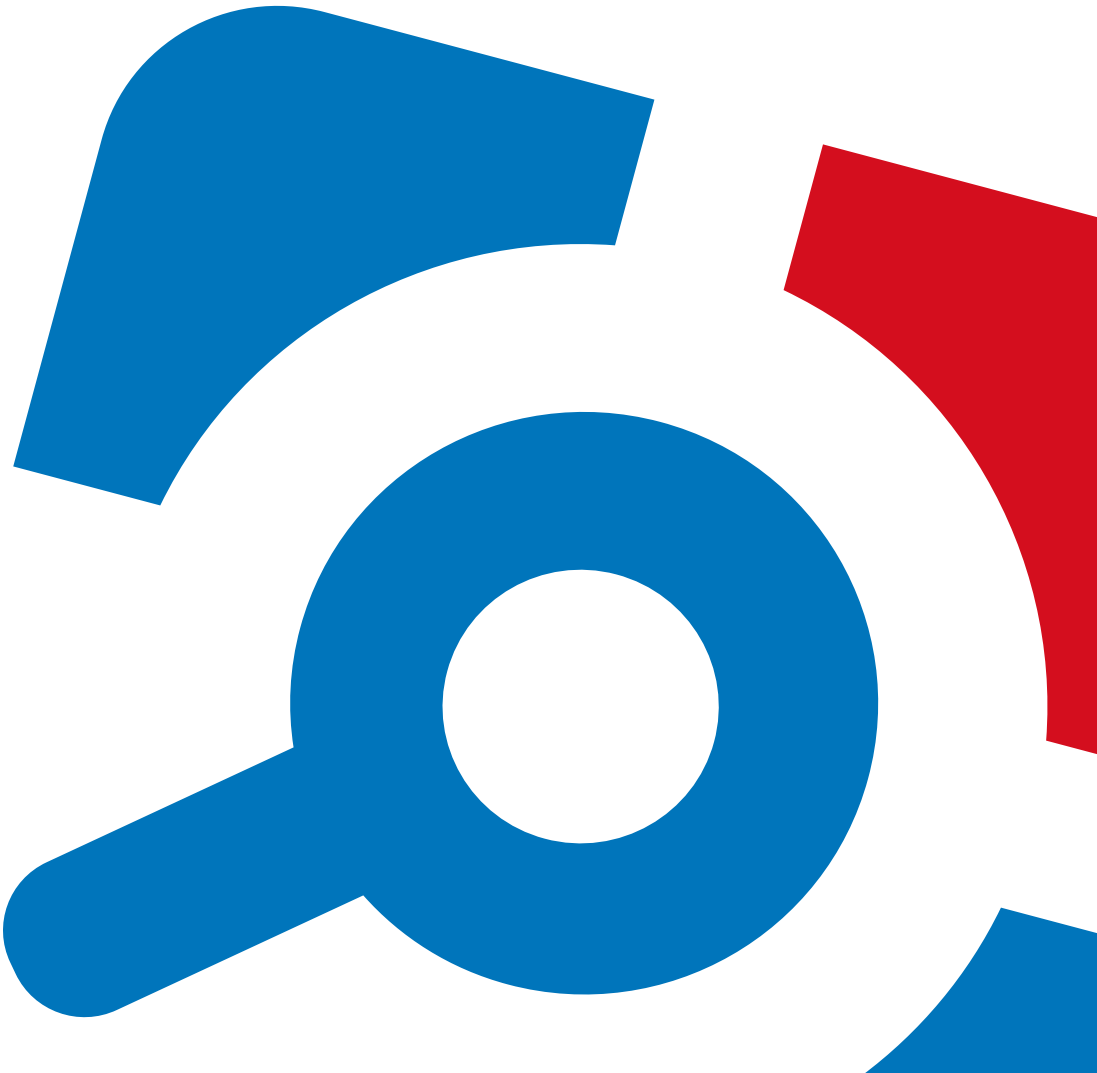
netwrix

Netwrix Auditor

Administration Guide

Version: 9.9
1/31/2020



Legal Notice

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

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

Disclaimers

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

Table of Contents

1. Introduction

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

This guide is intended for 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.

This guide is intended for developers and Managed Service Providers. It provides instructions on how to use Netwrix Auditor Configuration API for managing Netwrix Auditor configuration objects.

NOTE: It assumed that document readers have prior experience with RESTful architecture and solid understanding of HTTP protocol. Technology and tools overview is outside the scope of the current guide.

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 Features and Benefits

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

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

Major benefits:

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

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

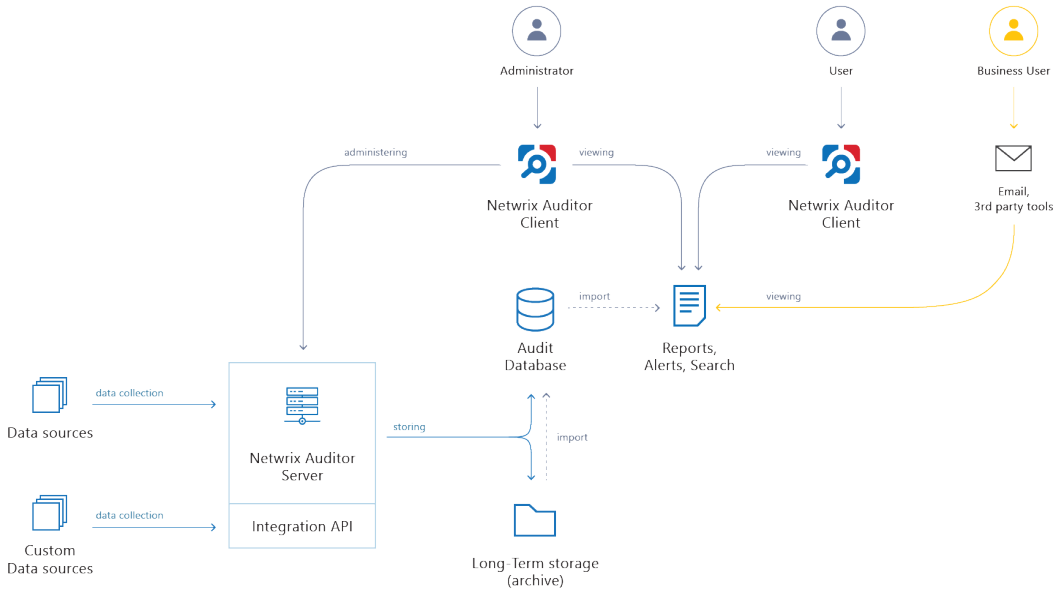
The table below provides an overview of each Netwrix Auditor application:

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

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

1.2. How It Works

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



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

1.2.1. Workflow Stages

General workflow stages are as follows:

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

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

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

2. Launch Netwrix Auditor

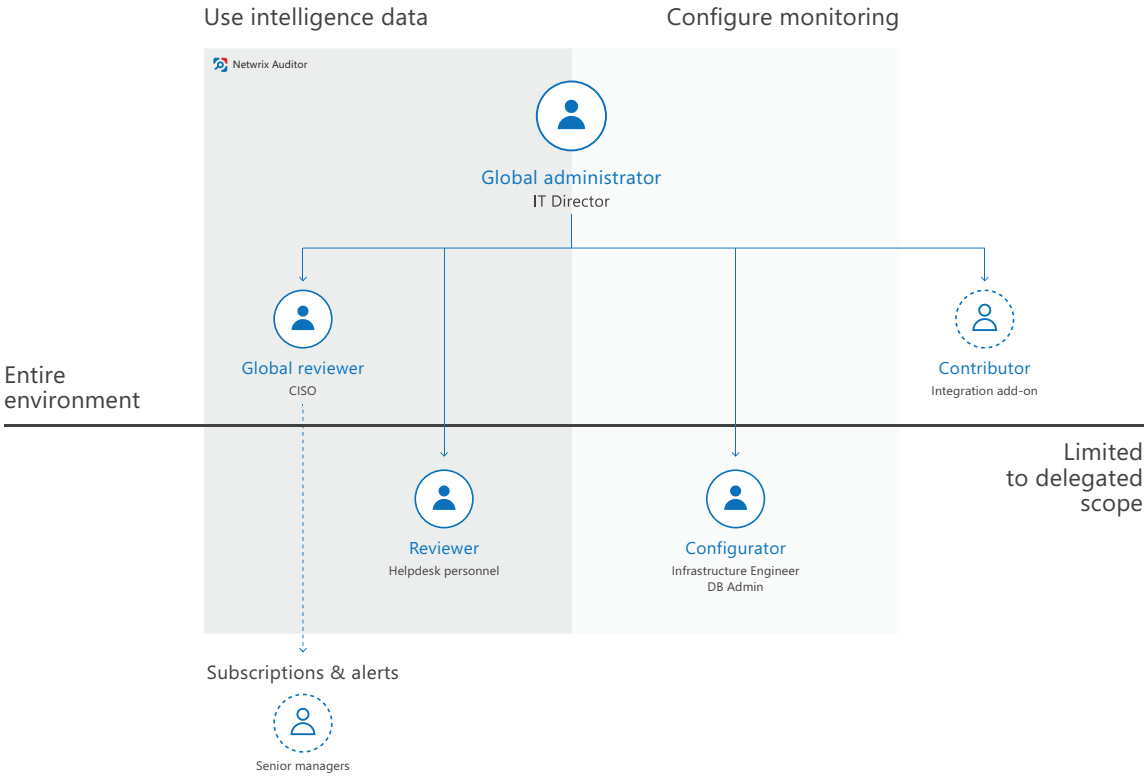
To start using Netwrix Auditor

- 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 permissions	+	–	–	–	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
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 remove Activity Summary	Some Add and remove Activity Summary	Some Restricted to the delegated scope (folder or monitoring	–

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
		recipients	recipients within the delegated scope	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 plan)	–	–
List report subscriptions	+	+	+	+	+

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Create, modify, remove subscriptions	+	+	–	–	–
See search results	+	+	Some Restricted to the delegated scope (folder or monitoring plan)	–	–
List, create, modify, delete custom reports	+	+	+	+	- (only can *list*)
List alerts	+	+	+	+	+
Create, modify, delete alerts	+	+	–	–	–
Import investigation data from the Long-Term Archive	+	–	–	–	–
View investigation data	+	+	–	–	–
View Behavior Anomalies list	+	+	–	–	–
Review user profile	+	+	–	–	–
Update anomaly status	+	+	–	–	–
Risk Assessment Overview dashboard and drill-down reports					
View Risk Assessment Overview results (dashboard, drill-down reports)	+	+	Some Restricted to delegated scope (folder or monitoring plan)	-	-

Feature	Global administrator	Global reviewer	Reviewer	Configurator	Contributor
Modify risk level thresholds	+	+	-	-	-
Customize risk indicators	+	+	-	-	-
Netwrix Auditor Integration API					
Write Activity Records	+	–	–	–	+
Retrieve Activity Records	+	+	+ Restricted to the delegated 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

Scope	Roles
	Contributor
Folder level	Configurator Reviewer
Plan level	Configurator Reviewer

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:

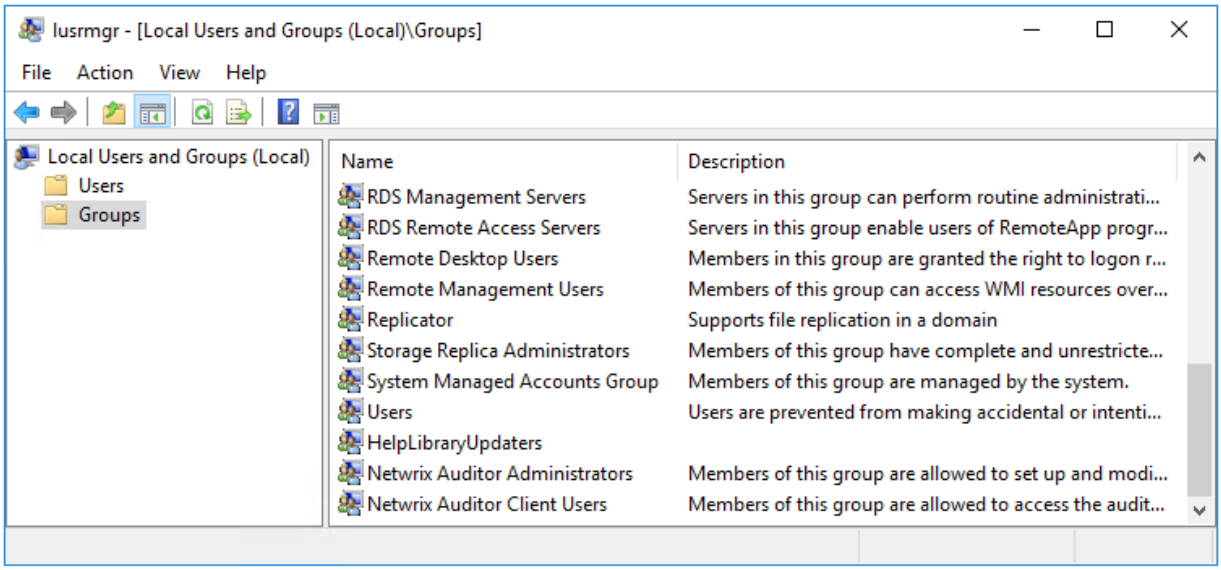
Account or group name	Role
Local Administrators	Global administrator

Account or group name	Role
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

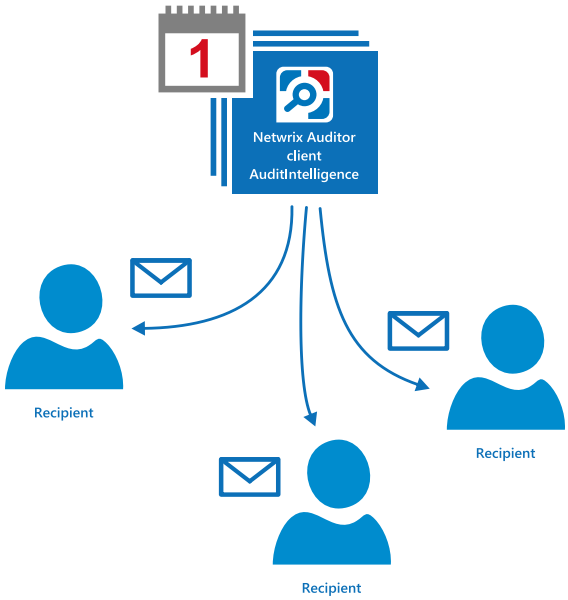
By default, only users designated in Netwrix Auditor are allowed to view its configuration and collected data. This policy ensures that only authorized and trustworthy users access sensitive data and make changes.

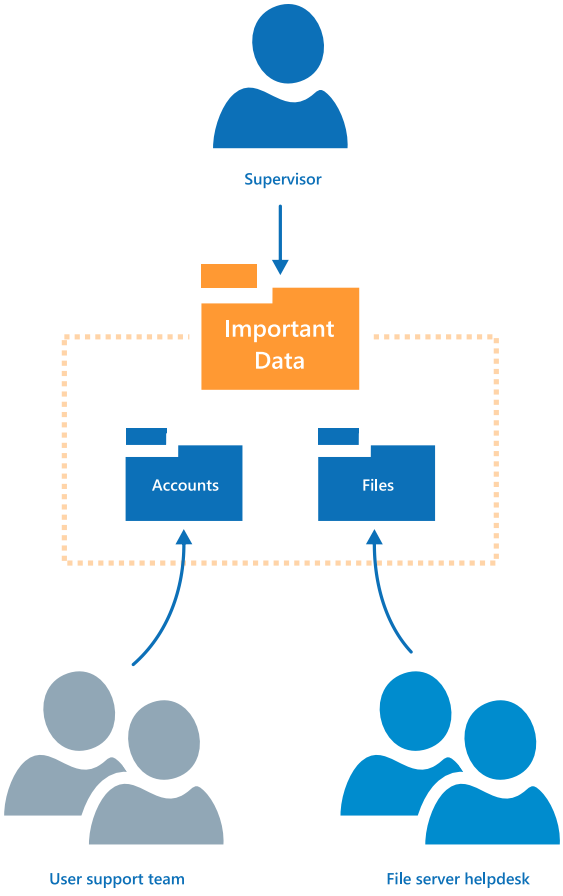
However, in some cases, organizations need to provide certain employees with access to a limited set of audit data. For example, an auditor might need to review particular access reports once or twice a year. You can provide these users (recipients) with means to review the data they need without actually 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	This scenario works great for a helpdesk with several departments. Assume, each

Do..	Recommended use
file shares	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. 
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

To create monitoring plans, user account must be assigned the *Global administrator* in Netwrix Auditor. Users with the *Configurator* role can create plans only within a delegated folder. See Role-Based Access and Delegation for more information.

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

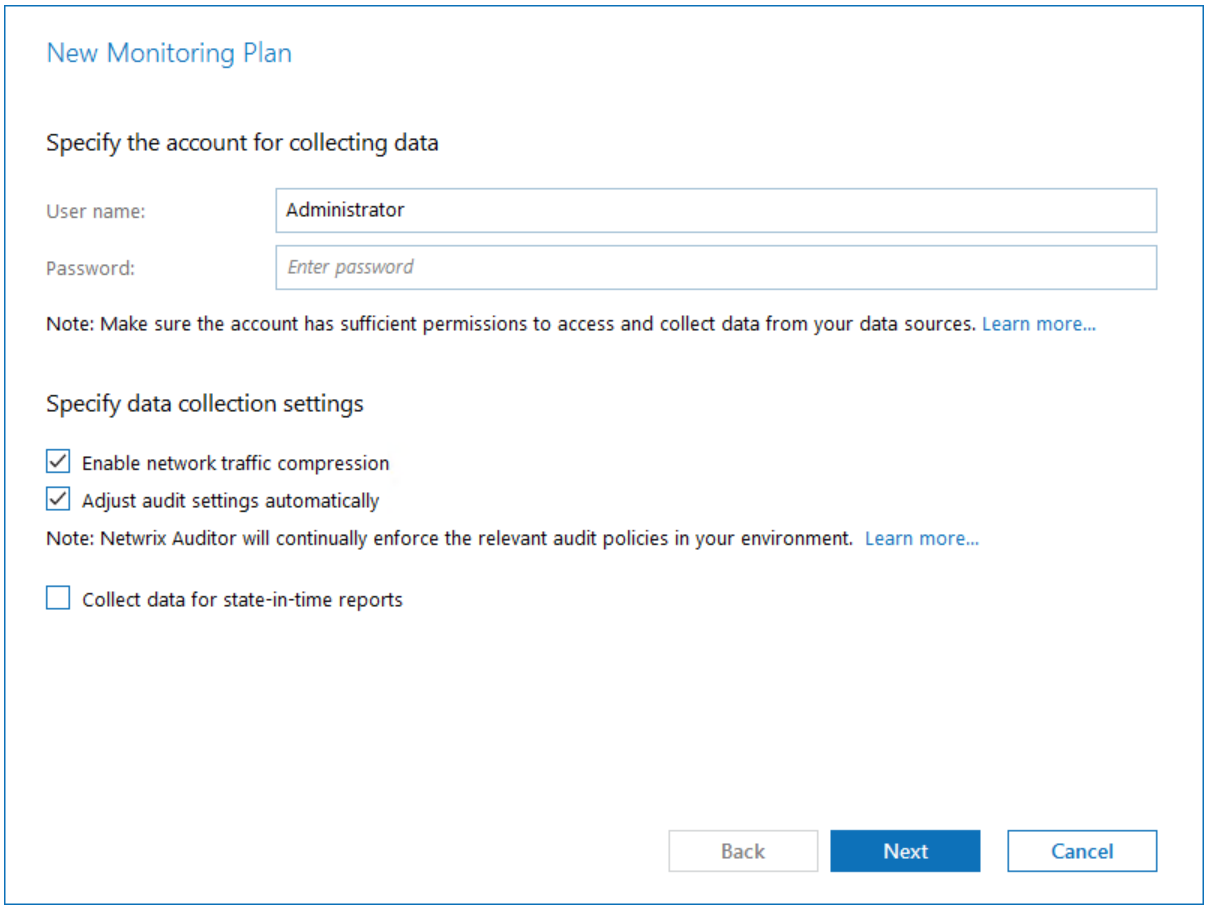
- On the main Netwrix Auditor page, in the **Quick Start** section, click the tile with a data source of your choice, e.g., Active Directory. If you need a data source that is not listed on the main page, click **All data sources**.
- On the main Netwrix Auditor page, in the **Configuration** section,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

Then follow the steps of the Monitoring Plan Wizard:

- 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. Settings for Data Collection

At this step of the wizard, specify the account that Netwrix Auditor will use to access the data source, and general settings for data collection.



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 Configure Data Collecting Account. Netwrix recommends creating a special service account with extended permissions. When you configure a monitoring plan for the first time, the account you specify for data collection will be set as default.
Enable network traffic compression	If selected, this option instructs Netwrix Auditor to deploy a special utility that will run on the audited computers and do the following: • collect and pre-filter audit data • compress data and forward it to Netwrix Auditor Server This approach helps to optimize load balance and reduce network traffic. So, using this option can be recommended especially for distributed networks with remote locations that have limited bandwidth. See Network Traffic

Option	Description
	Compression for more information.
Adjust audit settings automatically	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. Consider, however, that for some data sources this approach is mostly recommended for evaluation purposes in test environments; in the production environment, manual cofniguration is used more often (for example, for Windows File Servers). You may also want to apply audit settings via GPO (for example, for Windows Servers). **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 Configure IT Infrastructure for Auditing and Monitoring.
Collect data for state-in-time reports	State-in-time reports are based on the daily configuration snapshots of your audited systems; they help you to analyze particular aspects of the environment. State-in-time configuration snapshots are also used for IT risks assessment metrics and reports. This data collection option is available if you are creating a monitoring plan for any of the following data sources: • Active Directory • File Servers • Windows Server • Group Policy • SharePoint • SharePoint Online • Exchange Online To read more, refer to State-in-Time Reports and IT Risk Assessment Overview.

4.1.2. Default SQL Server Instance

To provide searching, alerting and reporting capabilities, Netwrix Auditor needs an SQL Server where audit data will be stored in the databases. To store data from the data sources included in the monitoring plan,

the wizard creates an Audit Database for each plan. At this step, you should specify the default SQL Server instance that will host Netwrix Auditor databases. To read more, refer to SQL Server and Audit Database.

NOTE: Alternatively, you can instruct Netwrix Auditor not to store data to the databases but only to the repository (Long-Term Archive) – in this scenario, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided.

NOTE: Netwrix Auditor skips this step if you have already configured Audit Database settings for other monitoring plans.

Select one of the following options:

- **Disable security intelligence and make data available only in activity summaries** — select this option if you do not want audit data to be written to the Audit Database. In this case, data will be available only in Activity Summary emails. Alerts, reports and search capabilities will not be supported.

  NOTE: If you later clear this option to start saving data to the database, consider that already collected audit data will not be imported in that database.

- **Install a new instance of Microsoft SQL Server Express automatically** — this option is available at the first run of the wizard. It allows you to deploy SQL Server 2016 SP2 Express with Advanced Services on the local machine. This SQL Server will be used as default host for Netwrix Auditor databases.

  NOTE: It is strongly recommended that you plan for your databases first, as described in Database Sizing section. Remember that database size in SQL Server Express edition may be insufficient for your audited infrastructure.

- **Use an existing SQL Server instance** — select this option to use an existing SQL Server instance.

  NOTE: Local SQL Server instance is detected automatically, and input fields are pre-populated with its settings.

  Complete the following fields:

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data. **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

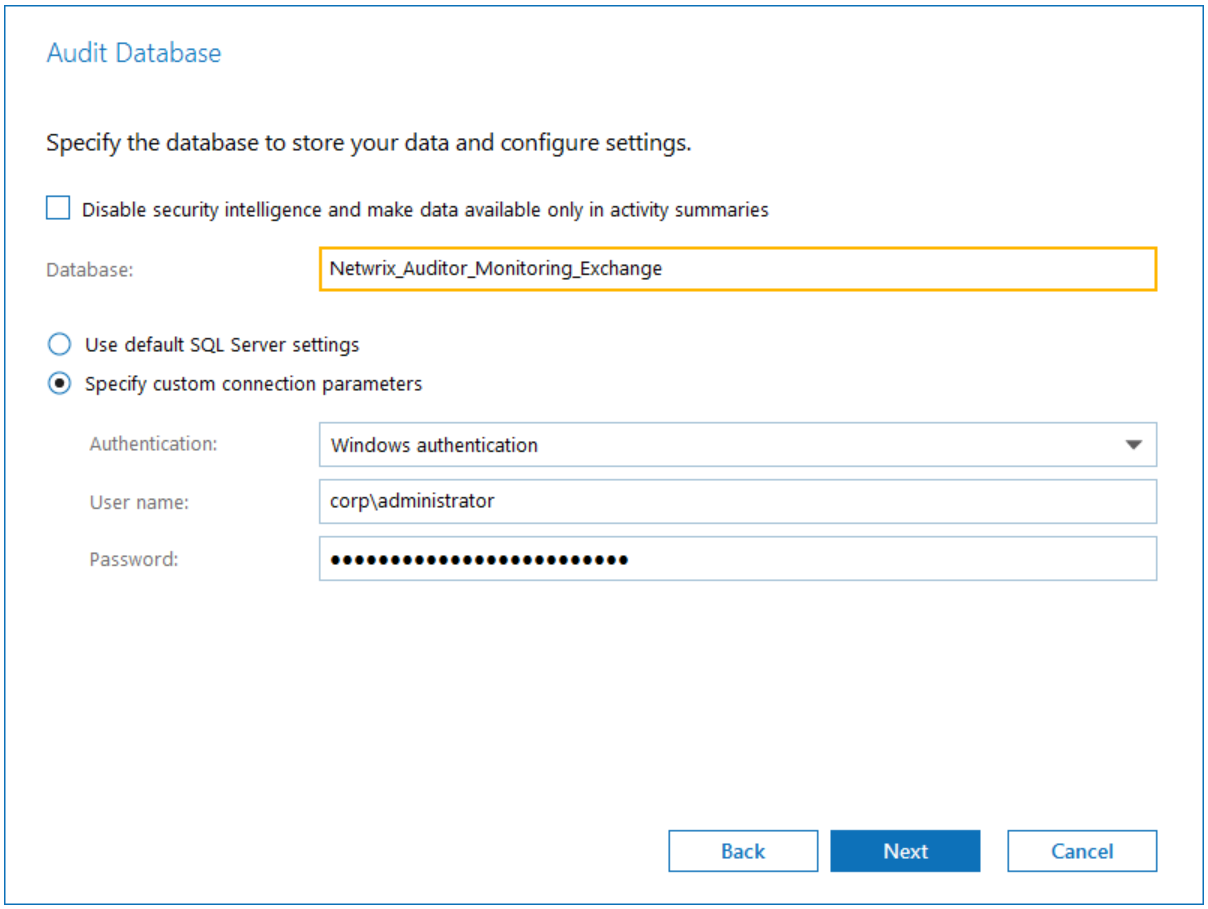
Option	Description
	SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. **NOTE:** This account must be granted the **database owner (db_owner)** role and the **dbcreator** server role. See Configure Audit Database Account for more information.
Password	Enter a password.

4.1.3. Database Settings

At this step, you need to specify a database where Netwrix Auditor will store data collected from the data sources included in this monitoring plan.

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

You can use default settings for your SQL Server instance or modify them (e.g., use a different authentication method or user). You can also change these settings later. See Audit Database for more information.



Configure the following:

Setting	Description
Disable security intelligence ...	Only select this option if you do not want your data to be stored in the database. In this case, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided. To store data to the database, leave this check box cleared.
Database	Default database name is *Netwrix_Auditor_<monitoring_plan_name>*. It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g. *Exchange_Audit_Data* or *OracleSrv02_Audit_Data*), or so. If you decided to use the existing SQL Server instance instead of dedicated, you may want to use *Netwrix_Auditor* prefix to distinguish Netwrix Auditor databases

Setting	Description
	from others.
Use default SQL Server settings	Select this option if you want Netwrix Auditor to connect to the SQL Server instance using the default settings you specified Default SQL Server Instance .
Specify custom connection parameters	Select this option to use custom credentials when connecting to SQL Server. Specify authentication method and the account that Netwrix Auditor will use. Make sure this account has sufficient rights to connect to SQL Server and work with the databases. See Configure Audit Database Account for details.

Netwrix Auditor will connect to the default SQL Server instance and create a database with the specified name on it.

NOTE: Global settings that apply to all databases with audit data (including retention period and SSRS server used for reporting) are available on the **Audit Database** page of Netwrix Auditor settings. See Audit Database for details.

4.1.4. SMTP Server Settings

When you create the first monitoring plan, you are prompted to specify the email settings that will be used for activity and health summaries, reports and alerts delivery. For the monitoring plans that follow, Netwrix Auditor will automatically detect SMTP settings; however, for your first plan you should provide them manually. See this section for details.

NOTE: You can skip this step if you do not want to receive email notifications, or configure SMTP settings later, as described in the related section.

4.1.5. Email Notification Recipients

Specify who will receive daily emails: Activity Summary Email on changes in the monitored infrastructure, and Health Summary Email on Netwrix Auditor operations and health.

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.

4.1.6. Monitoring Plan Summary

At this step of the wizard, to provide a meaningful name and optional description for your monitoring plan.

To start collecting data, you should specify the objects (items) that belong to the target data source and should be processed according to the settings of this monitoring plan. For example, for Exchange data source the item will be your Exchange server, for Windows Server data source - computer, IP range or AD container, and so on. To add items right after finishing the monitoring plan wizard, select the **Add item now** checkbox. See Add Items for Monitoring for details.

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.

NOTE: Netwrix Auditor for Oracle Database incompatible with Oracle Data Access Components for .Net Framework 4.0 and above. Check that the .Net Framework 3.5 feature is enabled prior to downloading prerequisites.

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

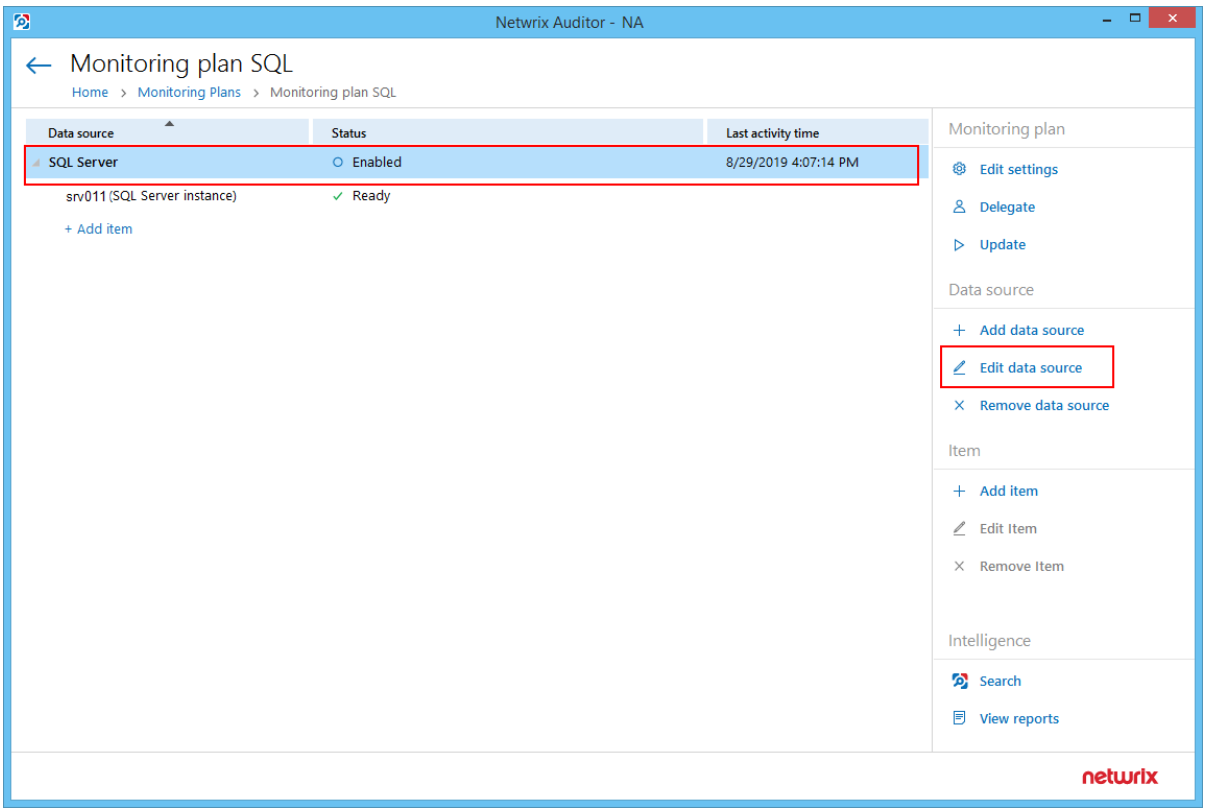
You can fine-tune data collection for each data source. Settings that you configure for the data source will be applied to all items belonging to that data source. Using data source settings, you can, for example:

- Enable state-in-time data collection (currently supported for several data sources)
- Depending on the data source, customize the monitoring scope (e.g., enable read access auditing, monitoring of failed attempts)

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 modify data source settings:

1. Select the monitoring plan you need and click **Edit**.
2. Within the monitoring plan window, highlight the data source (the first one is the row right under the blue table header) and click **Edit data source** on the right:



3. Modify data source settings as you need.
4. When finished, click **Save**.

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

Also, you can add a data source to the monitoring plan, or remove a data source that is no longer needed.

To add a data source to existing plan

1. Select the monitoring plan you need 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.
5. When finished, click the **Add** button to save the settings.

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.
Monitor 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

Option	Description
	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. Select **Group membership**if you want to include Group membership of the account under which the change was made.
Specify data collection method	You can enable network traffic compression. If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. **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 SharePoint Online configuration required for further state-in-time reports generation. See State–in–Time Reports for more information. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database. For that, in the **Manage historical snapshots** section, click **Manage** and select the snapshots that you want to import. **NOTE:** To import snapshots, you must be assigned the **Global**

Option	Description
	administrator or the **Global reviewer** role . Move the selected snapshots to the **Snapshots available for reporting** list using the arrow button. When finished, click **OK**.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See 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. Active Directory Federation Server (AD FS)

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.
Schedule AD FS logons collection	Specify period for AD FS logons collection.
Specify data collection method	You can enable network traffic compression. If enabled, a Compression Service will be automatically launched on the audited computer, collecting and pre-filtering data. This significantly

Option	Description
	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:** 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 Configure IT Infrastructure for Auditing and Monitoring.

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

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. Select **Group membership**if you want to include Group membership of the account under which the change was made.
Specify data collection method	You can enable network traffic compression. If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary.

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 on non-owner access to mailboxes	Enable monitoring of unauthorized access to mailboxes within your Exchange organization. Configure the following: • **Enable automatic audit configuration** — 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 select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary. 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.

4.2.5. 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. 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 Exchange Online configuration required for further state-in-time reports generation. See State–in–Time Reports for more information. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. **NOTE:** Import of historical snapshots to Audit Database is not available for Exchange Online.
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.

4.2.6. 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. Select **Group membership**if you want to include Group membership of the account under which the change was made.
Specify data collection method	You can enable network traffic compression. If enabled, a Compression Service will be automatically launched on the audited computer, collecting and prefiltering data. This significantly improves data transfer and minimizes the impact on the target computer performance.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. **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.

4.2.7. 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 Audited Object Types, Actions and Attributes for more information.
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

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>and minimizes the impact on the target computer performance.

NOTE: To collect data from 32-bit operating systems, network traffic compression must be disabled.

To collect data from Windows Failover Cluster, network traffic compression must be enabled.

See File Servers for more information.</td></tr>
<tr><td>Configure audit settings</td><td>You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary.

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\VNX</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>
<tr><td>Nutanix Files</td><td>n/a</td><td>n/a</td><td>+</td><td>+</td><td>n/a</td><td>n/a</td></tr>
</table>
</td></tr>
</table>

Option	Description
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your system configuration required for further state-in-time reports generation. See State–in–Time Reports for more information. When auditing file servers, changes to effective access permissions can be tracked in addition to audit permissions. By default, **Combination of file and share permissions** is tracked. File permissions define who has access to local files and folders. Share permissions provide or deny access to the same resources over the network. The combination of both determines the final access permissions for a shared folder—the more restrictive permissions are applied. Upon selecting **Combination of file and share permissions** only the resultant set will be written to the Audit Database. Select **File permissions** option too if you want to see difference between permissions applied locally and the effective file and share permissions set. To disable auditing of effective access, unselect all checkboxes under **Include details on effective permissions**. **NOTE:** The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.

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 if **Object Access Auditing** is enabled on DFS file shares or on every cluster node.

- When adding a cluster file server for auditing, it is recommended to specify a server name of the **Role** server or a UNC path of the shared folder located on the **Role** server.
- When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path of the whole namespace or UNC path of the DFS link (folder). For example:
  - *"\\domain\dfsnamespace\"* (domain-based namespace) or *"\\server\dfsnamespace\"* (in case of stand-alone namespace);
  - *"\\domain\dfsnamespace\link"* (domain-based namespace) or *"\\server\dfsnamespace\link"* (in case of stand-alone namespace).
- For recommendations on configuring DFS replication, refer to this Knowledge Base article.

4.2.8. 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.

4.2.9. Network Devices

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
Specify actions for monitoring	Specify monitoring rules for your network devices.
Specify port and protocol for incoming connections	Use **Port** and **Protocol** to provide the port required for incoming connections (default is **UDP port 514**).

4.2.10. Oracle Database

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.
Monitor Oracle Database logon activity	Specify what types of logon events you want to monitor: • Failed logons • Successful logons • Logoffs
	Users
Specify users to track their activity	Use controls in this section to populate the corresponding lists -click **Add** and specify user name and type (OS or database user). • **Include**—Add users to be included in the auditing scope. • **Exclude**—Add users to be excluded from the auditing scope by specifying their names and type (OS or database user). **NOTE:** User names are case-sensitive.
	Database Objects
Data objects to monitor	Create rules for objects and actions that you want to audit: 1. Click **Add Rule**. 2. Specify a name of the Oracle database *Object* or *Schema*. 3. Select the necessary actions (successful or failed changes, successful or failed reads). 4. Click **Add**.

Option	Description
	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.

4.2.11. 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. Select **Group membership**if you want to include Group membership of the account under which the change was made.
Configure audit settings	You can adjust audit settings automatically. Your current audit settings will be checked on each data collection and adjusted if necessary. **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. See State–in–Time Reports for more information. **NOTE:** The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.

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. 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.
Collect data for state-in-time reports	Configure Netwrix Auditor to store daily snapshots of your SharePoint Online configuration required for further state-in-time reports generation. See State–in–Time Reports for more information. The product updates the latest snapshot on the regular basis to keep users up-to-date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database. For that, in the **Manage historical snapshots** section, click **Manage** and select the snapshots that you want to import. **NOTE:** To import snapshots, you must be assigned the **Global administrator** or the **Global reviewer** role . Move the selected snapshots to the **Snapshots available for reporting** list using the arrow button. When finished, click **OK**.

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See Add Items for Monitoring for more information.

4.2.13. SQL Server

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.
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
	Data
Monitor changes to data in the database tables	Enable monitoring of changes to data stored in the database tables hosted on the SQL Server.
Changes (per transaction) to collect and report:	Specify how many changes per a database transaction you want to be collected. For example, you can limit this number to 10 changes per transaction, or collect all changes. **NOTE:** It is recommended to adjust this setting carefully, as collecting large number of changes from a highly-transactional server may affect its performance.
Monitoring rules	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.

Option	Description
	• **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.

4.2.14. 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.
Record video of user activity within sessions	When enabled, the product records video in addition to user sessions events collection. This option is disabled by default.
	Video Recording
NOTE: For these settings to become effective, enable video recording on the **General** tab.	
Adjust video quality	Optimize video file by adjusting the following: • File size and video quality • Save video in grayscale • CPU load and Video smoothness.
Adjust video duration	Limit video file length by adjusting the following: • **Recording lasts for <...> minutes**—Video recording will

Option	Description
	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. **NOTE:** If the **Record video of user activity within sessions** option is enabled, the **User Sessions** report shows active time calculated without including user idle period. Mind that a computer is considered to be idle by Windows if there has not been user interaction via the mouse or keyboard for a given time and if the hard drives and processors have been idle more than 90% of that time. • **Free disk space is less than <...> MB**—Video recording will be stopped when upon reaching selected disk space limit.
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 track	Select the applications that you want to monitor. You can select **All applications** or create a list of **Specific applications**. Certain applications can also be added to **Exceptions** list.
	Monitored Computers
For a newly created monitoring plan for User Activity, the list of monitored computers is empty. Add items to your monitoring plan and wait until Netwrix Auditor retrieves all computers within these items. See Add Items for Monitoring for more information. The list contains computer name, its current status and last activity time.	

Review your data source settings and click **Add** to go back to your plan. The newly created data source will appear in the **Data source** list. As a next step, click **Add item** to specify an object for monitoring. See Add Items for Monitoring for more information.

4.2.15. 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.
Monitor VMware configuration changes	Configuration changes are always monitored for VMware data source. See this section for details.
Monitor VMware logon activity	Specify what types of logon events you want to monitor for VMware infrastructure.

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.

4.2.16. 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. • **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

Option	Description
	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 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

Option	Description
	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. See State–in–Time Reports for more information. **NOTE:** The product updates the latest snapshot on the regular basis to keep users up to date on actual system state. Only the latest snapshot is available for reporting in Netwrix Auditor. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.

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.

4.2.17. 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 add as many items for a data source as you want. In this case, all items will share settings you specified for this data source.

Each data source has a dedicated item type. Netwrix Auditor automatically suggests item types associated with your data source.

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

Data Source	Item
	IP Range NetApp Windows File Share Nutanix SMB Shares
Network Devices	Computer IP Range
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 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. Federation Server

NOTE: If you are going to audit an entire AD FS farm, consider adding all AD FS server one by one as items to your monitoring plan. Otherwise, your audit scope may contain warnings, errors or incomplete data.

Complete the following fields:

Option	Description
Specify AD FS federation server	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click **Browse** to select a computer from the list of computers in your network.
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.

4.3.5. EMC Isilon

Complete the following fields:

Option	Description
	General
Specify EMC Isilon storage array	Provide the IP address or the host name of the name server used to connect to your access zone. For example, account.corp.lab
Access Zone	Enter the name of access zone partition within your EMC Isilon cluster. For example, zone_account
OneFS web administration interface URL	Enter EMC Isilon web administration URL (e.g., *https://isiloncluster.corp.lab:8080*). This URL is used to get configuration details about your Isilon cluster via OneFS API.
File Share UNC path to audit logs	Path to the file share located on a EMC Isilon with event log files (e.g., *\\srv\netwrix_audit$\logs*\).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. **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. EMC VNX/VNXe

Complete the following fields:

Option	Description
	General

Option	Description
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.

4.3.7. 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.

4.3.8. 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. **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.

Option	Description
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.

4.3.9. Nutanix SMB Shares

Complete the following fields:

Option	Description
	General
Specify Nutanix File Server	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click **Browse** to select a computer from the list of computers in your network. **NOTE:** If you need to audit a 3-node cluster, it is recommended to use FQDN or NETBIOS name.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. **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.
Specify listening port for incoming connections	Provide the name of the TCP port to listen to notifications on the operations with Nutanix file shares. Default is **9898**. For details on how to open the port, refer to Open 9898 and 9699 Ports for Inbound Connections.
	Nutanix File Server REST API
Specify account for connecting to Nutanix File Server REST API	Specify the account that will be used to connect to Nutanix REST API. This account should have sufficient privileges on the Nutanix File Server. For details, refer to Create User Account to Access Nutanix REST API.
	Scope
Monitor the following shares	By default, all file shares (except hidden) hosted on this server will be audited. To limit your auditing scope to the certain shares, select **Specific file shares**, then click **Add** and in **the Add File Share** dialog specify a path to the shared folder you need, or a subfolder of the share.

Option	Description
	NOTE: Currently, auditing is available for SMB shares only. Auditing of NFS shares is not supported due to known limitations.

4.3.10. 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.

4.3.11. 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.

4.3.12. SharePoint Farm

Complete the following fields:

Option	Description
	General

Option	Description
Specify SharePoint farm for monitoring	Enter the SharePoint Central Administration website URL.
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. **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

Option	Description
	Netwrix Auditor Installation and Configuration Guide for more information. • **Manually**—See Netwrix Auditor Installation and Configuration Guide for more information. **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.

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

4.3.13. 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.

4.3.14. 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

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

4.3.15. Windows File Share

Complete the following fields:

Option	Description
Specify Windows file share	Provide UNC path to a shared resource. See the section below for special considerations. **NOTE:** Do not specify a default file share mapped to a local drive (e.g., \\Server\e$).
Specify the account for collecting data	Select the account that will be used to collect data for this item. If you want to use a specific account (other than the one you specified during monitoring plan creation), select **Custom account** and enter credentials. The credentials are case sensitive. **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.

4.3.15.1. Peculiarities and Considerations

4.3.15.1.1. Working with DFS File Shares

Netwrix Auditor supports auditing of DFS and clustered file servers if **Object Access Auditing** is enabled on DFS file shares or on every cluster node.

- When adding a cluster file server for auditing, it is recommended to specify a server name of the **Role** server or a UNC path of the shared folder located on the **Role** server.
- When adding a DFS file share for auditing, specify a Windows file share item and provide the UNC path of the whole namespace or UNC path of the DFS link (folder). For example:
  - *"\\domain\dfsnamespace\"* (domain-based namespace) or *"\\server\dfsnamespace\"* (in case of stand-alone namespace);
  - *"\\domain\dfsnamespace\link"* (domain-based namespace) or *"\\server\dfsnamespace\link"* (in case of stand-alone namespace).

- For recommendations on configuring DFS replication, refer to this Knowledge Base article.

4.3.15.2. Working with Mount Points

You can specify a mount point as a monitored item. However, consider the following:

- If a mount point represents a shared folder, then the objects in its root will be initially collected by Netwrix Auditor and appear as processed by *System* account. Wait for the next data collections - then all actions for these objects will be monitored in a normal way.
- To monitor the mount points targeted at the subfolder of a file share, provide network path to the target subfolder.

4.3.16. 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.
	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

Option	Description
	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. See See Network Traffic Compression for more information.
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 period, 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 alerts. The alerts that are included in Behavior Anomalies assessment, appear in the Behavior Anomalies dashboard.
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 and updated several times a day.

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

   - Active Directory
   - File Servers
   - SharePoint
   - Windows Server

- Group Policy
- SharePoint Online
- Exchange Online

See also: Data Collection from VMware Servers.

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.

NOTE: Not applicable to Netwrix Auditor for User Activity. For this data source, the product sends real-time data about sessions and activity.

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**.

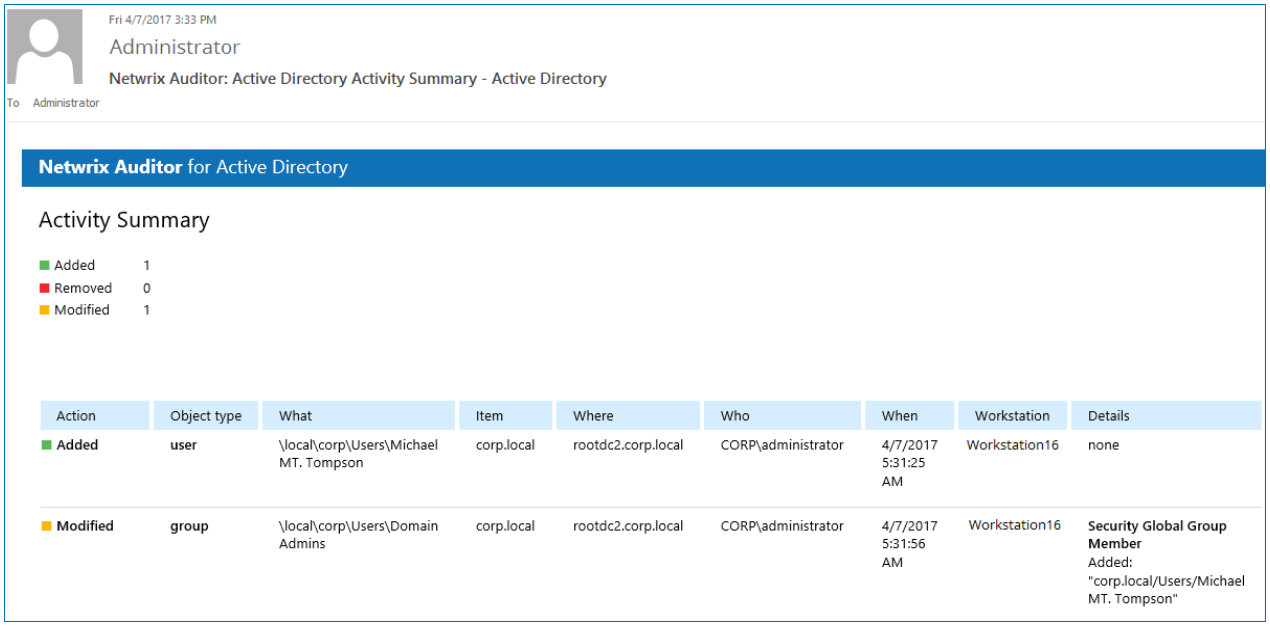
NOTE: Depending on the size of the monitored environment and the number of changes, data collection may take a while.

6. Activity Summary Email

Activity Summary email is generated automatically by Netwrix Auditor and lists all changes / recorded user sessions that occurred since the last Activity Summary delivery. By default, for most data sources an Activity Summary is generated daily at 3:00 AM and delivered to the specified recipients. You can also launch data collection and Activity Summary generation manually.

NOTE: Notifications on user activity and event log collection (Event Log Collection Status) are a bit different and do not show changes.

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



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 • Activated (User Activity)
Object Type	Shows the type of the modified AD object, for example, 'user'.
What	Shows the path to the modified AD object.

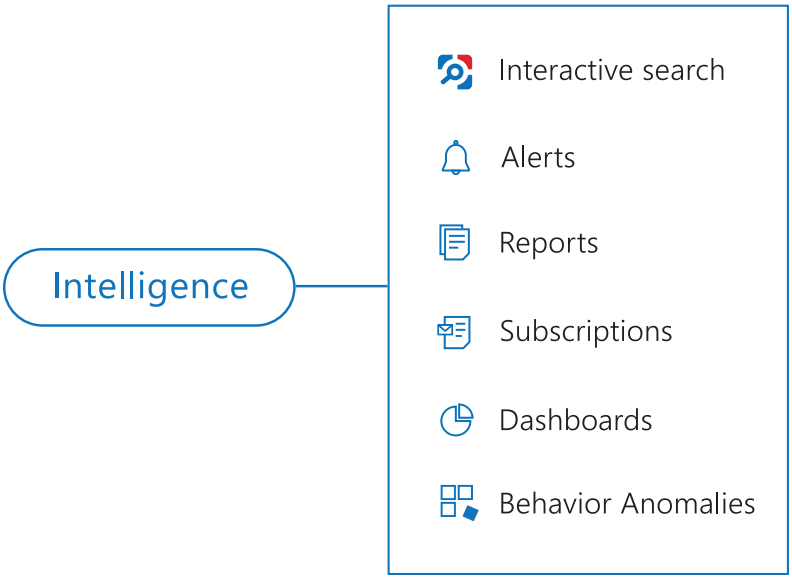
Column	Description
Item	Shows the item associated with the selected monitoring plan.
Where	Shows the name of the domain controller where the change was made.
Who	Shows the name of the account under which the change was made.
When	Shows the exact time when the change occurred.
Workstation	Shows the name / IP address of the computer where the user was logged on when the change was made.
Details	Shows the before and after values of the modified AD object.

To initiate an on-demand Activity Summary delivery, navigate to the **Monitoring Plans** section, select a plan, click **Edit**, and then select **Update**. A summary will be delivered to the specified reciptient, listing all activity that occurred since the last data collection.

7. Intelligence

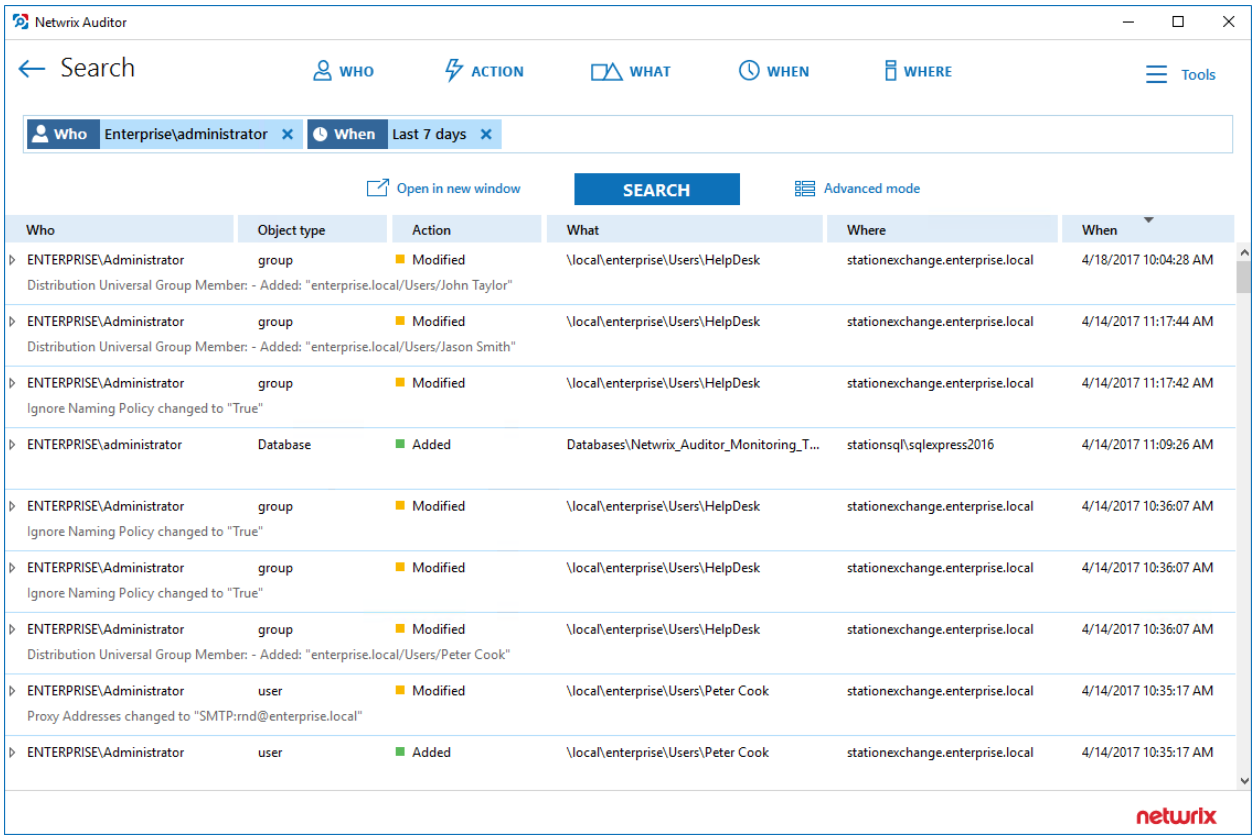
Besides notifying about the changes on a daily basis, Netwrix Auditor brings security intelligence into your IT infrastructure and enables complete visibility.

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.). Friendly, interactive search interface allows users to run custom search queries, while alerts keep them 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 monitoring 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 product settings, such as default SQL Server instance for Audit Database, the Long-Term Archive location and retention period, etc. You can also review information about the product version and your licenses. Review the following for additional information:

- General
- Audit Database
- Long-Term Archive
- Investigations
- Notifications
- Integrations
- Licenses
- About Netwrix Auditor

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. These 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

Option	Description
	individually. To specify custom settings (e.g., use a different account or authentication type), navigate to the monitoring plan's settings. See 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 Configure Audit Database Account 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.

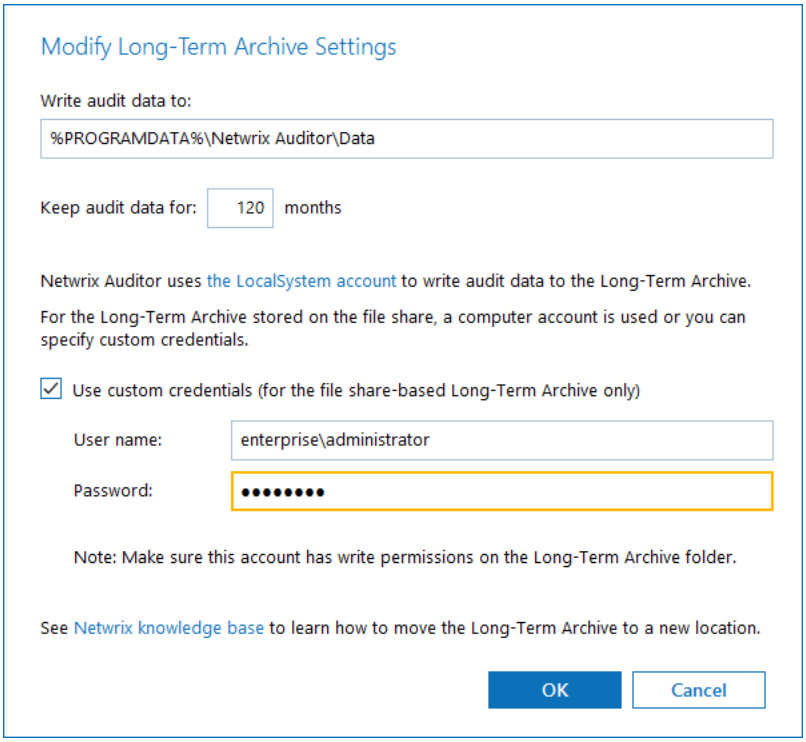
Option	Description
Report Server URL	Specify the Report Server URL. Make sure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Make sure that the resource is reachable.
User name	Specify the account to be used to connect to SSRS. Make sure this account is granted the **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
Long-Term Archive settings	

Option	Description

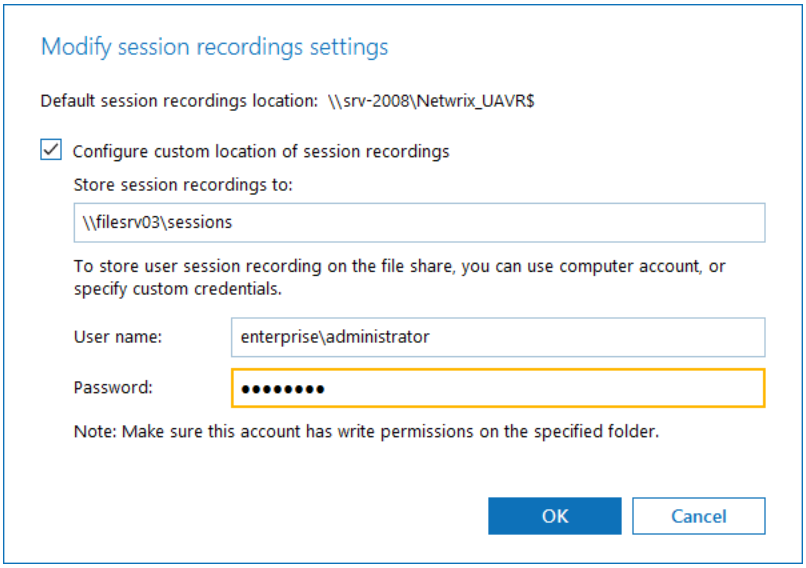


Write audit data to	Specify the path to a local or shared folder where your audit data will be stored. By default, it is set to *"C:\ProgramData\Netwrix Auditor\Data"*. By default, the **LocalSystem** account is used to write data to the local-based Long-Term Archive and computer account is used for the file share-based storage. Subscriptions created in the 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

Option	Description
	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:
	• Advanced permissions on the folder where the Long-Term Archive is stored:
	  • **List folder / read data**
	  • **Read attributes**
	  • **Read extended attributes**
	  • **Create files / write data**
	  • **Create folders / append data**
	  • **Write attributes**
	  • **Write extended attributes**
	  • **Delete subfolders and files**
	  • **Read permissions**
	• On the file shares where report subscriptions are saved:
	  • **Change** share permission
	  • **Create files / write data** folder permission
	
	NOTE: Subscriptions created in the Netwrix Auditor client are uploaded to file servers under the Long-Term Archive service account as well.

	Session recording settings

Option	Description
	
Configure custom location of session recordings	Default location for storing session recordings is set to *"\\<NetwrixAuditorServerName>\Netwrix_UAVR$"*. However, storing extra files on Netwrix Auditor server may produce additional load on it, so consider using this option to specify another location where session recordings will be stored.
Enter UNC path to shared folder:	Specify UNC path to the shared folder where user session video recordings will be stored. You can use server name or IP address, for example: *\\172.28.6.33\NA_UserSessions* **NOTE:** Using a local folder for that purpose is not recommended, as storing extra files on Netwrix Auditor server will produce additional load on it. Make sure the specified shared folder has enough capacity to store the video files. Retention period for the video files can be adjusted in the related monitoring plan settings (targeted at User Activity data source); default retention is **7 days**. See User Activity for details. **NOTE:** After you specify and save settings for session recordings, it is recommended that you leave them unchanged. Otherwise — if you change the storage location while using Netwrix Auditor for User Activity — please be aware of possible data loss, as Netwrix Auditor will not automatically

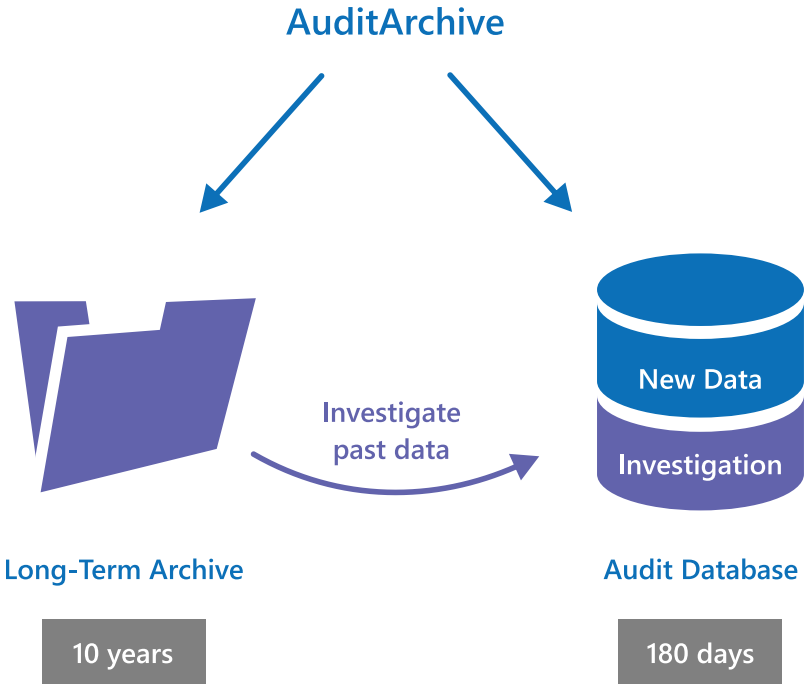
Option	Description
	move session recordings to a new location.
User name / Password	Provide user name and password for the account that will be used to store session recordings to the specified shared folder. Make sure the account has at least **Write** permission for that folder.

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, the Netwrix services responsible for audit data collection will be stopped.

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. **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 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 send summary emails and notifications 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.

After that, you can specify the recipient who will receive product activity and health summary emails.

To send summary emails and notifications about critical events

1. Navigate to the **Summary email recipient** and click **Modify**.
2. Specify recipient address:
   - To send to a single recipient, enter personal mailbox address.
   - To send to multiple recipients, make sure they are added to a distribution group, and enter the group address. Entering multiple individual addresses is not supported.

To learn more about product health, you can also navigate to the **Health status** tile in the main window. It will take you to the **Health Status** dashboard that contains information on the product activity and system health state. See Review Health Status Dashboard 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**: Solidify security and meet regulatory compliance standards by enabling visibility into what is going on in any third-party application.
- **Data out**: Further automate your business processes, IT security and operations workflows by enriching third-party solutions with actionable audit data.

Netwrix Auditor Integration API is enabled by default and communicates through port 9699. Navigate to **Settings → Integrations** to adjust port settings and review information about possible integrations.

Netwrix recommends adding a special data source to your monitoring plan—Netwrix API. 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 learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs.

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
"	**"**
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**.

8.7. About Netwrix Auditor

The **About Netwrix Auditor** tab contains complete information on the product:

Option	Description
Netwrix Auditor9.9	Review current version of Netwrix Auditor.
Check for updates	Select to check for available updates now.
Check for updates automatically and show notifications about new product versions	Netwrix Auditor periodically checks for updates so you don't have to. When an update is available, a user is immediately noticed.
Getting Help	Click the link to visit Netwrix Auditor Help Center and access user guidelines online.

9. Monitor Netwrix Auditor Operations and Health

This section describes how you can monitor Netwrix Auditor operations, health and resource usage. For that, the following means are provided:

- Review Health Status Dashboard
- Netwrix Auditor Self-Audit
- Netwrix Auditor Health Summary Email
- Netwrix Auditor System Health Log

9.1. Netwrix Auditor System Health Log

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

You can review events directly in the product:

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

  OR

- In the main screen, in the **Configuration** section click the **Health status** tile, then in the **Health log** dashboard widget click **Open health log**. See Health Log for more information.

NOTE: You can also inspect the log in the **Event Viewer**.

There are three types of events that can be logged:

Event Type	Description
Information	An event that describes the successful operation beginning or completion. For example, the product successfully completed data collection for a monitoring plan.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, the product failed to process a domain controller.
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, the product failed to retrieve settings for your data source.

Review the following:

- Inspect Events in Health Log

If you want to monitor Netwrix Auditor health status in more depth, you can do the following:

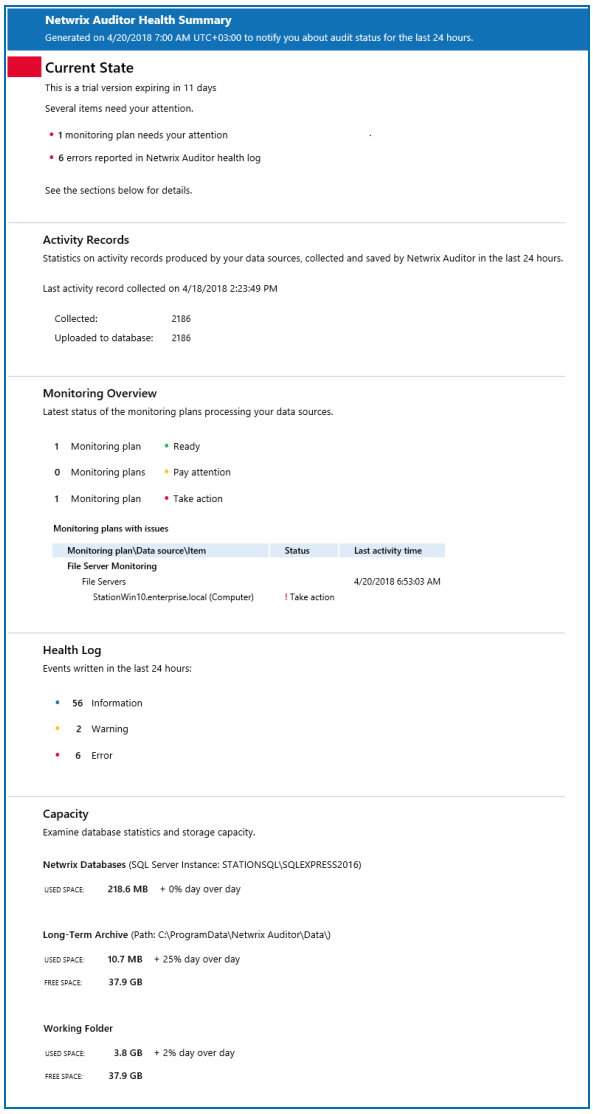
- Create a monitoring plan for this log using Netwrix Auditor Event Log Manager too to collect activity data. See Create Monitoring Plan for Netwrix Auditor System Health Log for more information.
- Configure alerts triggered by specific events in the product's health log. See Create Alerts on Netwrix Auditor Server Health Status for more information.

9.1.1. Netwrix Auditor Health Summary Email

Netwrix Auditor Health Summary email includes all statistics on the product operations and health for the last 24 hours; it also notifies you about license status. By default, this email is generated daily at 7:00 AM and delivered to the recipient specified in the Notifications settings. Email content is very similar to data presented in the Health Status dashboard.

For greater usability, to depict overall product health state, the email includes a color indicator in the topmost section: green means Netwrix Auditor had no issues while auditing your IT infrastructure, and red means there were some problems that require your attention.

The email looks like shown below:



Netwrix Auditor Health Summary

Generated on 4/20/2018 7:00 AM UTC+03:00 to notify you about audit status for the last 24 hours.

Current State

This is a trial version expiring in 11 days

Several items need your attention.

- 1 monitoring plan needs your attention
- 6 errors reported in Netwrix Auditor health log

See the sections below for details.

Activity Records

Statistics on activity records produced by your data sources, collected and saved by Netwrix Auditor in the last 24 hours.

Last activity record collected on 4/18/2018 2:23:49 PM

Collected:	2186
Uploaded to database:	2186

Monitoring Overview

Latest status of the monitoring plans processing your data sources.

1	Monitoring plan	Ready
0	Monitoring plans	Pay attention
1	Monitoring plan	Take action

Monitoring plans with issues

Monitoring plan\Data source\Item	Status	Last activity time
File Server Monitoring		
File Servers		4/20/2018 6:53:03 AM
StationWin10.enterprise.local (Computer)	! Take action	

Health Log

Events written in the last 24 hours:

- 56 Information
- 2 Warning
- 6 Error

Capacity

Examine database statistics and storage capacity.

Netwrix Databases (SQL Server Instance: STATIONSQL\SQLEXPRESS2016)

USED SPACE: **218.6 MB** + 0% day over day

Long-Term Archive (Path: C:\ProgramData\Netwrix Auditor\Data\)

USED SPACE: **10.7 MB** + 25% day over day

FREE SPACE: **37.9 GB**

Working Folder

USED SPACE: **3.8 GB** + 2% day over day

FREE SPACE: **37.9 GB**

NOTE: The **Monitoring Overview** section of the email provides detail information only for the monitoring plans with issues. Successfully completed monitoring plans are not included.

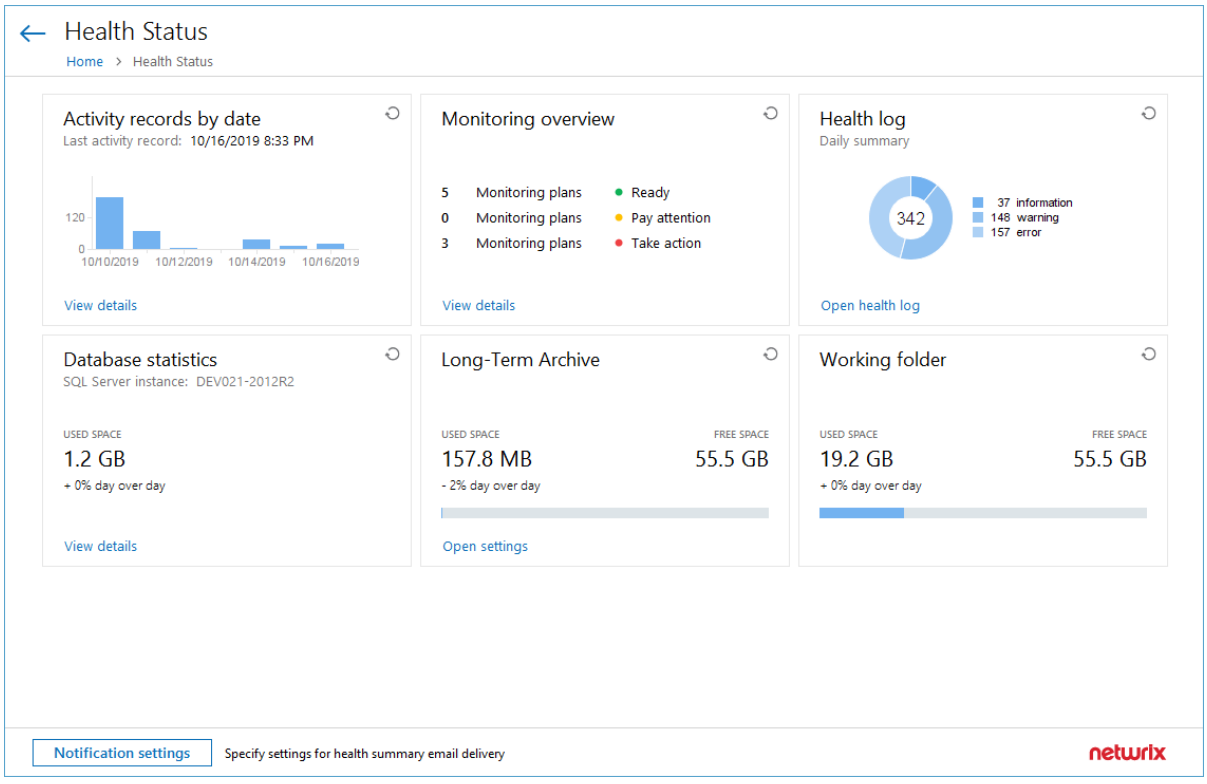
9.1.2. Review Health Status Dashboard

New Health Status dashboard facilitates Netwrix Auditor maintenance and troubleshooting tasks, providing IT specialists with at-a-glance view on the most critical factors: data collection performance, product health and storage capacity. The dashboard comprises a set of widgets that display the status of these aspects using aggregated statistics and charts. Nearly each widget allows you to drill down to the detailed information on the aspect you are interested in.

To view the dashboard, on the main Netwrix Auditor page, click the **Health status** tile located in the **Configuration** section.

The dashboard includes the following widgets:

- The **Activity records by date** chart—Shows the number of activity records produced by your data sources, collected and saved by Netwrix Auditor during the last 7 days. See Activity Records Statistics for details.
- The **Monitoring overview** widget—Shows aggregated statistics on the statuses of all monitoring plans configured in Netwrix Auditor at the moment. See Monitoring Overview for details.
- The **Health log** chart—Shows the statistics on the events written in the Netwrix Auditor health log in the last 24 hours. Click the link in this widget to view the log. See Health Log for details.
- The **Database statistics** widget—Helps you to estimate database capacity on the default SQL Server instance that hosts the product databases. See Database Statistics for details.
- The **Long-Term Archive** widget—Helps you to estimate the capacity of the Long-Term Archive file-based storage. To modify its settings, including location and retention, click the link in this widget. See Long-Term Archive Capacity for details.
- The **Working Folder** widget—Helps you to estimate the capacity of the Netwrix Auditor working folder used to keep operational information (configuration files of the product components, log files, and other data) on the Netwrix Auditor Server. See Netwrix Auditor Working Folder for details.

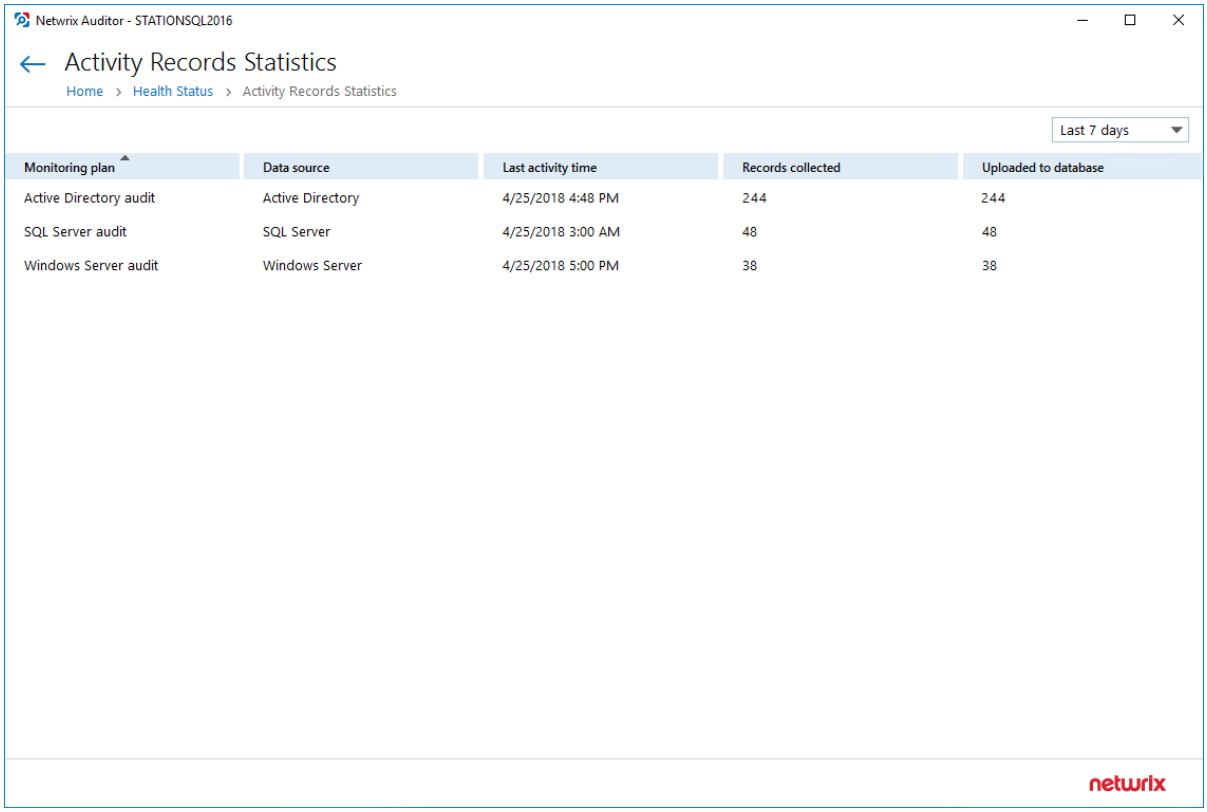


You can also instruct Netwrix Auditor to forward similar statistics as a health summary email to personnel in charge. For that, click **Notification settings**, then follow the steps described in the Notifications section. See also Netwrix Auditor Health Summary Email.

9.1.2.1. Activity Records Statistics

Aggregated statistics on the activity records is provided in the **Activity records by date** widget. The chart shows the number of activity records produced by your data sources, collected and saved by Netwrix Auditor during the last 7 days. This data can help you to assess the activity records generation intensity in your IT infrastructure, and product load.

After you click **View details**, the **Activity Records Statistics** window will be displayed.



By default, statistics on activity records processing is grouped by **Monitoring plan** and presented for the **Last 7 days**. To modify the timeframe, use the drop-down list in the upper right corner.

Other fields provide the following information: data source that produces activity records, with date and time of the last collected record, and the overall number of records collected and uploaded to the corresponding Audit database during the specified timeframe.

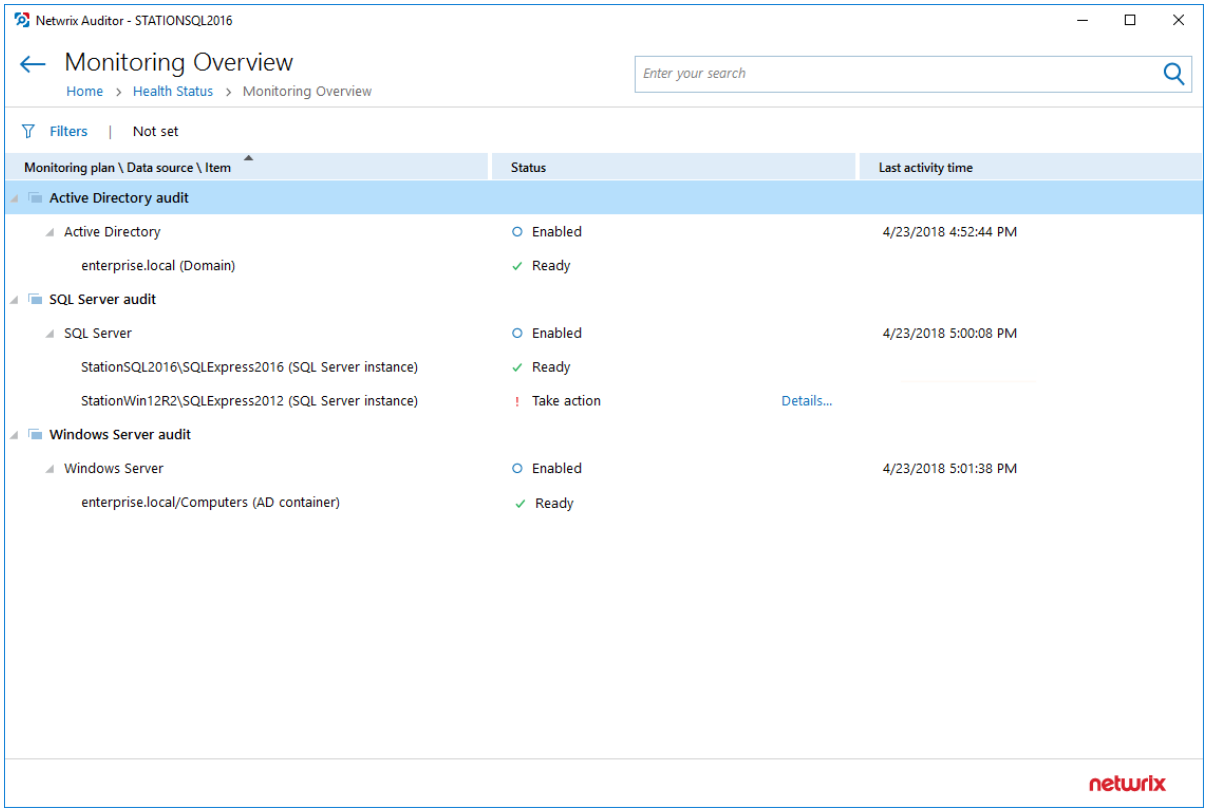
NOTE: If the data sources processed by a monitoring plan did not produce any activity records during the specified timeframe, this monitoring plan will not appear in the list.

9.1.2.2. Monitoring Overview

Aggregated statistics on the monitoring plans is provided in the **Monitoring overview** widget. It displays current statuses of all monitoring plans:

- **Ready (green indicator)**—The monitoring plans (one or several) successfully processed the data sources with all their items and are ready for the next run.
- **Pay attention (yellow indicator)**—The monitoring plans (one or several) require your attention, as some items were not processed completely but only partially. This status applies to the monitoring plans targeted at Logon Activity and Windows File Server. See the table below for details.
- **Take action (red indicator)**—Any data source or item in the monitoring plan (one or several) was processed with errors.

After you click **View details**, the **Monitoring Overview** window will be displayed.



It provides the hierarchical list of monitoring plans, processed data sources and corresponding items with their current status and date/time of the last data processing session. For data sources and items their current status is depicted as follows:

Entity	Status	Description
Data source	Disabled	A data source can be disabled manually via its settings (by switching **Monitor this data source and collect activity data** to OFF), or automatically, if the license is not valid any more (for example, the count of licensed objects was exceeded, or the trial period has expired).
	Empty	No items have been added to this data source

Entity	Status	Description
		yet.
	Enabled	**Monitor this data source and collect activity data** is set to ON in the data source settings.
	Not available	The monitoring plan is corrupted and cannot process its data sources, so it is recommended to remove it and create anew.
	Not responding	Data collector for this data source is not responding. The underlying items will not be displayed for such data source.
	Working	The data source is being processed at the moment.
	(not displayed)	The data source status is unknown.
Item	Pay attention	The item was processed with some issues (non-critical). This status applies to the monitoring plans targeted at Logon Activity and Windows File Server. It means that data collection from at least one entity completed with errors. For example, a **MyFileServer** item included in the File Server monitoring plan contains all CIFS shares hosted on the **MyFileServer** computer. If any of these shares was processed with errors while others were processed successfully, the processing of the whole **MyFileServer** item will be considered partially completed, and the monitoring plan will have a yellow indicator, requiring your attention. Click the **Details** link to examine the product log.
	Ready	The item was processed successfully and is ready for the next run of data collection.
	Take action	Critical error(s) occurred while processing this item. Click the **Details** link to examine the product log.
	Working	The item is being processed at the moment.

You can use the **Search** field, or apply a filter to display the information you need. For example, in the **Apply Filters** dialog you can select the **Show only plans with issues** to display only the monitoring plans that require attention and corrective actions.

This information will help you to troubleshoot the product operation, detect and eliminate the root cause of the monitoring errors, providing for auditing continuity and compliance.

9.1.2.3. Health Log

Daily summary of the Netwrix Auditor health log is displayed in the **Health log** widget. The chart shows how many events with different severity levels were written to the product health log in the last 24 hours. To open the health log, click the corresponding link.

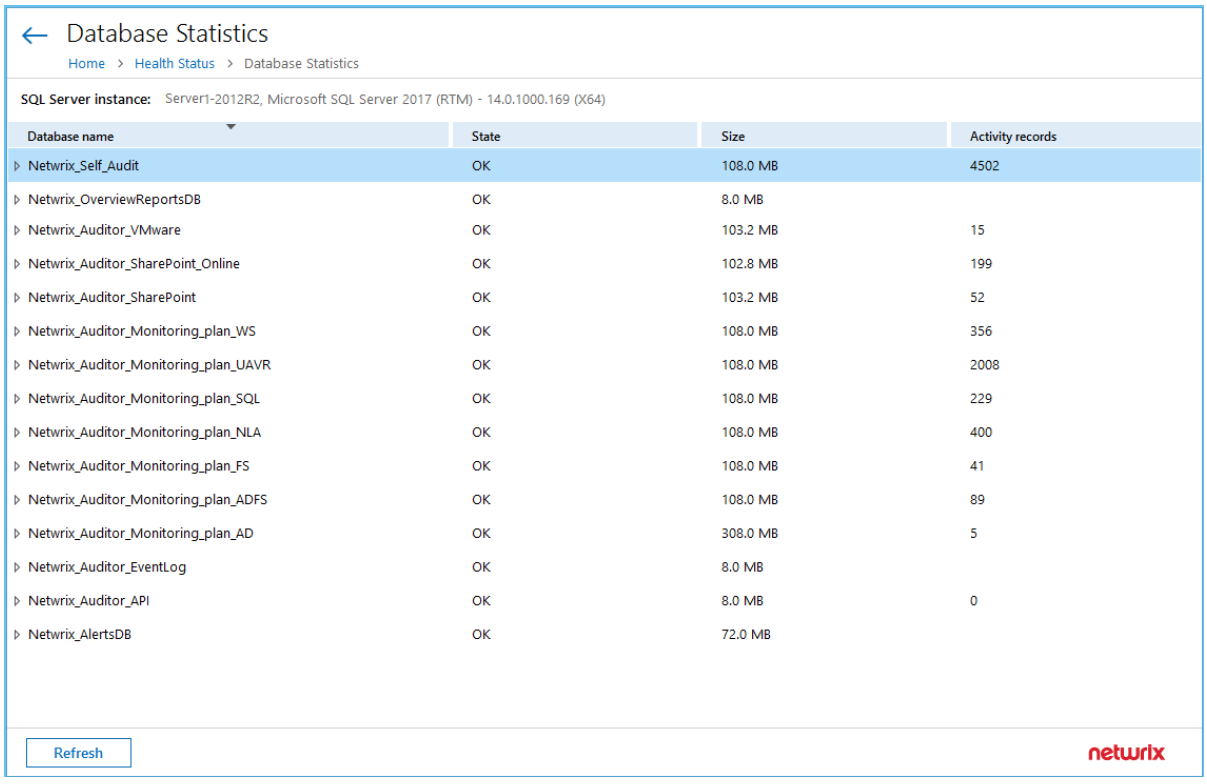
See Inspect Events in Health Log for more information.

9.1.2.4. Database Statistics

Databases may tend to run out of free space due to poor capacity provisioning or to retention settings not configured properly. Use the **Database statistics** widget to examine database size and adjust retention accordingly. The widget displays the name of default SQL Server instance hosting all Netwrix Auditor databases, the overall database capacity at the moment and its change over the last day (24 hours).

NOTE: Transaction logs size is not included in the calculations.

After you click **View details**, the following information will be displayed for the specified SQL Server instance:



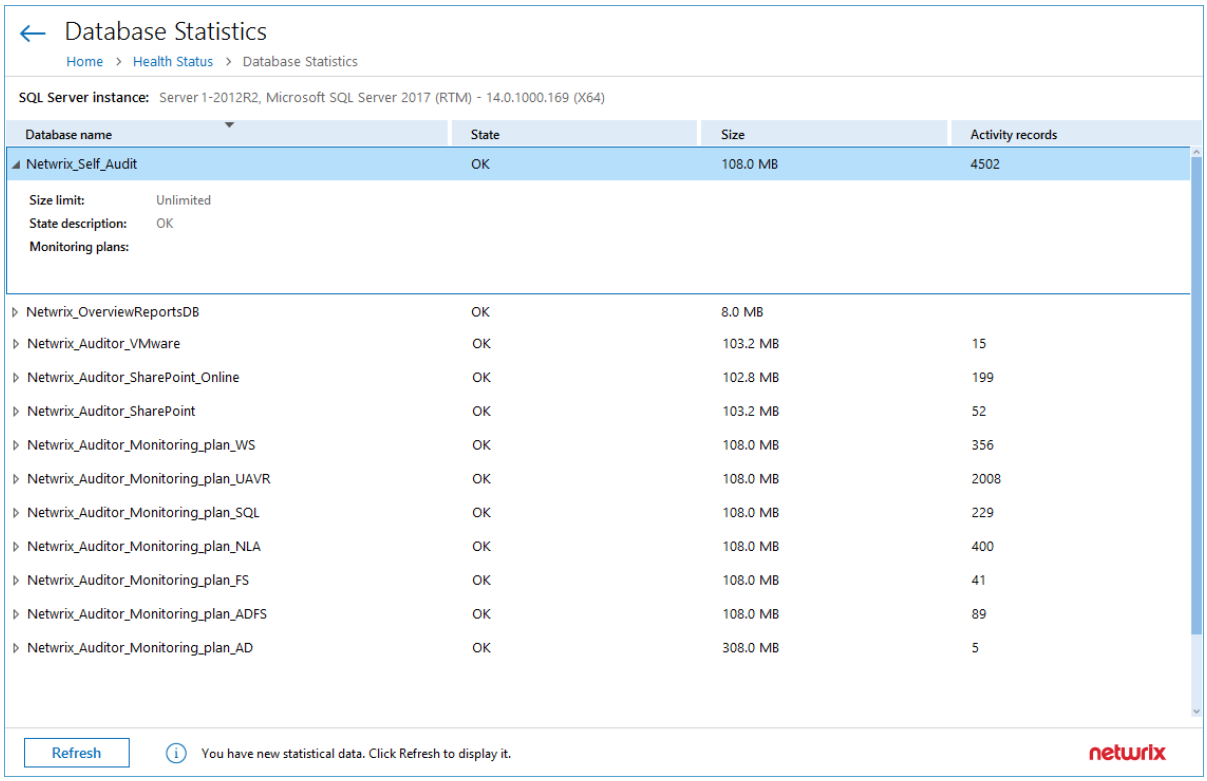
The **Database name** column contains the list of Netwrix Auditor databases hosted by the specified instance of the SQL Server:

- Special databases are created automatically on the default SQL Server instance to store:
  - alerts—*Netwrix_AlertsDB* database
  - activity records collected using Integration API—*Netwrix_Auditor_API* database
  - internal event records—*Netwrix_Auditor_EventLog* database
  - data collected by Netwrix Auditor self-audit—*Netwrix_Self_Audit* database
  - data needed for overview reports generation—*Netwrix_OverviewReportsDB*
- To store data from the data sources included in the monitoring plan, dedicated Audit databases are created and named by user (default name format is *Netwrix_Auditor_<monitoring_plan_name>*)

The following capacity metrics are displayed for each database:

- **State**—database state summary
- **Size**—current database size (logs are not included)
- **Activity records**—number of the activity records stored in the database at the moment

After you expand the database node, the detailed database properties will be shown:



These properties are as follows:

Property	Possible Values	Description
Size limit	*<size_limit>*	For SQL Server Express Edition–shows database size limitations
	Unlimited	
State description	OK	Database is operating properly.
	Capacity error	Database is running low on disk space. -OR- Size limit for SQL Server Express Edition will be reached soon (threshold is 500 MB, i.e. 5% of 10 GB limit remaining).
	Failed to store data	Failed to store data to the database due to some issues.
	Unavailable	Failed to connect to the database.
	Upgrade in progress	Database is being upgraded.
Monitoring plans	*<monitoring_plan>*	All monitoring plans for which this database is a target. **NOTE:** Usually it is recommended to configure a dedicated database for each plan.

You can use the **Search** field, or apply a filter to display the information you need. For example, in the **Apply Filters** dialog you can select the **Show only plans with issues** to display only the monitoring plans that require attention and corrective actions.

This information will help you to troubleshoot the product operation, detect and eliminate the root cause of the monitoring errors, providing for auditing continuity and compliance.

9.1.2.5. Long-Term Archive Capacity

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

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

See Long-Term Archive for more information.

9.1.2.6. Netwrix Auditor Working Folder

The working folder is a file-based storage that keeps operational information (configuration files of the product components, log files, and other data). Netwrix Auditor also caches some audit data in this folder for a short period (up to 30 days) prior to storing it to the Long-Term Archive or Audit database. By default, the working folder is located on the system drive at *%PROGRAMDATA%\Netwrix Auditor*.

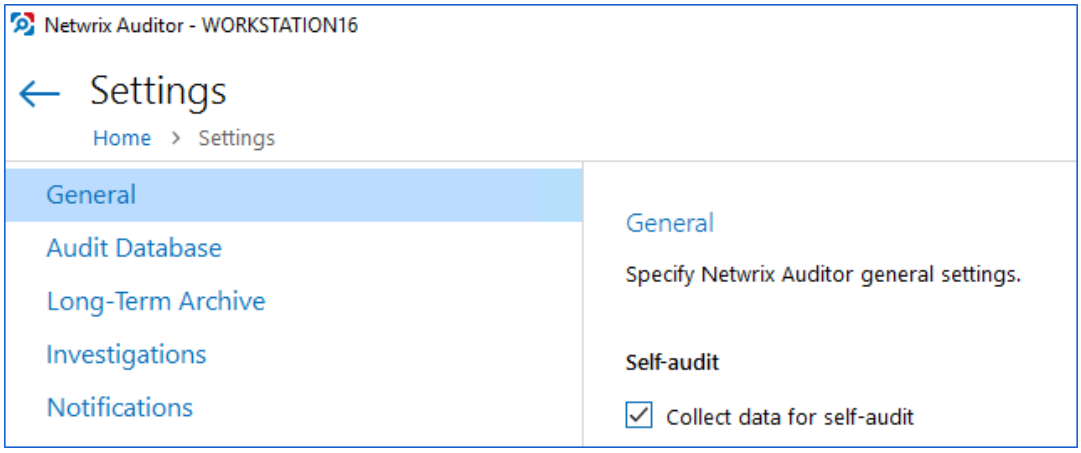
In busy environments and during activity peaks, working folder size may grow significantly. To track the working folder capacity, use the **Working Folder** widget.

NOTE: If you need to change the working folder location, follow the instructions provided in this Knowledge Base article.

9.1.3. Netwrix Auditor Self-Audit

Built-in Netwrix Auditor self-audit allows tracking every change to monitoring plan, data source, and audit scope and details about it (before-after values) so that you know that scope of data to be audited is complete and changed only in line with workflows adopted by our organization.

The "*self-audit*" option is enabled in **Settings** by default.



Review the following for additional information:

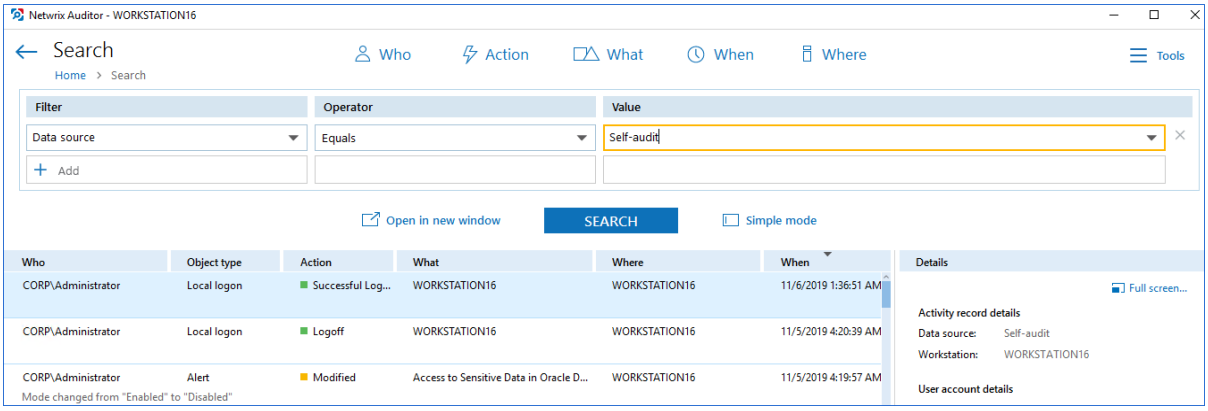
- To search for self audit results
- To review Netwrix Auditor Self-Audit report

To search for self audit results

All Netwrix Auditor self audit Activity Records can be found quickly using **AuditIntelligence Search**.

1. In Netwrix Auditor, navigate to **Search**.
2. Set the "Data source" filter to "Self-audit".

3. Click **Search** to review results:



NOTE: Having reviewed your results, apply filters to narrow your data. See Apply Filters for more information.

After browsing your data, navigate to **Tools** to use the search results as intended. See Make Search Results Actionable for more information.

To review Netwrix Auditor Self-Audit report

Also, there is a new *Netwrix Auditor Self-Audit* report available under **Organization Level Reports** in the predefined set of reports. This report shows detailed information on changes to Netwrix Auditor monitoring plans, data sources and audited items. Use this report to ensure that the scope of data to be audited is complete and all changes are in line with the workflows adopted by your organization.

1. In Netwrix Auditor, navigate to **Reports** → **Organization Level Reports**.
2. Select the **Netwrix Auditor Self-Audit** report and click **View**.

9.1.4. Inspect Events in Health Log

To inspect events in Netwrix Auditor health log

1. On the main Netwrix Auditor page, select the **Health status** tile, then in the **Health log** dashboard widget click **Open health log**.
2. Select an entry to review it in details. You can also copy event details. Select the event in the list and click **Copy details** at the bottom of the window.

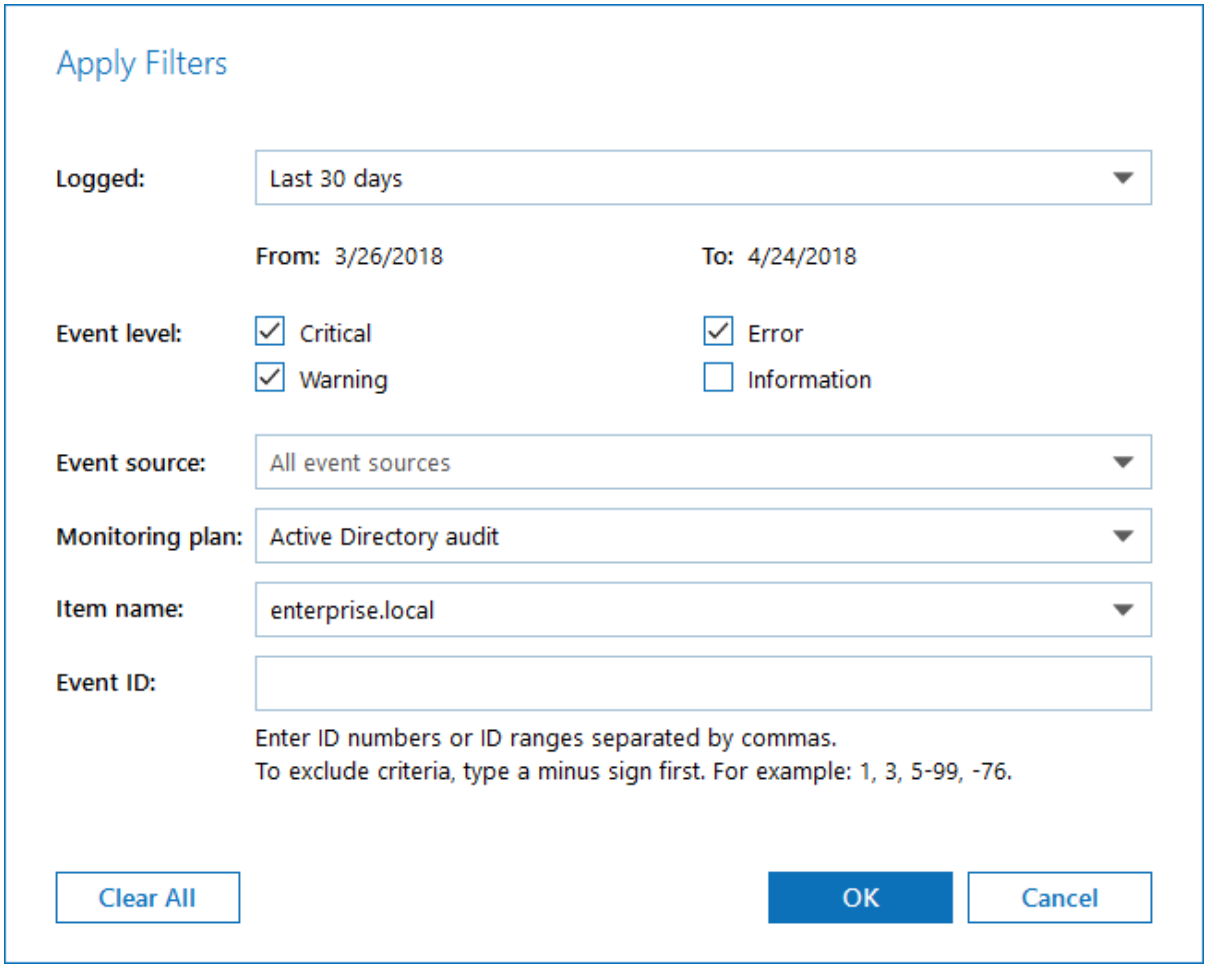
For your convenience, Netwrix Auditor provides you with filters so that you can narrow down the number of events on the screen and focus on those that matter most. For example, warnings on failed data collection or events of an important monitoring plan.

To filter events

1. Select **Filters** in the upper part of the **Netwrix Auditor Health Log** window.

2. Complete the following fields:

Option	Description
Logged	Specify event logging time period (date range, yesterday, etc.).
Event level	Select level of the events that you want to be displayed.
Event source	Select services and applications whose events you want to view.
Monitoring plan	Select to display events from one or several monitoring plans.
Item name	Select to display events from the certain item(s) you need.
Event ID	Enter event ID number or range of event IDs separated by commas. For example, 1, 3, 5-99. **NOTE:** You can also exclude unwanted event IDs from being displayed. Type the minus sign before selected event ID. For example, -76.



The applied filters will be listed on the top of the screen under the window title.

10. Address Specific Tasks with Netwrix Auditor Tools

10.1. 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 inactive users . 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.
Notify managers only once	If this checkbox is selected, managers receive one

Option	Description
	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:

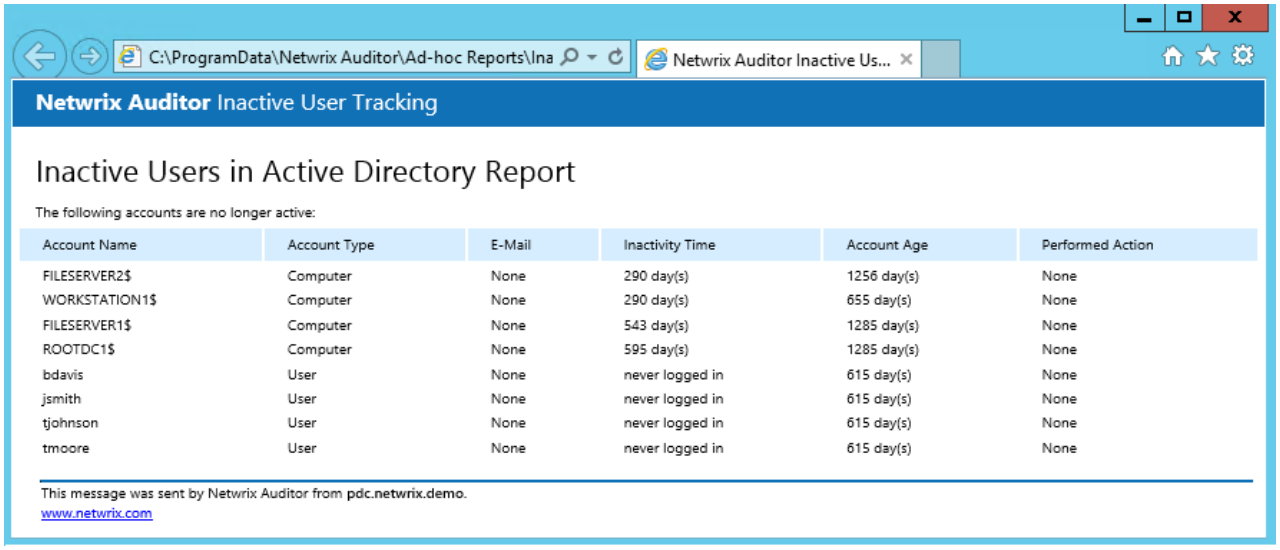
Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the **From** field.

Option	Description
	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.



10.2. 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

Option	Description
	Configuration Guide.
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:

Option	Description
Send report to the users' managers	Enable this option to deliver reports to the user's managers. *To review and edit the user's managers* 1. Start **Active Directory Users and Computers**. 2. Navigate to each group where the user belongs to, right-click it and select **Properties**. 3. In the **<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.

Option	Description
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. In order to send a test email, click **Test** and select an account. Make sure this account has a password that expires within the period you specifed next to this option.
First/Second/Last time when password expires in <> days	Select this option for users to be notified three times, and specify the number of days before the expiration date for each of three notifications. To edit a report template, click **Customize**. You can use HTML tags when editing a template. In order to send a test email, click **Test** and select an account. Make sure this account has a password that expires within the period you specifed next to this option.
Notify users by email every day if their accounts expire in <> days	Select this option for users to be notified daily that their account is going to expire, and specify the number of days before the expiration date.
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.

Option	Description
	• **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. In order to send a test email, click **Test** and select an account. Make sure this account has a password that expires within the period you specifed next to this option.

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	Select this checkbox if your SMTP server requires SSL to be

Option	Description
encrypted connection (SSL)	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. **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:

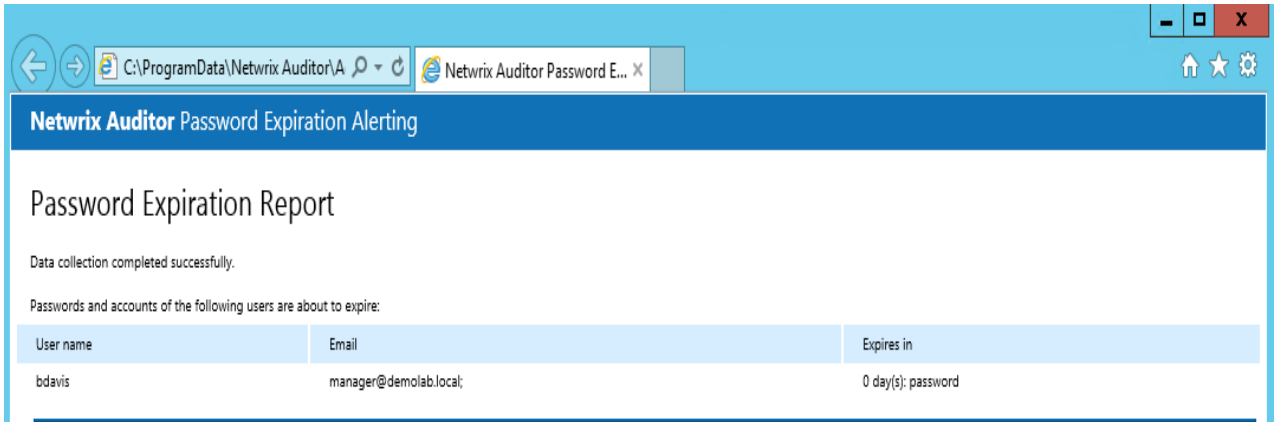
Option	Description
Modify scheduled task start time	The default start time of the scheduled task is 3.00 AM every day. Click **Modify** to configure custom schedule.
Customize the report template	Click **Customize** to edit the notification template, for example, modify the text of the message. You can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

Option	Description
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.



10.3. 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 for Event Logs
- Configure Audit Archiving Filters for Event Log
- Create Alerts for Event Log
- Create Monitoring Plan for Netwrix Auditor System Health Log
- Create Alerts for Non-Owner Mailbox Access Events
- Review Past Event Log Entries
- Import Audit Data with the Database Importer

10.3.1. Create Monitoring Plans for Event Logs

Review the following for additional information:

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

To configure monitoring plan for event logs

1. Navigate to **Start → Netwrix Auditor → Netwrix AuditorEvent 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**

Option	Description
	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

Option	Description
	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.

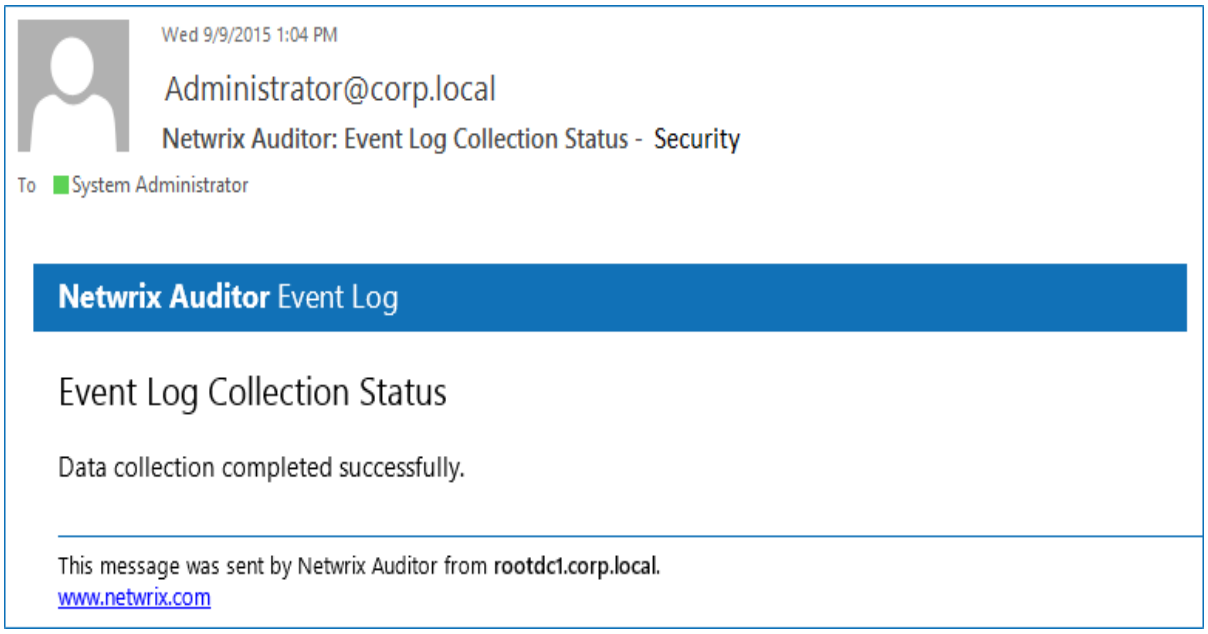
   NOTE: You cannot edit SQL Server settings for **Netwrix Auditor Event Log Manager**.

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.



10.3.2. 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
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.

Option	Description
	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 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.

Option	Description
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**.

10.3.3. Create Monitoring Plan for Netwrix Auditor System Health Log

If you want to generate reports on health state and to be alerted on important Netwrix Auditor health events, you need to create a dedicated monitoring plan for this log with **Netwrix Auditor Event Log Manager** standalone tool.

NOTE: You can also review and filter Netwrix Auditor health events right in the product. See Netwrix Auditor System Health Log for more information.

To configure the Netwrix Auditor System Health log monitoring

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 for 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.

10.3.4. 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.

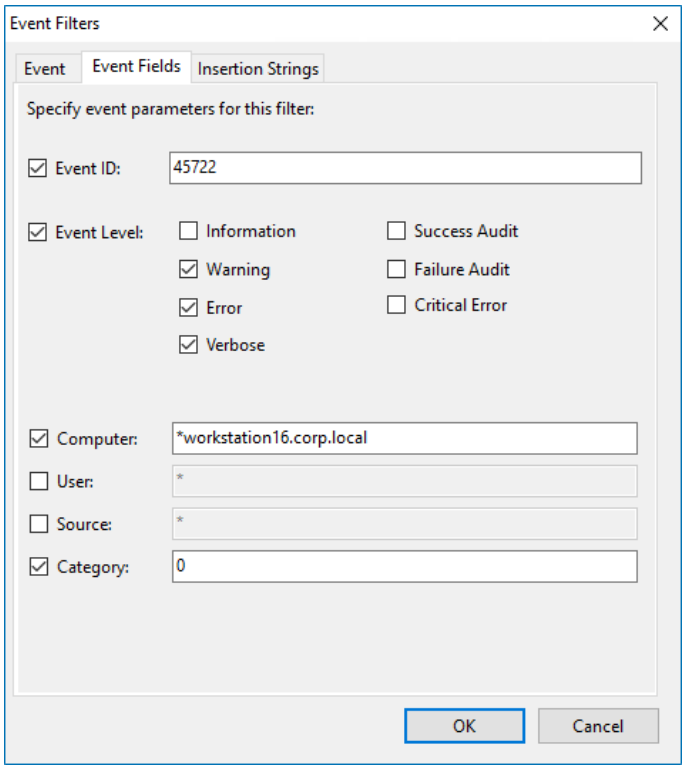
   Complete the **Event Filters** wizard. Complete the following fields:

   - 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: • * - 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.

10.3.5. Create Alerts 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

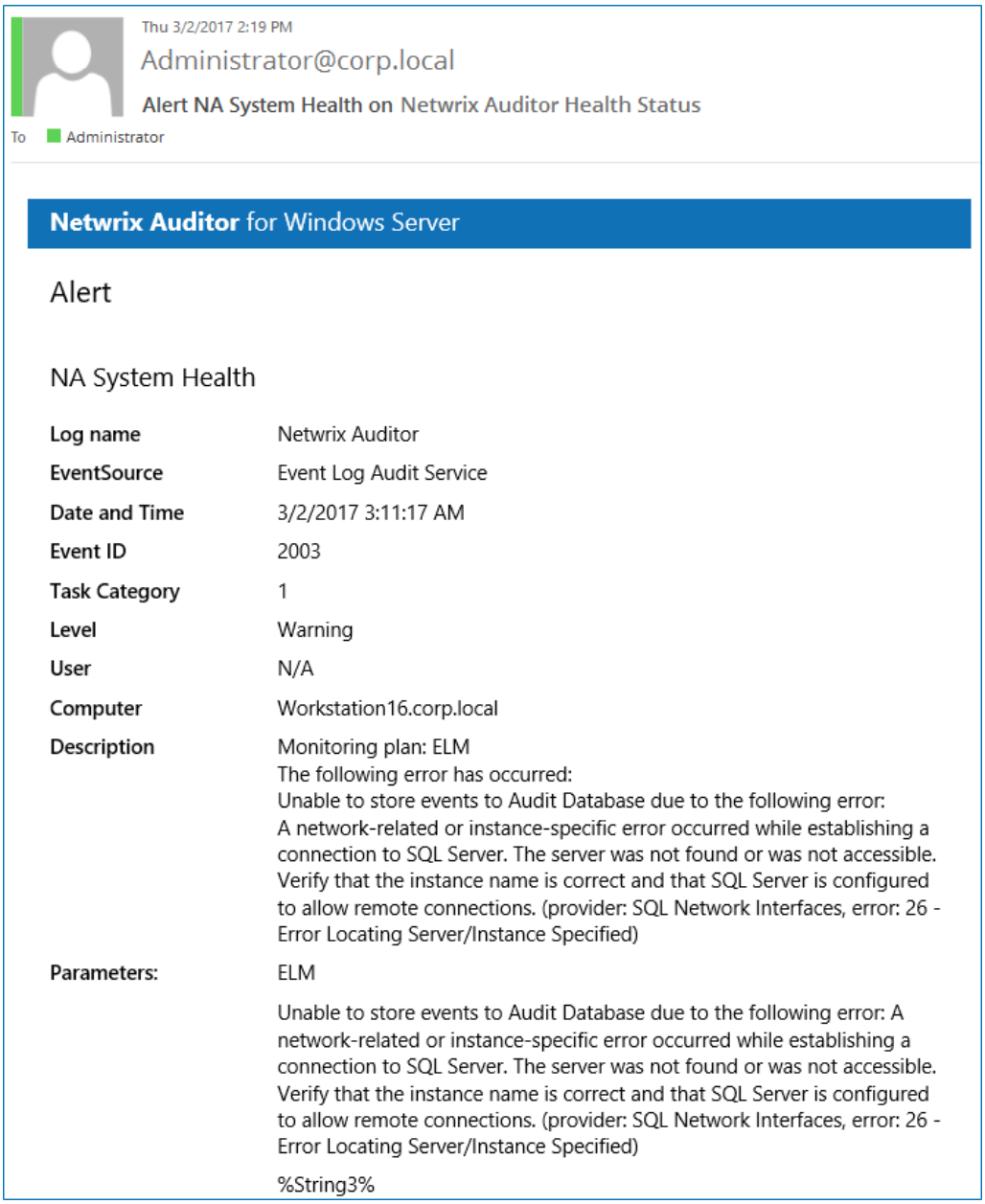
NOTE: The procedure below describes the basic steps, required for creation of the monitoring plan that will be used to collect data on Netwrix Auditor health status events. See Create Monitoring Plans for Event Logs for more information.

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%

10.3.6. 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 for 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

ID	Description	Access Type (as displayed in XML view of event details)
6	A folder was deleted	actFolderDeleted
7	The entire contents of a folder was deleted	actAllFolderContentsDeleted
8	A message was created and saved	actMessageCreatedAndSaved
9	A message was moved or/and copied	actMessageMoveCopy
10	A folder was moved or/and copied	actFolderMoveCopy
14	A folder was created	actFolderCreated

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.

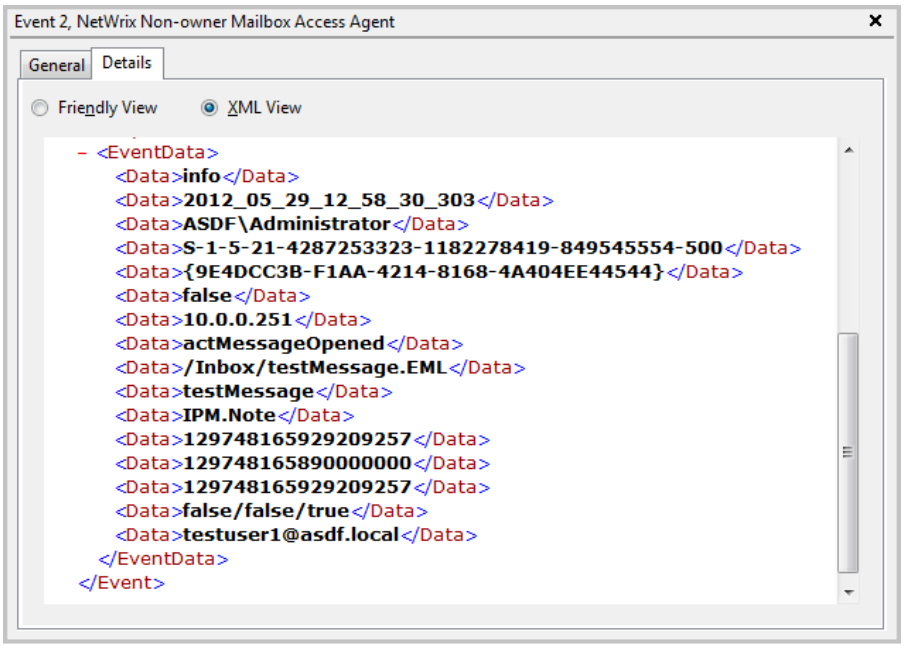
8. In the **Netwrix Auditor Event Log Manager** wizard, navigate to **Notifications** section and specify the email address where notifications will be delivered.

   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

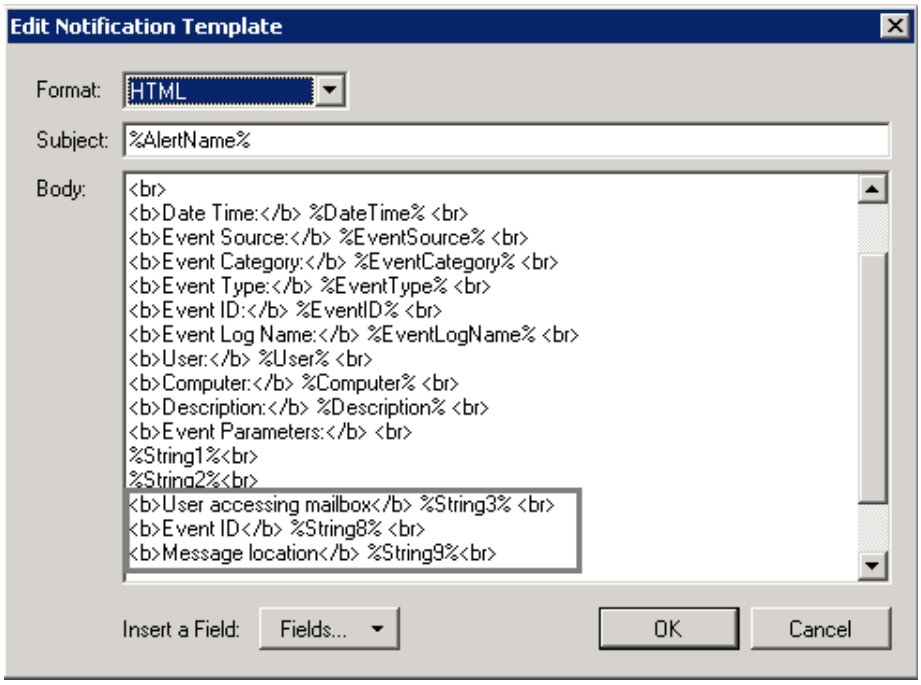
Event ID	Access type (String 8)	Strings	Description
		String12	The destination folder URL
		String13	The message type: IPM.Note— Email, IPM.Contact – contact, etc.
10	actFolderMoveCopy	Strings 9 -13	The string descriptions for the folder are similar to those for messages.
14	actFolderCreated	String9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



10.3.7. 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.

10.3.8. 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**.

10.4. 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

10.4.1. Modify Schema Container Settings

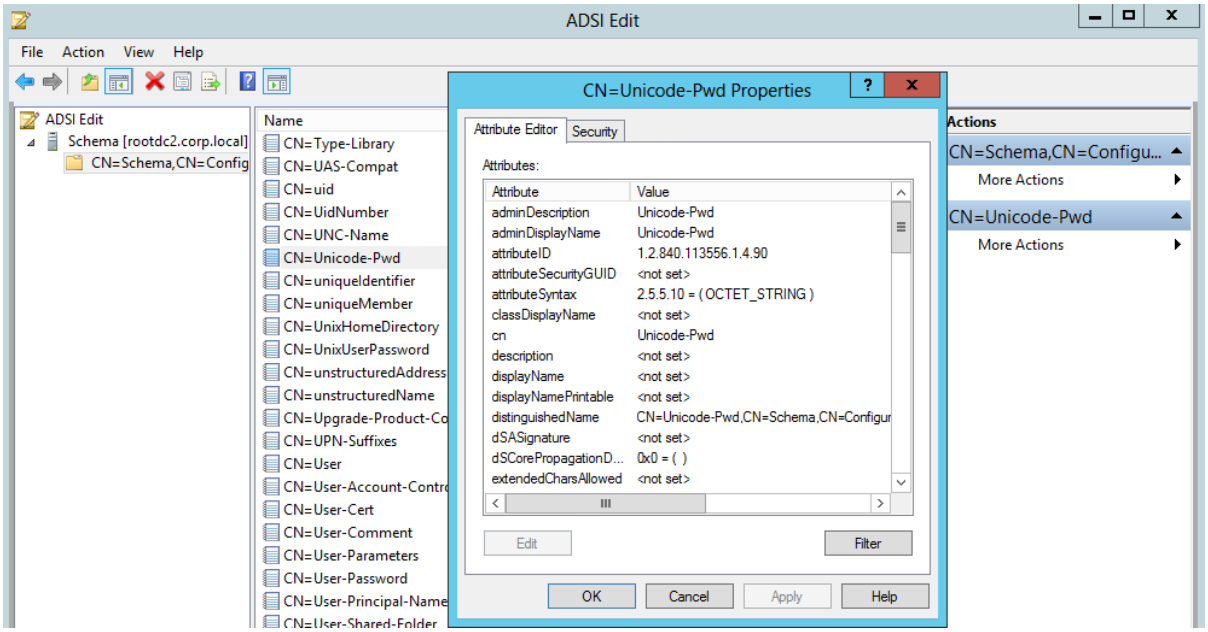
By default, when a user or computer account is deleted from Active Directory, its password is discarded as well as a domain membership. When you restore deleted accounts with the **Netwrix Auditor Object**

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.

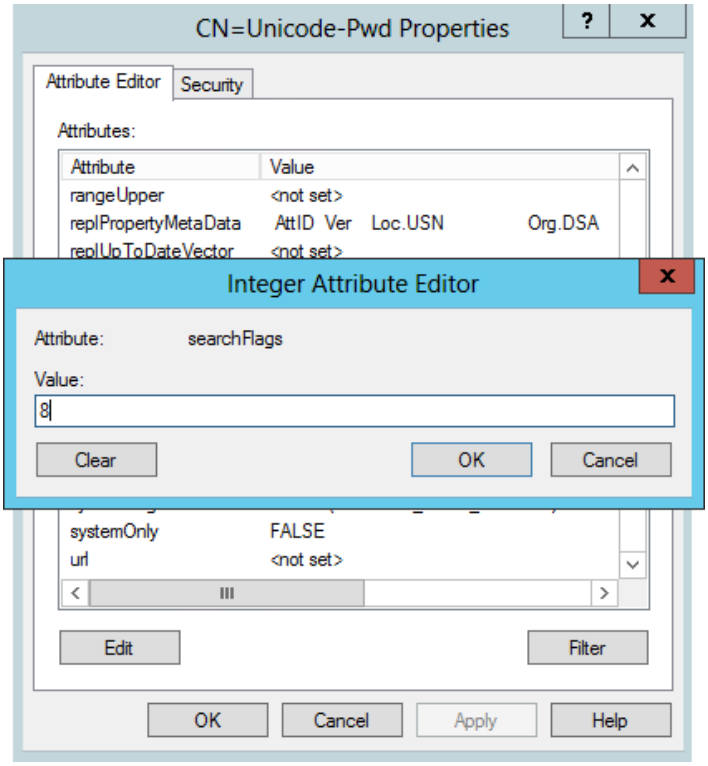
To modify schema container settings

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.

10.4.2. 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 occurred.

Option	Description
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.

11. Additional Configuration

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

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

11.1. Exclude Objects from Monitoring Scope

You can fine-tune Netwrix Auditor by specifying data that you want to exclude from the monitoring 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 monitoring scope, perform the following procedures:

- Exclude Data from Active Directory Monitoring Scope
- Exclude Data from Azure AD Monitoring Scope
- Exclude Data from Exchange Monitoring Scope
- Exclude Data from Exchange Online Monitoring Scope
- Exclude Data from File Servers Monitoring Scope
- Exclude Oracle Database Users from Monitoring Scope
- Exclude Data from SharePoint Monitoring Scope
- Exclude Data from SharePoint Online Monitoring Scope
- Exclude Data from SQL Server Monitoring Scope
- Exclude Data from VMware Monitoring Scope
- Exclude Data from Windows Server Monitoring Scope
- Exclude Data from Event Log Monitoring Scope
- Exclude Data from Group Policy Monitoring Scope
- Exclude Data from Inactive Users Monitoring Scope
- Exclude Data from Logon Activity Monitoring Scope
- Exclude Data from Password Expiration Monitoring Scope

11.1.1. Exclude Data from Active Directory Monitoring Scope

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

To exclude data from the Active Directory monitoring 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 Summary emails. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.
		`Object type:property:`
		
		For example, to show a group description on this group's creation, add the following line:
		`group:description:`

allowedpathlist.txt	Contains a list of AD paths to be included in Activity Summaries, reports, and search results.	`Path` **NOTE:** The path must be provided in the same format as it is displayed in the **What** column. For example, if you only want to monitor specific OU(s) in the AD domain, but not the entire domain. You can put a wildcard (*) in theomitpathlist.txt file to exclude all paths, and then specify the OU(s) you want to monitor in the

File	Description	Syntax
		allowedpathlist.txt file. **NOTE:** Adding the widlcard (*) to **omitpathlist.txt** will not allow Netwrix Auditor to run AD state-in-time data collection.
omitallowedpathlist.txt	Contains a list of AD paths to be excluded from Activity Summaries, reports, and search results. This file can be used if you want to exclude certain paths inside those specified in the allowedpathlist.txt file.	`Path` **NOTE:** The path must be provided in the same format as it is displayed in the **What** column. For example, you can put a wildcard (*) in the omitpathlist.txt file to exclude all paths, then specify the OU(s) you want to monitor in the allowedpathlist.txt file, and then specify the paths you want to exclude from within them in the **omitallowedpathlist.txt** file. **NOTE:** Adding the widlcard (*) to **omitpathlist.txt** will not allow Netwrix Auditor to run AD state-in-time data collection.
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,	`object_type.property_name` **NOTE:** If there is no separator (.)

File	Description	Syntax
	reports, and search results.	between an object type and a property, the whole entry is treated as an object type. For example to exclude the **adminCount** property from reports, add the following line: `*.adminCount`.

omitreporterrors.txt	Contains a list of errors to be excluded from Netwrix Health Log. Thus, these errors will not appear in the Activity Summary emails.	`Error message text`
		
		For example, if you have advanced audit settings applied to your domain controllers policy, the following error will be returned in the Activity Summary emails:
		
		`Auditing of Directory Service Access is not enabled for this DC. Adjust the audit policy settings using the Active Directory Audit Configuration Wizard or see the product documentation for more information.`
		
		Add the text of this error message to this file to stop getting it in the Activity Summary emails.

omitsnapshotpathlist.txt	Contains a list of AD paths to be excluded from AD snapshots.	`Path` **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.

File	Description	Syntax
		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`.
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`

11.1.2. Exclude Data from Azure AD Monitoring Scope

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

To exclude data from the Azure AD monitoring 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`
adomiteventuserlist.txt	Contains a list of users whose user names you want to exclude from Azure AD search results, reports and	`user@tenant.com`

File	Description	Syntax
	Activity Summaries. The rest of change details (action, object type, etc.) will be reported, but the Who value will be "system".	
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 results, reports, and Activity Summaries.	`object=friendlyname`
		
		`object.property=friendlyname`
		
		For example:
		
		`*.PasswordChanged = Password Changed`

proptypes.txt	Defines how values will be displayed in the Details columns in Azure AD	For example:

File	Description	Syntax
	search results, reports, and Activity Summaries.	`*.Role.DisplayName = MultiValued`

11.1.3. Exclude Data from Exchange Monitoring Scope

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

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

To exclude data from Exchange monitoring 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`

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.	`classname.attrname= intelligiblename`
		For example:
		`*- OutlookAnywhere.SSLOffloading = Allow secure channel (SSL)`

File	Description	Syntax
	To exclude a change from the reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`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 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	`FQDN_server_name` For example:

File	Description	Syntax
	excluded from data collection.	`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 monitoring scope

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

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.

NOTE: You can also limit your reports by specific mailboxes. Edit the **mailboxestoinclude.txt** file to specify mailboxes.

File	Description
mailboxestoexclude.txt	This file contains a list of mailboxes and folders that must be excluded from reports. **NOTE:** Folder exclusion is supported for Exchange 2010 only. 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.
mailboxestoinclude.txt	This file contains a list of mailboxes that must be included to reports. You can specify email address to be included in the list. For example, `analyst@enterprise.com`. **NOTE:** In this case, reports will contain only non-owner access events of the mailboxes added to this list.
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 affects reports and snapshots only if **Network traffic compression** is enabled.

11.1.4. Exclude Data from Exchange Online Monitoring Scope

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

To exclude data from Exchange Online monitoring 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	`domain\user`

File	Description	Syntax

	names to be excluded from reports, search results and Activity Summaries.	For example:
		`Enterprise\analyst`
		`email address`
		For example:
		`analyst@Enterprise.onmicrosoft.com`

propnames.txt	Contains a list of human-readable names for object classes and their and their properties to be displayed in search results, reports and Activity Summaries.	`cmdletobject=friendlyname`
		`cmdlet.param=friendlyname`
		For example:
		`RoleGroupMember = Role Group`
		`UMHuntGroup = Unified Messaging Hunt Group`

11.1.5. Exclude Data from File Servers Monitoring 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 monitoring scope.

To exclude data from Windows File Server, NetApp Filer and EMC Storage monitoring 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 monitored.	`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*`

File	Description	Syntax

omiterrors.txt	Contains a list of errors and warnings to be omitted from logging to the Netwrix Auditor System Health event log.	`monitoring plan name,server name,error text`
		For example:
		`*,productionserver1.corp.local, *Access is denied*`

omitreportlist.txt	Contains a list of objects to be excluded from reports and Activity Summary emails. In this case audit data is still being collected.	`monitoring plan name,action,who,object type,resource path,property name`
		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	`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`

File	Description	Syntax
	collected.	

omitstoreprocesslist.txt	Contains a list of processes to be excluded from being stored to the AuditArchive and showing up in reports.	`monitoring plan name,resource path, executable path`
		
		NOTE: Only local applications can be excluded.
		For example:
		`*,*,*notepad.exe`

11.1.6. Exclude Oracle Database Users from Monitoring Scope

You can fine-tune Netwrix Auditor by specifying users that you want to exclude from the Oracle Database monitoring scope.

To exclude data from the Oracle Database monitoring scope

1. In Netwrix Auditor, navigate to your Oracle Database monitoring plan and click **Edit**.
2. In the right pane, select **Edit data source**.
3. Navigate to Users tab and click **Add** next to **Exclude**.
4. In the **Add User** dialog, type name of the user you want to exclude and select its type (OS user or Database user).
5. Click **Add** to exclude selected user from being monitored.

11.1.7. Exclude Data from SharePoint Monitoring Scope

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

To exclude data from SharePoint monitoring scope

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

NOTE: If you have several monitoring plans for monitoring 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

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.

omitscreadaccesslist.txt	Contains a list of site collections for which the product will not monitor read access attempts.	`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.
		For example:
		`http://sharepointsrv:3333/`

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.
		For example:
		`https://siteColl*`

File	Description	Syntax

omitsitscstorelist.txt	Lists site collections to exclude from being monitored and reported in state-in-time report.	`http(s)://URL`
		
		NOTE: Enter root web site URLs.
		
		If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs to specify a child site collection.
		
		You can use a wildcard (*) to replace any number of characters.
		
		Examples:
		`http://siteCollection1:3333/`
		`https://siteColl*`

omitsitstorelist.txt	Contains SharePoint lists and list items that you want to exclude from being audited.	URI Reference
		
		NOTE: URI Reference does not include site collection URL. For example, to exclude the list item with URL *http://sitecollection/list/document.docx*, specify only "*list/document.docx*" instead of full URL.
		
		Wildcard (*) is supported to replace any number of characters.
		
		Examples:
		`*list/document.docx`
		`*/_catalogs/*`
		`*/_vti_inf.html`
		`*/Style Library*`
		`*/SitePages*`

omituserviewstorelist.txt	Contains a list of user or service accounts to be excluded from read access monitoring.	`Login name` For example: SHAREPOINT\System
omitviewstorelist.txt	Contains lists and list items to be excluded from	`URI Reference`

File	Description	Syntax
	being monitored for read access.	**NOTE:** Only specify URI reference to a list or list item without `https:\\<siteCollection_name>` part. For example: `*list/document.docx`

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/`

11.1.8. Exclude Data from SharePoint Online Monitoring Scope

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

To exclude data from SharePoint Online monitoring 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 monitoring 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 monitored for read access.	`https://URL`
		For example:
		`https://Corp.sharepoint.com/*`
		`*list/document.docx`

omituserreadstorelist.txt	Contains a list of user	Provide user name in the UPN format. For example:

File	Description	Syntax
	accounts to be excluded from read access monitoring.	`account@example.*.com`
OmitSitScStoreList.txt	Contains a list of SharePoint Online site collections to be excluded from state-in-time data collection.	Enter root web site URLs. For example: `https://URL`
OmitSitStoreList.txt	Contains SharePoint Online lists and list items to be excluded from state-in-time data collection.	Enter URI (Unique resource identifier, or endpoint) reference. Note that URI Reference does not include site collection URL. For example, to exclude a list item with the `https://sitecollection.sharepoint.com/list/document.docx`, URL, you should specify the corresponding endpoint (URI), i.e. `list/document.docx`.

11.1.9. Exclude Data from SQL Server Monitoring Scope

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

To exclude data from the SQL Server monitoring 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

omitarlist.txt	Lists activity records you want to exclude from showing up in reports, search, and activity summaries.
	
	NOTE: This .txt file has no effect on SQL logons monitoring. To exclude SQL logons from being monitored, use the *omitlogonlist.txt*.
		`Monitoring plan name,`
		`SQL Server instance,object type,`
		`account,workstation,application name`
		
		NOTE: Wildcard (*) is supported and can replace any number of characters.
		
		For the account, workstation, application name fields, you can specify a mixed expression that contains both a value and a wildcard (e.g., Admin*).
		
		For example:
		
		`SQLPlan,Ent-SQL,Table,guest,WksSQL,MyInternalApp`

omitlogonlist.txt	Contains a list of logons to be excluded from being monitored.	`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:

File	Description	Syntax
		`DB_M0,Ent-SQL,SQLFailedLogon,guest,WksSQL,MyInternalApp`

omitobjlist.txt	Contains a list of object types to be excluded from Activity Summaries and reports.
	
	NOTE: This .txt file has no effect on SQL logons monitoring. Use the omitlogonlist.txt to exclude SQL logons from being monitored.
		`object_type_name`
		
		For example:
		
		`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 monitored 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

File	Description	Syntax
		the * character. For example to exclude information about the **Size** attribute of the **Database File** property in all databases: `Database.Database File.Size`.
omitstorelist.txt	Contains a list of 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 monitoring of SQL logons, SQL trace for these logons will be created anyway.	`server\instance name`
pathtotracelogs.t	Contains a list of SQL	`SQLServer\Instance|UNC path`

File	Description	Syntax
xt	Server instances whose traces must be stored locally.	For example: `server\instance|C:\Program Files\Microsoft SQL Server\MSSQL\LOG\`

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`

11.1.10. Exclude Data from VMware Monitoring Scope

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

To exclude data from VMware monitoring 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 aproperty, the whole entry is treated as an object type. For example, to exclude the **config.flags.monitorType** property from reports, add the following line: `*.config.flags.monitorType`.
hidepropvalues.txt	Contains a list of object types and properties to be excluded from the reports	`object_type.property_name=property_value:object_type.hidden_property` For example, to exclude the

File	Description	Syntax
	when the property is set to certain value.	**config.cpuAllocation.shares.level** property when it equals to *"Low"*, add the following line: `*.config.cpuAllocation.shares .level=low:` `*.config.cpuAllocation.shares.shares .`
proplist.txt	Contains a list of human-readable names for object types and properties to be displayed in the reports.	`inner_type:object_ type.property=intelligiblename` **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.`

omitstorelist.txt	Contains a list of objects to be excluded from being saved to data storage and showing up in reports.
	
	NOTE: Audit data will still be collected.
		Monitoring plan name, who, where, object type, what, property name, property value
		
		For example, to exclude internal logons:
		`*,*,*,Logon,*,UserAgent,VMware vim-java*`
		
		NOTE: The following characters must be preceded with a backslash (\) if they are a part of an entry value:
		`*`
		`,`
		`\`
		`?`
		
		NOTE: Characters may be also specified with hex value using *\xnnnn* template.
		
		TIP: The spaces are trimmed. If they are required, use hex notation. For example: `Word\x0020 where \x0020` (with space at the end) means blank character.

11.1.11. Exclude Data from Windows Server Monitoring Scope

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

To exclude data from the Windows Server monitoring 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 monitored.
	
	NOTE: If you want to restart monitoring these objects, remove them from the omitcollectlist.txt and run data collection at least twice.
		`monitoring plan name,server name,class name,property name,property value`
		
		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`
		`#*,*,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.txt	Contains a list of objects to be excluded from reports and Activity Summary emails. In this case audit data is still being collected.	`monitoring plan name,who,where,object type,what,property name`
		
		For example:
		`*,CORP\\jsmith,*,*,*,*`

File	Description	Syntax

omitsitcollectlist	Contains a list of objects to be excluded from State-in-time reports.	`monitoring planname,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`
		`*,*,StdServerRegProv`

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*,*`

11.1.12. Exclude Data from Event Log Monitoring Scope

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

To exclude data from the Event Log monitoring 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`

File	Description	Syntax

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.*`

11.1.13. Exclude Data from Group Policy Monitoring Scope

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

To exclude data from the Group Policy monitoring 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`.
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`.

11.1.14. Exclude Data from Inactive Users Monitoring Scope

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

To exclude data from the Inactive Users monitoring 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 organizational units to be excluded from processing.	`Path`
		
		For example:
		
		`*OU=C,OU=B,OU=A*`

11.1.15. Exclude Data from Logon Activity Monitoring Scope

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

To exclude data from the Logon Activity monitoring scope

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

   NOTE: If you have several monitoring plans for monitoring 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 monitored.	`DC_name`
		For example:
		`<v v= "*ROOTDC1*"/>`

`<n n="Hubs">`	Determines whether to enable network traffic compression for a Domain Controller or not.
	NOTE: If configured, overrides the **Enable network traffic compression** option in monitoring plan configuration.
		`<n n="localhost">`
		`<a n="DCWithCompressionService" t="258">`
		`<v v="DomainControllerNameInFQDNFormat1"/>`
		`</a>`
		`<a n="DCWithoutCompressionService" t="258">`
		`<v v="DomainControllerNameInFQDNFormat2"/>`
		`</a>`
		`<a n="DataCollectionIntervalInSeconds" v="0"/>`
		`</n>`
		`</n>`

`<n n="UserOmitList">`
`<a n="Names">`
	Contains a list of users to be excluded from being monitored.	`User name`
		For example:
		`<v v="*NT AUTHORITY*"/>`

Configuration String	Description	Syntax
	Allows specifying a user by name.	

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

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**"**
' 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

11.1.16. Exclude Data from Password Expiration Monitoring Scope

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

To exclude data from the Password Expiration Alerting monitoring 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*`

11.2. 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 Monitoring Active Directory
- Registry Keys for Monitoring Exchange
- Registry Keys for Monitoring File Servers
- Registry Keys for Monitoring Windows Server
- Registry Keys for Monitoring Event Log
- Registry Keys for Monitoring Group Policy
- Registry Keys for Monitoring Password Expiration
- Registry Keys for Monitoring Inactive Users
- Registry Keys for Monitoring Logon Activity

11.2.1. Registry Keys for Monitoring Active Directory

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

Registry key (REG_DWORD type)	Description / Value
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
IgnoreRootDCErrors	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
LogonResolveOptions	Defines what will be shown in the Workstation field: • 2—MAC address • 4—FQDN or IP address (set by default) • 6—Both
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

Registry key (REG_DWORD type)	Description / Value
	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).

11.2.2. Registry Keys for Monitoring Exchange

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
IgnoreRootDCErrors	Defines whether to display audit check errors for the root domain (when data is collected from a child domain) in the Activity Summary footer: • 0—Display errors • 1—Do not display errors
LogonResolveOptions	Defines what will be shown in the Workstation field:

Registry key (REG_DWORD type)	Description / Value
	• 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 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

Registry key (REG_DWORD type)	Description / Value
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).

11.2.3. Registry Keys for Monitoring File Servers

NOTE: Information in this section refers to EMC VNX and Isilon storage systems and NetApp filers older than 8.3.2.

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

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.

11.2.4. Registry Keys for Monitoring Windows Server

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

Registry key (REG_DWORD type)	Description / Value
HKEY_ LOCAL_ MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Windows Server Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes **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.

11.2.5. Registry Keys for Monitoring Event Log

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager\<monitoring plan name>\Database Settings	
ConnectionTimeout	Defines SQL database connection timeout (in seconds).
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager\<monitoring plan name>\ElmDbOptions	

Registry key (REG_DWORD type)	Description / Value
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: • 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

11.2.6. Registry Keys for Monitoring Group Policy

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups:

Registry key (REG_DWORD type)	Description / Value
	• 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 (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

Registry key (REG_DWORD type)	Description / Value
	• 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 • 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	

Registry key (REG_DWORD type)	Description / Value
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).

11.2.7. Registry Keys for Monitoring Password Expiration

Review the basic registry keys that you may need to configure for monitoring expiring passwords within your Active Directory domain with Netwrix Auditor. Navigate to **Start → Run** and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Password Expiration Notifier	
HideEmailAdditionalInfo	Defines whether to show or hide the header and footer in emails sent to users and their managers (emails sent to administrators always have default header and footer): • 0—Show • Any other number—Hide

11.2.8. Registry Keys for Monitoring Inactive Users

Review the basic registry keys that you may need to configure for monitoring inactive users within your Active Directory domain with Netwrix Auditor. Navigate to **Start → Run** and type *"regedit"*.

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Inactive Users Tracker	
HideEmailAdditionalInfo	Defines whether to show or hide the header and footer in emails sent to managers (emails sent to administrators always have default header and footer):

Registry key (REG_DWORD type)	Description / Value
	• 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

11.2.9. Registry Keys for Monitoring Logon Activity

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

11.3. 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.

11.4. Customize Branding

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

Review the following for additional information:

- Customize Branding in AuditIntelligence Outputs
- Customize Branding in Reports

11.4.1. Customize Branding in AuditIntelligence Outputs

You can customize branding for the following AuditIntelligence outputs:

- Search results delivered as pdf file in the search subscription email;
- Search results exported to pdf file;
- Risk Assessment dashboard exported to pdf file;
- Risk Assessment dashboard delivered in the subscription email;
- Overview dashboard exported to pdf file;
- Overview dashboard delivered in the subscription email.

Rebranding limitations and requirements to logo file

1. Make sure you have full Netwrix Auditor installation: Netwrix Auditor Server and Client to enable rebranding.
2. Since Netwrix applies company's logo as is, keep in mind reasonable limitations of your logo dimensions. You can find examples of appropriate logo files in the rebranding archive (file **Logo.png**). Re-size your logo and verify that subscriptions emails and pdf files look fine after rebranding.
3. Only PNG images can be used as logo files.
4. Endure that image file is located in the default directory or custom folder. Consider the following:
   - For subscription emails, just put the logo file to *%ALLUSERSPROFILE%\Netwrix Auditor\Branding* and run the script to update email look and feel.
   - For exported pdf files, make sure that the logo file is located in the default directory for each user that is going to work with exported search results, Risk Assessment and Overview dashboards. Otherwise, specify custom path to logo file. Default path to logo for exported files is *%LOCALAPPDATA%\Netwrix Auditor\Audit Intelligence\Resources*.

To customize branding

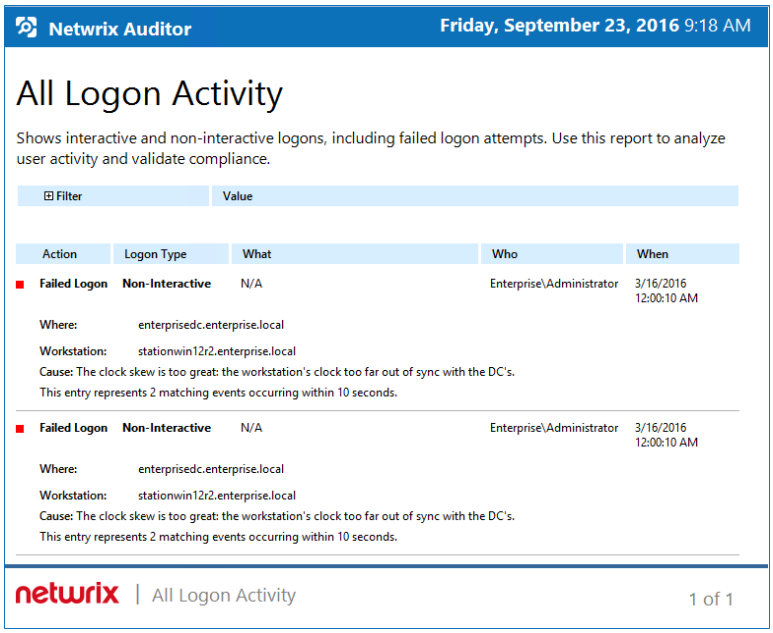
1. On the computer where the Netwrix Auditor Server is installed, navigate to *%ALLUSERSPROFILE%\Netwrix Auditor* and locate the **Rebranding.zip** package.
2. Unzip the package to any folder on the computer where Netwrix Auditor Server is installed.
3. Run **SearchRebranding.ps1** considering the following:
   - Use default paths to logo files—Run the script and type your company name as the `report_title`.
   - Use custom paths to logo files—run the script as follows:

     ```
     SearchRebranding.ps1 -subscriptions_logo_path <custom_path> -export_logo_path <custom_path>
     ```
4. Generate any test subscription email or export a dashboard to pdf file to verify that rebranding applied.

   NOTE: To restore original look and feel, run the script and replace"*True*" with "*False*" in the "*enabled*" section.

11.4.2. 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

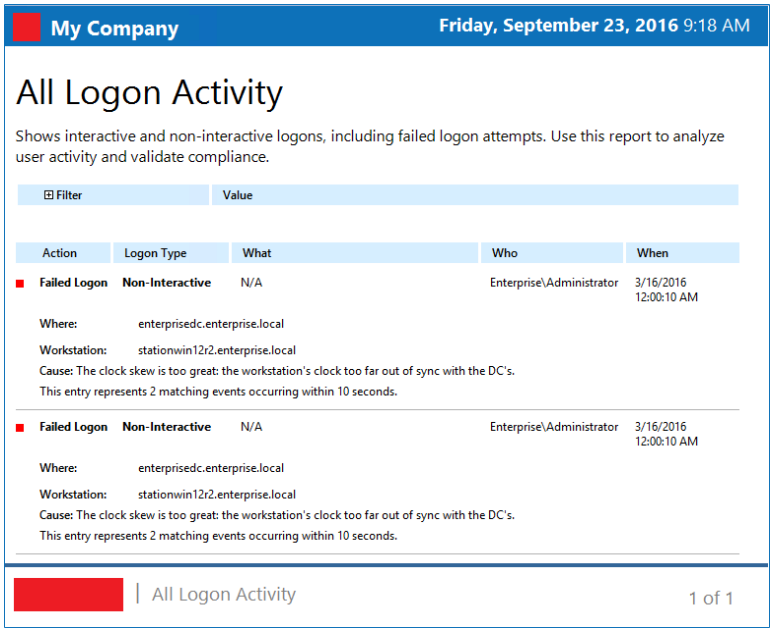
1. On the computer where Netwrix Auditor Server resides, navigate to *C:\Program Data\Netwrix Auditor\Rebranding*.
2. Right-click the **Rebranding.ps1** script and select **Edit**. **Windows PowerShell ISE** will start.
3. Review the script and provide parameters.

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

Parameter	Description
	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.

12. Appendix

This section contains information out of the scope of Netwrix Auditor administration, but is beneficial to Administrators to leverage full scope of the product capabilities. Review the following for additional information:

- Network Traffic Compression

12.1. Network Traffic Compression

To reduce network traffic in distributed deployments, multi-site networks and other environments with remote locations that have limited bandwidth, it is recommended to use network traffic compression. For that purpose, special Netwrix utilities should be installed in the audited environment. These utilities will run on the target computers (depending on your monitoring plan), collect, pre-filter data and send it to Netwrix Auditor Server in a highly compressed format.

With network traffic compression, data from the target machines is collected simultaneously, providing for network load balance and minimizing data collection time. (Unlike that, without network traffic compression the target machines will be processed sequentially, i.e. one at a time.) So, network traffic compression helps to increase scalability and optimize network traffic.

Its key capabilities are as follows:

- Allows Netwrix Auditor to collect detailed metrics for the servers, log files, hardware and individual processes
- Collects audit data with no recognizable load on the server
- Communicates with Netwrix Auditor Server at predefined intervals, relaying data back to a central repository for storage

Network traffic compression is available for the following data sources:

- Active Directory
- Exchange
- File Servers
- EMC
- NetApp
- Windows Server
- Event Logs
- Group Policy
- Logon Activity

- SharePoint
- User Activity

To learn how to enable this feature, refer to the Settings for Data Collectionsection.

Index