.
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 audited.
	
	NOTE: If you want to restart auditing these objects, remove them from the
		`monitoring plan name,server name,class name,property name,property value`
		
		NOTE: `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`

File	Description	Syntax
	omitcollectlist.txt and run data collection at least twice.	`#*,*,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:
		`*,productionserver1.corp.local,*Access is denied*`

omitreportlist.txts	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,*,*,*,*`

omitstorelist.txt	Contains a list of objects to be excluded from being stored to the AuditArchive 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\\User_Feed_Synchronization*,*`

10.2.11. Exclude Data from Event Log Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Event Log auditing scope.

To exclude data from the Event Log auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Event Log Management* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - 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.*`

10.2.12. Exclude Data from Group Policy Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Group Policy auditing scope. To do it, edit the **omitobjlist_gp.txt**, **omitproplist_gp.txt** and **omituserlist_gp.txt** files.

To exclude data from the Group Policy Auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.
2. Edit **omitobjlist_gp.txt**, **omitproplist_gp.txt** and **omituserlist_gp.txt** files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported and can be used to replace any number of characters.
   - 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`.

File	Description	Syntax
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`.

10.2.13. Exclude Data from Inactive Users Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Inactive User auditing scope.

To exclude data from the Inactive Users auditing scope

1. Navigate to the *%ProgramData%\Netwrix Auditor\Inactive Users Tracker* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - 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. Netwrix 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 Netwrix Auditor functions properly.	`Full DNS name` or `NetBIOS name` **NOTE:** IP addresses are not supported.
omitoulist.txt	Contains a list of	`Path`

File	Description	Syntax
	organizational units to be excluded from processing.	For example: `*OU=C,OU=B,OU=A*`

10.2.14. Exclude Data from Logon Activity Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the Logon Activity auditing scope.

To exclude data from the Logon Activity auditing scope

1. Navigate to *%ProgramData%\Netwrix Auditor\NLA\Settings* folder and locate your monitoring plan.

   NOTE: If you have several monitoring plans for auditing Logon Activity, configure omitlist for each monitoring plan separately.

2. Edit the **Settings.cfg** file 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 <!-- are treated as comments and are ignored.

Configuration String	Description	Syntax

`<n n="DCOmitList">`	Contains a list of DCs to be excluded from being audited.	`DC_name`
		For example:
		`<v v= "*ROOTDC1*"/>`

`<n n="DCCompression ServiceUsage">`	Determines whether to enable network traffic compression for a Domain Controller or not.
	NOTE: If configured,
		`DC_name`
		`v="1"`—enables the Netwrix Auditor Logon Activity Compression Service for the specified DC
		`v="0"`—disables Netwrix Auditor Logon Activity Compression Service for the specified DC
		For example:
		`<a n="*ROOTDC1*" v="0"/>`

Configuration String	Description	Syntax
	overrides the **Enable network traffic compression** option in monitoring plan configuration.	

`<n n="UserOmitList">`
`<a n="Names">`
	Contains a list of users to be excluded from being audited. 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 audited. Allows specifying a user by security identifier (SID).	`User SID`
		For example:
		`<v v="*S-1-5-21-1180699209-877415012-318292XXXX-XXX*"/>`

NOTE: 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**"**

Symbol	XML entity
' 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

10.2.15. Exclude Data from Password Expiration Auditing Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from auditing and alerting on password expiration.

To exclude data from the Password Expiration Alerting auditing scope

1. Navigate to the *%Netwrix Auditor install folder%\Password Expiration Alerting* folder.
2. Edit the **omitoulist.txt** file, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitoulist.txt	Contains a list of organizational units to be excluded from processing.	`Path`
		For example:
		`*OU=C,OU=B,OU=A*`

10.3. Fine-tune Netwrix Auditor with Registry Keys

You can fine-tune Netwrix Auditor using the registry keys as described below. This functionality is currently available for the following data sources:

- Registry Keys for Auditing Active Directory
- Registry Keys for Auditing Exchange

- Registry Keys for Auditing File Servers
- Registry Keys for Auditing Windows Server
- Registry Keys for Auditing Event Log
- Registry Keys for Auditing Group Policy
- Registry Keys for Auditing Password Expiration
- Registry Keys for Auditing Inactive Users
- Registry Keys for Auditing Logon Activity

10.3.1. Registry Keys for Auditing Active Directory

Review the basic registry keys that you may need to configure for auditing Active Directory 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
LogonResolveOptions	Defines what will be shown in the Workstation field: • 2—MAC address • 4—FQDN or IP address (set by default) • 6—Both

Registry key (REG_DWORD type)	Description / Value
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"
ShortEmailSubjects	Defines whether to contract the email subjects: • 0—No • 1—Yes
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** 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).

10.3.2. Registry Keys for Auditing Exchange

Review the basic registry keys that you may need to configure for auditing 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
LogonResolveOptions	Defines what will be shown in the Workstation field: • 2—MAC address • 4—FQDN or IP address (set by default) • 6—Both
ShortEmailSubjects	Defines whether to contract the email subjects (e.g., Netwrix Auditor: Activity Summary): • 0—No • 1—Yes
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.
ShowReportFooter	Defines whether to display the footer in the Activity Summary

Registry key (REG_DWORD type)	Description / Value
	email: • 0—No • 1—Yes
ShowReportGeneratorServer	Defines whether to display the report generation server in the Activity Summary footer: • 0—No • 1—Yes
ShowSummaryInFooter	Defines whether to display the summary in the Activity Summary footer: • 0—No • 1—Yes
ShowSummaryInHeader	Defines whether to display the summary in the Activity Summary header: • 0—No • 1—Yes
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).

10.3.3. Registry Keys for Auditing File Servers

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

Registry key (REG_DWORD type)	Description / Value
HKEY_ LOCAL_ MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\File Server Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from file servers • [X]— Backups are deleted after [X] hours
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.

10.3.4. Registry Keys for Auditing Windows Server

Review the basic registry keys that you may need to configure for auditing 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

Registry key (REG_DWORD type)	Description / Value
	NOTE: Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.

10.3.5. Registry Keys for Auditing Event Log

Review the basic registry keys that you may need to configure for auditing 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	
ConnectionTimeout	Defines SQL database connection timeout (in seconds).
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager\<monitoring plan name>\ElmDbOptions	
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 **NOTE:** 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:

Registry key (REG_DWORD type)	Description / Value
	• 0—Disabled • 1—Enabled
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

10.3.6. Registry Keys for Auditing Group Policy

Review the basic registry keys that you may need to configure for auditing 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 **NOTE:** 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
IgnoreRootDCErrors	Defines whether to display audit check errors for the root domain

Registry key (REG_DWORD type)	Description / Value
	(when data is collected from a child domain) in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
LogonResolveOptions	Defines what will be shown in the Workstation field: • 2—MAC address • 4—FQDN or IP address (set by default) • 6—Both
ShortEmailSubjects	Defines whether to contract the email subjects (e.g., Netwrix Group Policy Change Reporter: Summary Report – GPCR Report): • 0—No • 1—Yes
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.
ShowReportFooter	Defines whether to display the footer in the Activity Summary email: • 0—No • 1—Yes
ShowReportGeneratorServer	Defines whether to display the report generation server in the Activity Summary footer: • 0—No • 1—Yes
ShowSummaryInFooter	Defines whether to display the summary in the Activity Summary footer: • 0—No

Registry key (REG_DWORD type)	Description / Value
	• 1—Yes
ShowSummaryInHeader	Defines whether to display the summary in the Activity Summary header: • 0—No • 1—Yes
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
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).

10.3.7. Registry Keys for Auditing Password Expiration

Review the basic registry keys that you may need to configure for auditing 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

10.3.8. Registry Keys for Auditing Inactive Users

Review the basic registry keys that you may need to configure for auditing 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

10.3.9. Registry Keys for Auditing Logon Activity

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Logon Activity Auditing	
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes

10.4. Automate Sign-in to Netwrix Auditor Client

Typically, when a user launches the Netwrix Auditor client, he or she must provide connection details. By default, this step is skipped if you start the Netwrix Auditor client on computer that hosts Netwrix Auditor Server. If you want to connect to an instance of Netwrix Auditor Server installed on another computer, you must force the start page to show up. To do it, add special parameters to a product shortcut.

Users who frequently connect to different Netwrix Auditor Servers (e.g., MSP users) installed both locally and remotely, may also leverage shortcuts to automate their sign-in process. The parameters pre-populate the start page with connection details. For security reasons, the password must be typed by a user.

To create a shortcut that will start Netwrix Auditor client with pre-populated connection details

1. Navigate to the Netwrix Auditor client installation directory and locate the **AuditIntelligence.exe** (by default, *C:\Program Files (x86)\Netwrix Auditor\Audit Intelligence\AuditIntelligence.exe).*
2. Create a shortcut for the executable.
3. Right-click a newly created shortcut and select **Properties**.
4. In the **Target** field you will see a path to your executable. Add the following parameters after the path.

   ```
   /s:server_name /u:user_name /specify_creds
   ```

   where:

   - `server_name`—Replace with Netwrix Auditor Server name (computer that hosts Netwrix Auditor Server) or its IP address.
   - `user_name`—Replace with a Netwrix Auditor user who wants to log in.

   For example, the **Target** field will show:

   ```
   "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. When you click the shortcut, the product will start with pre-populated connection details.

10.5. Customize Branding

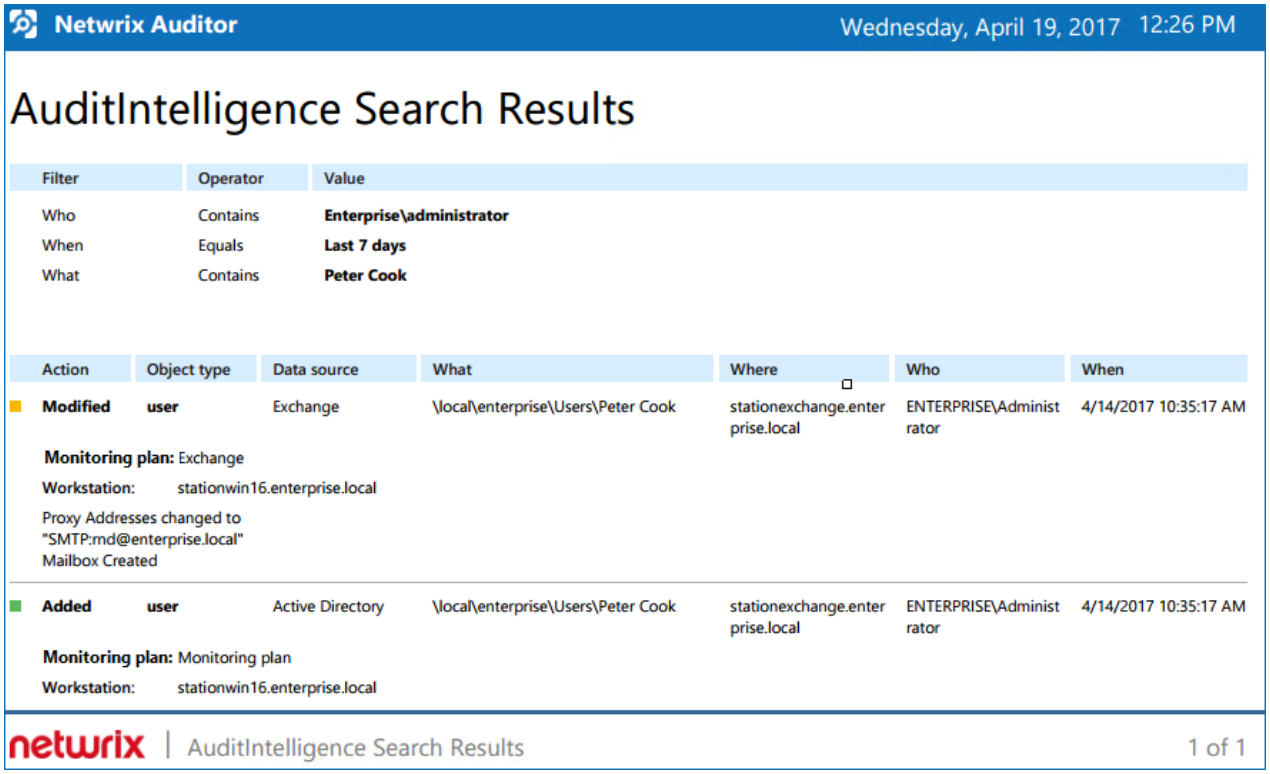
Netwrix Auditor allows customizing look and feel of your reports and exported search results—you can skip Netwrix logo, add your company logo and title. Nonetheless, users are not empowered to customize layout or color scheme.

Review the following for additional information:

- Customize Branding in Exported Search Results
- Customize Branding in Reports

10.5.1. Customize Branding in Exported Search Results

By default, after exporting to pdf the search results look as follows:



Branding can be customized on the Netwrix Auditor client side that means that clients connected to the same Netwrix Auditor Server may have different branding.

To customize branding

1. On the computer where the Netwrix Auditor client is installed, navigate to *%UserProfile%\AppData\Local\Netwrix Auditor\Audit Intelligence\branding.xml*.

   NOTE: The file is recreated automatically after the first data export.

The file contains:

```
<nr>
<n n="\branding_config" t="branding_config">
  <a n="enabled" t="7" v="False"/>
  <a n="header_title" t="2" v="Replace with your title"/>
  <a n="logo_file" t="2" v="Logo.png"/>
  <a n="logo_path" t="2" v="%localappdata%\Netwrix Auditor\Audit
  Intelligence\Resources"/>
</n>
</nr>
```

2. Update the file contents to customize your look and feel.

To..	Do..
Enable branding	In the "enabled" section, replace "False" with "True".
Add your company name in the header	In the "header_title" section, type your company name instead of "Replace with your company title". In this case "Netwrix Auditor" will no longer appear in pdf output.
Add your company logo	1. Prepare a png file with your company logo. Supported size—105x22px. 2. In the "logo_file" section, replace "Logo.png" with a file name. 3. In the "logo_path" section, provide a path to your logo. It is recommended to save your logo to *"%UserProfile%\AppData\Local\Netwrix Auditor\Audit Intelligence\Resources* ". Make sure to create this folder manually. **NOTE:** To skip Netwrix logo without providing your own, keep both sections as it is.

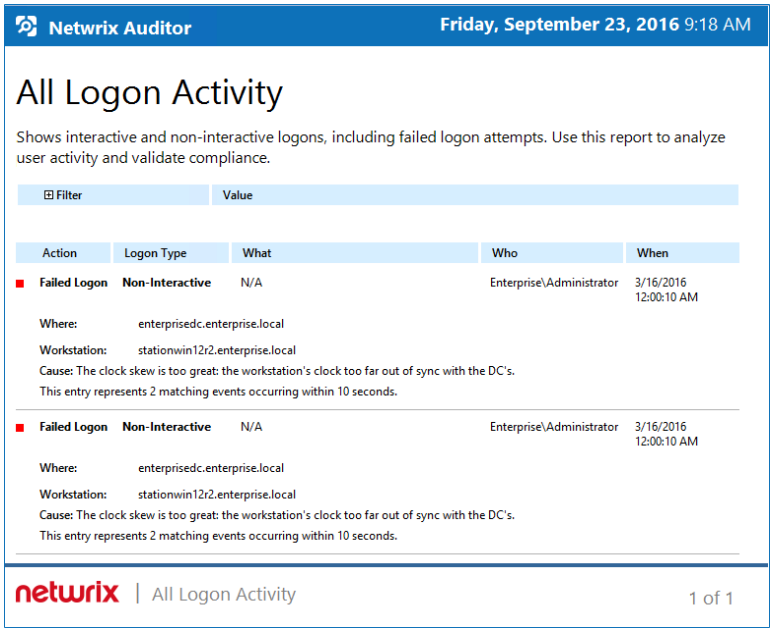
NOTE: The file must be formatted in accordance with XML standard. The following symbols must be replaced with corresponding XML entities: **&** (ampersand), " (double quotes), ' (single quotes), < (less than), and > (greater than) symbols.

Symbol	XML entity
&	**&**
e.g., Ally **&** Sons	e.g., Ally **&** Sons
"	**"**

Symbol	XML entity
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

10.5.2. 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.

To customize branding

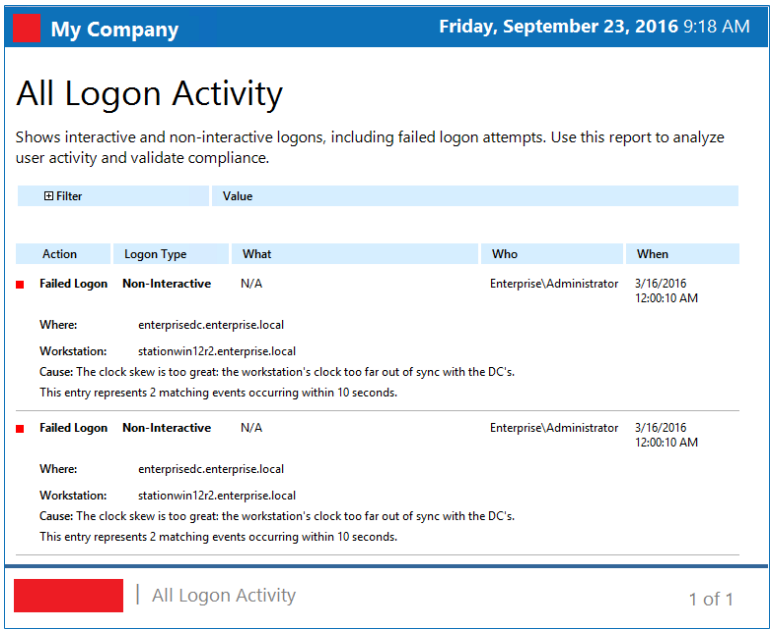
1. On the computer where Netwrix Auditor Server resides, navigate to *C:\Program Data\Netwrix Auditor\Rebranding*.
2. Right-click the **Rebranding.ps1** script and select **Edit**. **Windows PowerShell ISE** will start.

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.
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.

4. Click  (**Run 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.



To restore original look and feel

1. On the computer where Netwrix Auditor Server resides, navigate to the script location.
2. Right-click a script and select **Edit**. **Windows PowerShell ISE** will start.
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.

11. Appendix

11.1. Monitored Object Types, Actions, and Attributes

Review the list of object types, attributes and components audited and reported by Netwrix Auditor.

- Object Types and Attributes Audited in Active Directory
- Object Types and Attributes Audited on File Servers
- Object Types and Attributes Audited on Oracle Database
- Object Types and Attributes Audited on SharePoint
- Object Types and Attributes Audited on SharePoint Online
- Object and Data Types Audited on SQL Server
- Object Types and Attributes Audited on VMware
- Components and Settings Audited on Windows Server
- Object Types and Attributes Audited with Syslog Message Processing Service
- Actions Captured When Auditing Mailbox Access
- Actions and Logon Types Captured When Auditing Logon Activity

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

Action	Data source										
											
											
											
Added	+	+	+*	+	+	+	+	+	+	–	–
Removed	+	+	+*	+	+	+	+	+	+	–	–
Modified	+	+	+*	+	+	+	+	+	+	–	–
Add	–	–	–	+	–	+	–	–	–	–	–

Action	Data source										
	 Active Directory	 Azure AD	 Exchange	 Windows File Servers	 SharePoint	 Oracle Database	 SQL Server	 VMware	 Windows Server	 Logon Activity	 User Activity
	 Group Policy		 Exchange Online	 EMC	 SharePoint Online						
				 NetApp							
(failed attempt)											
Remove (failed attempt)	–	–	–	+	–	+	–	–	–	–	–
Modify (failed attempt)	–	–	–	+	–	+	–	–	+	–	–
Read	–	–	+*	+	+	+	–	–	–	–	–
Read (failed attempt)	–	–	–	+	–	+	–	–	–	–	–
Renamed	–	–	–	+	+**	+	–	–	–	–	–
Moved	–	–	+*	+	+	–	–	–	–	–	–
Rename (failed attempt)	–	–	–	+	–	+	–	–	–	–	–
Move (failed attempt)	–	–	–	+	–	–	–	–	–	–	–
Checked in	–	–	–	–	+	–	–	–	–	–	–
Checked out	–	–	–	–	+	–	–	–	–	–	–

Action	Data source										
											
											
											
Discard check out	–	–	–	–	+	–	–	–	–	–	–
Successful logon	–	+	–	–	–	+	+	–	–	+	–
Failed logon	–	+	–	–	–	+	+	–	–	+	–
Logoff	–	–	–	–	–	+	–	–	–	–	–
Copied	–	–	+*	+	+**	–	–	–	–	–	–
Copy (failed attempt)	–	–	–	+	–	–	–	–	–	–	–
Sent	–	–	+*	–	–	–	–	–	–	–	–
Activated	–	–	–	–	–	–	–	–	–	–	+

NOTE: Actions marked with asterisk (*) are reported when auditing non-owner mailbox access for Exchange or Exchange Online.

For Windows file servers, NetApp appliances, and EMC storages, audited actions vary depending on the file server type and object (file, folder, or share). For detailed information, refer to the table below.

Actions marked with asterisk (**) are reported for SharePoint Online only.

Action	Windows-based			NetApp			EMC		
	file	folder	share	file	folder	share	file	folder	share
Added	+	+	+	+	+	+	+	+	+

Action	Windows-based			NetApp			EMC		
	file	folder	share	file	folder	share	file	folder	share
Add (failed attempt)	+	+	–	–	–	–	+*	+*	–
Modified	+	+	+	+	+	+	+	+	+
Modify (failed attempt)	+	+	+	+	+	–	+	+	–
Moved	+	+	–	+	+	–	+	+	–
Move (failed attempt)	–	–	–	+**	+**	–	+*	+*	–
Read	+	–	+***	+	-	–	+	–	–
Read (failed attempt)	+	+	+	+	+	–	+	+	–
Renamed	+	+	–	+**	+**	–	+*	+*	–
Renamed (failed attempt)	–	–	–	+**	+**	–	+*	+*	–
Removed	+	+	+	+	+	+	+	+	+
Remove (failed attempt)	+	+	–	+	+	–	+	+	–
Copied	+	–	–	+	+	+	+	+	+
Copy (failed attempt)	–	–	–	+	+	+	+	+	+

NOTE: Actions marked with asterisk (*) are reported for EMC Isilon only.

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

By default, actions marked with asterisks (***) are reported for Windows-based file servers as a summary—each entry represents several identical reads occurring from the same workstation within 10 minutes.

11.1.1. Object Types and Attributes Audited in Active Directory

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

NOTE: 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 audited 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.

11.1.2. Object Types and Attributes Audited on File Servers

NOTE: For the Windows-based file servers running Windows Server 2008 or Windows Vista SP2, NetApp appliances, and EMC storages, changes to shares are reported without *who* ("Not applicable" is displayed).

For NetApp appliances and EMC VNX/VNXe storages, the modification of the **Audit** attribute on files and folders is reported without *who* ("System" is displayed).

For entries mentioned above, Netwrix Auditor displays not the actual time when the event occurred but the data collection time.

Due to Windows Server 2008 SP2 limitations, Netwrix Auditor may be unable to retrieve workstation name for failed read attempts made this servers.

Due to Windows limitations, the copy/rename/move actions on remote file shares may be reported as two sequential actions: copy as adding a new file and reading the former file; renaming\moving as removing the former file and adding a new file with the same name. The copy action is not reported on DFS servers.

Refer to the following Microsoft article for more information on attributes marked with *

Review a full list of object types Netwrix Auditor can audit on file servers.

Object type	Attributes
File	• Attributes* • Location • Name

Object type	Attributes

	• Ownership
	• Permissions:
	  • Group Permissions
	  • User Permissions
	• Primary Group
	• Security descriptor control flags
	• Size

Folder	• Attributes*
	
	NOTE: The **Reparse point** attribute content is available for reviewing only when State-In-Time snapshot collection 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

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

- Session ID—GUID generated by the product and can be helpful if you have to review large amount of changes and need to distinguish those made within one session.
- Statement ID—This attribute appears when an object was moved/renamed due to its root object modifications.

11.1.3. Object Types and Attributes Audited on Oracle Database

Review a full list of object types Netwrix Auditor can audit on Oracle Database. If you deployed your Oracle Database in a cluster mode (Oracle Real Application Cluster), a host name also will be reported.

NOTE: 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		
• 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	• Added / Add (Failed attempt) • Modified / Modify (Failed attempt) • Removed / Remove	• Cause (for failed attempts) • Container name** • Database User • Privilege for action

Object type	Actions	Details
• Java	(Failed attempt)	• Program name / Database session requester** • Session ID • Unified policy name**
Logons		
• Logon	• Successful logon / Failed logon • Logoff	• Cause (for failed attempts) • Client IP (only for logon events) • Container name** • Database User • 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**

Object type	Actions	Details
		• 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) • Removed / Remove (Failed attempt)	• Captured SQL statement • Cause (for failed attempts) • Container name** • Database user • 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	• Captured SQL statement

Object type	Actions	Details
	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**
	Rename	
• Object	• Renamed / Rename (Failed attempt)	• Cause (for failed attempts) • Container name** • Database user • New object name • With option • 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**

Object type	Actions	Details
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)	
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

Object type	Actions	Details
	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 • Unified policy name**
	Views	
• View	• Added / Add (Failed attempt) • Removed / Remove	• Cause (for failed attempts) • Container name** • Database user

Object type	Actions	Details
	(Failed attempt)	• 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
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

Object type	Actions	Details
		requester** • Session ID

11.1.4. Object Types and Attributes Audited on SharePoint

Review a full list of object types and attributes Netwrix Auditor can audit on SharePoint.

NOTE: 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***
List	• Permissions*** • Permission Inheritance***
List Item	• Attachments • Permissions*** • Permission Inheritance*** • List Item Properties*
Document	• Document URL • Permissions*** • Permission Inheritance***

Object type	Attributes
	• 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" • 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

Object type	Attributes
Service**	• Name • 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

11.1.5. Object Types and Attributes Audited on SharePoint Online

Review a full list of object types and attributes Netwrix Auditor can audit on SharePoint Online. OneDrive for Business changes are reported as SharePoint Online.

Object type	Attributes
Site Collection	• Site Collection administrators
Document	• Name • Permissions • URL
Site	• Permissions

Object type	Attributes
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
Document Library	• Permissions
Group	• Members • Name
Folder	• Permissions
Sharing Invitation	• Expiration date • Shared with
Access Request	• Expiration date

11.1.6. Object and Data Types Audited on SQL Server

Review a full list of all object and data types Netwrix Auditor can audit on SQL Server.

- Audited Object Types
- Audited Data Types

11.1.6.1. Audited Object Types

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 • Identity • Identity increment • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision

Object type	Attributes
	• 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 • Schema published
Credential	• Id • Identity • Date Created • Date Modified • Name
Database	• Compatibility • Database Size • Database Space Available • Date Created • Date Modified • Extended Properties • File Id

Object type	Attributes
	• File Group • File Name • Growth • Id • Name • Options • Owner • Permissions • 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) • Step • Type
Jobs Schedules	• Date Created • Date Modified • Enabled • ID

Object type	Attributes
	• 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 • Index Key Columns • Padded • Hypothetical • Unique
Keys	• Name • ID • Date Created • Date Modified • MS shipped • Published • Schema published • Disabled • Not for replication

Object type	Attributes
	• Not trusted • Delete referential action • Update referential action • Is system named
Login	• Date Created • Date Modified • Default Database • Default Language • 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) • Lightweight Pooling • Locks • Max Degree Of Parallelism • Max Full-text Crawl Range • Max Server Memory (M)

Object type	Attributes
	• 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 • 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

Object type	Attributes
	• 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 • Id • Name • Role Members
Stored Procedure	• ANSI NULLs • Date Created • Date Modified • Encrypted • Execute us • FOR replication • Id • Name • Permissions • Quoted Identifier • Recompile • Schema

Object type	Attributes
Table	• ANSI NULLs • Date Created • Date Modified • Filegroup • Id • Name • Partition scheme • Permissions • Schema • Table is partitioned • Table is replicated • Text filegroup
Triggers	**NOTE:** 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 • Owned Schemas

Object type	Attributes
	• 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 • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale • Rule

Object type	Attributes
	• 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 • 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

Object type	Attributes
	• Sort Order • View Name
	Logons
SQL logon	• Cause (for failed logons)
Windows logon	• Cause (for failed logons)

11.1.6.2. Audited Data Types

The following list contains the names of all data types audited by Netwrix Auditor:

bigint	hierarchyid	smallint
bit	int	smallmoney
char	float	table
cursor	money	time
date	nchar	timestamp
datetime2	nvarchar	tinyint
datetime	numeric	uniqueidentifier
datetimeoffset	real	varchar
decimal	smalldatetime	xml

11.1.7. Object Types and Attributes Audited on VMware

Review a full list of object types and attributes Netwrix Auditor can audit on VMware.

Object type	Attributes
Virtual Machine	• Snapshot Name • Snapshot Description • Current Snapshot • Power State • Guest State • Virtual Machine Name

Object type	Attributes
	• Guest OS • Guest OS Version • Memory Size (M) • Power Off Type • Suspend Type • 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 • Guest Power Management • Disable Acceleration • Enable Logging • Record Debugging Information • Synchronize guest time with host • Check and upgrade Tools • Hyper-threaded Core Sharing • Swap file Location • Hardware Page Table Virtualization • Force BIOS Setup • Power-on Boot Delay • Power On • Advanced Configuration • Number of virtual processors • Operation mode of guest OS • Notes • Annotation • ResourcePool • Template

Object type	Attributes
	• Connected • Connect at power on • VirtualCdrom Device Type • VirtualCdrom Mode • VirtualParallelPort Port • VirtualParallelPort Connection • VirtualSerialPort Connection • VirtualSerialPort Yield CPU on poll • VirtualSerialPort Near End • VirtualSerialPort Far End • VirtualPCNet32 MAC Address Type • VirtualPCNet32 MAC Address • VirtualPCNet32 Wake on LAN • VirtualPCNet32 IP Address • VirtualPCNet32 Network Adapter Name • VirtualPCNet32 Network Adapter Network • VirtualPCNet32 Network Adapter MAC • VirtualFloppy Device Type • VirtualSCSIController Controller Type • VirtualSCSIController Bus Sharing • VirtualSCSIController Bus Number • VirtualDisr Disk Mode • VirtualDisr Unit Number • VirtualDisr Capacity(K) • VirtualDisr Share Level • VirtualDisr Datastore
Authorization Manager	• Privilege • Authorization Manager Name

Object type	Attributes
Cluster Resource	• Name • VMware HA • VMware DRS • VMware HA Admission Control • VMware HA Isolation Response • VMware HA Restart Priority • VMware HA Number of host failures allowed • VMware HA Advanced Option • VMware DRS Automation Level • VMware DRS Migration threshold • Swap Policy for Virtual Machines • VMware HA Isolation Response • VMware HA Restart Priority • 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 • Available CPU • Available Memory • Available Hosts
Computer Resource	• Name

Object type	Attributes
Datacenter	• Name
Data Store	• Accessible • Name
Folder	• Folder Name
Host System	• Overall Status • Configuration Status • CPU Expandable Reservation • CPU Limit • CPU Reservation • CPU Shares Level • CPU Shares • Memory Expandable Reservation • Memory Limit • Memory Reservation • Memory Shares Level • Memory Shares • Datastore accessible to Host • NTP required • NTP uninstallable • NTP running • NTP policy • NTP Servers • Port Group Allow Promiscuous • Port Group MAC Address Changes • Port Group Forged Transmits • Port Group VLAN ID • Port Group Attached uplink adapter

Object type	Attributes
	• 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 • Service Console IP Address of port
Resource Pool	• Name

11.1.8. Components and Settings Audited on Windows Server

Review a full list of all components and settings Netwrix Auditor can audit on Windows Server.

- General Computer Settings
- Add / Remove Programs
- Services
- Audit Policies
- Hardware
- DHCP configuration
- Removable media**
- Scheduled Tasks
- Local Users and Groups
- DNS Configuration***
- DNS Resource Records***
- File Shares
- Windows Registry Settings

NOTE: A single asterisk is a wildcard that replaces any number of characters.

The **Who** value is reported as *"Not Applicable"* for the components and settings marked with double asterisks (**).

The **Who** value is reported for the components and settings marked with triple asterisks (***) if the DNS server runs Windows Server 2012 R2 with Microsoft update KB2956577 applied.

The **Who** value is reported as *"Not Applicable"* for DHCP server configuration events if DHCP server runs on Windows Server 2008 and below.

For removable storages, the **When** value shows actual time when a change was made and/or a target server was started.

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 • 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

Object type	Attributes
	• Send Alert • System Startup Delay • Write an Event
System Time	• System time changed from ... to ... • Time zone changed **NOTE:** Not supported on Windows Server 2008 SP2 and Windows Server 2008 R2.
	Add / Remove Programs
Add or Remove Programs	• Installed For** • Version
	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	• Added Audit settings

Object type	Attributes
Policy	**NOTE:** 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 • 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

Object type	Attributes
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)
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

Object type	Attributes
	• 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 • Total Tracks • Tracks/Cylinder
IDE**	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Status

Object type	Attributes
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
Network Adapter	• Adapter Type • Configuration Manager Error Code • Default IP Gateway • DHCP Enabled • DHCP Server • DNS Server Search Order • IP Address

Object type	Attributes
	• Last Error Description • Last Error Code • MAC Address • Network Connection Name • Network Connection Status • Service Name • Status
Network Protoco*l*	• 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 • Speed • Part Number • Serial Number
Pointing Device**	• Configuration Manager Error Code • Double Click Threshold • Handedness

Object type	Attributes
	• 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	
Server role	• Added • Removed

Object type	Attributes

DHCP scope	• Type:
	  • IPv4
	  • Multicast IPv4
	  • Superscope for IPv4
	  • IPv6

Removable media**	

Removable Storage Media	**NOTE:** Netwrix Auditor does not report on floppy/optical disk and memory card storage medias.
	• Device class:
	  • CD and DVD
	  • Floppy Drives
	  • Removable Disk
	  • Tape Drives
	  • Windows Portable Devices
	
	NOTE: 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 • Comment • Creator • Enabled • Parameters • Triggers

Object type	Attributes
	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* **
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 • Ds Available • Ds Polling Interval • Ds Tombstone Interval • EDns Cache Timeout

Object type	Attributes
	• 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

Object type	Attributes
DNS Zone***	• Aging State • Allow update • Auto created • Data file name • Ds integrated • 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

Object type	Attributes
DNS Resource Records* **	
DNS AAAA***	• Container name • IPv6 Address • Owner name • Record class • TTL • Zone type
DNS AFSDB***	• Container name • Owner name • 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

Object type	Attributes
	• 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 • 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

Object type	Attributes
	• Signatory field • TTL • Zone type
DNS DS***	• Algorithm • Container name • Data • DigestType • Key tag • Owner name • Record class • TTL • Zone type
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

Object type	Attributes
	• 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
DNS MD***	• Container name • MD host • Owner name • Record class • TTL • Zone type
DNS MF***	• Container name • MF host • Owner name • Record class • TTL

Object type	Attributes
	• 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 • 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

Object type	Attributes
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 • TTL • Zone type
DNS PTR***	• Container name • Owner name • PTR domain name • Record class • TTL

Object type	Attributes
	• 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 • Preference • Record class

Object type	Attributes
	• 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

Object type	Attributes
	• Record class • Text • TTL • Zone type
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

Object type	Attributes
	File Shares
Share	• Access-based enumeration • Caching • Description • Enable BranchCache • Encrypt data access • Folder path • Share permissions • User limit
	Windows Registry Settings
OS Security	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\FileSystem(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\NetworkProvider (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\Print\\Providers\\LanMan Print Services(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SecurePipeServers (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SessionManager\\Environment(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SessionManager\\SubSystems(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SessionManager\\Memory Management(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SessionManager\\Executive(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SessionManager\\KnownDLLs(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\Windows(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Image File ExecutionOptions(|\\.*)

Object type	Attributes
Security Settings	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\DrWatson(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Driver Signing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Non-Driver Signing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\MSDTC(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\NetDDE(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows\\CurrentVersion\\Policies\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Explorer\\BitBucket(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Group Policy(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Installer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\Policies\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\policies\\Network(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\policies\\Ratings(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\policies\\system(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows NT\\CurrentVersion\\AEDebug(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows

Object type	Attributes
	NT\\CurrentVersion\\AsrCommands(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Perflib(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\SeCEdit(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Setup\\RecoveryConsole(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\PCHealth\\ErrorReporting(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Conferencing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\EventViewer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Messenger\\Client(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\SearchCompanion(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\SystemCertificates\\AuthRoot(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\W32time\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows NT\\DCOM(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows NT\\IIS(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows NT\\Printers(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows NT\\Rpc(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\DriverSearching(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Group Policy(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Installer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Internet Connection Wizard(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Network Connections(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Registration Wizard Control(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Peernet(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\ StandardProfile\\IcmpSettings(|\\.*) • HKEY_LOCAL_MACHINE\\System\\Clone(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\Control\\SessionManager(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\WinLogon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\CrashControl (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\FileSystem(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\LSA(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Print\\Providers\\LanManPrint Services\\Servers(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\ProductOptions (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SecurePipeServers\\WinReg(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0- 9]+\\Control\\SessionManager\\kernel(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\WMI\\Security (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Enum(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Hardware Profiles(|\\.*) • HKEY_USERS\\.DEFAULT\\Software\\ Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_USERS\\.Default\\Software\\Microsoft\\NetDDE(|\\.*) • HKEY_USERS\\.Default\\Software\\Microsoft\\ SystemCertificates\\Root\\ProtectedRoots(|\\.*)
Patches	• HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\ Component Based Servicing\\Packages(|\\.*)
Windows Firewall	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\DomainProfile(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\StandardProfile(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\cryptography(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\windows\\safer\\codeidentifiers(|\\.*)
Remote Desktop	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Terminal Server\\WinStations\\RDP-Tcp(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\ Policies\\Microsoft\\Windows NT\\Terminal Services(|\\.*)
File Sharing Settings	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\LanmanServer\\Shares(|\\.*)
USB Devices	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\USBSTOR(|\\.*)
Important Services	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Schedule(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WebClient(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WmiApSrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\upnphost(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AFD(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Alerter(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgmt(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Appmon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\BINLSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\ \Services\\Browser(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Cdrom(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\CiSvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Clipsrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\Application(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\Security(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Fax(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\HTTPFilter(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\IISADMIN(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\IPSEC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\LanManServer\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\LanmanWorkstation\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\LicenseService(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSDTC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSFtpsvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacFile(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacPrint(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Messenger(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MrxSmb(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NTDS(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\NWCWorkstation (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NetBT(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netman(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NntpSvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NtFrs(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\POP3Svc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RDSessMgr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasAuto(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasMan(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteAccess (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteRegistry (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Remote_Storage_Server(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Remote_Storage_User_Link(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RpcLocator(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SMTPSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\SNMPTRAP(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMP(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SharedAccess (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Spooler(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SrvcSurg(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TapiSrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Tcpip(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TermService (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TlntSvr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\W3SVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WZCSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\helpsvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\ldap(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\mnmsrvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\tftpd(|\\.*)
Startup and autorun	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\IniFileMapping(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows\\CurrentVersion\\Run(|\\.*)

To enable auditing of custom registry keys

1. On the computer where Netwrix Auditor Server resides, navigate to *%Netwrix Auditor installation folder%\Windows Server Auditing*.
2. Edit the **customregistrykeys.txt** file.

   Review the following for additional information:

File	Syntax
customregistrykeys. txt	`monitoring plan name, server name, registry key name` • 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.

File	Syntax
	For example: `#*,productionserver1.corp.local,HKEY_LOCAL_MACHINE\\SYSTEM\\RNG`

11.1.9. Object Types and Attributes Audited with Syslog Message Processing Service

Review a full list of object types Netwrix Auditor can collect on Cisco network devices.

NOTE: Details marked with * are specific for their object types and may vary depending on access type, connection details, etc. For example, for the "*Authentication*" object type, the "*Interface*" attribute will be reported if a user tries to access Cisco device via SSH protocol.

Object type	Actions	Details
Cisco ASA devices		
Authentication	• Successful logon / Failed logon	• Facility • Interface* • Kerberos Server* • Message ID • Raw Message • Severity • Source
Configuration	• Add / Added (Failed attempt) • Modified / Modify (Failed attempt) • Read / Read (Failed attempt) • Removed / Remove (Failed attempt)	• Facility • Message ID • Raw Message • Severity • Source
CPU	• Modified / Modify (Failed attempt)	• Facility • Message ID

Object type	Actions	Details
		• Raw Message • Severity • Source
Environment (IPMI)	• Modified / Modify (Failed attempt)	• Facility • Message ID • Raw Message • Severity • Source
GroupPolicy	• Add / Added (Failed attempt)	• Facility • Message ID • Policy Type • Raw Message • Severity • Source
Logon	• Successful logon / Failed logon	• Facility • Message ID • Raw Message • Severity • Source
RAM	• Modified / Modify (Failed attempt)	• Actual • Facility • Message ID • Raw Message • Required • Severity • Source
RIP authentication	• Successful logon /	• Facility

Object type	Actions	Details
	Failed logon	• Interface* • Message ID • Raw Message • Severity • Source
Session	• Session start / Session end	• Facility • Message ID • Private IP* • Raw Message • Severity • Source
URL	• Read / Read (Failed attempt)	• Facility • Message ID • Raw Message • Severity • Source
User	• Modified / Modify (Failed attempt)	• Facility • Message ID • Raw Message • Privilege level • Severity • Source • User Status*
	Cisco IOS	
Logon	• Successful logon • Failed logon	• Facility • Local Port • Raw Message

Object type	Actions	Details
		• Reason • Severity • Source
Configuration	• Read	• Facility • Raw Message • Severity • Source
	• Modified	• Facility • Interface • Raw Message • State • Severity • Source
Environment	• Modified	• Facility • Raw Message • Severity • Source

11.1.10. Actions and Logon Types Captured When Auditing Logon Activity

Review a full list of actions captured when auditing Logon Activity with Netwrix Auditor.

NOTE: For the attributes marked with asterisk (*) *what* changed is not reported.

Action	Object Type	Attributes
Successful Logon	Logon	—
	Interactive Logon	A session was reconnected.

Action	Object Type	Attributes
Failed Logon	Logon*	Cause description.
	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).

11.1.11. Actions Captured When Auditing Mailbox Access

Review a full list of actions captured when auditing mailbox access with Netwrix Auditor:

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 <...>
	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.
	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.**

11.2. Install ADSI Edit

The ADSI Edit utility is used to view and manage objects and attributes in an Active Directory forest. ADSI Edit is required to manually configure audit settings in the target domain. It must be installed on any domain controller in the domain you want to start auditing.

To install ADSI Edit on Windows Server 2008 and Windows Server 2008 R2

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Server Manager** dialog, select **Features** in the left pane, and then click **Add Features**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools** .
4. Click **Next** to proceed to the confirmation page.
5. Click **Install** to enable it.

To install ADSI Edit on Windows Server 2012 and above

1. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
2. In the **Add Roles and Features Wizard** dialog that opens, proceed to the **Features** in the left pane.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **Next** to proceed to the confirmation page.
5. Click **Install** to enable it.

11.3. Install Microsoft SQL Server

This section provides instructions on how to:

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

Netwrix Auditor uses Microsoft SQL Server Reporting Services to run data searches and generate reports on changes to the audited environment and on its point-in-time configuration.

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

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

NOTE: It is recommended to consider the maximum database size in different SQL Server versions and make your choice based on the size of the audited environment. Note that the maximum database size in SQL Server Express editions may be insufficient.

11.3.1. Install Microsoft SQL Server 2014 Express

This section only provides instructions on how to install SQL Server 2014 Express with Advanced Services and configure the Reporting Services required for Netwrix Auditor to function properly. For full installation and configuration instructions, refer to Microsoft documentation.

1. Download SQL Server 2014.
2. Run the installation package and follow the instructions of the wizard until you get to the **Feature Selection** page. On this page, ensure that the **Reporting Services** option is selected under **Instance Features**.
3. Proceed with the wizard until you get to the **Server Configuration** page. On this page, ensure that the **SQL Server Reporting Services** will run under the **Network Service account**, and its startup type is set to *"Automatic"*.
4. Follow the instructions of the wizard to complete the installation.

11.3.2. Verify Reporting Services Installation

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

NOTE: You must be logged in as a member of the **local Administrators** group on the computer where SQL Server 2014 Express is installed.

1. Depending on SQL Server version installed, navigate to **Start** → **All Apps** → **SQL ServerReporting Services Configuration Manager**.
2. In the **Reporting Services Configuration Connection** dialog, make sure that your local report server instance (for example, *"SQLExpress"*) is selected and click **Connect**.
3. In the **Reporting Services Configuration Manager** left pane, select **Web Service URL**. Make sure that **Virtual Directory** is set to *"ReportServer_<YourSqlServerInstanceName>"* (e.g., *ReportServer_SQLEXPRESS* for *SQLEXPRESS* instance) and **TCP Port** is set to *"80"*.
4. In the **Reporting Services Configuration Manager** left pane, select **Database**. Make sure that the **SQL Server Name** and **Database Name** fields contain correct values. If the fields contain incorrect values, click **Change Database** and complete the **Report Server Database Configuration** wizard.
5. In the **Reporting Services Configuration Manager** left pane, select **Report Manager URL**. Make sure **Virtual Directory** is set correctly, and that the URL is valid.

Index