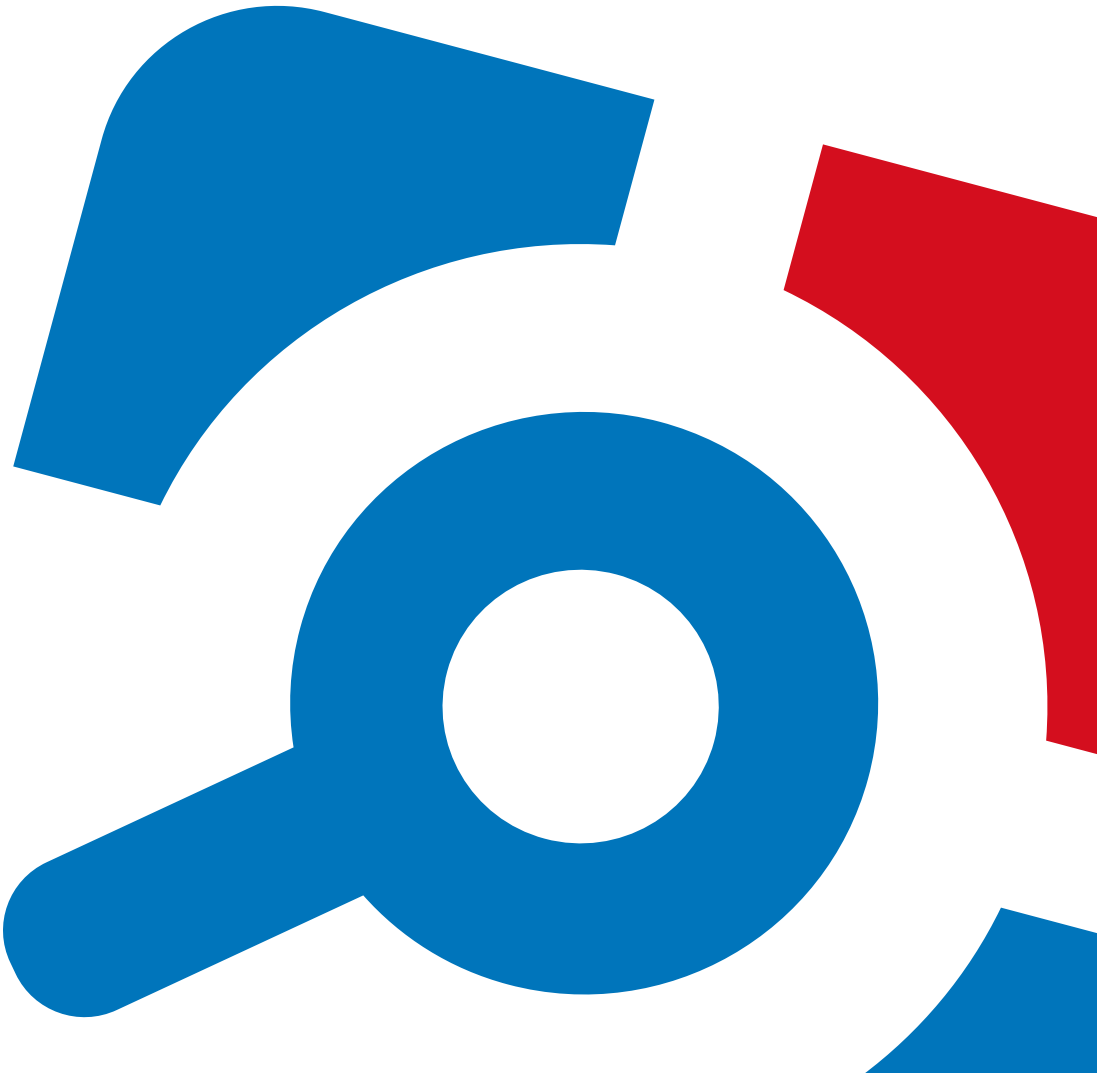
netwrix

Netwrix Auditor

Administrator's Guide

Version: 8.0
4/21/2016



Legal Notice

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

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

Disclaimers

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

Table of Contents

1. Introduction

This guide is intended for Netwrix Auditor administrators and provides step–by–step instructions on how to start auditing IT infrastructure with Netwrix Auditor Administrator Console, configure Audit Database settings and email notifications. It also provides information on fine-tuning the product, additional configuration, etc.

1.1. Netwrix Auditor Overview

Netwrix Auditor is an IT auditing platform that delivers complete visibility into changes and data access in hybrid cloud IT environments by providing actionable audit data about *who* changed *what*, *when* and *where* each change was made, and *who* has access to *what*. Netwrix Auditor helps organizations prevent security breaches caused by insider attacks, pass compliance audits with far less effort and expense, and keep tabs on what privileged users are doing in the environment.

Netwrix Auditor enables auditing of the broadest variety of IT systems, including Active Directory, Exchange, file servers, SharePoint, SQL Server, VMware and Windows Server. It also supports monitoring of privileged user activity in all other systems, even if they do not produce any logs, by enabling video recording of user screen activity and later search and replay. More than 160,000 IT departments worldwide rely on Netwrix Auditor to secure IT infrastructure, prove compliance and increase operational efficiency. The product has earned over 70 awards from leading industry publications, including SC Magazine, Windows IT Pro, Redmond Magazine and WindowSecurity.com.

Major benefits:

- **Change auditing and alerting:** Netwrix Auditor detects all configuration, content and security changes across your entire IT infrastructure. Reports and real-time alerts include the critical who, what, when and where details, including before and after values, enabling quick and effective response.
- **AuditIntelligence interactive search:** Netwrix Auditor enables you to easily search through audit data and fine-tune sorting and filtering criteria so you can quickly hone in on exactly the information you need.
- **Configuration assessment:** State-in-time™ reports show configuration settings at any point in time, such as group membership or password policy settings as they were configured a year ago.
- **Access auditing:** Monitoring of and reporting on successful and failed access to systems and data helps keep sensitive data safe.
- **Predefined reports and diagrams:** Netwrix Auditor includes more than 150 predefined reports and diagrams. Reports can be exported to a range of formats, including PDF and XLS, and stakeholders can subscribe to reports to stay informed automatically by email.
- **AuditArchive™:** Netwrix Auditor's scalable two-tiered storage system (file-based + SQL database)

holds consolidated audit data for more than 10 years.

- **Unified platform:** Many vendors require multiple standalone tools that are hard to integrate, but Netwrix Auditor is a unified platform that can audit the entire IT infrastructure.

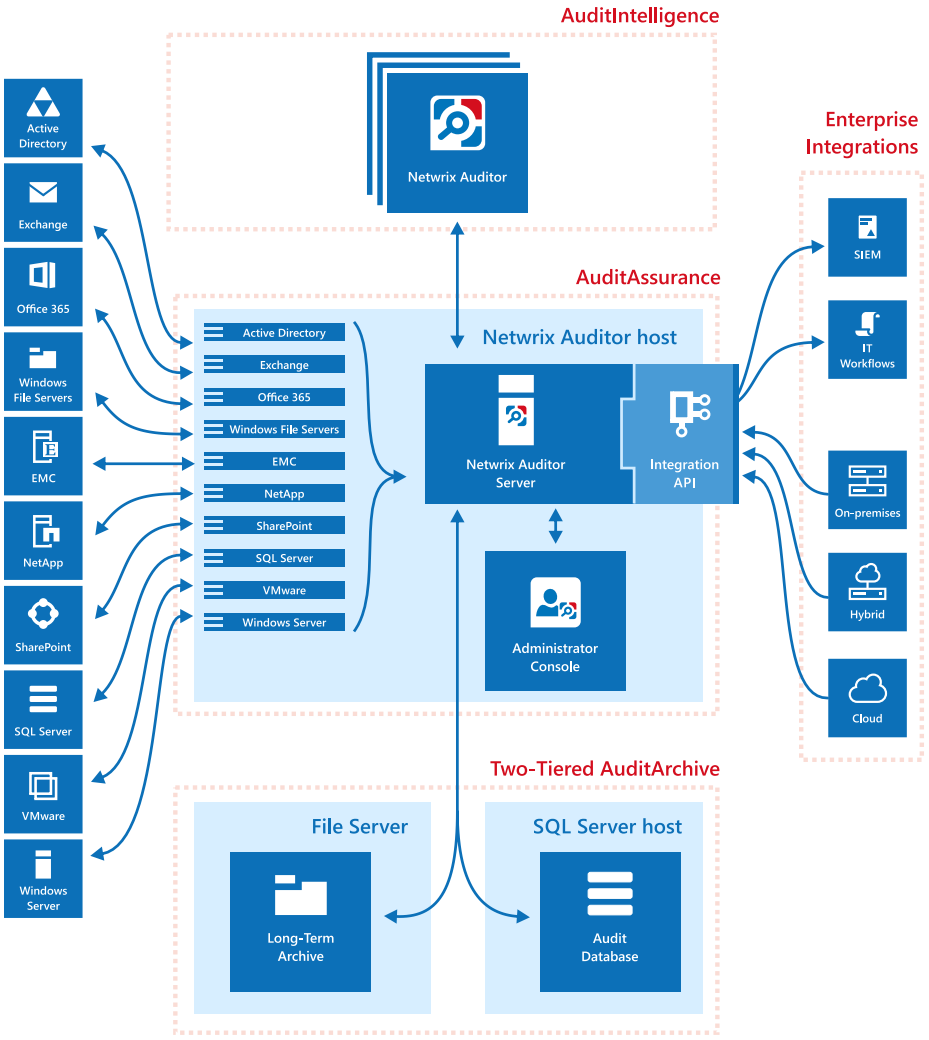
The table below provides an overview of each Netwrix Auditor solution:

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 detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a built–in Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.
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 configuration and permissions. 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.
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 Celerra, VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to

Application	Features
	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 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 and database content.
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. Netwrix Auditor collects Windows event logs and syslog events from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

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



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

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

AuditAssurance is provided by **Netwrix Auditor Server** and **Integration API**. **Netwrix Auditor Server** is a core part of **Netwrix Auditor** that collects, transfers and processes audit data. It contains several internal components responsible for gathering audit data from audited systems. **Netwrix Auditor Server** is managed with **Netwrix Auditor Administrator Console**, an interface for IT administrators designed to

configure IT infrastructure for auditing, define auditing scope, specify data collection, Audit Database and SMTP settings. **Netwrix Auditor Administrator Console** does not provide access to audit data. **Integration API** is a RESTful API that leverages audit data with custom on-premises or cloud data sources even if they are not supported as audited systems yet. API enables integration with third-party SIEM solutions by importing and exporting data to and from Netwrix Auditor.

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

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

1.3. Netwrix Auditor Workflow

This section describes a typical workflow in Netwrix Auditor.

Having installed Netwrix Auditor

A user who installed Netwrix Auditor Administrator Console is referred to as Netwrix Auditor administrator.

1. Netwrix Auditor administrator configures audit settings for systems that are going to be audited with the product.
2. Netwrix Auditor administrator creates the Data Processing Account that is going to collect data from the audited systems. Netwrix recommends to create a special account for it.
3. The Netwrix Auditor administrator grants permissions to the dedicated users (IT managers, business analysts, etc.) to access the Netwrix Auditor client.

See Netwrix Auditor Installation and Configuration Guide for more information.

In Netwrix Auditor Administrator Console

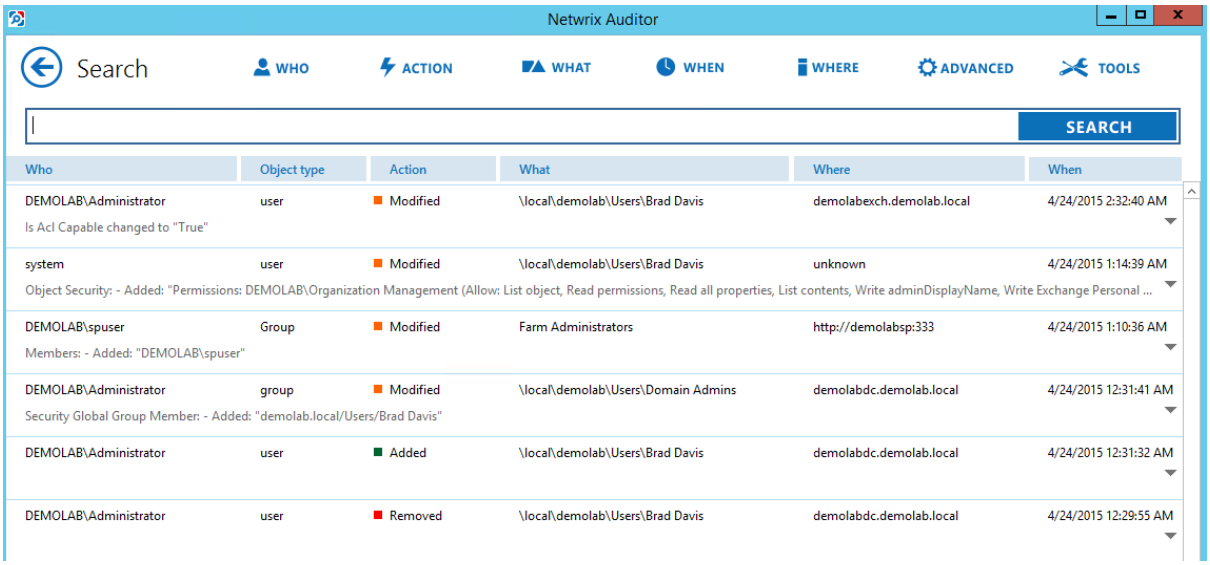
1. An administrator configures Managed Objects—containers that store information on the auditing scope, the Data Processing Account used for data collection, the Change Summary and reports delivery settings, etc. See Managed Objects Overview for more information.
2. The administrator configures the **Audit Database** settings (SQL Server and SSRS settings). See Manage Audit Database for more information.
3. Netwrix Auditor audits IT infrastructure and collects data on changes and state-in-time configuration snapshots. See Data Collection Workflow for more information.

   NOTE: Collected audit data is written to the AuditArchive that includes both the file-based Long-Term Archive and the short-term SQL Server-based Audit Database.

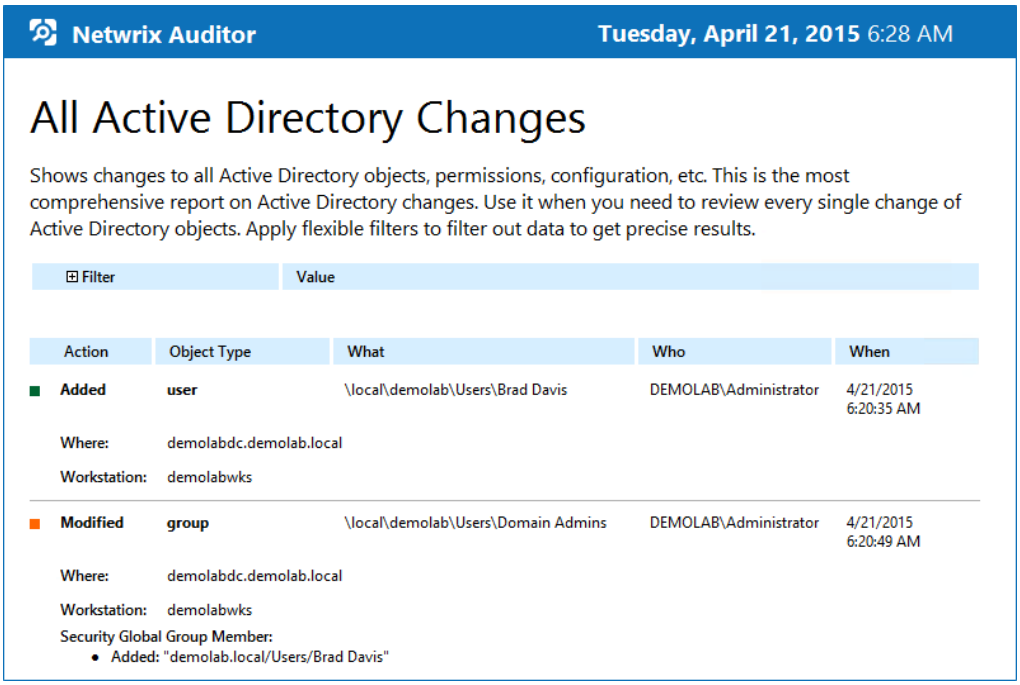
4. For some audited systems, the administrator can configure alerts to be triggered if some critical event is detected. In this case an email notification is sent immediately to the specified recipients. See Real-Time Alerts for more information.
5. By default, the product emails Change Summaries that list all changes that occurred during last 24-hours to the specified recipients daily at 3:00 AM. See Change Summary for more information.
6. The administrator can generate ad-hoc reports to detect inactive users and expiring passwords. See Additional Reports Available in Netwrix Auditor Administrator Console for more information.

In the Netwrix Auditor client

1. IT manager or any user, granted permissions to access to the product, logs in.
2. In the Netwrix Auditor client this user can:
   - Search across audit data



   - Generate reports



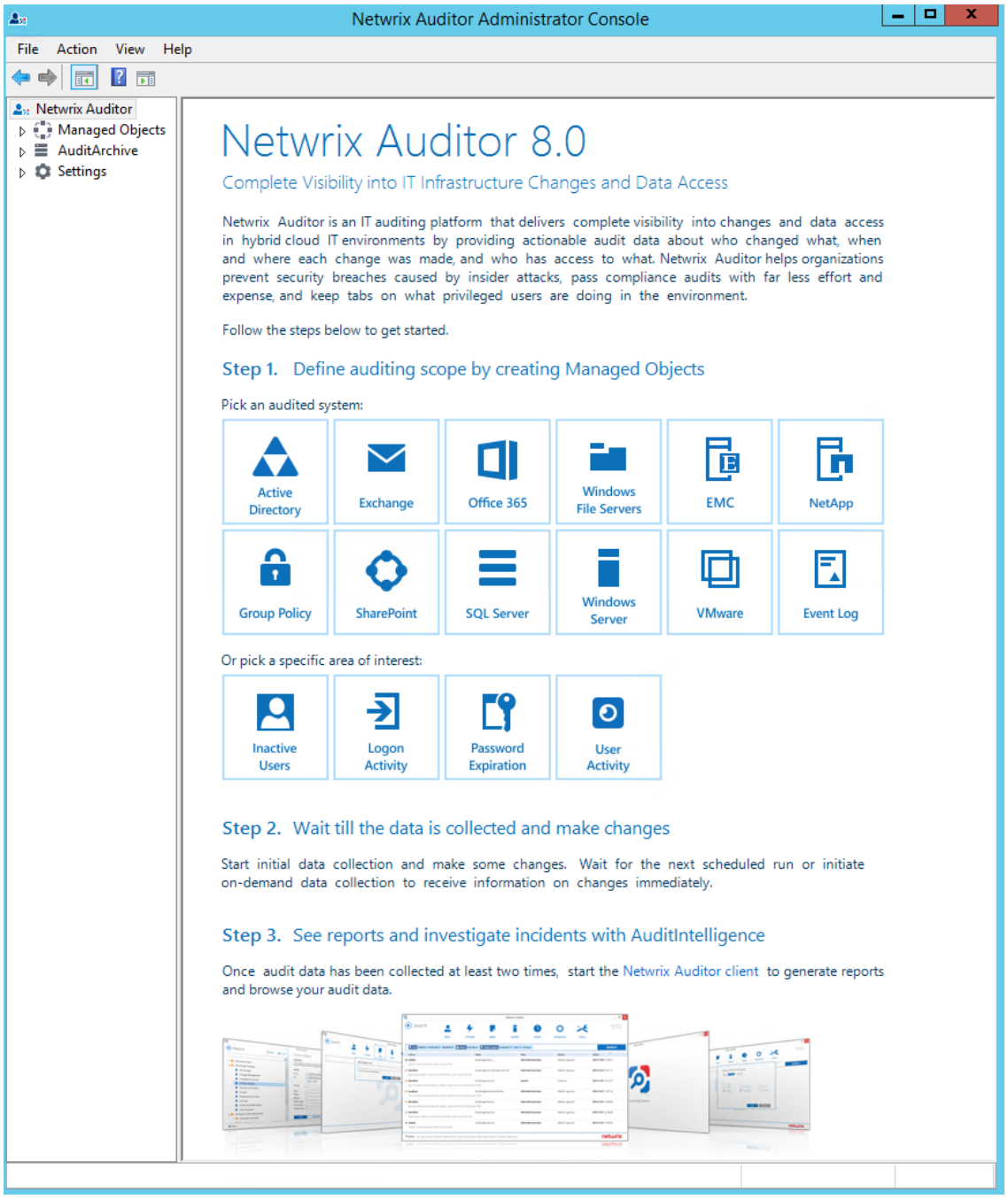
- Create subscriptions
- Save your favorite data searches to access them instantly
- Export audit data in the pdf and csv files.

See Netwrix Auditor User Guide for more information.

2. Launch Netwrix Auditor Administrator Console

To start using Netwrix Auditor Administrator Console

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



3. Start Auditing Your IT Infrastructure

3.1. Managed Objects Overview

To start auditing your IT Infrastructure with Netwrix Auditor, you must create a Managed Object. A Managed Object is a container within Netwrix Auditor that stores information on the auditing scope, the Data Processing Account used for data collection, Audit Database settings, etc.

Review the table below to find out what Managed Object types can be created depending on the system you want to audit:

With this Managed Object...	You can audit...
Domain	Active Directory Exchange Group Policy Inactive users in your AD domain Logon Activity Password expiration in your AD domain
Organizational Unit	Inactive users in your AD organizational unit Password expiration in your AD organizational unit
Office 365	Exchange Online
Computer Collection	File Servers: • Windows file servers • EMC Isilon • EMC Celerra/VNX • NetApp filer appliances SQL Server Windows Server Event Log, including IIS User Activity

With this Managed Object...	You can audit...
SharePoint Farm	SharePoint
VMware Virtual Center	VMware

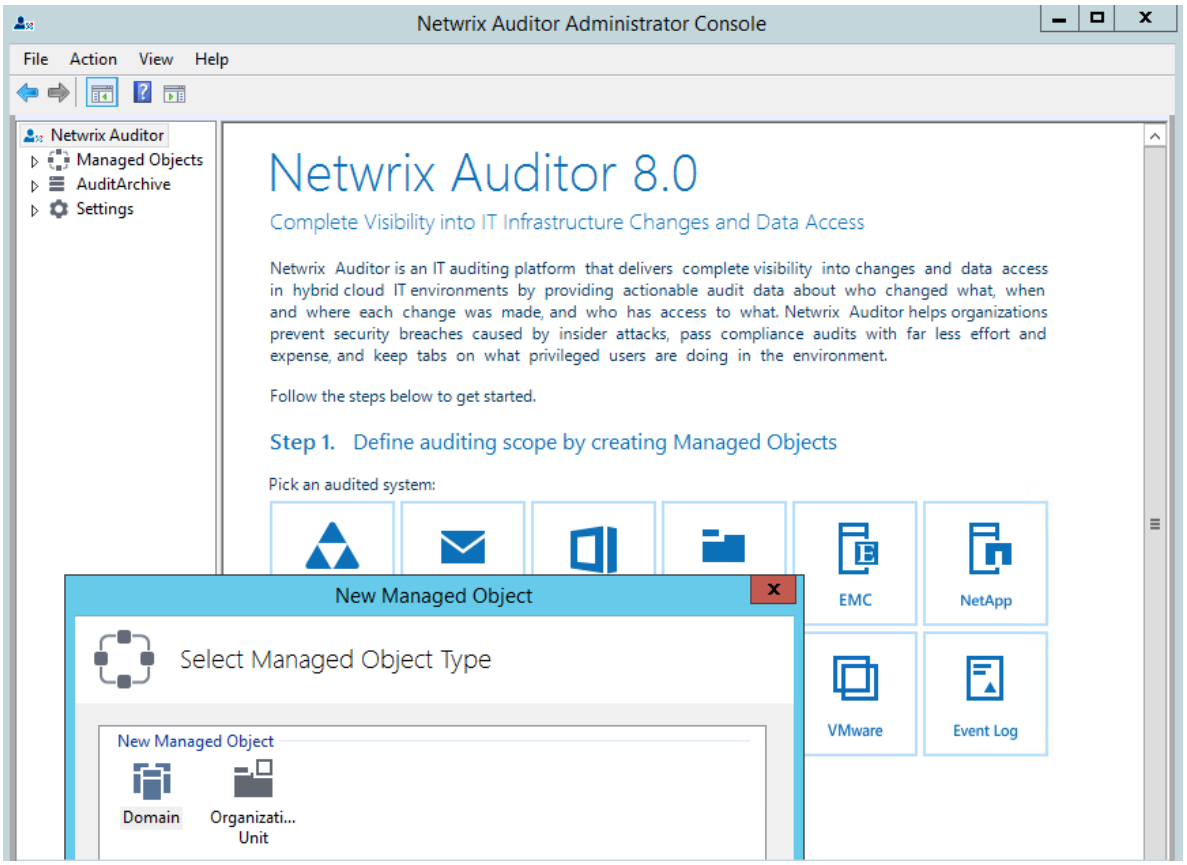
For instructions on how to perform different operations with Managed Objects, refer to the following sections:

- Create Managed Objects
- Group Managed Objects
- Modify Managed Objects
- Delete Managed Objects

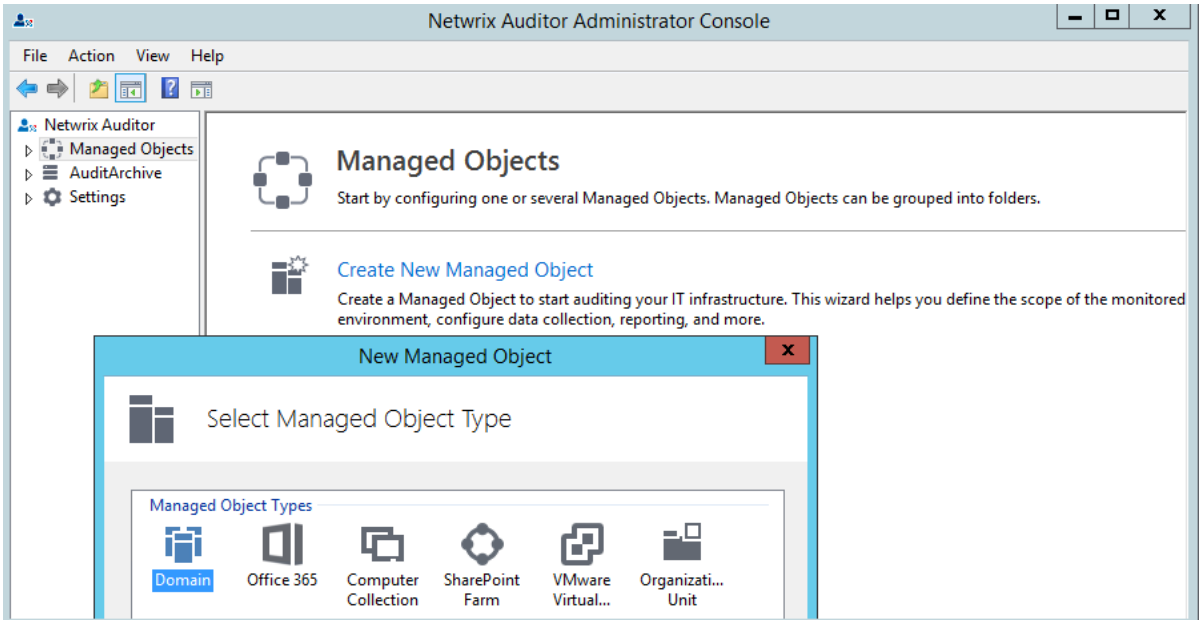
3.1.1. Create Managed Objects

To create a Managed Object, do one of the following:

- On the main Netwrix Auditor Administrator Console page, click the system you want to audit. Some systems can be audited under several Managed Object types (for example, you can audit inactive users within the **Domain** or **Organizational Unit** Managed Object), so you will be prompted to select a Managed Object type on the next step of the **New Managed Object** wizard.



- In the left pane, navigate to the **Managed Objects** node and select **Create New Managed Object** in the right pane. In the **New Managed Object** wizard, select a Managed Object type. Some Managed Objects allow auditing several target systems (for example, within the **Domain** Managed Object you can audit Active Directory, Exchange, Group Policy and Logon Activity). You will be prompted to select the systems you want to audit on the further steps of the **New Managed Object** wizard.



Perform the following procedures to start auditing your IT Infrastructure:

- Create Managed Objects to Audit Active Directory
- Create Managed Objects to Audit Exchange
- Create Managed Objects to Audit Office 365 (Exchange Online)
- Create Managed Objects to Audit File Servers
- Create Managed Objects to Audit SharePoint
- Create Managed Objects to Audit SQL Server
- Create Managed Objects to Audit VMware
- Create Managed Objects to Audit Windows Server
- Create Managed Objects to Audit Event Log
- Create Managed Objects to Audit Group Policy
- Create Managed Objects to Audit Inactive Users in Active Directory

  Create Managed Objects to Audit Logon Activity
- Create Managed Objects to Audit and Alert on Password Expiration in Active Directory
- Create Managed Objects to Audit User Activity

3.1.2. Group Managed Objects

For your convenience, you can group Managed Objects into folders. To create a folder, navigate to the **Managed Objects** node, select **Create New Folder** in the right pane, and specify the folder name. You can drag-and-drop existing Managed Objects into folders, or create new Managed Objects inside folders.

3.1.3. Modify Managed Objects

To modify your Managed Object settings, perform the following procedures depending on the Managed Object type, your audited system and changes you want to apply:

To...	Do...
To modify a list of systems audited within a Managed Object	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. In the right pane, click **Modify Managed Object**. 3. In the **Modify Managed Object** wizard on the **Add/Remove Systems** step, select or clear checkboxes to add or remove systems. 4. Complete the wizard.

To...	Do...
To modify common settings that affect all Managed Objects and all audited systems (such as SMTP settings, licensing, the default Data Processing Account, etc.)	1. In the left pane, navigate to **Settings**. 2. In the right pane, select a subnode depending on the settings you want to modify. 3. Apply the new settings. See Configure Settings for more information.
To modify the settings that affect a specific audited system (for example, enable or disable audit, modify the auditing scope, enable or disable network traffic compression, modify the list of Change Summary recipients, modify the Change Summary delivery schedule, etc.).	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. Expand your Managed Object and select an audited system. 3. In the right pane, modify the required settings. Depending on the audited system, some settings are located in the right pane and can be modified there, while others are invoked as a pop-up dialog after clicking **Configure** next to **Advanced Options/Configure Options/Advanced Settings**. **NOTE:** For more information on the available options and settings, see the Managed Objects creation procedures and Additional Configuration topics.
To change the Data Processing Account for a Managed Object	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. In the right pane, click **Modify Account** next to the **Data Processing Account** section. 3. Update the Data Processing Account. **NOTE:** A custom account must be granted the same permissions and access rights as the default Data Processing Account. See Netwrix Auditor Installation and Configuration Guide for more information.
To modify Active Directory/ Exchange/Group Policy audit settings within your Managed Object	1. In the left pane, navigate to your Managed Object under the **Managed Objects** node. 2. Expand your Managed Object and select an audited system. 3. In the right pane, select **Configure Audit** next to **Audit Configuration**.
To modify the auditing scope	1. In the left pane, navigate to your Managed Object under the

To...	Do...
and recording settings of the Managed Object that audits user activity	**Managed Objects** node. 2. Expand your Managed Object and select **User Activity**. 3. In the right pane, do one of the following: • Click **Specify Users** next to **Users** to limit auditing to certain users. Create a list of users, specify exceptions if necessary. • Click **Specify Applications** next to **Applications** to limit auditing to certain applications. Create a list of applications, specify exceptions if necessary. • Click **Configure Video** next to **Video Recording Settings** to modify recording quality, duration and retention settings.

3.1.4. Delete Managed Objects

1. In the left pane, navigate to your Managed Object under the **Managed Objects** node.
2. Right-click a Managed Object and select **Delete**.

NOTE: After deleting a Managed Objects, its audit data remains in the AuditArchive.

3.2. Create Managed Objects to Audit Active Directory

1. Do one of the following:
   - On the main Netwrix Auditor Administrator Console page, click the **Active Directory** tile. In this case you will be prompted to select **Domain** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Domain** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Active Directory** as the audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Domain Name** step, specify the audited domain name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter the credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

Option	Description
	SQL Server Settings
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.

Option	Description
	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.
	SQL Server Reporting Services Settings
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **State-in-Time Reports** step, you can enable or disable **State-in-Time Reports**. This feature allows generating reports on your system configuration state at a specific moment of time in addition to change reports. If enabled, snapshots will be created daily and written to the Audit Database. This option is unavailable if the **Audit Database** settings are not configured.
7. On the **Select Data Collection Method** step, 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.
8. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

NOTE: This method is recommended for evaluation purposes in test environments. 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.

- **Manually**

  For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

NOTE: Netwrix recommends you to exclude read-only domain controllers from the Active Directory auditing scope. See Exclude Data from Active Directory Auditing Scope for more information.

9. On the **Specify Active Directory Change Summary Recipients** step, click **Add** to specify the emails where Change Summaries are to be sent.

   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.

10. On the **Configure Real-Time Alerts** step, enable or disable the predefined alerts, or click **Add** to configure custom alerts. See Real-Time Alerts for more information.

11. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.3. Create Managed Objects to Audit Exchange

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **Exchange** tile. In this case you will be prompted to select **Domain** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Domain** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Exchange** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data

Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Domain Name** step, specify the audited domain name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter the credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

Option	Description
	SQL Server Settings
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.

Option	Description
	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.
	SQL Server Reporting Services Settings
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Select Data Collection Method** step, 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.
7. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

     NOTE: This method is recommended for evaluation purposes in test environments. 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.

- **Manually**

  For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

8. On the **Specify Exchange Change Summary Recipients** step, click **Add** to specify the emails where Change Summaries are to be sent.

   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. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

In addition to change auditing, you can configure Netwrix Auditor to audit non-owner access to mailboxes. See Start Auditing Mailbox Access for more information.

3.4. Create Managed Objects to Audit Office 365 (Exchange Online)

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **Office 365** tile.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Office 365** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Exchange Online** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Office 365 Account** step, specify email address and password of your personal Microsoft account that will be used to connect to the audited Exchange Online organization.

   NOTE: The necessary Exchange admin roles must be assigned to this account. See Netwrix Auditor Installation and Configuration Guide for more information.

5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

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

Option	Description
Password	Enter a password.
SQL Server Reporting Services Settings	
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

     NOTE: This method is recommended for evaluation purposes in test environments. 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.

   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

7. On the **Specify Exchange Online Change Summary Recipients** step, click **Add** to specify the emails where Change Summaries are to be sent.

   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.

8. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

In addition to change auditing, you can configure Netwrix Auditor to audit non-owner access to mailboxes. See Start Auditing Mailbox Access for more information.

3.5. Create Managed Objects to Audit File Servers

1. Do one of the following:
   - On the main Netwrix Auditor Administrator Console page, click the **Windows File Servers**, **EMC** or **NetApp** tile. In this case you will be prompted to select **Computer Collection** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **File Servers** as the audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

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

Setting	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

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

Option	Description
User name	Specify the account to be used to connect to SSRS.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **State-in-Time Reports** step, you can enable or disable **State-in-Time Reports**. This feature allows generating reports on your system configuration state at a specific moment of time in addition to change reports. If enabled, snapshots will be created daily and written to the Audit Database. This option is unavailable if the **Audit Database** settings are not configured.

   By default, Netwrix Auditor collects data on effective permissions in addition to configuration and settings. Refer to Effective access permissions for information on how to adjust or disable this option.

   NOTE: The following reports on effective permissions can be generated for Windows file servers only: Account Permissions, Object Permissions by Object, and Excessive Access Permissions.

7. On the **Add Items to Computer Collection** step, click **Add** to select items that you want to audit. You can add several items to collection. In the **Computer Collection New Item** dialog that opens, select the item type:

   - **EMC Celerra/VNX**—On the **Specify Items** step, provide a server name by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network. Select **Only these** and click **Add** to select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.
   - **EMC Isilon**—Complete the following:

     1. On the **Specify Items** step, provide a server name by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network. Select **Only these** and click **Add** to select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.
     2. On the **Configure EMC Isilon Auditing** step, complete the following fields:

Option	Description
Provide a name of Access Zone you want to audit	Enter the name of access zone on your file server (e.g., zone1).
Provide URL for Isilon OneFS web administration interface	Enter EMC Isilon web administration URL (e.g., *https://172.28.15.126:8080/*).
Provide a 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*\).

- **NetApp Filer**—Complete the following:

  1. On the **Specify Items** step, provide a server name by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network. Select **Only these** and click **Add** to select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.
  2. On the **Configure NetApp Filer Auditing** step, complete the following fields:

Option	Description
Use protocol	Select one of the following: • **Automatically detected** — 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 account	Select an account to be used to collecting data from NetApp Filer. If you want to use a specific account (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. The credentials are case sensitive. **NOTE:** See Netwrix Auditor Installation and Configuration Guide for more information on required rights and permissions.

Option	Description
Provide a File Share UNC path to audit logs	Select one of the following: • **Automatically detected**—If selected, a shared resource will be detected automatically. • **UNC path**—Path to the file share located on a NetApp Filer with event log files (e.g., *CORP**ETC$**log*\).

- **Windows File Share**—Provide a path to a shared resource.
- **Windows Server**—Complete the following fields:

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 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 Computers** dialog, click **Add** and specify an object. **NOTE:** The list of containers does not include child domains of trusted domains. Use other options (**Computer name**, **IP address range**, or **Import computer names from a file**) to specify the target computers.
IP address range	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**.
Import computer names from a file	Allows specifying multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it automatically.

Option	Description
	If you select the **Import on every data collection** option, you can later modify the list of your audited computers by editing the .txt file. The audited computers list will be updated on the next data collection.

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

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

8. On the **Select Data Collection Method** step, 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.
9. On the **Configure Audit in Target Environment** step, select one of the following:
   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly. If you select to automatically configure audit in the target environment, your current audit settings will be periodically checked and adjusted if necessary.

File Server	SACL Check	SACL Adjust	Policy Check	Policy Adjust	Log Check	Log Adjust
Windows	+	+	+	+	+	+
EMC Celerra	+	+	+	—	+	—
EMC Isilon	n/a	n/a	+	—	n/a	n/a
NetApp Data ONTAP 7 and 8 in 7-mode	+	+	+	+	+	+
NetApp Clustered Data ONTAP 8	+	+	+	—	+	—

NOTE: This method is recommended for evaluation purposes in test environments. For a full list of settings required to collect comprehensive audit data and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

- **Manually**

  For a full list of audit settings and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

Netwrix Auditor checks audit settings and notifies on errors even if automatic audit configuration is disabled.

10. On the **Configure File Server Auditing Settings** step, add recipients, to whom the audit reports on file/folder modifications and audit reports on file/folder read access will be sent. Specify actions you want to track.

Access Type	Description
Successful modifications	Commonly used option to track important data. Helps find out *who* created, modified, moved, renamed or removed files and *when* these changes were done.
Failed modification attempts	Used to track suspicious activity on your file server. Helps find out *who* tried to change or delete files, etc., but failed to do it. Investigate incidents with AuditIntelligence and figure out *why* that user tried to do it.
Successful reads	Used to supervise important files with confidential information for privileged users only. Browse your audit data in the Netwrix Auditor client and discover *who* accessed important files besides your trusted users. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.
Failed read attempts	Used to track suspicious activity. Helps find out *who* was trying to read files, but failed to do it. Investigate your incidents with AuditIntelligence and figure out *why* that user tried to do it. **NOTE:** Netwrix recommends not to enable this option for frequently used files in public shares as it will lead to logging a great many read events in your Audit Database.

Click **Configure** next to **Advanced settings** or **Audit trail settings** to customize processing settings. Review the following for additional information:

Option	Description
	Advanced settings
Attach as a CSV file	Select this option to receive reports as attachments. Otherwise, you will receive reports as a part of the email body. You can select **Archive before sending** to receive reports in a compressed format.
Enable integration with third-party SIEM products	See Enable Integration with Third-Party SIEM Solutions for more information.
	Audit trail settings
Basic mode (large servers)	Select this option to process only native audit events generated by Windows Security event log. This option is recommended to speed up data collection from file servers storing a large amount of data (500 000 and more files).
Enhanced mode (small servers)	Select this option to process attributes and permissions in addition to native Windows audit events.

11. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.6. Create Managed Objects to Audit SharePoint

1. Do one of the following:
   - On the main Netwrix Auditor Administrator Console page, click the **SharePoint** tile.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane.

   See Managed Objects Overview for more information.
2. On the **Select Managed Object Type** step, select **SharePoint Farm** as a Managed Object type.
3. On the **Specify Default Data Processing Account** step, click **Specify Account**.

NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

4. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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. On the **Specify SharePoint Farm** step, enter the SharePoint Central Administration website URL. If you want to use a specific account to access data from this SharePoint Farm (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.

NOTE: Netwrix Auditor cannot verify the Central Administration URL address if your Data Processing Account does not belong to the **Farm Administrators** group on your SharePoint Central

Administration site. It does not affect the product operability, you can proceed with the Managed Object creation.

6. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

Option	Description
	SQL Server Settings
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:

Option	Description
	• 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.
SQL Server Reporting Services Settings	
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

7. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

     NOTE: This method is recommended for evaluation purposes in test environments. 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.

- **Manually**

  For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

8. On the **Configure SharePoint Auditing Scope** step, select the type of changes you want to track and the scope of objects that will be audited in addition to SharePoint farm configuration.

   Complete the following fields:

Option	Description
Audit SharePoint farm configuration changes	SharePoint configuration changes are always audited.
Audit SharePoint permission 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 **Specified SharePoint objects** and click **Specify**. In the **Specify SharePoint Objects** dialog, do one of the following: • Click **Add** and provide URL to web application or site collection. • Click **Import** 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.
Audit Read Access	Configure Netwrix Auditor to track reading of lists and list items within your SharePoint farm except Central Administration web sites. Select **Read access for specified sites** and click **Specify**. In the **Specify SharePoint Sites** dialog, do one of the following: • Click **Add** and provide URL to a SharePoint site. • Click **Import** and browse for a file that contains a list of sites.

Option	Description
	Select **Include subsites** to enable read access auditing on each subsite. **NOTE:** Read access auditing significantly increases the number of events generated on your SharePoint and the amount of data written to the AuditArchive.

9. On the **SharePoint Change Summary Delivery** step, click **Add** to specify emails where the Change Summaries are to be sent. By default, the emails are generated at 3:00 AM, modify the schedule and delivery format (in email body, attached as csv or archived) if necessary.

   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.

10. On the **Deploy Netwrix Auditor for SharePoint Core Service** step, specify deployment method for the Core Service. Select one of the following:

    - **Automatically**—The installation will run under the Data Processing Account on the New Managed Object 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.
      - The **SharePoint Administration (SPAdminV4)** service is started on the target computer. See Netwrix Auditor Installation and Configuration Guide for more information.
      - The user that is going to run the Core Service installation:
        - Is a member of the **local Administrators** group on SharePoint server, where the Core Service will be deployed.
        - Is granted the **SharePoint_Shell_Access** role on SharePoint SQL Server configuration database. See Netwrix Auditor Installation and Configuration Guide for more information.
    - **Manually**—See Netwrix Auditor Installation and Configuration Guide for more information.

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

11. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.7. Create Managed Objects to Audit SQL Server

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **SQL Server** tile. In this case you will be prompted to select **Computer Collection** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **SQL Server** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.

Setting	Description
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

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

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. Click **Add**, select an item type and specify a SQL Server instance. You can add several instances to collection.
7. On the **Configure SQL Server Auditing Settings** step, specify Change Summary recipients.

   To audit database content, select **Enable database content audit.** Netwrix Auditor allows setting rules for the data to be audited and therefore to receive change reports on the selected data only. Click **Specify** to create columns auditing rules and 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.

   NOTE: The following column types are currently not supported: `text, ntext, image, binary, varbinary, timestamp, sql_variant`.

   You can also configure the format of reports sent by email. Click **Configure** to edit the settings. In the **Change Summary Format** dialog that opens, the following options are available:

   - **Attach as a CSV file**—If selected, the Change Summary report will be sent as a file attached to an email. Otherwise, you will receive the report as html text.
   - **Compress before sending**—If selected, the attached file will be sent in the compressed format.
8. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.8. Create Managed Objects to Audit VMware

1. Do one of the following:
   - On the main Netwrix Auditor Administrator Console page, click the **VMware** tile.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane.

   See Managed Objects Overview for more information.
2. On the **Select Managed Object Type** step, select **VMware Virtual Center** as a Managed Object type.
3. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data

Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

4. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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. On the **Specify VMware Virtual Center Name** step, specify the VMware Center URL. If you want to use a specific account to access data from your virtual machines (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
6. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

Option	Description
	SQL Server Settings
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.

Option	Description
	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.
	SQL Server Reporting Services Settings
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

7. On the **VMware Change Summary Delivery** step, click **Add** to specify emails where audit reports should be sent.

   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.

   In the **VMware Credentials** section, specify a user name and a password to be used when connecting to VMware instance.

8. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.9. Create Managed Objects to Audit Windows Server

NOTE: DNS changes can be audited under the Window Server auditing scope.

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **Windows Server** tile. In this case you will be prompted to select **Computer Collection** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Windows Server** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.

Setting	Description
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

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

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add several items to collection. Click **Add**, select an item type and add/browse for a computer name. Review the following for additional information:

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 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 Computers** dialog, click **Add** and specify an object. **NOTE:** The list of containers does not include child domains of trusted domains. Use other options **(Computer name, IP address range**, or **Import computer names from a file**) to specify the target computers.
IP address range	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**.
Import computer names from a file	Allows specifying multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it automatically. If you select the **Import on every data collection** option, you can later modify the list of your audited computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Select Data Collection Method** step, 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.

NOTE: If you disable the **Network traffic compression** option, you will not be able to configure audit automatically on the next step of the wizard.

8. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

     NOTE: This method is recommended for evaluation purposes in test environments. 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.

   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

9. On the **Select Monitored Systems Components** step, select the system components that you want to audit for changes.
10. On the **Configure Windows Server Change Summary Delivery Settings** step, specify the Change Summary recipients.
11. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.10. Create Managed Objects to Audit Event Log

NOTE: You can audit Cisco under the Event Log auditing scope. For details, refer to Netwrix knowledge base articles How to audit Cisco devices with Netwrix Auditor.

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **Event Log** tile. In this case you will be prompted to select **Computer Collection** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Event Log** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Computer Collection Name** step, enter the computer collection name. If you want

to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.

5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

Option	Description
	SQL Server Settings
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:

Option	Description
	• 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.
SQL Server Reporting Services Settings	
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add several items to collection. Click **Add** and select one of the predefined platform types: **Windows Server** or **Syslog-based Platform.**

   NOTE: If you have configured custom syslog platforms previously, they will appear in the **Syslog-based Platforms list**.

   Depending on the platform type selected, specify the object to be audited. Review the following for additional information:

Option	Description
Computer name / Single computer or device	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 (available for **Windows Server** platform only)	Allows specifying a whole AD container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be monitored within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Click **Exclude** to specify domains, OUs, and containers you do not want to audit. **NOTE:** The list of containers does not include child domains of trusted domains. Use other options (**Computer name, IP address range**, or **Import computer names from a file**) to specify the target computers.
IP address range / Computers within an IP range	Allows specifying an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP range you want to exclude, and click **Add**.
Import computer names from a file / Import servers or devices list	Allows specifying multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it on every data collection. If you select the **Import on every data collection** option, you can later modify the list of your monitored computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Select Data Collection Method** step, 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.
8. On the **Specify Notifications Recipients** step, click **Add** to specify the emails where Event Log Collection Status notifications are to be sent.

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. On the **Configure Real-Time Alerts** step, enable or disable the predefined alerts, or click **Add** to configure custom alerts. See Real-Time Alerts for more information.
10. On the **Configure Audit Archiving Filters** step, enable or disable predefined filters, or click **Add** to configure custom filters. Audit Archiving filters define what event will be stored to the Long-Term Archive or the Audit Database, and what will be skipped. With no filters applied, your reports may be excessively large and contain unnecessary information. See Configure Audit Archiving Filters for more information.

    NOTE: If you are going to track Netwrix Auditor health status, enable the **Netwrix Auditor System Health** filter. In case, you need to keep up with important Internet Information Services events, enable the **Internet Information Services Events** filter.
11. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.11. Create Managed Objects to Audit Group Policy

1. Do one of the following:
    - On the main Netwrix Auditor Administrator Console page, click the **Group Policy** tile. In this case you will be prompted to select **Domain** as a Managed Object type on the next step.
    - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Domain** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Group Policy** as the audited system later in the wizard.

    See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

    NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

    Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Domain Name** step, specify the audited domain name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter the credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

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

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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **State-in-Time Reports** step, you can enable or disable **State-in-Time Reports**. This feature allows generating reports on your system configuration state at a specific moment of time in addition to change reports. If enabled, snapshots will be created daily and written to the Audit Database. This option is unavailable if the **Audit Database** settings are not configured.
7. On the **Select Data Collection Method** step, 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.
8. On the **Configure Audit in Target Environment** step, select one of the following:

   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

     NOTE: This method is recommended for evaluation purposes in test environments. 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.

   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

9. On the **Specify Group Policy Change Summary Recipients** step, click **Add** to specify the emails where Change Summaries are to be sent.

   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.

10. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.12. Create Managed Objects to Audit Inactive Users in Active Directory

Inactive User Tracking within Netwrix Auditor 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.

To create a Managed Object to audit inactive users

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **Inactive Users** tile. In this case you will be prompted to select **Domain** or **Organizational Unit** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select a **Domain** or **Organizational Unit** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Inactive Users** as the audited system later in the wizard.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. Depending on your Managed Object, on the **Specify Domain Name** or **Specify Organizational Unit Name** step, specify the target domain name or OU name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Configure Inactive User Tracking Settings** step, specify the following settings:

Parameters	Description
Consider user inactive after	Specify account inactivity period, after which a user is considered to be inactive.

Parameters	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 account 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.
Delete accounts after	Specify account inactivity period, after which the account will be deleted.
Process user accounts	Select this checkbox to audit user accounts.
Process computer accounts	Select this checkbox to audit computer accounts.
Delete account with all its subnodes (Windows Server 2008 or above)	Select this checkbox to delete an account that is a container for objects.
Notify managers only once	If this checkbox is selected, managers receive one notification on account inactivity and one on every action on accounts. Managers will receive a notification in the day when the account inactivity time will be the same as specified in the inactivity period settings. By default, managers receive notifications every day after the time interval of inactivity specified in the Notify managers after entry field.
Send report to	Enter the email addresses where reports are to 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.

6. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the

Managed Objects node.

NOTE: Once the Managed Object is configured, you can set additional options under **Managed Objects** → **your_Managed_Object_name** → **Inactive User Tracking** (for example, edit email template).

3.13. Create Managed Objects to Audit Logon Activity

1. Do one of the following:
   - On the main Netwrix Auditor Administrator Console page, click the **Logon Activity** tile. In this case you will be prompted to select **Domain** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Domain** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Logon Activity** as the audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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

Setting	Description
	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Domain Name** step, specify the audited domain name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select **Custom** and enter the credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

   Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

     NOTE: It is recommended to consider the maximum database size in different SQL Server versions, and make your choice based on the size of the environment you are going to

audit, the number of users and other factors. Note that the maximum database size in SQL Server Express editions may be insufficient.

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

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

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Select Data Collection Method** step, 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.
7. On the **Configure Audit in Target Environment** step, select one of the following:
   - **Automatically for the selected audited systems**

     Click the arrow button next to an audited system to expand the list of settings that are required for the product to function properly.

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

     NOTE: This method is recommended for evaluation purposes in test environments. 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.
   - **Manually**

     For a full list of audit settings, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

   NOTE: Netwrix Auditor detects and configures audit policies within the audited domain only. If any other policies affect your domain (e.g., root domain policies or site policies), configure audit manually.
8. On the **Specify Logon Activity Summary Recipients** step, click **Add** to specify the emails where Change Summaries are to be sent.

   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. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.14. Create Managed Objects to Audit and Alert on Password Expiration in Active Directory

Password Expiration Alerting within Netwrix Auditor checks which domain accounts and/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 allows checking the effects of a password policy change before applying it to the managed domain.

To create a Managed Object to audit expiring passwords

1. Do one of the following:
   - On the main Netwrix Auditor Administrator Console page, click the **Password Expiration** tile. In this case you will be prompted to select **Domain** or **Organizational Unit** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Domain** or **Organizational Unit** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **Password Expiration** as the audited system later in the wizard.

   See Managed Objects Overview for more information.
2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
3. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).

Setting	Description
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. Depending on your Managed Object, on the **Specify Domain Name** or **Specify Organizational Unit Name** step, specify the target domain name or OU name in the FQDN format. If you want to use a specific account to access data from this domain (other than the one you specified as the default Data Processing Account), select the **Custom** option and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Configure Password Expiration Alerting Settings** step, specify the following settings:

Parameters	Description
Send report to administrators	Enable this option and specify one or several email addresses for administrators to receive daily reports with a list of users whose accounts/passwords are going to expire in the specified number of days. Use semicolon to separate several addresses. **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.

Parameters	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. **NOTE:** To edit a report template, click **Customize**. You can use HTML tags when editing a template.
List users whose accounts or passwords expire in <> days or less	Specify the expiration period for accounts and/or passwords to be included in the administrators and managers reports.
Notify users	Select this option to notify users that their passwords and/or accounts are about to expire.
Every day if their 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. **NOTE:** To edit a report template, click **Customize**. You can use HTML tags when editing a template.
First/Second/Last time when their 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. **NOTE:** To edit a report template, click **Customize**. You can use HTML tags when editing a template.
Notify users every day if their account expires in	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.
Filter users by organizational unit	To audit users for expiring accounts/passwords that belong to certain organizational units within your Active Directory domain,

Parameters	Description
	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.

6. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

3.15. Create Managed Objects to Audit User Activity

1. Do one of the following:

   - On the main Netwrix Auditor Administrator Console page, click the **User Activity** tile. In this case you will be prompted to select **Computer Collection** as a Managed Object type on the next step.
   - Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Computer Collection** as a Managed Object type in the **Create New Managed Object** wizard. In this case you will prompted to select **User Activity** as the audited system later in the wizard.

   See Managed Objects Overview for more information.

2. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   NOTE: If you have already configured Netwrix Auditor to audit other systems, and specified the default Data Processing Account and the email settings on their configuration, the **Specify Default Data Processing Account** and **Configure Email Settings** steps of the wizard will be omitted.

   Enter the default Data Processing Account (in the *DOMAIN\user* format) that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

3. On the **Specify Email Settings** step, specify the email settings that will be used for Change

Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

4. On the **Specify Computer Collection Name** step, enter the computer collection name. If you want to use a specific account to access data from this computer collection (other than the one you specified as the default Data Processing Account), select **Custom** and enter credentials. This account must be granted the same permissions and access rights as the default Data Processing Account.
5. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   NOTE: Select the **Make audit data available via summary emails only** checkbox only if you do not want to generate reports and run data searches in the Netwrix Auditor client. With this checkbox selected audit data will not be written to the Audit Database. In this case information on changes will be available via Change Summary emails only.

Even if you select this checkbox now, you will still be able to configure these settings later, but already collected audit data will not be imported in the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the **Audit Database** settings.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.

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

- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

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

Option	Description
Password	Enter a password.
SQL Server Reporting Services Settings	
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.
Password	Enter a password.

If you have already created other Managed Objects, and configured Audit Database settings for them, on this step you will be prompted to enable or disable this feature (by selecting or clearing the **Make audit data available via summary emails only** checkbox). Fields will be prepopulated with default SQL Server settings that you can update if necessary (e.g., update connection information, select another SQL Server instance where to write audit data to). You can also change these settings later. See Manage Audit Database for more information.

6. On the **Add Items to Computer Collection** step, select items that you want to audit. You can add several items to collection. Click **Add** and define the items. Review the following for additional information:

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 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 Computers** dialog, click **Add** and specify an object.

Option	Description
	NOTE: The list of containers does not include child domains of trusted domains. Use other options (**Computer name, IP address range**, or **Import computer names from a file**) to specify the target computers.
IP address range	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**.
Import computer names from a file	Allows specifying multiple computer names by importing a list from a .txt file (one computer name/IP address per line is accepted). You can choose whether to import the list once, or to update it automatically. If you select the **Import on every data collection** option, you can later modify the list of your audited computers by editing the .txt file. The audited computers list will be updated on the next data collection.

7. On the **Specify Users For Activity Auditing** step, select the users whose activity should be recorded. You can select **All users** or create a list of **Specific users**. Certain users can also be added to **Exceptions** list.
8. On the **Specify User Activity Summary Recipients** step, set the delivery schedule and click **Add** to specify emails where Activity Summaries will be sent.

   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. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

4. Data Collection

This chapter explains the Netwrix Auditor data collection workflow, describes how to launch it manually and explains how to check data collection status in Netwrix Auditor Administrator Console.

For more information see:

- Data Collection Workflow
- Launch Data Collection Manually

4.1. Data Collection Workflow

The Netwrix Auditor data collection workflow is as follows:

1. Once a Managed Object is created, Netwrix Auditor starts collecting audit data from the managed Active Directory domain or organizational unit, computer collection, a SharePoint farm, or VMware Virtual Center.

   For most of the audited systems, a dedicated scheduled task is created and it runs periodically to collect audit data. The first data collection gathers information on the audited system'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.

   If you do not want to wait until a scheduled data collection, you can launch it manually. See Launch Data Collection Manually for more information.

   NOTE: When auditing SharePoint farms and User Activity, Netwrix Auditor employs a different data collection method. Instead of using a scheduled task for data collection, Netwrix Auditor creates a service and also requires a Core Service to be installed on the audited 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 audited system's current configuration state.

   For all audited systems, the latest data collection status can be reviewed in Netwrix Auditor Administrator Console. To do it, navigate to the Managed Object which includes the audited system whose data collection status you want to check. Review data collection status in the **Status** column.

   NOTE: The status is updated automatically every time you navigate to a Managed Object.

2. If a critical event is detected, an email notification—an alert—is sent immediately to the specified recipients.

   NOTE: This functionality is currently available for the following audited systems:

- Active Directory
- Event Log

Refer to Real-Time Alerts for detailed instructions on how to use predefined alerts and create custom alerts.

3. Once a day (at 3:00 AM by default for most of audited systems), Netwrix Auditor writes collected audit data to the local file-based Long-Term Archive.

   If Audit Database is configured, audit data is imported into the Audit Database. Refer to Manage Audit Database for detailed instructions on how to configure the Audit Database settings.

4. If the State-in-Time Reports functionality is enabled, Netwrix Auditor also writes a state-in-time snapshot of the audited system current state to the Audit Database.

   NOTE: This functionality is currently available for the following audited systems:

   - Active Directory
   - File Servers
   - Group Policy

5. At the same time, Netwrix Auditor generates a Change Summary and emails it to the specified recipients. Refer to Change Summary for detailed instructions on how to modify the default Change Summary delivery schedule and generate on-demand Change Summary.

4.2. Launch Data Collection Manually

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

- A Change 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 Change Summary delivery.
- Changes that occurred between data collections will be imported to the Audit Database and become available in the Netwrix Auditor client.

To launch data collection manually

Audited System	Instructions
• Active Directory • Exchange • Exchange Online • File Servers	1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name**. 2. In the right pane, select the audited system and click **Run**.

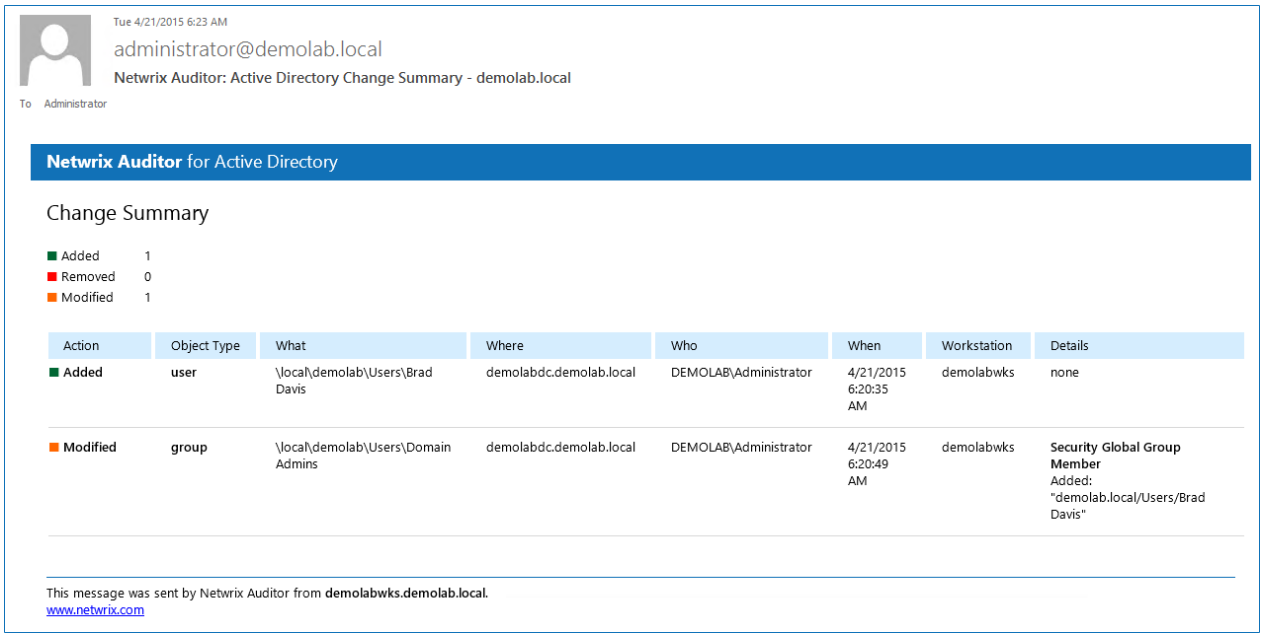
Audited System	Instructions
• SharePoint • SQL Server • VMware • Windows Server • Event Log • Group Policy • Inactive Users in Active Directory • Logon Activity • Password Expiration in Active Directory	
Mailbox access within Exchange	1. Start **Task Scheduler**, select the **Task Scheduler Library** node and locate the **Netwrix Non-owner Mailbox Access Reporter for Exchange** task. 2. Right-click the task and select **Run**.
User Activity	You cannot launch on-demand data collection and Activity Summary generation.

NOTE: Depending on the size of the audited environment and the number of changes, data collection may take quite long.

5. Change Summary

A Change Summary is email that lists all changes/ recorded user sessions that occurred since the last Change Summary delivery. Notifications on user activity (Activity Summaries) and event log collection (Event Log Collection Status) are a bit different and do not show changes. By default, for most of audited systems a Change Summary is generated daily at 3:00 AM and delivered to the specified recipients. You can also launch data collection and a Change Summary generation manually.

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



Tue 4/21/2015 6:23 AM
administrator@demolab.local
Netwrix Auditor: Active Directory Change Summary - demolab.local
To Administrator

Netwrix Auditor for Active Directory

Change Summary

Added 1
Removed 0
Modified 1

Action	Object Type	What	Where	Who	When	Workstation	Details
Added	user	\local\demolab\Users\Brad Davis	demolabdc.demolab.local	DEMOLAB\Administrator	4/21/2015 6:20:35 AM	demolabwks	none
Modified	group	\local\demolab\Users\Domain Admins	demolabdc.demolab.local	DEMOLAB\Administrator	4/21/2015 6:20:49 AM	demolabwks	**Security Global Group Member** Added: "demolab.local/Users/Brad Davis"

This message was sent by Netwrix Auditor from **demolabwks.demolab.local.**
www.netwrix.com

The example Change Summary provides the following information on Active Directory changes:

Column	Description
Action	Shows the type of action that was performed on the object. • Added • Removed • Modified
Object Type	Shows the type of the modified AD object, for example, 'user'.
What	Shows the path to the modified AD object.
Where	Shows the name of the domain controller where the change was made.

Column	Description
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.

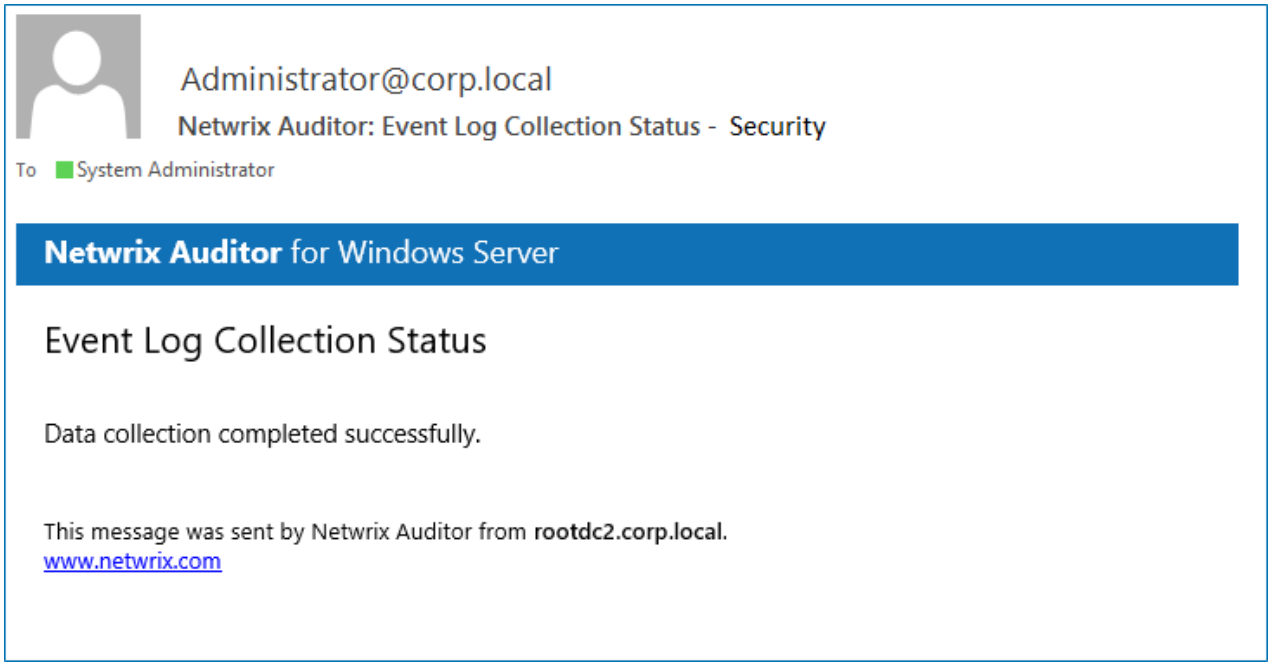
Refer to the following procedures for instructions on how to modify the default Change Summary delivery schedule and initiate an on-demand Change Summary delivery:

- Modify Change Summary Delivery Schedule
- Initiate On-Demand Change Summary Delivery

The following audited systems have another format of regular Change Summary emails:

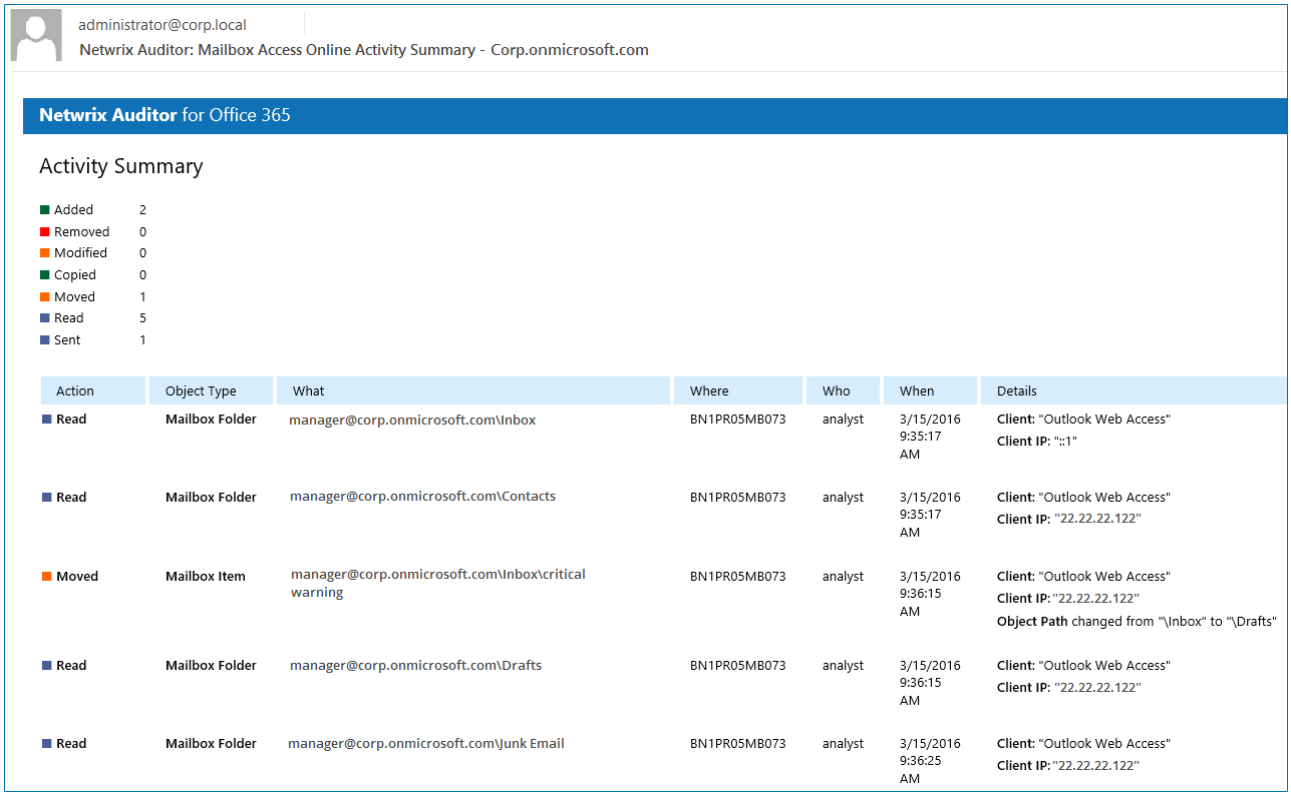
- Event Log. See Event Log Collection Status for more information.
- Non-Owner Mailbox Access for Exchange and Exchange Online. See Mailbox Access Activity Summary for more information.
- User Activity. See User Activity Summary Report for more information.

5.1. Event Log Collection Status



The **Event Log Collection Status** email shows whether data collection for your Computer Collection completed successfully or with warnings and errors.

5.2. Mailbox Access Activity Summary



administrator@corp.local

Netwrix Auditor: Mailbox Access Online Activity Summary - Corp.onmicrosoft.com

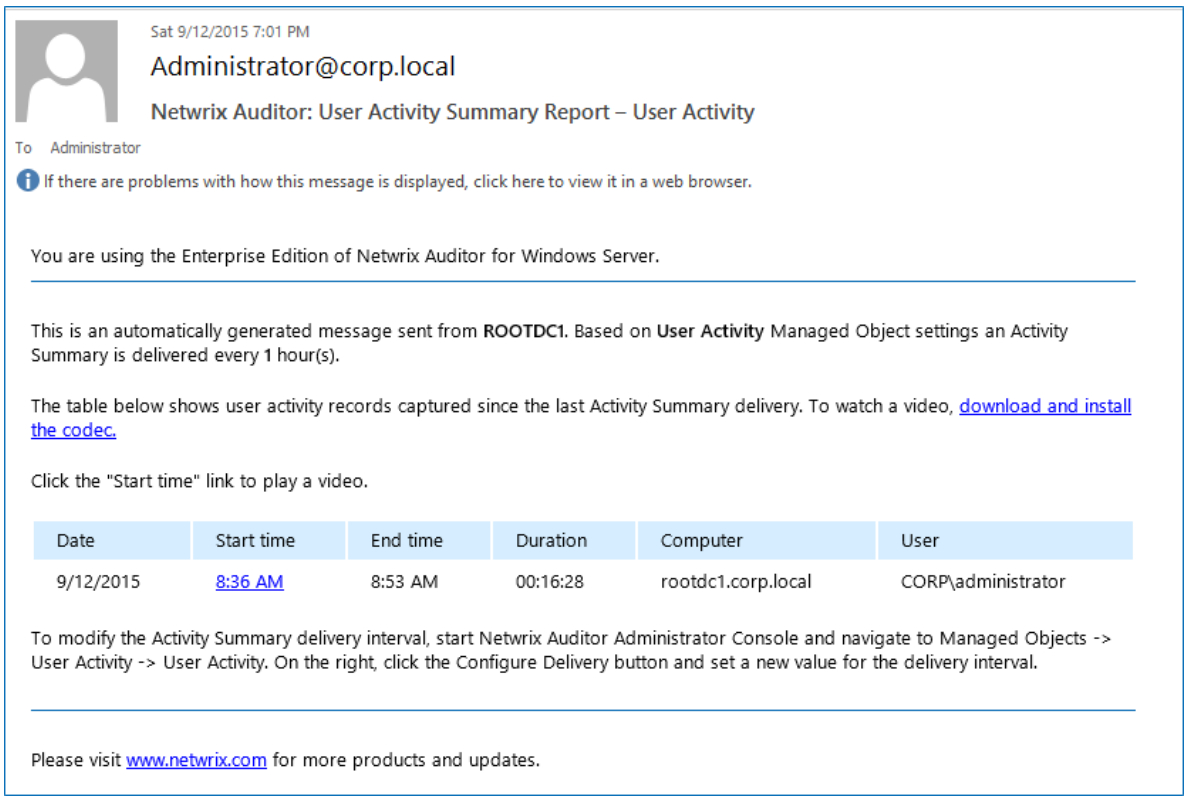
Netwrix Auditor for Office 365

Activity Summary

Added	2
Removed	0
Modified	0
Copied	0
Moved	1
Read	5
Sent	1

Action	Object Type	What	Where	Who	When	Details
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Inbox	BN1PR05MB073	analyst	3/15/2016 9:35:17 AM	**Client:** "Outlook Web Access" **Client IP:** "::1"
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Contacts	BN1PR05MB073	analyst	3/15/2016 9:35:17 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"
Moved	**Mailbox Item**	manager@corp.onmicrosoft.com\Inbox\critical warning	BN1PR05MB073	analyst	3/15/2016 9:36:15 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122" **Object Path** changed from "\Inbox" to "\Drafts"
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Drafts	BN1PR05MB073	analyst	3/15/2016 9:36:15 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Junk Email	BN1PR05MB073	analyst	3/15/2016 9:36:25 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"

5.3. User Activity Summary Report



Sat 9/12/2015 7:01 PM

Administrator@corp.local

Netwrix Auditor: User Activity Summary Report – User Activity

To Administrator

If there are problems with how this message is displayed, click here to view it in a web browser.

You are using the Enterprise Edition of Netwrix Auditor for Windows Server.

This is an automatically generated message sent from **ROOTDC1**. Based on **User Activity** Managed Object settings an Activity Summary is delivered every **1** hour(s).

The table below shows user activity records captured since the last Activity Summary delivery. To watch a video, download and install the codec.

Click the "Start time" link to play a video.

Date	Start time	End time	Duration	Computer	User
9/12/2015	8:36 AM	8:53 AM	00:16:28	rootdc1.corp.local	CORP\administrator

To modify the Activity Summary delivery interval, start Netwrix Auditor Administrator Console and navigate to Managed Objects -> User Activity -> User Activity. On the right, click the Configure Delivery button and set a new value for the delivery interval.

Please visit www.netwrix.com for more products and updates.

The example Activity Summary provides detailed information on User Activity in your IT infrastructure.

5.4. Modify Change Summary Delivery Schedule

To modify the Change Summary generation and delivery schedule, follow the instructions in the table below depending on audited system:

Audited System	Instructions
Active Directory Exchange Group Policy	1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Active Directory**. 2. In the right pane, modify the Change Summary delivery time and interval. This change affects Active Directory, Group Policy and Exchange audited systems.
File Servers SQL Server VMware Windows Server	1. In Netwrix Auditor Administrator Console, navigate to **Settings** → **Data Collection**. 2. Click **Modify** next to **Default Data Collection and Change Summary generation schedule**.

Audited System	Instructions
Inactive users in Active Directory Password expiration in Active Directory	3. Modify data collection and Change Summary generation schedule. **NOTE:** See Configure Data Collection Settings for more information.
Event Log Logon Activity SharePoint	1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **audited_system**. 2. In the right pane, modify the delivery time.
Mailbox access within Exchange	1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Exchange**. 2. In the right pane, click **Track Access** in the **Non-owner Mailbox Access Auditing** section. 3. In the dialog that opens, click **Modify** in the **Reports** section and edit the default Change Summary delivery schedule. 4. Click **Apply** to save the changes.
User Activity	1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **User Activity**. 2. In the right pane, click **Configure Delivery** in the **Activity Summary Delivery** section and modify the Activity Summary delivery time and interval.

5.5. Initiate On-Demand Change Summary Delivery

If you do not want to wait until a scheduled delivery, you can generate a Change Summary on-demand. Force the data collection, after which a Change Summary will be generated and sent to the specified recipients. It will list all changes that occurred since the last scheduled or on-demand Change Summary delivery. See Launch Data Collection Manually for more information.

6. Manage Data in AuditArchive

AuditArchive is a scalable repository that stores audit data collected by Netwrix Auditor. AuditArchive consists of two tiers:

Tier	Description	Default retention
Audit Database	The SQL-based operational storage used for browsing audit data with the Netwrix Auditor client.	180 days
Long-Term Archive	The file-based repository used to store past audit data for future reference.	120 months

By default, audit data is written to both the Audit Database and the Long-Term Archive that is designed to store data in a compressed format for a longer period of time.

With two-tiered AuditArchive you can store your audit data as long as required in the Long-Term Archive, but keep your operational storage fast and clean and use it for browsing recent data. At the same time, Netwrix Auditor allows you to extract data from the Long-Term Archive and import it to the Audit Database if you want to investigate past issues. Review the following for additional information:

- Manage Audit Database
- Manage Long-Term Archive
- Import Audit Data to Investigation Database

6.1. Manage Long-Term Archive

To review and update the Long-Term Archive location and the retention period for the local repository of audit data, navigate to **AuditArchive** → **Long-Term Archive** and click **Modify** to configure these settings.

Setting	Description
Write audit data to	Specify the path to the folder where your audit data will be stored. **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.
Keep audit data for (in months)	Specify the number of months for which audit data will be stored.

Setting	Description
	By default, it is set to 120 months. Data will be deleted automatically when its retention period is over. If the retention period is set to *0*, data will be automatically stored for the last 4 data collections for most of the audited systems (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).

If you want to regularly access audit data collected with the previous versions of the product, you can migrate your AuditArchive. See Migrate Legacy Data From Old Audit Archive for more information.

NOTE: Netwrix Auditor informs you if you are running out of space on a system disk where the Long-Term Archive is stored by default. You will see events in the **Netwrix Auditor System Health** log once the free disk space starts approaching minimum level. When the free disk space is less than 3 GB all Netwrix services will be stopped (except for services responsible for user activity, SharePoint and syslog auditing).

6.1.1. Migrate Legacy Data From Old Audit Archive

In 7.0, Netwrix Auditor introduced a new format for storing audit data—Long-Term Archive. For your convenience, Netwrix provides the AuditArchive Migration tool that allows you to import data from the old file-based Audit Archive (available in Netwrix Auditor 6.5 or below) to the new file-based Long-Term Archive.

To migrate audit data

1. In the Netwrix Auditor Administrator Console, navigate to **AuditArchive** → **Long-Term Archive** and select the **Migrate** link.
2. In the **Audit Archive Migration Tool** window, browse for your Netwrix Auditor 6.5 AuditArchive (the default path is *C:\ProgramData\NetWrix\Management Console\Data*).
3. Click **Migrate** to start the migration process. **AuditArchive Migration Tool** automatically moves your audit data to the new location.

   NOTE: Depending on the amount of your Netwrix Auditor 6.5 audit data, migration may take a while to complete. You can minimize the **AuditArchive Migration Tool** screen and keep working with Netwrix Auditor.

Once migration completes, you will see a message with migration status— successful or with warnings/errors.

6.2. Manage Audit Database

If you want to enable AuditIntelligence (including reports and search capabilities) provided by the Netwrix Auditor client, Audit Database settings must properly configured in Netwrix Auditor Administrator Console. Review the following for additional information:

Option	Description
SQL Server settings	Define the Audit Database location to store audit data, connection information, etc. Netwrix Auditor allows you to specify SQL Server settings (SQL Server instance, connection information, etc.) for each audited system within a Managed Object individually or use default settings and synchronize them across all Managed Objects. See To configure SQL Server and SSRS settings for more information.
Database retention settings	Can be configured if you want audit data to be deleted automatically from your Audit Database after a certain period of time. Netwrix Auditor allows you to specify retention settings for each audited system within a Managed Object or use default settings and synchronize them across all Managed Objects. 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 Managed Object. See To configure SQL Server and SSRS settings for more information.
State-in-time reports settings	Can be configured to create snapshots on the system's configuration state at a specific moment of time in addition to change reports. Available for Active Directory, Group Policy and File Servers audited systems. These settings are configured for each audited system that supports this functionality individually. See Report Types for more information on state-in-time reports available in the Netwrix Auditor client. **NOTE:** Use this section to import historical snapshots for reporting. See To configure State-in-Time reports and import historical snapshots to the Audit Database for more information.

6.2.1. Configure Default Audit Database Settings

Normally, Audit Database settings are configured when you create a first Managed Object. The settings you specified then are set as default and are listed on the **AuditArchive** → **Audit Database** page. Later, when you create other Managed Objects these settings prepopulate fields on the **Audit Database Settings** step of the wizard.

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

NOTE: To synchronize SQL Server settings across all Managed Objects and overwrite custom settings with default, click **Apply**. The settings are not updated until you click **Apply**.

Audit data stored in databases with custom names will become unavailable. Netwrix Auditor will create new databases with default names (e.g., Netwrix_Auditor_Active_Directory) and store new audit data there.

To configure SQL Server and SSRS settings

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

Option	Description
	SQL Server Reporting Services Settings
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.
Password	Enter a password.

To configure database retention

Option	Description
Database retention enabled	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. By default, it is set to 180 days. If you have migrated from Netwrix Auditor 6.5 and below, retention will be set to 3650 days (10 years) by default. Data will be deleted automatically when its retention period is over.

6.2.2. Configure Custom Audit Database Settings

You can configure Netwrix Auditor to use custom Audit Database settings for a certain audited system within a Managed Object, e.g., store your audit data on another SQL Server instance, change database name, connection information, change retention settings.

NOTE: To employ AuditIntelligence (including reports and search capabilities) provided by the Netwrix Auditor client, you must configure Audit Database settings for the audited systems you are interested in under each Managed Object individually or apply default.

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.

To enable and update custom Audit Database settings

1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **audited_system** → **Audit Database Settings**.

2. Make sure the **Make audit data available via summary emails only** checkbox is cleared. If the checkbox is selected, no audit data will be written to the Audit Database.
3. Review settings and update them if necessary. You can also import historical state-in-time snapshots to the Audit Database.

NOTE: It is recommended to check custom settings for each audited system under each Managed Object. If custom Audit Database settings differ from those listed on the **AuditArchive** → **Audit Database** page, audit data is written to the Audit Database according to the settings specified on the audited system page, as they overwrite default settings.

To configure State-in-Time reports and import historical snapshots to the Audit Database

1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **audited_system** → **Audit Database Settings** and click **Modify** next to **State-in-Time Reports**.
2. Select **Enable State-in-Time Reports**.

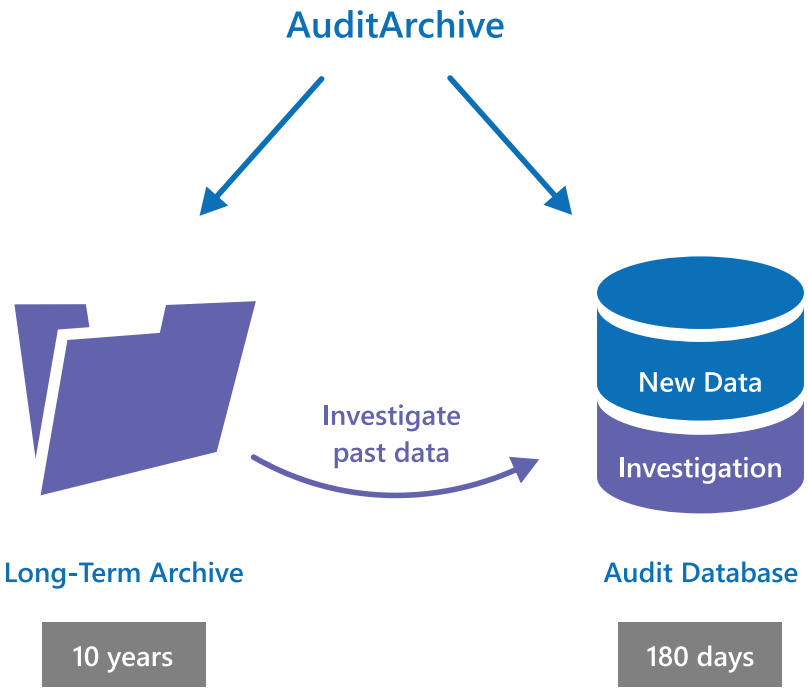
   When auditing file servers, changes to effective access permissions can tracked in addition to audit permissions. By default, **Combination of file and share permissions** is tracked. File permission define who has access to local files and folders. Share permissions provide or deny access to the same resources over the network. The combination of both determines the final access permissions for a shared folder—the more restrictive permissions are applied. Upon selecting **Combination of file and share permissions** only the resultant set will be written to the Audit Database. Select **File permissions** option too if you want to see difference between permissions applied locally and the effective file and share permissions set. To disable auditing of effective access, select all checkboxes under **Include details on effective permissions**.
3. In the **Historical Snapshot Management** section, select the snapshots that you want to import to the Audit Database, and move them to the **Snapshots available for reporting** list using the arrow button.

   NOTE: By default, only a latest snapshot is available for reporting in the Netwrix Auditor client. If you want to generate reports based on different snapshots, you must import snapshots to the Audit Database.
4. Click **Apply** to save the changes and wait until connection to SQL Server is established and snapshots are imported.

6.3. Import Audit Data to Investigation Database

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 in the Netwrix Auditor client.

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 AuditIntelligence searches and generate reports with your past data.



To extract past audit data collected by Netwrix Auditor, use one of the following data import tools depending on your audited system:

Audited System	Data import tool
• Active Directory (including Group Policy) • Exchange • Exchange Online • File Servers • SharePoint • SQL Server • VMware • Windows Server	**Archive Data Investigation**. See To import audit data with the Archive Data Investigation wizard for more information.
• Event Log • User Activity	**DB Importer**. See To import audit data with the DB Importer for more information.

To import audit data with the Archive Data Investigation wizard

1. In Netwrix Auditor Administrator Console, navigate to **AuditArchive** → **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 AuditIntelligence searches and generate reports in the Netwrix Auditor client, select the same SQL Server instance as the one specified on **AuditArchive** → **Audit Database** page. See Manage Audit Database for more information.
Database	Select import database name. By default, data is imported to a specially created **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 **Import to investigation database** configuration. Click **Configure** to specify import

scope.

Option	Description
From... To...	Specify the time range for which you want to import past audit data.
Audited Systems	Select audited systems whose audit data you want to import to the Audit Database.
Managed Objects	Select Managed Objects whose audit data you want to import to the Audit Database. Netwrix Auditor lists Managed Objects that are currently available in the product configuration. **NOTE:** Select **All** to import audit data for all Managed Objects, including those that were removed from Netwrix Auditor Administrator Console (or removed and then recreated with the same name—Netwrix Auditor treats them as different Managed Objects). For example, you had a Managed Object **corp.local** used for auditing Active Directory. You removed this Managed Object from Netwrix Auditor Administrator Console, but its audit data was preserved in the Long-Term Archive. Then, you created a new Managed Object 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** Managed Objects— the removed and the current— as different. If you select **corp.local** in the Managed Objects list, only Exchange data will be imported to Audit Database (as it corresponds to the current Managed Object configuration). To import Active Directory data from the removed Managed Object, select **All** Managed Objects.

4. Click **Run**.

To import audit data with the DB Importer

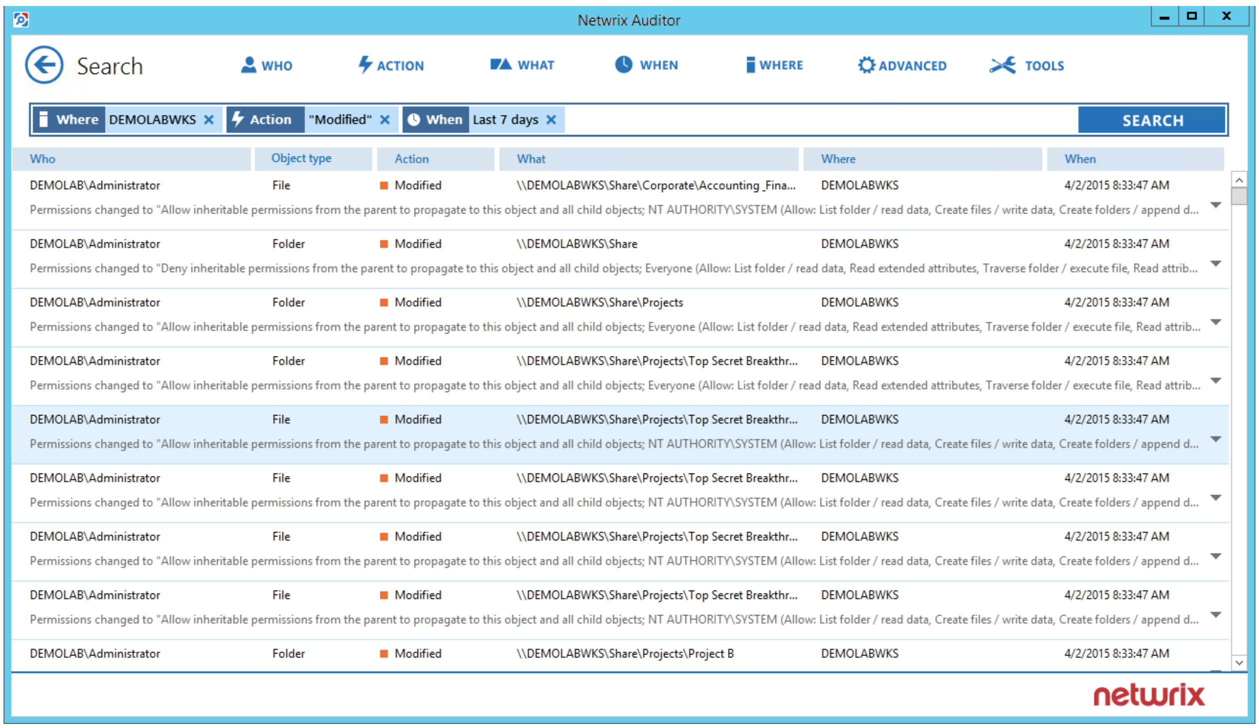
1. In the *%Netwrix Auditor installation folder%* folder, navigate to one of the following locations:
   - Event Log Management
   - User Activity Video Recording
2. Locate **DB Importer**, and double-click to launch it.

3. Select the Managed Object and the time range for which you want to import data.
4. Click **Import**.

7. AuditIntelligence

Besides notifying on changes a daily basis, Netwrix Auditor brings real AuditIntelligence into your IT infrastructure and enables its 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. The Netwrix Auditor client uses data stored in the Audit Database to generate reports and run data searches. The product provides a variety of predefined reports for each audited system that help you keep track of all changes in your IT infrastructure and validate compliance with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.). A straight-forward search interface allows a user to run custom searches.



NOTE: To employ AuditIntelligence (including reports and search capabilities) provided by the Netwrix Auditor client, you must configure Audit Database settings for the audited systems you are interested in under each Managed Object individually or apply default.

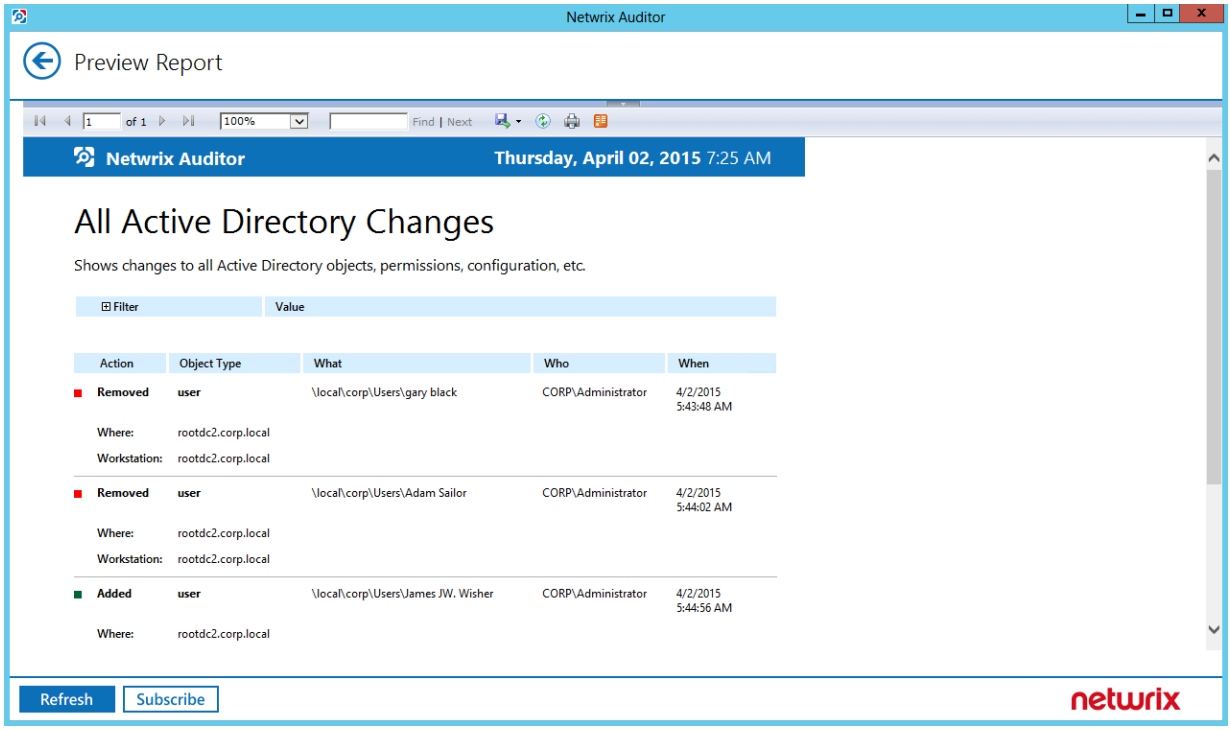
Also, make sure all databases that store audit data reside on the same default SQL Server instance. Otherwise, this data will not be available in the search results and reports.

Review the following for additional information:

- Manage Audit Database
- Reports Available in Netwrix Auditor
- Additional Reports Available in Netwrix Auditor Administrator Console
- Import Audit Data to Investigation Database

7.1. Reports Available in Netwrix Auditor

Netwrix Auditor provides a wide variety of predefined reports for each audited system 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.). See Netwrix Auditor User Guide for detailed instructions how to use Reports functionality.



7.1.1. Report Types

In the Netwrix Auditor client, the following report types are available:

- **Organization Level reports**—Aggregate data from all audited systems and Managed Objects. They list all changes that occurred across the audited IT infrastructure. **Enterprise Overview** aggregates information on changes from all audited systems and provides a centralized overview.
- **Overview diagrams**—System-specific diagram reports that aggregate audit data for an auditing system. They provide a high-level overview of changes within a selected time period. Overviews consist of four charts, showing the activity trends by date, user, object type or server, and drill through to detailed reports for further analysis.
- **Change reports**—System-specific reports that aggregate audit data for a specific audited system within an individual Managed Object. Change reports show detailed data on changes and provide grouping, sorting and filtering capabilities. Each change report has a different set of filters allowing you to manage collected data in the most convenient way. Some audited systems provide activity reports as well.

- **State-in-time reports**—System-specific reports that aggregate data for a specific audited system within an individual Managed Object and allow reviewing the point-in-time state of the audited system. These reports are based on daily snapshots and help you paint a picture of your system configuration at a specific moment in time.
- **Changes with Video**—Provide video recordings of user activity on audited computers.
- **Changes with Review Status**—System-specific reports that aggregate data for a specific audited system within an individual Managed Object and can be used as a tool in the basic change management process. These reports allow setting a review status for each change and providing comments.

If you are looking for some specific information and cannot find it in reports, try browsing audit data with **Search**. You can also order custom report templates from Netwrix.

7.1.2. View Reports

Reports can be viewed in the Netwrix Auditor client, or in a web browser. A user can also create a subscription to receive reports by email on a regular basis.

NOTE: Users who are going to view reports must be assigned the **Browser** role on the Report Server. See Netwrix Auditor Installation and Configuration Guide for more information.

To view reports in the Netwrix Auditor client

- Navigate to **Reports** and select a report you are interested in and click **View**. See Netwrix Auditor User Guide for more information.

To view reports in a web browser

1. Open a web browser and type the Report Manager URL (it can be found in Netwrix Auditor Administrator Console under **AuditArchive** → **Audit Database**). In the page that opens, navigate to the report you want to generate and click the report name. You can modify the report filters and click **View Report** to apply them.

To receive reports by email

- Create a subscription in the Netwrix Auditor client.

7.2. Additional Reports Available in Netwrix Auditor Administrator Console

In Netwrix Auditor Administrator Console, you can generate additional reports to review inactive users and expiring passwords.

Review the following for additional information:

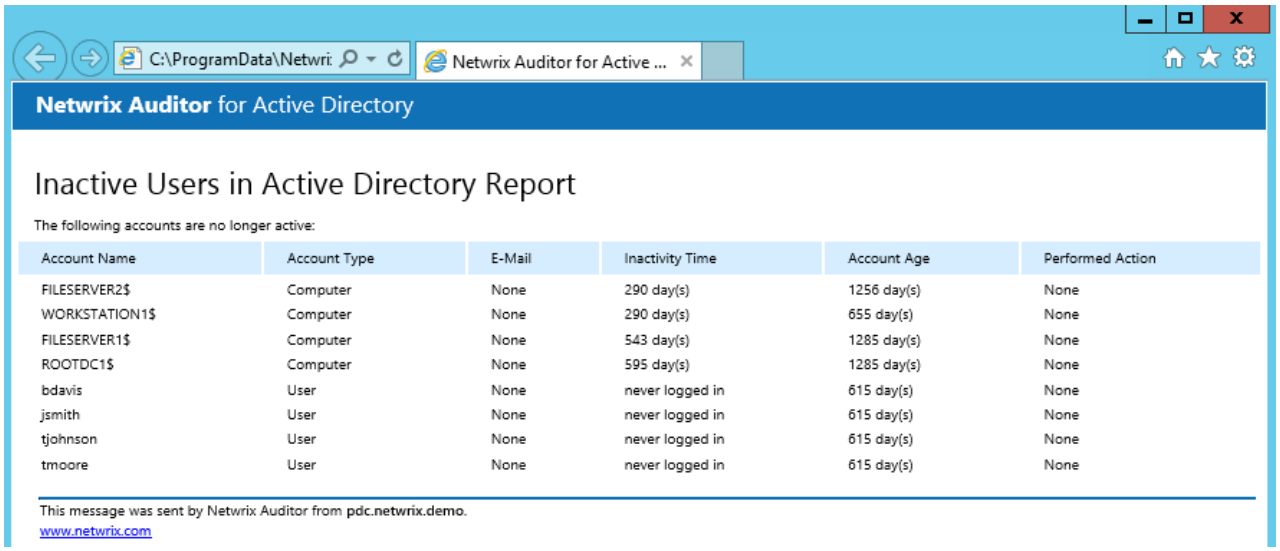
- Inactive Users Ad-hoc Report
- Password Expiration Ad-hoc Report

7.2.1. Inactive Users Ad-hoc Report

After creating a Managed Object for Inactive User Tracking, you can schedule daily emails listing all inactive user and computer accounts. This report can be also generated on demand and reviewed in a web browser.

To generate an ad-hoc report on inactive users

1. In the left pane, navigate to your **Managed Object** → **Inactive Users**.
2. Make sure that the **Enable Inactive Users tracking** checkbox is selected.
3. In the right pane, specify the account inactivity period, after which a user is considered to be inactive in the **Consider user inactive after < > days of inactivity** field.
4. Apply the corresponding filters under the **Scope** section.
5. Navigate to **Ad-hoc Report** under the **Inactive Users** node and click **Run** to generate a report. The report will be displayed in the default web browser:

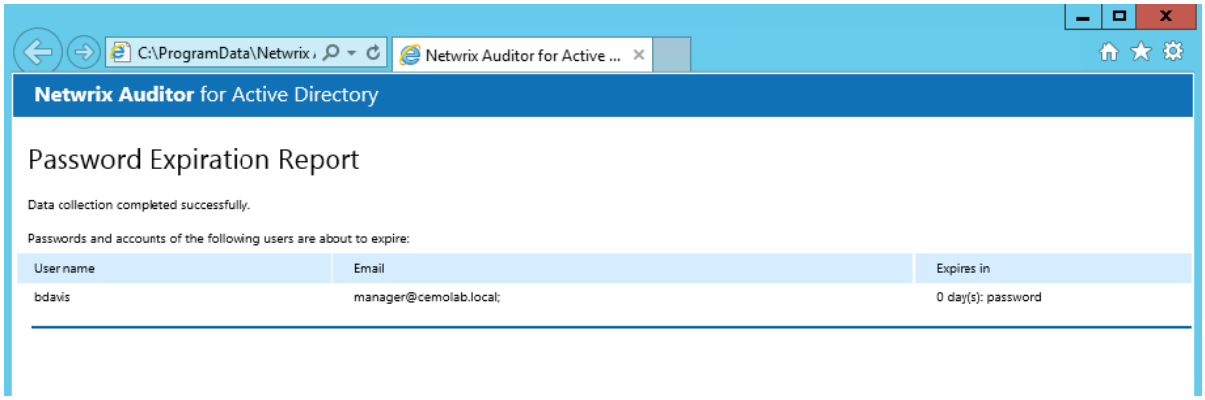


7.2.2. Password Expiration Ad-hoc Report

After creating a Managed Object for Password Expiration Alerting, you can schedule daily emails listing users with expiring passwords. This report can be also generated on demand and reviewed in a web browser.

To generate an ad-hoc report on expiring passwords

1. In the left pane, navigate to your **Managed Object** → **Password Expiration Alerting** .
2. Make sure that the **Enable Password Expiration alerting** checkbox is selected.
3. Navigate to **Ad-hoc Report** under the **Password Expiration** node and click **Run** to generate the report.
4. In the **Maximum Password Age Setting** dialog, select domain policy settings or specify the maximum password age in days.
5. The report will be displayed in the default web browser:



8. Real-Time Alerts

If you want to be notified immediately about changes to certain objects, you can configure real-time alerts that will be triggered by specific events. Alerts are emailed immediately after the specified event has been detected.

This functionality is currently available for the following audited systems:

- Active Directory
- Event Log (including alerts for non-owner mailbox access events)

You can create your own custom alerts, enable/disable and modify the predefined real-time alerts provided by Netwrix. To do it, perform the following procedures:

To..	In the Netwrix Auditor Administrator Console	In the Managed Object wizard
Enable/ disable an existing alert	1. Navigate to one of the following locations: • **Managed Objects** → **your_ Managed_Object_name** → **Active Directory** → **Real-Time Alerts.** • **Managed Objects** → **your_ Managed_Object_name** → **Event Log** → **Real-Time Alerts.** 2. Select an alert from the list in the left pane. 3. Right-click an alert and select **Enable** or **Disable**.	1. Proceed to the **Configure Real-Time Alerts** step. 2. Double-click an alert to enable or disable it.
Modify an existing alert	1. Navigate to one of the following locations: • **Managed Objects** →**your_ Managed_Object_name** → **Active Directory** → **Real-Time Alerts.** • **Managed Objects** → **your_ Managed_Object_name** → **Event Log** → **Real-Time**	1. Proceed to the **Configure Real-Time Alerts** step. 2. Select an alert and click **Edit**. The **Edit Real-Time Alert** wizard will open.

To..	In the Netwrix Auditor Administrator Console	In the Managed Object wizard
	Alerts. 2. Select an alert from the list in the left pane. 3. In the right pane, check **Enable** since only the enabled alerts can be modified. 4. Navigate to the options that require modification and update them.	
Create a new alert	1. Navigate to one of the following locations: • **Managed Objects** → **your_Managed_Object_name** → **Active Directory** → **Real-Time Alerts.** • **Managed Objects** → **your_Managed_Object_name** → **Event Log** → **Real-Time Alerts.** 2. Right-click the **Real-Time Alerts** node and select **New Real-Time Alert**. The **New Real-Time Alert** wizard will open.	1. Proceed to the **Configure Real-Time Alerts** step . 2. Click **Add**. The **New Real-Time Alert** wizard will open.

Review the following for additional information:

- Create Real-Time Alerts for Active Directory
- Create Real-Time Alerts for Event Log
- Create Real-Time Alerts for Non-Owner Mailbox Access Events

The table below lists the predefined real-time alerts, provided by Netwrix:

Alert	Description
	Active Directory
Changes to Admin Group	Alerts on changes to the **Domain Admins** and the **Enterprise Admins**

Alert	Description
Membership	group.
Changes to AD Objects by "Administrator"	Alerts on any changes to Active Directory objects made under the **Administrator** account.
Changes to Any Active Directory Objects	Alerts on any changes made to any Active Directory object.
Changes to Domain Configuration	Alerts on changes to objects in domain configuration partition, such as sites, trusts, and so on.
Domain Controller Demotion	Alerts on a domain controller demotion.
Domain Controller Promotion	Alerts on a domain controller promotion.
Organizational Unit Deletion	Alerts on an Organizational Unit deletion.
Event Log	
System Errors	Alerts on errors in the System event log.
Application Errors	Alerts on errors in the Application event log.

8.1. Create Real-Time Alerts for Active Directory

1. Start the **New Real-Time Alert** wizard. See Real-Time Alerts for more information.
2. On the **Specify Real-Time Alert Name** step, specify the alert name and enter alert description (optional).
3. On the **Configure Real-Time Alert Filters and Notifications** step, specify the alert filters and configure email notifications. Click **Add** in the **Alert Filters** section to specify a condition that will trigger the alert.
4. Complete the **Alert Filter** wizard. Complete the following fields:
   - In the **General** tab:

Option	Description
Name	Specify the filter name.

Option	Description
Description	Enter the description for this filter (optional).
Alert severity	Select alert severity level from the drop-down list (*Critical/High/Normal/Low*). **NOTE:** Alert severity level will be displayed in the email notification.

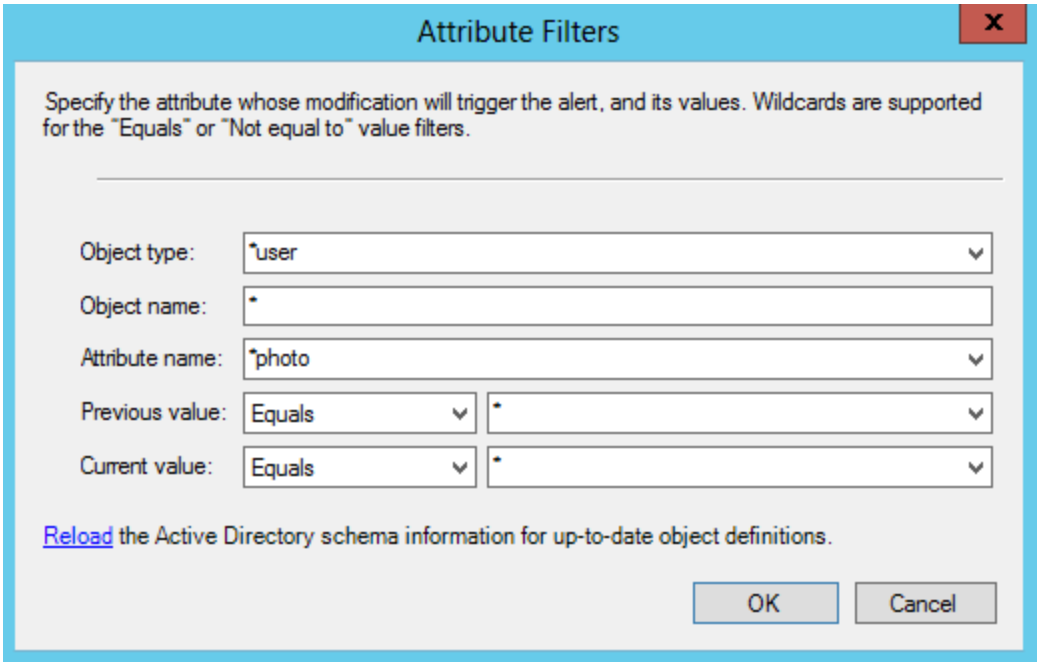
- In the **Change** tab:

Option	Description
Who changed	Specify the name of the user whose actions must trigger the alert. In case a group membership is audited, you can specify a group name. Click  to select users from your domain. Alternatively, you can use a wildcard (*). In this case, the alert will be triggered if the action is performed by any user. If the product is configured to collect the information on group membership of the users who make changes, you can also select a group if you want to be notified when a change is made by any member of this group.
Change type	Select a change type (*Add/Modify/Remove*) from the drop-down list.
Object path	Specify the object path, e.g., the path to the AD object whose modification you want to track. Click  to select a container within your domain (e.g., *\local\enterprise\File Servers*).You can use wildcard (*).
Include child objects	Select this option if you want the filter to be applied to all child objects in the specified path.

- In the **Attributes** tab, click **Add** to specify an AD object attribute whose modification must trigger the alert:

Option	Description
Object type	Select object type from the drop-down list. This list contains all Active Directory object types. You can use wildcard (*).

Option	Description
Object name	(Optional) Select object name to limit alerting to certain objects. You can use wildcard (*).
Attribute name	Select the attribute whose modification must trigger the alert. This list is populated depending on the selected object type. You can use wildcard (*).
Values	This field is displayed if a multi-value attribute is selected (e.g., "photo"). Select the type of change (e.g., *Added* or *Removed*), and specify the filter values.
Previous value	This field is displayed if a single-value attribute is selected. Select a value (possible values are: *Equals*, *Not equal to*, *Starts with*, *Ends with*, *Less than*, *Greater than*, *Less or equal*, *Greater or equal*) and specify the previous value of the attribute. You can use wildcard (*).
Current value	This field is displayed if a single-value attribute is selected. Select a value (possible values are: *Equals*, *Not equal to*, *Starts with*, *Ends with*, *Less than*, *Greater than*, *Less or equal*, *Greater or equal*) and specify the current value of the attribute. You can use wildcard (*).



NOTE: Sometimes, it can be quite difficult to select the appropriate attribute for the type of change that must trigger an alert. If you are unsure which attribute is responsible for the type of change you want to track, refer to Identify Correct Attributes for detailed instructions on how to identify an attribute.

Click **OK** to save the changes and close the **Attribute Filters** dialog. And **OK** to save the changes and close the **Alert Filter** dialog.

5. In the **Notifications** section of the **New Real-Time Alert** wizard, click **Add** and select one of the following:

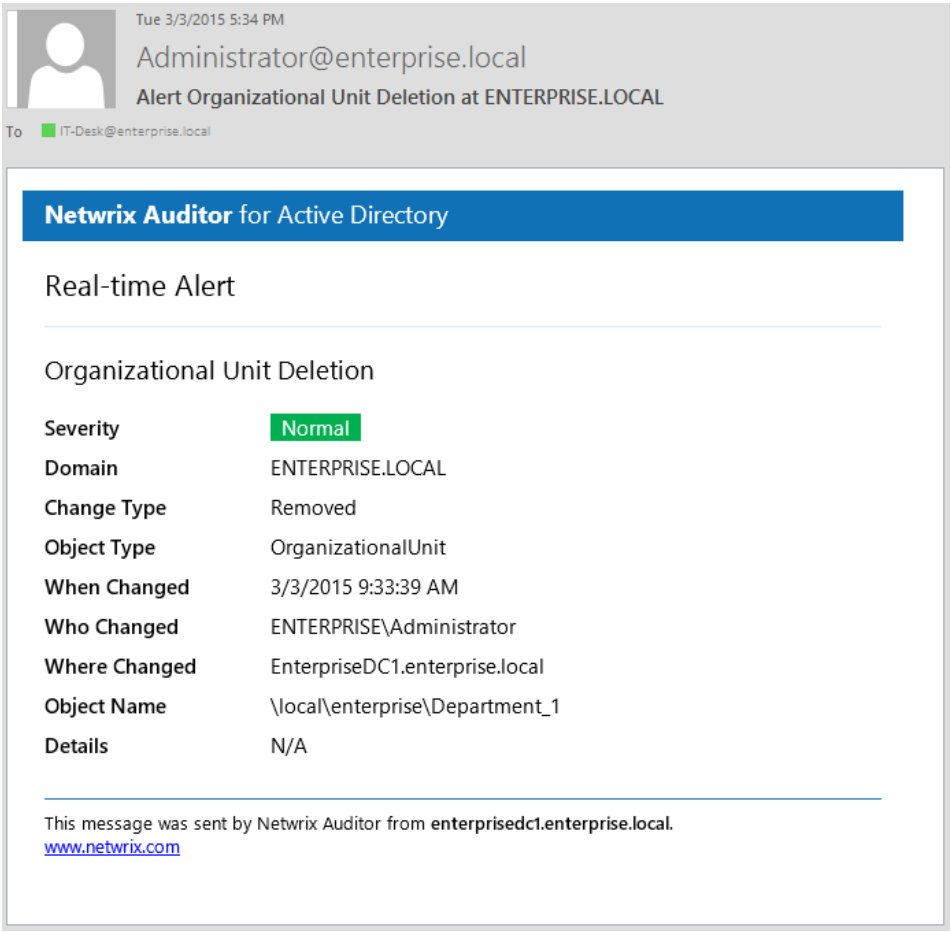
   - **Email**—Specify the email address where notifications will be delivered. You can add as many recipients as necessary.

     Click **Verify** to check your email settings. The product will send a test message to the specified address and will inform you if any problems are detected.

   - **Text (SMS)**—Specify the phone number where SMS-notifications will be delivered. Select you **Carrier** in the drop-down list.

     NOTE: In the current Netwrix Auditor version only AT&T, Sprint, Verizon and T-Mobile carriers are supported.

6. Review your real-time alert settings and click **Finish** to exit the wizard. The new alert will be created under the **Real-Time Alerts** node. If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients:



Refer to Create Custom Alerts for detailed instructions on how to create some popular custom alerts ("User granted VPN permissions", "User account lockout").

8.1.1. Identify Correct Attributes

1. On the domain controller, make a test change that you want to configure a real-time alert for and that will act as a trigger.
2. In the Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** and click **Run** in the right pane. On data collection completion, you will receive a Change Summary email containing a list of changes that have been detected.
3. In this email, look for the parameter name in the **Details** column of the corresponding change.
4. Open the `propnames.txt` file located in the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder and search for this parameter name. The value corresponding to this parameter is the name of the attribute you are looking for.

NOTE: If you are unable to locate the parameter name in the `propnames.txt` file, that means that the Change Summary email contains the internal AD name for this attribute instead of a

friendly name. In this case, this is the name of the attribute you are looking for that must be specified in the **Attribute Filters** dialog.

For example, if you want to create an alert that is triggered by modifications of a user's Dial-in/VPN permissions, and you are unsure which attribute is responsible for this change, do the following:

1. On the domain controller, navigate to **Start** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Expand the domain node and select **Users**.
3. Right-click a user and select **Properties** from the pop-up menu.
4. In the **Dial-in** tab, select **Allow access** in the **Network Access Permission** section.
5. In the Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** and click **Run** in the right pane. On data collection completion, you will receive a Change Summary email containing the change you have made.
6. In the **Details** column, locate the change parameter: **Allow Dial-in**.
7. Open the `propnames.txt` file and search for this parameter name. The entry in this file must say: `*.msNPAllowDialin=Allow Dial-In.` "`msNPAllowDialin`" is the name of the attribute that must be selected from the drop-down list in the **Attribute Filters** dialog when creating the alert.

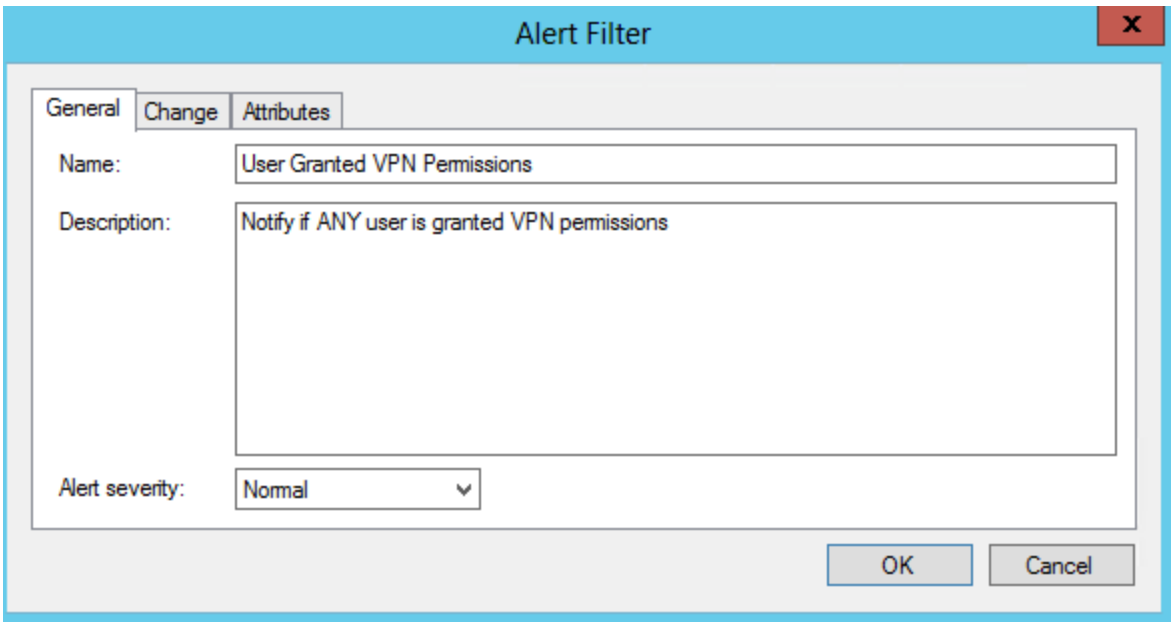
8.1.2. Create Custom Alerts

1. Start the **New Real-Time Alert** wizard:
   - In the Netwrix Auditor Administrator Console— Navigate to **Managed Objects** → **your_Managed_Object_name** → **Active Directory,** right-click the **Real-Time Alerts** node and select **New Real-Time Alert**.
   - In the **Managed Object** wizard— Proceed to the **Configure Real-Time Alerts** step and click **Add**.
2. On the **Specify Real-Time Alert Name** step, specify the alert name, e.g., "User Account Lockout" or "User Granted VPN Permissions", and enter alert description (optional).
3. On the **Configure Real-Time Alert Filters and Notifications** step, specify the alert filters and configure email notifications. Click **Add** in the **Alert Filters** section to specify a condition that will trigger the alert.
4. Complete the **Alert Filter** wizard. Depending on the alert you want to create, complete the following fields:

Option	The User Account Lockout Alert	The User Granted VPN Permissions Alert
	The **General** tab	
Name	E.g., “User Account Lockout”	E.g., "User Granted VPN Permissions"
Description	Enter the description for this filter (optional).	
Alert severity	**Normal**	**Normal**

NOTE: Alert severity level will be displayed in the email notification.

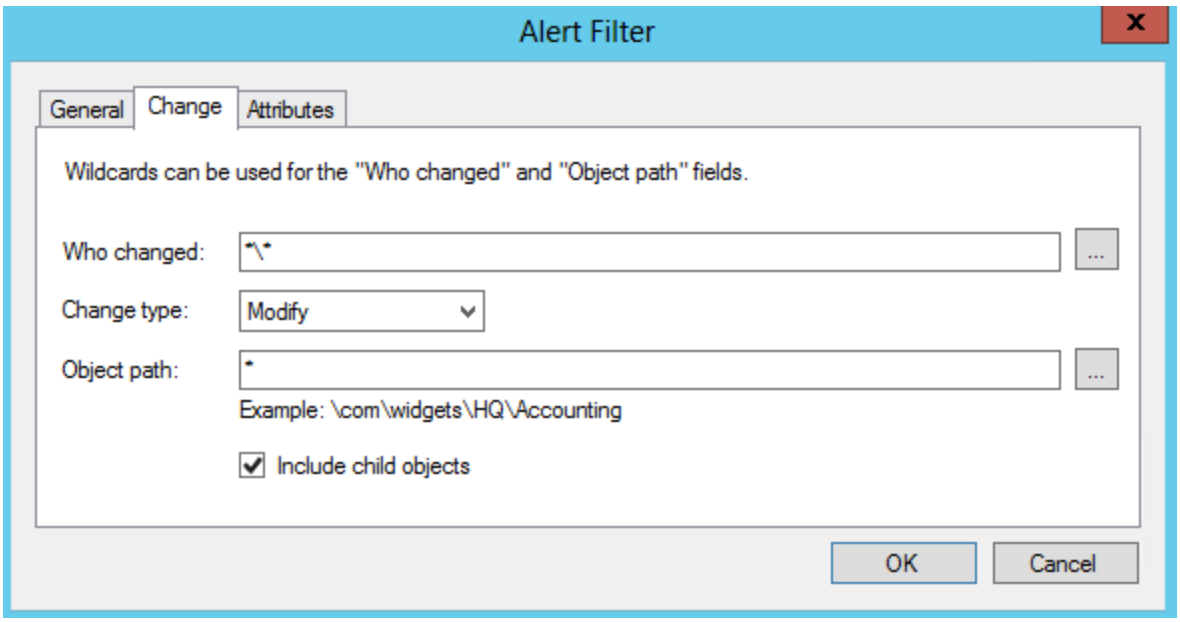
NOTE: The picture below corresponds to the **User Granted VPN Permissions** alert.



Option	The User Account Lockout Alert	The User Granted VPN Permissions Alert
	The **Change** tab	

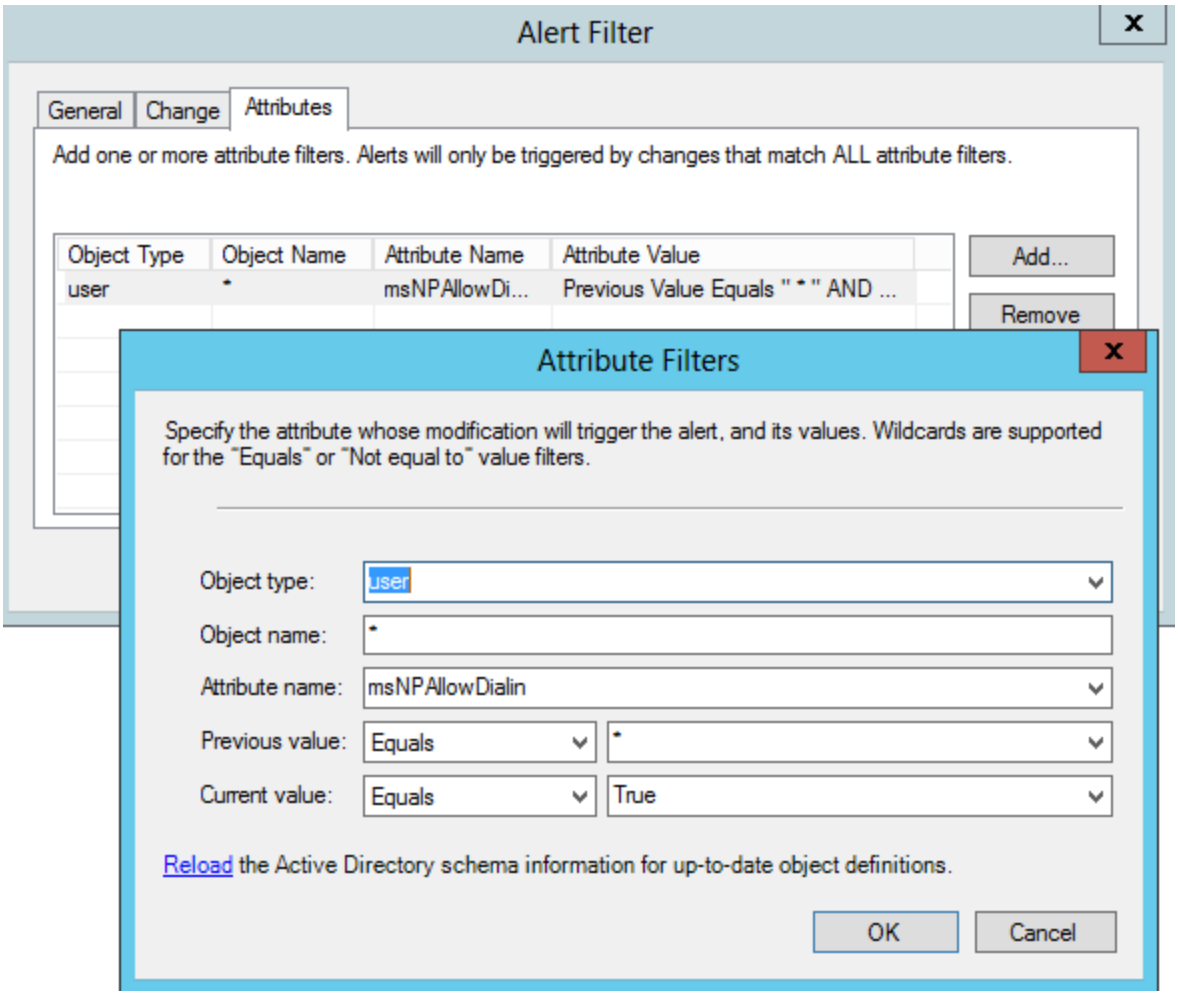
Option	The User Account Lockout Alert	The User Granted VPN Permissions Alert
Who changed	** **NOTE:** Active Directory is responsible for locking accounts. An account used by the system will be returned as the "Who changed" parameter.	** **NOTE:** This alert will be triggered if any user's VPN permissions are modified.
Change type	**Modify**	**Modify**
Object path	Leave this field empty. **NOTE:** This alert will be triggered by any account lockout in your Active Directory domain.	Leave this field empty.
Include child objects	Select this option.	Select this option.

NOTE: The picture below corresponds to the **User Granted VPN Permissions** alert.



Option	The User Account Lockout Alert	The User Granted VPN Permissions Alert
	The **Attributes** tab	
Object type	**User**	**User**
Object name	Leave this field empty.	Leave this field empty.
Attribute name	**lockoutTime** **NOTE:** If you cannot locate this attribute in the list, type it in manually.	**msNPAllowDialin**
Previous value	**Equals** Leave the second entry field empty.	**Equals** Leave the second entry field empty.
Current value	**Equals** Select **User Account Locked Out** from the second drop-down list. **NOTE:** If you cannot locate this value in the list, type it in manually.	**Equals** Select **True** from the second drop-down list.

NOTE: The picture below corresponds to the **User Granted VPN Permissions** alert.

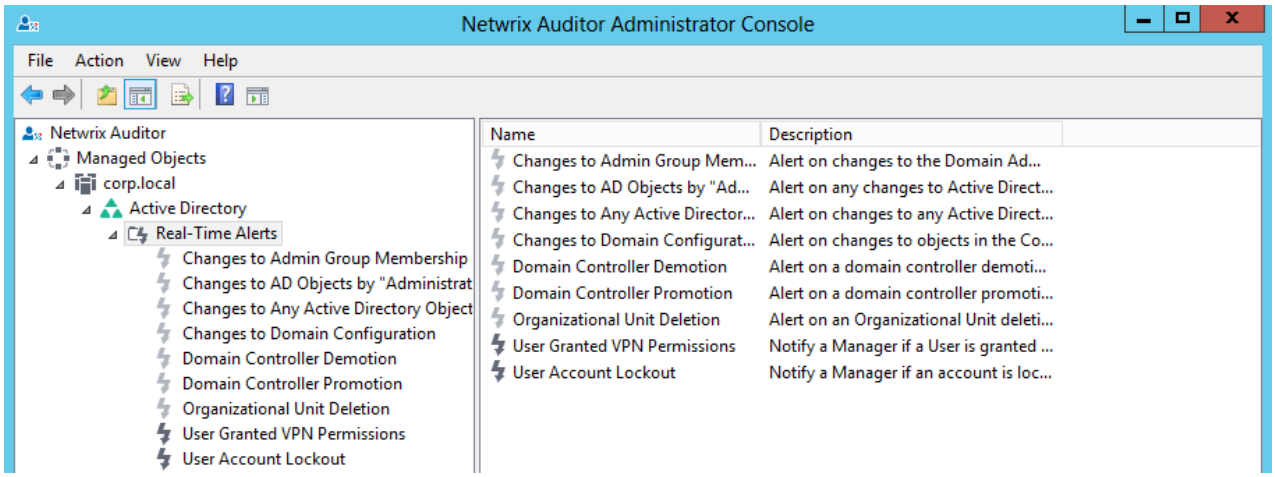


Click **OK** to save the changes and close the **Attribute Filters** dialog. And **OK** to save the changes and close the **Alert Filter** dialog.

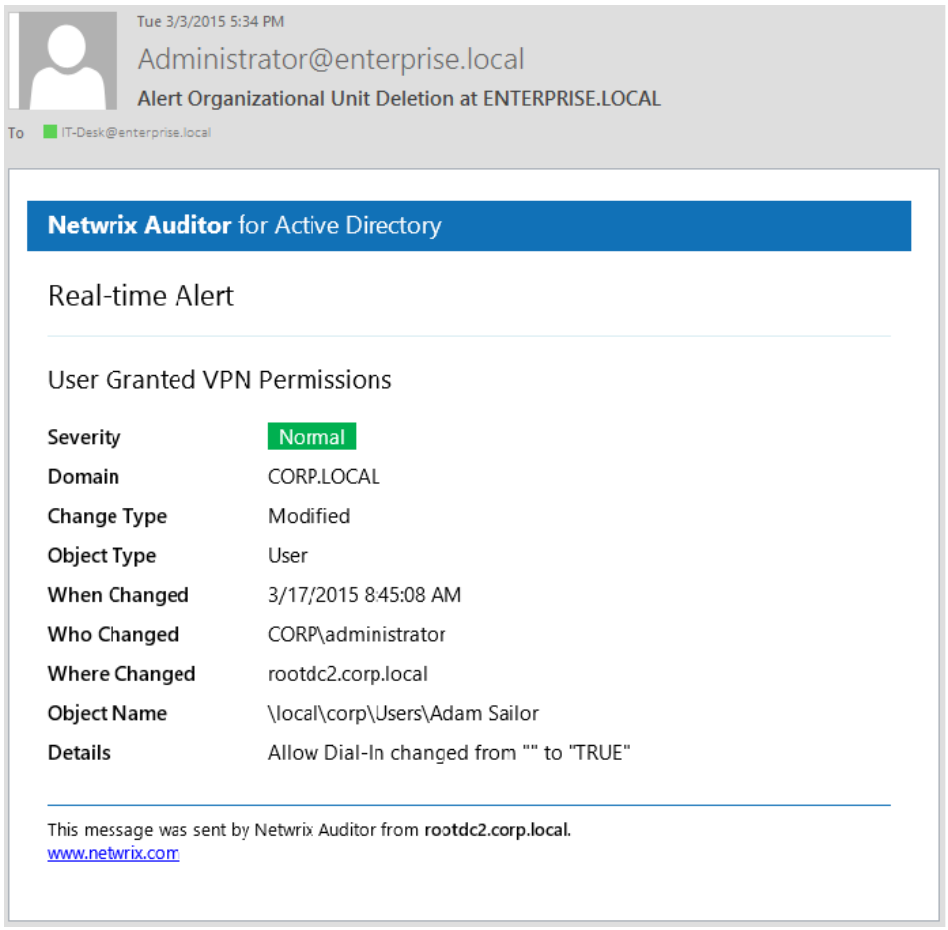
5. In the **Notifications** section of the **New Real-Time Alert** wizard, click **Add** and select **Email**. Specify the email address where notifications will be delivered. You can add as many recipients as necessary.

   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.

6. Review your Real-Time Alert settings and click **Finish** to exit the wizard. The new alert will be created under the **Real-Time Alerts** node and triggered if a specified change is detected.



Now, if a specified event is detected in your IT infrastructure, an email notification will be sent the recipients. For example, if VPN access is allowed for any user in your Active Directory domain, the following email will be sent:



8.2. Create Real-Time Alerts for Event Log

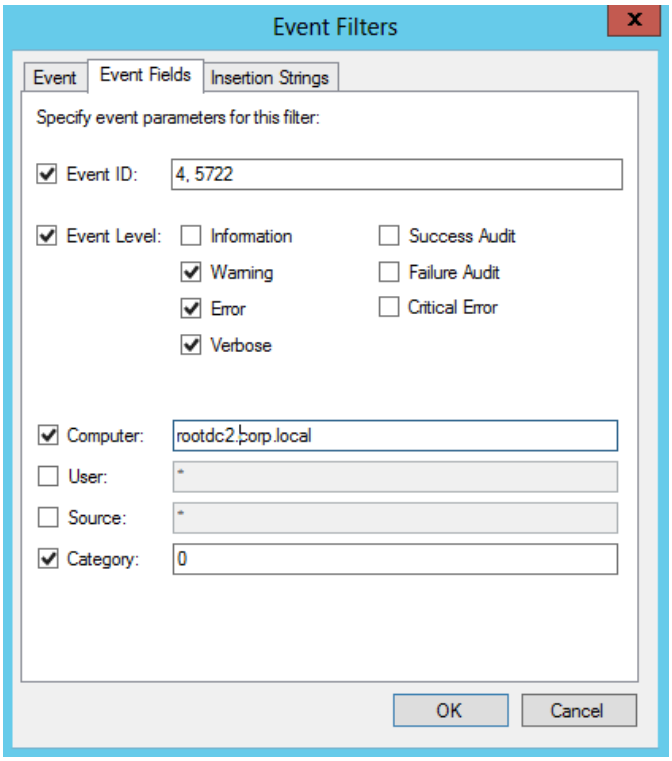
1. Start the **New Real-Time Alert** wizard. See Real-Time Alerts for more information.
2. On the **Specify Real-Time Alert Properties** step, specify the alert name and enter alert description (optional). Specify the number alerts per email. Grouped alerts for different computers will be delivered in 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 **Configure Real-Time Alert Filters and Notifications** step, specify the alert filters and configure email notifications. Click **Add** in the **Event Filters** section to specify an event that will trigger the alert.
4. 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** → **Control Panel** → **Administrative Tools** → **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. Syslog events will be ignored.

   - 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.

Option	Description
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**.

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

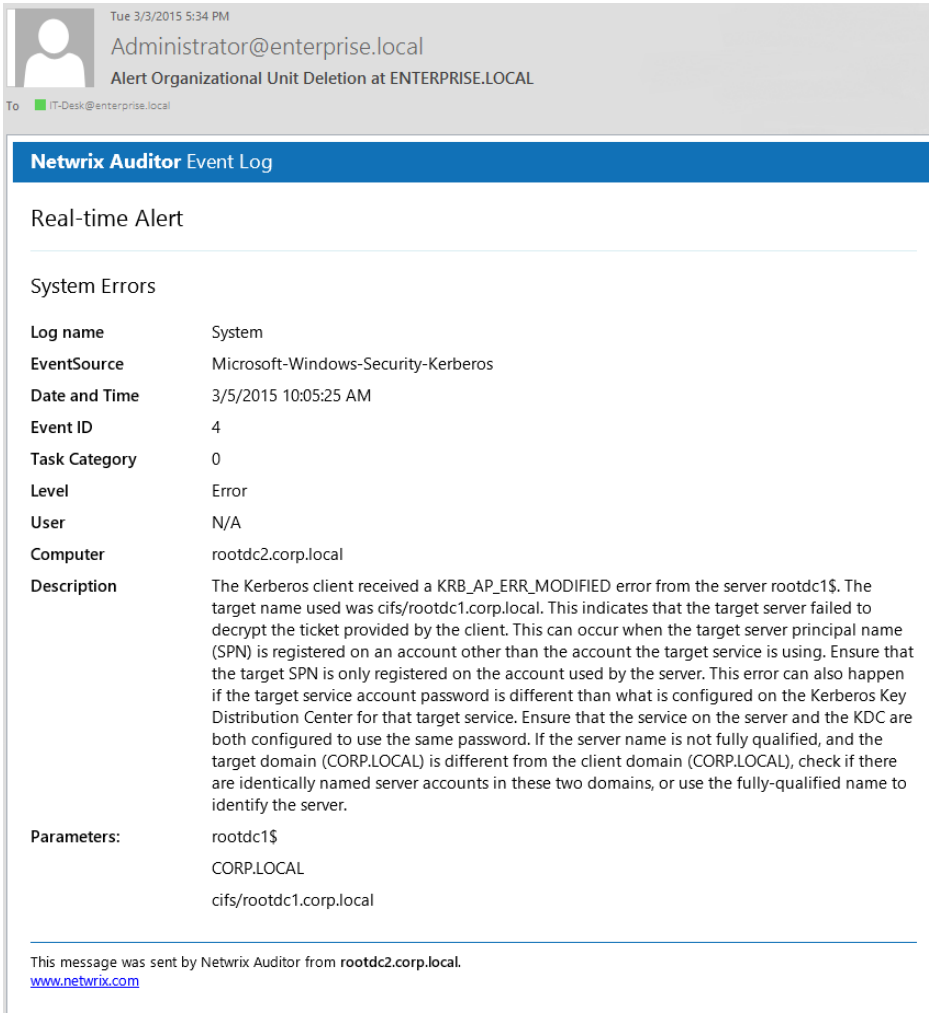
5. On the **Configure Real-Time Alerts Filers and Notifications** step of the **New Real-Time Alert** dialog, navigate to the **Notifications** section. Select **Event Log Collection Status notification recipients**, if you want the notifications to be delivered to the same email addresses as specified for daily Event Log Collection Status notifications (the list of Event Log Collection Status notification recipients is configured during the Managed Object creation and can be modified under **Managed Objects** → **your_Managed_Object_name** → **Event Log**). Alternatively, select **Specify recipients**, click **Add** and specify the email address where notifications are to 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.

6. On the **Configure Real-Time Alerts Filers and Notifications** step, customize the notification template if needed. Click **Edit** next to **Customize notifications template**. Edit the template by deleting or inserting information fields.

7. Review your Real-Time Alert settings and click **Finish** to exit the wizard. The new alert will be created

under the **Real-Time Alerts** node. If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients.



Tue 3/3/2015 5:34 PM

Administrator@enterprise.local

Alert Organizational Unit Deletion at ENTERPRISE.LOCAL

To IT-Desk@enterprise.local

Netwrix Auditor Event Log

Real-time Alert

System Errors

Log name	System
EventSource	Microsoft-Windows-Security-Kerberos
Date and Time	3/5/2015 10:05:25 AM
Event ID	4
Task Category	0
Level	Error
User	N/A
Computer	rootdc2.corp.local
Description	The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server rootdc1$. The target name used was cifs/rootdc1.corp.local. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Ensure that the target SPN is only registered on the account used by the server. This error can also happen if the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and the KDC are both configured to use the same password. If the server name is not fully qualified, and the target domain (CORP.LOCAL) is different from the client domain (CORP.LOCAL), check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.
Parameters:	rootdc1$
	CORP.LOCAL
	cifs/rootdc1.corp.local

This message was sent by Netwrix Auditor from **rootdc2.corp.local.**

www.netwrix.com

8.3. Create Real-Time Alerts for Non-Owner Mailbox Access Events

You can configure real-time 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 real-time alerts for non-owner mailbox access events, you need to create a **Computer Collection** Managed Object for auditing event logs.

To create real-time alerts for non-owner mailbox access events

NOTE: The procedure below describes the basic steps, required for creation of the Computer Collection Managed Object that will be used to collect data on non-owner mailbox access events. See Create Managed Objects to Audit Event Log for more information.

1. On the Netwrix Auditor Administrator Console page, click the **Event Log** tile. In this case you will be prompted to select **Computer Collection** as a Managed Object type on the next step.
2. On the **Specify Computer Collection Name** step, enter the computer collection name.
3. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared.
4. On the **Add Items to Computer Collection** step, select the **Windows Server** item type and add a server where your Exchange organization resides.
5. On the **Specify Notifications Recipients** step, do not provide email address to receive the summary as you have already configured notification delivery via Netwrix Mailbox Access Auditing tool.
6. On the **Configure Real-Time Alerts** step, make sure the predefined Real-Time Alerts are disabled. Click **Add** to create an alert for non-owner mailbox access event.
7. On the **Specify Real-Time Alert Properties** step of the **New Real-Time Alert** 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.
8. On the **Configure Real-Time Alert Filters and Notifications** step of the **New Real-Time Alert** wizard, specify the alert filters and configure email notifications. Click **Add** in the **Event Filters** section to specify an event that will trigger the alert.
9. Complete the **Event Filter** dialog.
   - In the **Event** tab, specify the filter name and description. In the **Event Log** field enter *"Netwrix Auditor Mailbox Access Core Service"*.
   - 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 Auditor Mailbox Access Core Service 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

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

See Review Event Description for more information.

- Source—Enter *"Netwrix Auditor Mailbox Access Core Service"*.

- 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.

10. On the **Configure Real-Time Alerts Filers and Notifications** step of the **New Real-Time Alert** dialog, navigate to the **Notifications** section. Select **Specify recipients**, click **Add** 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.

11. On the **Configure Real-Time Alerts Filers and Notifications** step, customize the notification template if needed. Click **Edit** next to **Customize notifications template**. Edit the template by deleting or inserting information fields.

12. Review your Real-Time Alert settings and click **Finish** to exit the **New Real-Time Alert** wizard. The new alert will be added to the **Real-Time Alerts** list on the **Configure Real-Time Alerts** step of the **New Managed Object** wizard.

    If an event occurs that triggers an alert, an email notification will be sent immediately to the specified recipients.

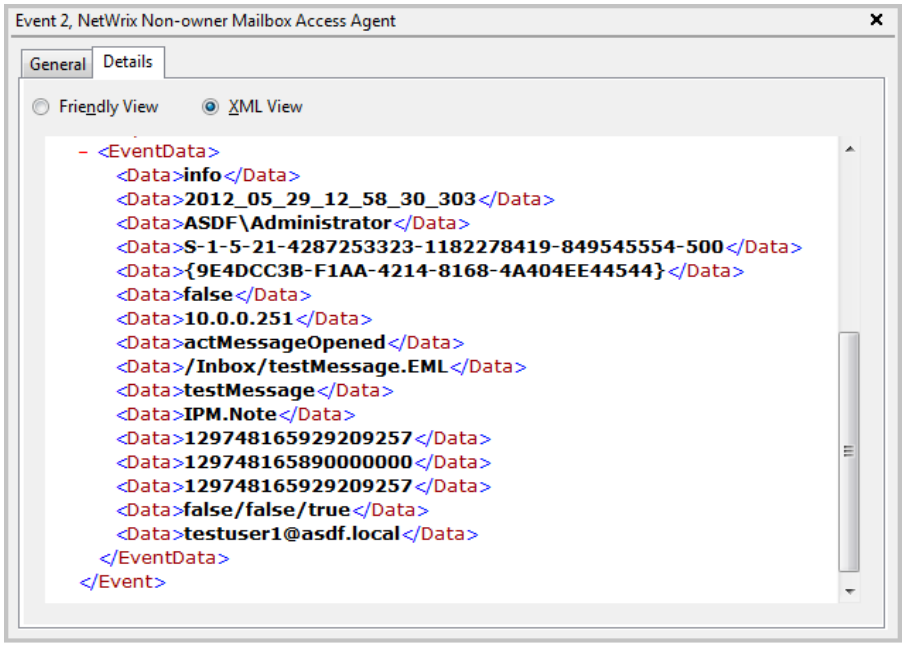
13. On the **Configure Audit Archiving Filters** step, in the **Inclusive Filters** section clear the filters you do not need, click **Add** and specify the following information:

- The filter name and description (e.g., Non-owner mailbox access event)
- In **Event Log**, enter *"Netwrix Auditor Mailbox Access Core Service"*.
- In **Write to**, select **Long-Term Archive**. The events will be saved into the local repository.

14. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

8.3.1. 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*

String	Description
String7	The IP of the computer accessing the mailbox
String8	The access type

The following strings depend on the non-owner access type, represented by different Event IDs:

Event ID	Access type (String 8)	Strings	Description
1	actFolderOpen	String9	The internal folder URL
2	actMessageOpened	String9	The internal message URL
		String10	The message subject
		String11	The message type: IPM.Note— Email, IPM.Contact – contact, etc.
3	actMessageSubmit	String9	The internal message URL
		String10	The message subject
		String11	Email addresses of the message recipients, separated by a semicolon
		String12	The message type: IPM.Note— Email, IPM.Contact – contact, etc.
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

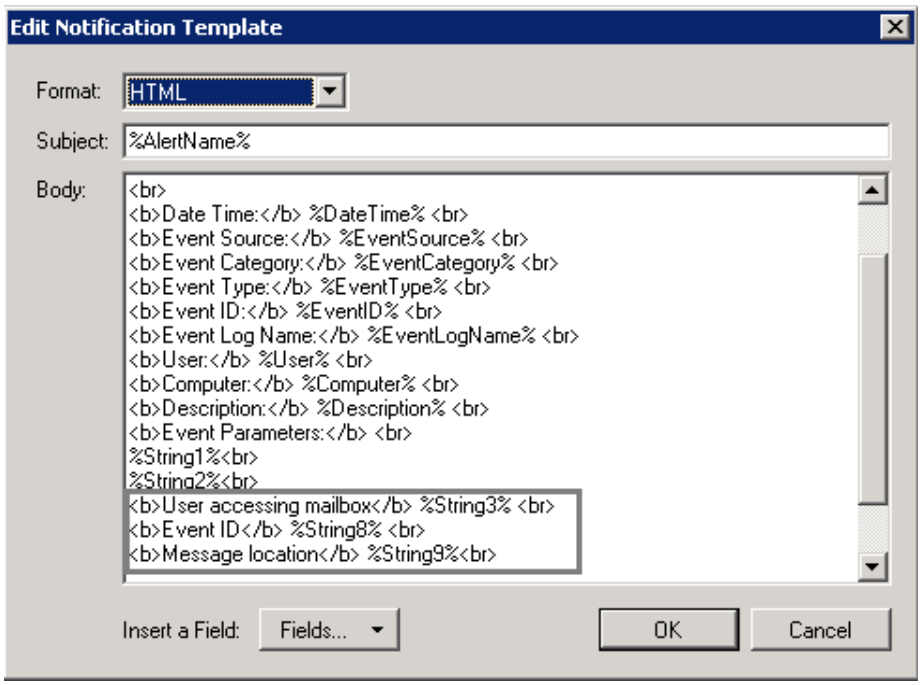
Event ID	Access type (String 8)	Strings	Description
8	actMessageCreatedAndSaved	String9	The internal message URL
9	actMessageMoveCopy	String9	The message being moved/copied—the final part of the message URL, e.g., /Inbox/testMessage.EML
		String10	The action – copy or move
		String11	The folder URL the message is copied/moved from
		String12	The destination folder URL
		String13	The message type: IPM.Note—Email, IPM.Contact – contact, etc.
10	actFolderMoveCopy	Strings 9 -13	The string descriptions for the folder are similar to those for messages.
14	actFolderCreated	String9	The new folder URL

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


Edit Notification Template
Format:
HTML
Subject:
%AlertName%
Body:

Date Time: %DateTime%
Event Source: %EventSource%
Event Category: %EventCategory%
Event Type: %EventType%
Event ID: %EventID%
Event Log Name: %EventLogName%
User: %User%
Computer: %Computer%
Description: %Description%
Event Parameters:
%String1%
%String2%
User accessing mailbox %String3%
Event ID %String8%
Message location %String9%
Insert a Field:
Fields...
OK
Cancel

9. Configure Settings

Netwrix Auditor provides a convenient interface for configuring or modifying settings that are applied to all existing Managed Objects and target systems audited within them. This chapter provides detailed instructions on how to configure these settings.

NOTE: For instructions on how to configure or modify settings for each Managed Object individually, or the target system audited with the product, refer to Modify Managed Objects.

To modify global settings

1. In Netwrix Auditor Administrator Console, navigate to **Settings**.
2. In the right pane, click on the setting name to see details. Review the following for additional information:
   - Configure Email Notifications Settings
   - Configure Data Collection Settings
   - Configure Syslog Platforms Settings
   - Configure Integration API Settings
   - Update Licenses

9.1. Configure Email Notifications Settings

The SMTP settings are configured when you create the first Managed Object in the **New Managed Object** wizard. Navigate to **Settings** → **Email Notifications** to review the SMTP settings used to deliver email notifications, reports, etc., and click **Modify** to adjust them if necessary.

Setting	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	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

Setting	Description
	authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
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.

You can also configure the product to notify you about critical events during Netwrix Auditor run-time.

1. Navigate to **Settings** → **Email Notifications**.
2. Click **Modify** next to **Notify on critical product health state**. Then specify the email address where notifications will be delivered. See Monitor Netwrix Auditor System Health for more information.

9.2. Configure Data Collection Settings

Navigate to **Settings** → **Data Collection** to review the default data collection settings, including the default Data Processing Account and data collection schedule, and update them if necessary.

NOTE: These settings affect auditing of the following systems:

- File Servers
- SQL Server
- VMware
- Windows Server
- Inactive users in Active Directory
- Password expiration in Active Directory

To modify default data collection and Change Summary generation schedule

1. Click **Modify** next to **Default data collection and Change Summary generation schedule**.
2. In the **Modify Schedule** dialog, set the new schedule (for example, increase the number of data collections per day or the start time).

- You can also create several scheduled tasks to collect data. To do it, select **Show multiple schedules**. After selecting this checkbox you will be able to expand the scheduled tasks list and create new tasks and modify them separately.
- Click **Advanced** to customize your scheduled data collection task. In the **Advanced Schedule Options** dialog, you can specify the **Start** and the **End** dates, frequency, task duration, etc.

To modify the default Data Processing Account

1. Click **Modify** next to **Default Data Processing Account**.
2. Provide the account credentials.

NOTE: Make sure that the new account is granted all required rights and permissions to collect data from the audited systems. See Netwrix Auditor Installation and Configuration Guide for more information.

9.3. Configure Syslog Platforms Settings

To review a list of Syslog-based platforms those event logs can be audited, navigate to **Settings** → **Syslog Platforms**. Netwrix Auditor provides the following predefined platform types: Generic, Red Hat Enterprise Linux 5, and Ubuntu.

You can also create and configure new Syslog-based platforms that can be subsequently selected as item types for your Managed Objects.

Do one of the following:

- Contact Netwrix Support to order a custom platform from Netwrix if the predefined platforms do not cover your needs.
- Click **Add** to add a new platform. See To create a Syslog-based platform for more information.
- Select a platform from the list and click **Edit** to modify it.

NOTE: You cannot edit a predefined platform. If you try to edit it, a copy of this platform will be created, which can be modified.

- Select a custom platform and click **Remove** to delete a platform.

NOTE: The predefined platforms cannot be deleted.

- Click **View** to view platform rules.
- Click **Modify** next to **Syslog server port** to update a port number.

To create a Syslog-based platform

1. Click **Add**.
2. In the **New Syslog Platform** dialog, select the following parameters:
   - Select the platform type. Select **New** to create a new platform and define its rules. Alternatively, you can select **Copy**, and create a platform based on a predefined platform, thus inheriting its rules and edit it afterwards.
   - Specify a platform name and add a description.
3. On the **Configure Rules** step, click **Add** to add events processing rules. You can also edit, re-order and delete rules on this step. To store events that do not match any of the rule patterns, select the corresponding checkbox.
4. In the dialog that opens, specify the following parameters:

Parameter	Description
Enable	Make sure that this option is selected.
Rule name	Specify the rule name.
Description	Specify the rule description (optional).
Regular expression pattern	Specify a pattern, according to which events will be collected. When an event matches this pattern, this event will be logged. The rows below contain information that will be added to a Syslog event if it matches a specified pattern. This information can be used to filter events and sort them by.
Source	Specify the name of a source. It can be any word that will help you identify the platform where an event was generated.
User name	Specify the number of a capturing group which defines a user name in a pattern in the following format: `%Capturing_Group_Number`. If needed, you can add more information, for example: `Domain_Name\%Capturing_Group_Number`. The right `Capturing_Group_Number` can be calculated if you enumerate capturing groups in a pattern starting from *0*.
Event ID	Specify a number which will be added to an event as its ID.
Event level	Specify the event level.

5. Review the details and complete the wizard. The platform will be added to the **Available platforms** list.

9.4. Configure Integration API Settings

Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

The Netwrix Auditor Integration API provides access to audit data collected by Netwrix Auditor through REST API endpoints. According to the RESTful model, each operation is associated with a URL. Integration API provides the following capabilities:

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

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

9.5. Update Licenses

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

To update/add a license

1. Click **Update Licenses**.
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.

9.5.1. 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. 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 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	HTML entity
&	**&**
e.g., Ally **&** Sons	e.g., Ally **&** Sons
"	**"**
e.g., Domain1\Users\"Stars"	e.g., Domain1\Users**"**Stars**"**
'	**'**
e.g., Domain1\Users\O'Hara	e.g., Domain1\Users\O**'**Hara

Symbol	HTML entity
<	**<**
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.**

10. Additional Configuration

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

- Start Auditing Mailbox Access
- Monitor Netwrix Auditor System Health
- Configure Audit Automatically with Active Directory Audit Configuration WizardConfigure Audit Automatically with Active Directory Audit Configuration Wizard
- Roll Back Changes with Active Directory Object Restore
- Enable Auditing of Active Directory Partitions
- Configure Audit Archiving Filters
- Exclude Objects From Auditing Scope
- Fine–tune Netwrix Auditor Using Registry Keys
- Enable Integration with Third-Party SIEM Solutions
- Automate Sign-in to Netwrix Auditor Client
- Customize Branding

10.1. Start Auditing Mailbox Access

To ensure security of sensitive information such as intellectual property, personally identifiable information, business plans, and trade secrets, you need to collect detailed information on unauthorized mailbox access. Non-owner Mailbox Access Auditing available for the following audited systems:

- **Exchange Online**. See To configure non-owner mailbox access auditing for Exchange Online for more information.

  NOTE: By default, non-owner mailbox access auditing enabled for Exchange Online.

- **Exchange**. See To configure non-owner mailbox access auditing for Exchange for more information.

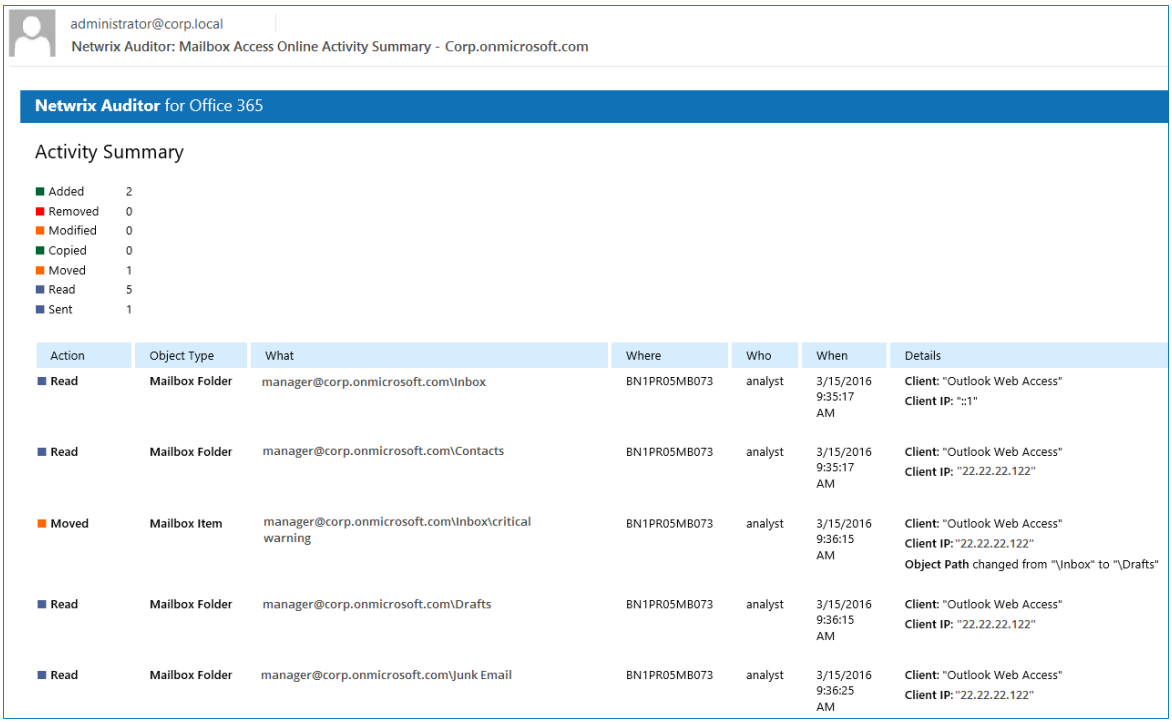
To configure non-owner mailbox access auditing for Exchange Online

1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Exchange Online**.
2. Click **Track Access** next to **Non-owner Mailbox Access Auditing** in the right pane and complete the

fields.

Option	Description
Enable Mailbox Access audit	Enable this option to start auditing non-owner mailbox access in your Exchange Online. **NOTE:** If later you disable the product by clearing this checkbox, and then re-enable it after some time, data will start to be collected only after the first scheduled data collection task is run (at 3:00 AM by default). As a result, events that occur after the product is re-enabled and before the first scheduled task will not be reported. To avoid audit data loss, it is recommended to run a scheduled data collection task manually immediately after the product is re-enabled.
Enable automatic audit configuration	If you select to automatically configure audit in the target environment, your current audit settings will be checked on each data collection and adjusted if necessary. **NOTE:** This method is recommended for evaluation purposes in test environments. For a full list of audit settings required for Netwrix Auditor to collect comprehensive audit data and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide. If you want to configure audit manually, refer to Netwrix Auditor Installation and Configuration Guide for a full list of audit settings, and instructions on how to configure them.
Notify users on non-owner access to their mailboxes	Select this checkbox if you want to notify on non-owner access to their mailboxes.
Notify only selected users	Select this checkbox and click **Add** 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.

3. Run data collection to receive a report on non-owner mailbox access events.



To configure non-owner mailbox access auditing for Exchange

1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Exchange**.
2. Click **Track Access** next to **Non-owner Mailbox Access Auditing** in the right pane and complete the fields.

Option	Description
Enable	Make sure the **Enable** option is checked. **NOTE:** If later you disable the product by clearing this checkbox, and then re-enable it after some time, data will start to be collected only after the first scheduled data collection task is run (at 3:00 AM by default). As a result, events that occur after the product is re-enabled and before the first scheduled task will not be reported. To avoid audit data loss, it is recommended to run a scheduled data collection task manually immediately after the product is re-enabled.
Monitored Exchange Servers	
Specify the Exchange servers you want to	Click **Add** and enter the FQDN name of audited server, or import the list of audited servers from a file.

Option	Description
monitor	You can import a list of servers from a *.txt file containing one FQDN computer name per line.
Use Core Service to collect detailed audit data (Exchange 2007 and 2010 only)	Select this checkbox to enable Netwrix Auditor Mailbox Access Core Services that collect the information required for detailed reports. **NOTE:** If this option is disabled, only summary reports will be available. If you choose not to use core services for audit data collection, you must configure native auditing on the audited Exchange. See Netwrix Auditor Installation and Configuration Guide for more information.
	Reports
Report delivery schedule (daily at 3:00 AM by default)	Click **Modify** to configure the data processing and report delivery schedule. **NOTE:** To be able to configure this schedule, you must save your configuration first by clicking **Apply** at the bottom of the dialog.
Summary report	Select this option to receive summary reports. These reports contain information on who accessed what mailbox and when.
Detailed report	Select this option to receive detailed reports. These reports contain information on who accessed what mailbox and when, and what actions were performed on the accessed mailbox contents, including information on unauthorized access to calendar, contacts and tasks. See Actions Captured When Auditing Mailbox Access for more information. **NOTE:** To receive detailed reports, the **Use Core Service to collect detailed audit data** option must be enabled.
Only report on mailboxes whose owners belong to these OUs	Select this checkbox to filter data in reports by organizational units. Click **Select OUs** and specify the organizational units you want to audit for non- owner mailbox access. Reports will include information only on non-owner access to mailboxes that belong to users from the specified OUs.
Report recipients	Enter the email addresses where reports are to be delivered, separated by commas.

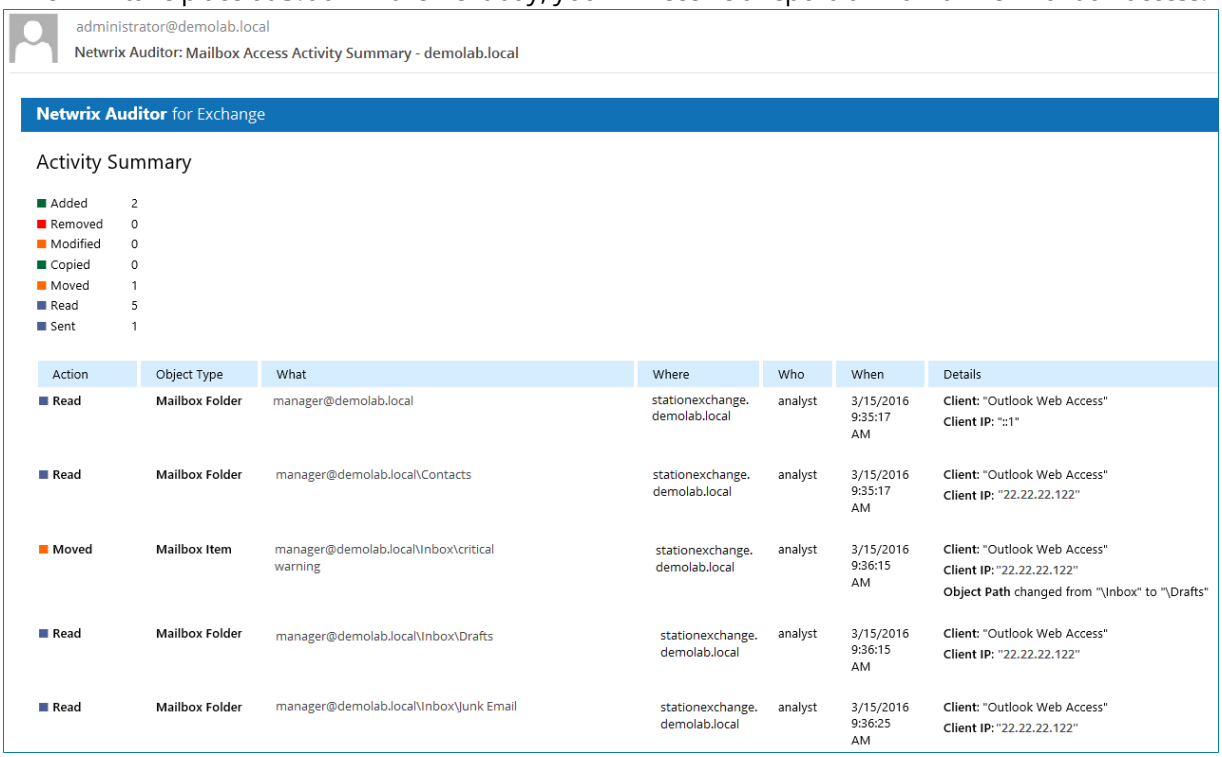
Option	Description
Attach reports as CSV files	Select this checkbox to receive reports attached to emails as CSV files.
Notify users on non-owner access to their mailboxes	Select this checkbox if you want to notify on non-owner access to their mailboxes.
Customize report template	Click **Customize** to edit the notification template, for example, modify the text of the message.
Notify only selected users	Select this checkbox and click **Specify Users** 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.
Report delivery settings	
SMTP server	Enter your SMTP server name.
Port	Specify your SMTP server port number.
From address	Enter the address that will appear in the "*From*" field in reports. **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.
Authentication	Click this button to specify authentication settings.
Use 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.
Confirm password	Confirm the password.
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.

3. In the **Scheduled Task Credentials** dialog, enter the account (in the *DOMAIN\user* format) and

password that will be used for data collection. To audit several Exchange organizations in the domain where Netwrix Auditor is installed, specify the user that belongs to the **Domain Admins** group. To monitor Exchange organizations in different domains of the same forest, specify the user that belongs to the **Enterprise Admins** group.

NOTE: You will be prompted to specify the default account every time you save your current configuration.

4. Run the first data collection based on instructions provided in the dialog. The first data collection creates the initial snapshot of the audited servers current state. After the second data collection, which will take place at 3.00 AM the next day, you will receive a report on non-owner mailbox access:



administrator@demolab.local

Netwrix Auditor: Mailbox Access Activity Summary - demolab.local

Netwrix Auditor for Exchange

Activity Summary

Added	2
Removed	0
Modified	0
Copied	0
Moved	1
Read	5
Sent	1

Action	Object Type	What	Where	Who	When	Details
Read	Mailbox Folder	manager@demolab.local	stationexchange.demolab.local	analyst	3/15/2016 9:35:17 AM	**Client:** "Outlook Web Access" **Client IP:** "::1"
Read	Mailbox Folder	manager@demolab.local\Contacts	stationexchange.demolab.local	analyst	3/15/2016 9:35:17 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"
Moved	Mailbox Item	manager@demolab.local\Inbox\critical warning	stationexchange.demolab.local	analyst	3/15/2016 9:36:15 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122" **Object Path** changed from "\Inbox" to "\Drafts"
Read	Mailbox Folder	manager@demolab.local\Inbox\Drafts	stationexchange.demolab.local	analyst	3/15/2016 9:36:15 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"
Read	Mailbox Folder	manager@demolab.local\Inbox\Junk Email	stationexchange.demolab.local	analyst	3/15/2016 9:36:25 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"

Mailbox Access Activity Summary email lists actions performed by someone other than the person who owns the mailbox, including both administrators and users, called *delegated* users, who have been assigned permissions to a mailbox.

10.2. Monitor Netwrix Auditor System Health

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

There are three types of events that can be logged:

Event Type	Description
Information	An event that describes the successful operation beginning and/or completion. For example, the product successfully completed data collection for a Managed Object.
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 audited system.

To view Netwrix Auditor System Health log

1. In Netwrix Auditor Administrator Console, navigate to your Managed Object.
2. Click **View Health Log** next to the **Netwrix Auditor System Health** section. The **Event Viewer** snap-in opens.

10.2.1. Netwrix Auditor Health Status Reporting

Now a system administrator is able to review all Netwrix Auditor warnings and errors in a dedicated report in Netwrix Auditor client and be notified on significant events with real-time alerts.

- To configure Netwrix Auditor to audit Netwrix Auditor System Health Log events
- To generate a report on Netwrix Auditor System Health Log events
- To create a real-time alert for Netwrix Auditor System Health Log events
- To configure email notifications on Netwrix Auditor critical events

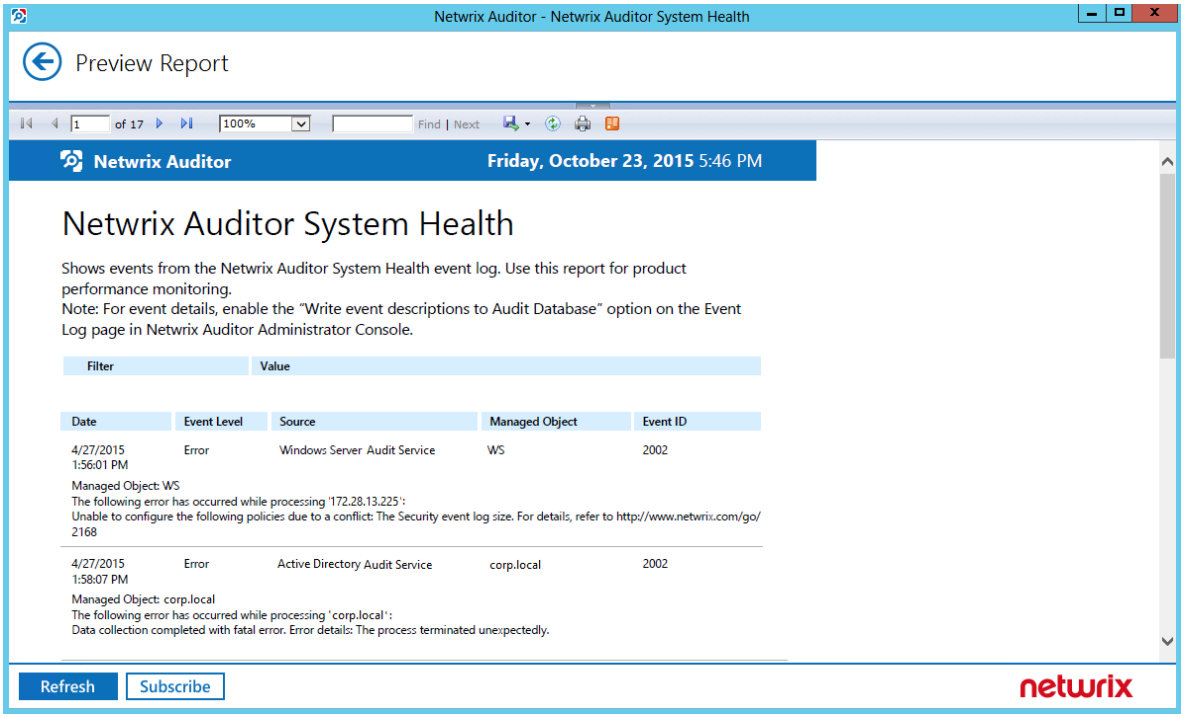
To configure Netwrix Auditor to audit Netwrix Auditor System Health Log events

1. Create a new Computer Collection Managed Object and add the computer where Netwrix Auditor Server resides as an item. You can also add a new item to an existing Managed Object. See Create Managed Objects to Audit Event Log for more information.
2. Navigate to **Managed Objects** → **your_Managed_Object_name** → **Event Log**. Select **Write event descriptions to Audit Database** if you want to see the exact error or warning text.
3. Navigate to the **Audit Archiving Filters** page and select the **Netwrix Auditor System Health Log** filter in the **Inclusive Filters** list.
4. Run initial data collection for your Managed Object.

5. Make sure that **Audit Database** settings are configured properly. See Manage Audit Database for more information.

To generate a report on Netwrix Auditor System Health Log events

1. Launch the Netwrix Auditor client and navigate to **Reports** → **Windows Server** → **Event Log**, and then select the **Netwrix Auditor System Health** report.

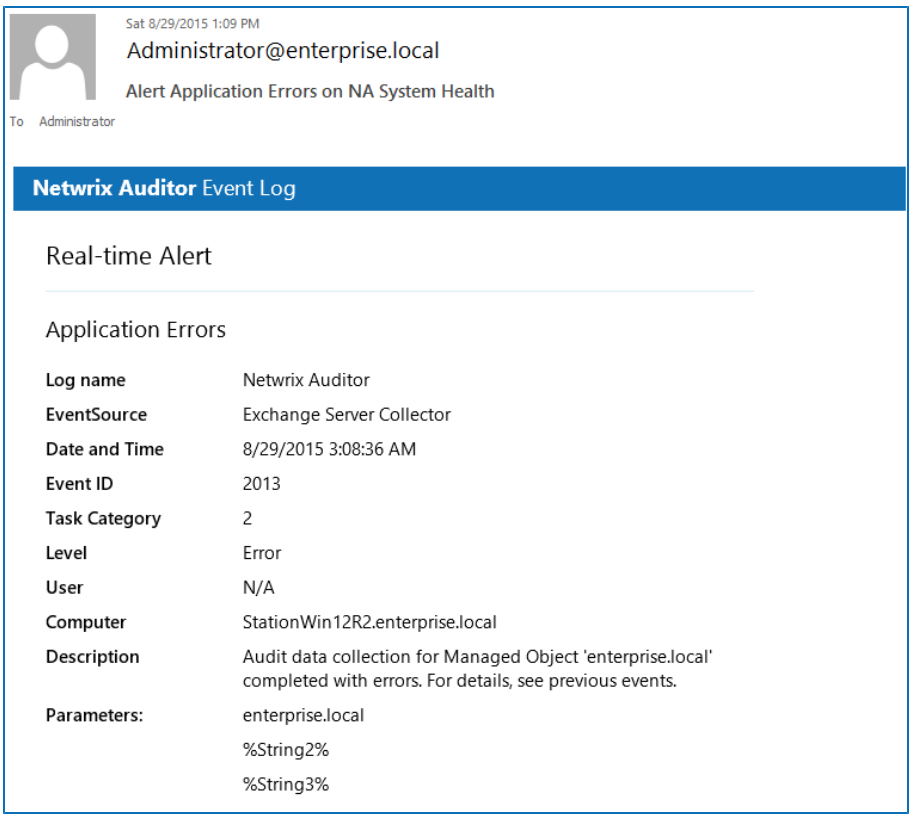


To create a real-time alert for Netwrix Auditor System Health Log events

1. Start the **New Real-Time Alert** wizard. Refer to Create Real-Time Alerts for Event Log for detailed instructions on how to configure real-time alerts.
2. On the **Configure Real-Time Alert Filters and Notifications** step, click **Add** in the **Event Filters** section and select **Netwrix Auditor** event log. Specify events you want to be alerted about (errors, warnings, etc.). Review your new alert settings and click **Finish**.

   Once the event that triggers an alert occurs, an email notification like in the example below will be

sent to the specified recipients.



To configure email notifications on Netwrix Auditor critical events

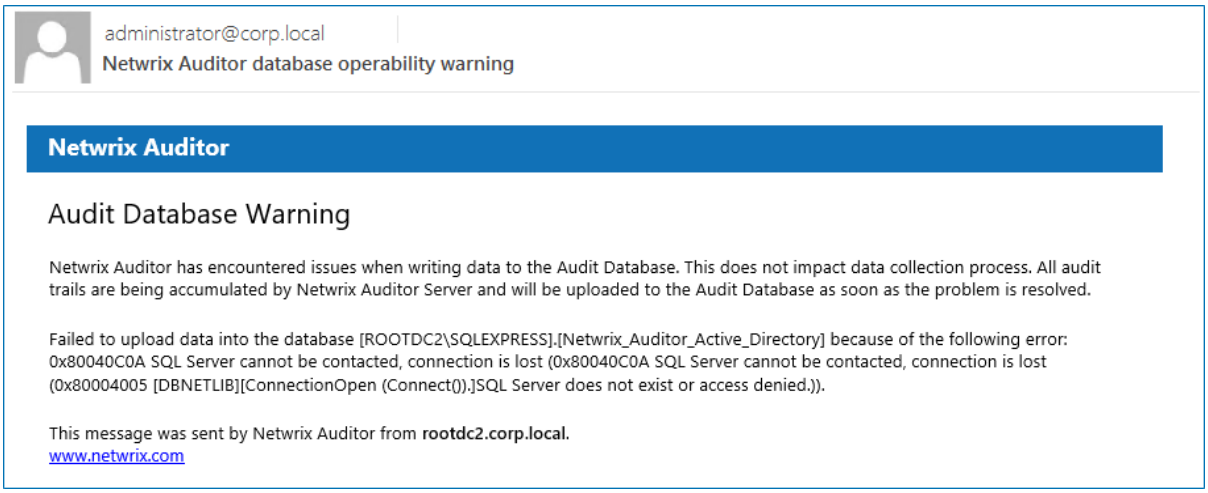
Netwrix Auditor can be configured to report about two types of critical events:

- Connection to Audit Database is lost.
- Insufficient space on the disk where Audit Database resides.

Perform the following steps to configure email notifications:

1. In Netwrix Auditor Administrator Console, navigate to **Settings** → **Email Notifications**.
2. Click **Modify** next to **Notify on critical product health state** and specify the email address where notifications will be delivered.

   If an event occurs that triggers an alert, an email notification like in the example below will be sent immediately to the specified recipients.



NOTE: When the product returns to its normal state, you will receive an information email notification.

10.3. Configure Audit Automatically with Active Directory Audit Configuration Wizard

If you have already configured a Managed Object to audit your Active Directory domain and Exchange organization, but for some reason decided to disable automatic audit configuration in the **New Managed Object** wizard, you can still configure audit settings automatically through the **Active Directory Audit Configuration** wizard.

To configure audit automatically through the Active Directory Audit Configuration wizard

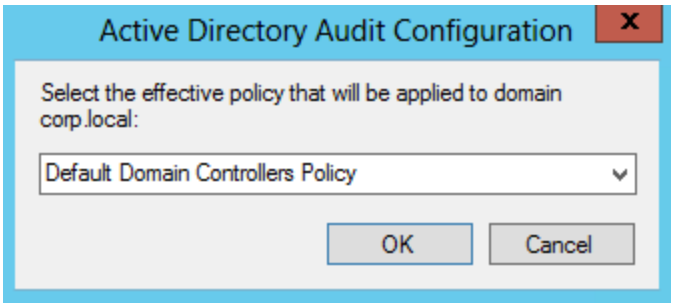
NOTE: For the wizard to work properly, you must run it under an account that is a member of the **Domain Admins** or **Enterprise Admins** group.

1. In Netwrix Auditor Administrator Console, navigate to your Managed Object that audits domain. Refer to Create Managed Objects to Audit Active Directory for detailed instructions on how to create a Managed Object that audits Active Directory domain.
2. Select **Active Directory** in the left pane, and click **Configure Audit** next to **Audit Configuration** to launch the **Active Directory Audit Configuration** wizard.
3. On the first step, specify the name of the domain that you want to configure for auditing.

4. Enable the **Apply to the forest root domain** option if you want to audit changes to Active Directory schema and configuration, as the forest root domain contains audit settings for the Configuration and Schema partitions.

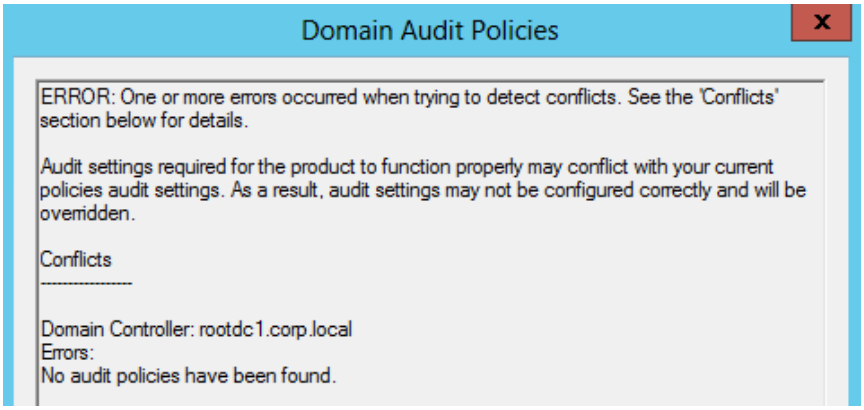
   NOTE: Refer to Enable Auditing of Active Directory Partitions for detailed instructions on how to enable monitoring of changes to the Schema partition in the target AD domain.

5. Select the effective policy that is currently applied to the domain controllers and that is subject to change.



6. On the **Domain Audit Policies** step, specify the **Data Processing Account** that will be used by Netwrix Auditor to collect data from the audited domain.

7. Click **Detect.** If your current settings do not match the configuration required for the product to function properly, a report will be displayed showing the current audit policy settings in the monitored domain as in the example below:



NOTE: If any of your other policies conflict with the settings required for the product to function properly, a warning message will be displayed listing these conflicts. If this happens, analyze carefully how your environment will be affected before applying the required settings.

The Active Directory Audit Configuration wizard cannot recognize whether advanced audit policies are applied and configure them.

To apply the required configuration automatically, click **Adjust**. Your audit policy settings and the **Manage auditing and security log** right will be adjusted and the confirmation dialog will be displayed on successful operation completion.

8. On the **Object-Level Audit Settings** step, click **Detect** to verify your object-level audit settings for the Domain, Configuration and Schema partitions. Click **Adjust** to configure the required settings

automatically.

9. On the **Event Log Size and Retention Settings** step, click **Detect** to verify your **Security event log** size and retention settings. Click **Adjust** to configure the required settings automatically.

10. On the **Exchange Server Administrator Audit Logging Settings** step, click **Detect** to verify your Exchange Administrator Audit Logging settings. Click **Adjust** to configure the required settings automatically.

NOTE: This step is required only if the audited AD domain has an Exchange organization running Microsoft Exchange 2010 or 2013. Otherwise, skip this step.

11. Review your audit settings and complete the wizard.

10.4. Roll Back Changes with Active Directory Object Restore

With Netwrix Auditor you can quickly restore deleted and modified objects using the **Active Directory Object Restore** tool integrated 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

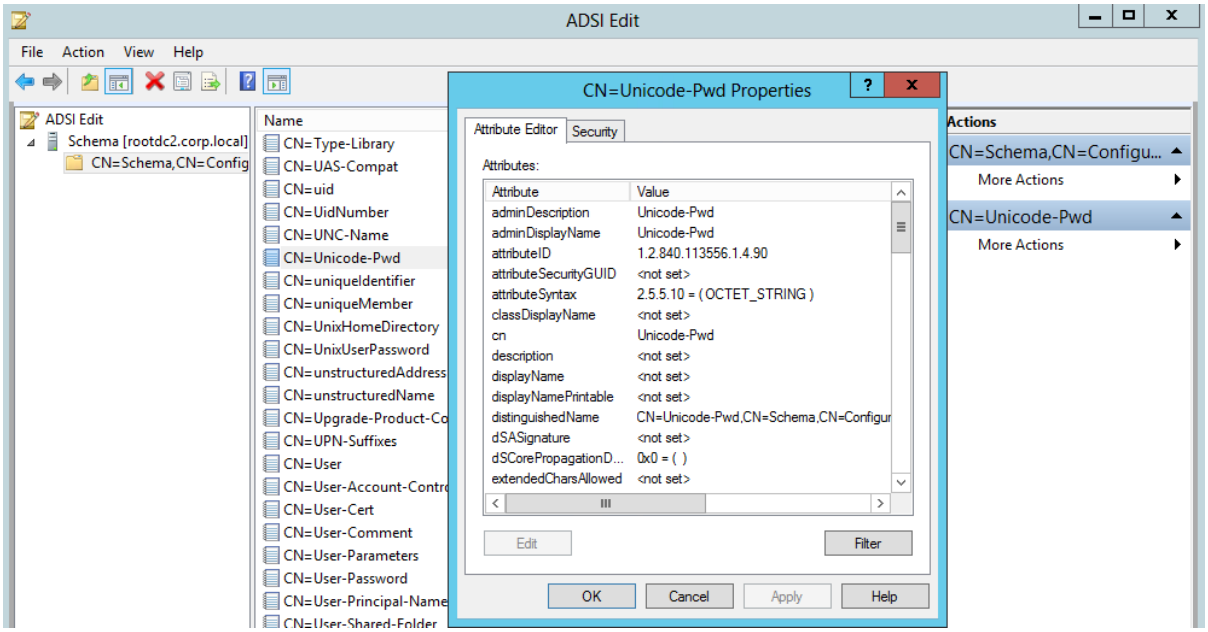
By default, when a user or computer account is deleted from Active Directory, its password is discarded as well as a domain membership. When you restore deleted accounts with the **Active Directory Object Restore** tool, it rolls back a membership in domain and sets random passwords which then have to 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

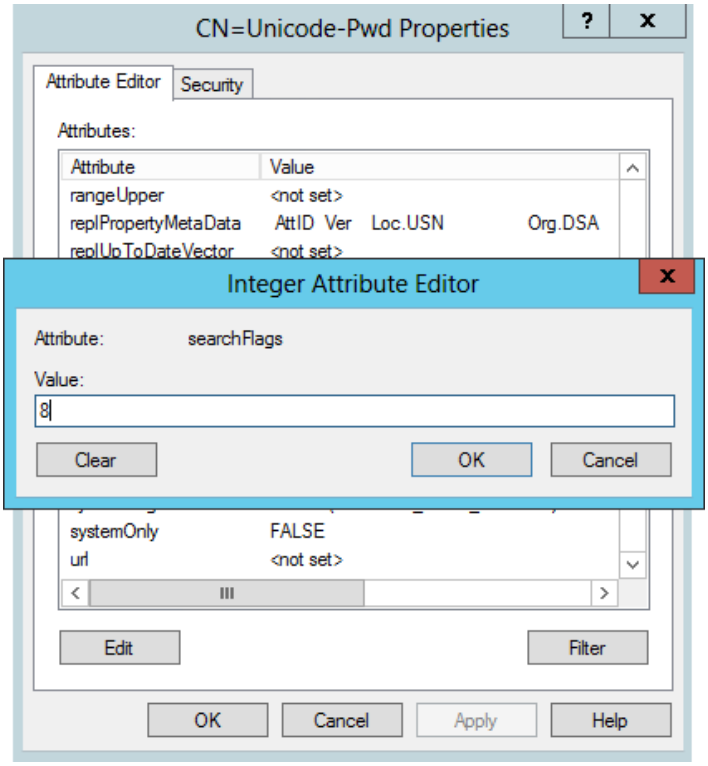
NOTE: To perform this procedure, you will need the ADSI Edit utility. In Windows Server 2008 and above, this component is installed together with the AD DS role, or it can be downloaded and installed

along with Remote Server Administration Tools.

1. Navigate to **Start** → **Programs** → **Administrative Tools** → **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. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Active Directory**.
2. In the right pane, click **Restore AD Objects** next to **Active Directory Object Restore**. The wizard opens.
3. 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.
4. On the **Select Rollback Source** step, specify the rollback source and monitored domain. The following restore options are available:

   - **Restore from 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.

     You can select the **Select a state-in-time snapshot** option 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.

- **Restore from AD 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.

5. 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.
6. On the **Select Changes to Roll Back** 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.
7. Wait until the tool has finished restoring the selected objects. On the last step, review the results and click **Finish** to exit the wizard.

10.5. Enable Auditing of Active Directory Partitions

NOTE: This topic applies to auditing Active Directory only.

Active Directory environment consists of the following directory partitions:

- **Domain partition**—Stores users, computers, groups and other objects. Updates to this partition are replicated only to domain controllers within the domain.
- **Configuration partition**—Stores configuration objects for the entire forest. Updates to this partition are replicated to all domain controllers in the forest. Configuration objects store the information on sites, services, directory partitions, etc.
- **Schema partition** — Stores class and attribute definitions for all existing and possible Active Directory objects. Updates to this partition are replicated to all domain controllers in the forest.

By default, Netwrix Auditor only tracks changes to the Domain partition and the Configuration partition of the audited domain. If you also want to audit changes to the Schema partition, or to disable auditing of changes to the Configuration partition do the following:

NOTE: You cannot disable auditing the Domain partition for changes.

To enable auditing of the Configuration and Schema partitions

1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Active Directory.**
2. In the right pane, click **Configure** next to **Advanced Options**.
3. In the **Advanced Options** dialog, select **Configuration** and **Schema**.

Information on changes to the selected partitions will be available in reports and will be saved in snapshots.

10.6. Configure Audit Archiving Filters

NOTE: Currently this functionality is available only for auditing event logs.

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 in one of the following locations:

- Configure audit archiving filters while creating a Managed Object for auditing event logs. See Create Managed Objects to Audit Event Log for more information.
- If you have a Managed Object configured to audit event logs, proceed with following steps. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name** → **Event Log** → **Audit Archiving Filters**.

Netwrix Auditor 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 select filters required to collect events for regulatory compliances (GLBA, HIPAA, PCI, SOX), click **Enable**, click **Select compliance** and choose a required regulation.

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.

Option	Description
	To find out a log's name, navigate to **Start** → **Control Panel** → **Administrative Tools** → **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. By selecting the **Syslog** option, only the events from Syslog-based platforms will be processed. Events from custom Windows logs with the same names will not be collected. **NOTE:** You can use a wildcard (*). For inclusive filters: all Windows logs except for the ones mentioned above will be saved. Syslog events will be ignored. For exclusive: all Windows logs events will be excluded. Syslog events will be stored.
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 to Investigation Database for more information.
	The **Event Fields** tab
Event ID	Enter the identifier of a specific event that you want to be save. You can add several IDs separated by comma.
Event Level	Select the event types that you want to be save. If the **Event Level** check box is cleared, all event types will be saved. **NOTE:** If you want to select the inclusive **Success Audit/Failure Audit** filters, note that on these platforms these events belong to the "Information" level, so they will not be collected if you select the **Information** checkbox in the **Exclusive Filters**.
Computer	Specify a computer (as it is displayed in the **Computer** field in the

Option	Description
	event properties). Only events from this computer will be saved. **NOTE:** If you want to specify several computers, you can define a case-sensitive mask for this parameter. Below is an example of a mask: • * - any machine • computer – a machine named 'computer' • *computer* - machines with names like 'xXxcomputerxXx' or 'newcomputer' • computer? – machines with names like 'computer1' or 'computerV' • co?puter - machines with names like 'computer' or 'coXputer' • ????? – any machine with a 5-character name • ???* - any machine with a 3-character name or longer
User	Enter a user's name. Only events created by this user will be saved. **NOTE:** If you need to specify several users, you can define a mask for this parameter in the same way as described above.
Source	Specify this parameter if you want to save events from a specific source. Input the event source as it is displayed in the **Source** field in the event properties. **NOTE:** If you need to specify several sources, you can define a mask for this parameter in the same way as described above.
Category	Specify this parameter if you want to save a specific events category.
	The **Insertion Strings** tab
Consider the following event Insertion Strings	Specify this parameter if you want to store events containing a specific string in the EventData. You can use a wildcard (*). Click **Add** and specify **Insertion String**.

10.7. Exclude Objects from Auditing Scope

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

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

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

10.7.1. Exclude Data from Active Directory Auditing Scope

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

Review the following for additional information:

- To exclude data from the Active Directory auditing scope
- To exclude read-only domain controllers from the Active Directory auditing scope

To exclude data from the Active Directory auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Active Directory Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- A wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
addprops.txt	Allows adding properties to appear in the Change Summaries for newly created AD objects. When a new object is added, Netwrix Auditor does not show any data in the **Details column** in the Change 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 change reports.
	
	This file can be used, for example, if you only want to monitor specific OU(s) inside your AD domain, but not the entire domain. In this case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, and then specify the OU(s) you want to monitor in the **allowedpathlist.txt** file.
		`Path`
		
		NOTE: The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What** column in reports.
		
		For example, to monitor only the **Users** OU in domain **CORP**, add the following line:
		
		`\local\corp\Users\*`
		
		In the omitpathlist.txt file, specify the wildcard (*)

omitallowedpathlist.txt	Contains a list of AD paths to be excluded from Change Summaries and reports. This file can be used if you want to exclude certain paths inside those specified in the allowedpathlist.txt file. In this	`Path` **NOTE:** The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What** column in reports. For example, to monitor the **Users** OU, but to exclude users **jsmith** and **pbrown**,

File	Description	Syntax

	case, put a wildcard (*) in the omitpathlist.txt file to exclude all paths, then specify the OU (s) you want to audit in the allowedpathlist.txt file, and then specify the paths you want to exclude from within them in the **omitallowedpathlist.txt** file.	do the following:
		1. Add the wildcard (*) to the **omitpathlist.txt** file.
		2. Add the following line to the **allowedpathlist.txt** file: `*\Users\*`
		3. Add the following lines to the **omitallowedpathlist.txt** file:
		`*\pbrown`
		`*\jsmith`

omitobjlist.txt	Contains a list of object types to be excluded from change reports.	`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 change reports.	`Path` **NOTE:** The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What** column in reports. 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 change reports.	`object_type.property_name` **NOTE:** If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example to exclude the **adminCount** property from reports, add the following line: `*.adminCount`.
omitreporterrors.txt	Contains a list of errors to be excluded from Change Summaries.	`Error message text` For example, if you have advanced audit

File	Description	Syntax
		settings applied to your domain controllers policy, the following error will be returned in the Change 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 Change Summary emails.
omitsnapshotpathlist.txt	Contains a list of AD paths to be excluded from AD snapshots.	`Path` **NOTE:** The path must be in the format displayed in the **Object Name** column in the Change Summary or the **What** column in reports. For example, to exclude data on the **Disabled Accounts** OU from the **Snapshot** report, add the following line: `*\Disabled Accounts*`.
omitstorelist.txt	Contains a list of object types and properties to be excluded from AD snapshots.	`object_type.property_name` **NOTE:** If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example to exclude data on the AD **adminDescription** property, add the following line: `*.adminDescription`.
processaddedprops.txt	Allows adding properties to appear in change reports (SSRS-based) for newly created AD objects. When a	`object type:property:` For example, if you want a user's **Description** property to be displayed in the reports when a user is added, add the

File	Description	Syntax
	new object is created, Netwrix Auditor does not show any data in the **Details** column in reports. If you want to see the information on certain attributes of a newly created object, specify these attributes in this file.	following line: `User:Description:`
processdeletedprops.txt	Allows adding properties to appear in change reports (SSRS-based) for deleted AD objects. When an object is deleted, Netwrix Auditor does not show any data in the **Details** column in reports. If you want to see the information on certain attributes of a deleted object, specify these attributes in this file.	`object type:property:` For example, if you want a user's **Description** property to be displayed in the reports when a user is deleted, add the following line: `User:Description:`
propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in change reports.	`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`

To exclude read-only domain controllers from the Active Directory auditing scope

NOTE: Netwrix recommends you to perform the steps below on a domain controller. If you want to do it on any other server in your domain, make sure that the **AD DS Snap-Ins and Command-Line Tools** installed on this computer.

For your convenience, the product can be configured to exclude read-only domain controllers from the Active Directory auditing scope in two ways: using Command Line or Windows PowerShell. Review the table below for more information.

Step	Command Line	Windows PowerShell

Generate a list of read-only DCs	Run command line as administrator and execute the following command:
	`dsquery * -filter "(&(objectCategory=computer)(primaryGroupId=521))" -attr dNSHostName > c:\excludeList.txt`
	where `c:\excludeList.txt` is the file where the list will be saved. You can select a custom file.
		Run **Windows PowerShell** as administrator and execute the following command:
		`Import-Module ActiveDirectory -Force`
		`Get-ADDomainController -Filter * | Where-Object {$_.IsReadOnly -eq $true} \| ForEach-Object{$_.HostName + "=skipsilent" > c:\excludeList.txt}`

Exclude read-only controllers	On the computer where Netwrix Auditor Administrator Console is installed, navigate to *%Netwrix Auditor installation folder%\Active Directory Auditing* and open the **agent.ini** file with **Notepad**.	

	Copy the DCs you want to be excluded to the configuration file using the following formatting:
	`dc2.acme.com=skipsilent`
	`dc3.acme.com=skipsilent`
		Copy the DCs you want to be excluded to the configuration file. No formatting required.

Save your changes to the **agent.ini** file.		

10.7.2. Exclude Data from Exchange Auditing Scope

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

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

To exclude data from Exchange auditing scope

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

for all classes.

- Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

aal_omitlist.txt	For Exchange 2010 and above, the file contains a list of changes performed by cmdlets. To exclude a change from reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`cmdlet.attrname`
		For example:
		`Set-User`
		`Set-ContactSet-Group`
		`#Update-AddressList`
		`Add-ADPermissionRemove-ADPermission`
		`#RBAC:`
		`*-MailboxAuditLogSearch`
		`*-AdminAuditLogSearch`

aal_propnames.txt	For Exchange 2010 and above, the file contains a list of human-readable names of changed attributes to be displayed in change reports. To exclude a change from the reports, specify name of a cmdlet and the attribute that is changed by the selected cmdlet.	`classname.attrname= intelligiblename`
		For example:
		`*- OutlookAnywhere.SSLOffloading = Allow secure channel (SSL) offloading`

omitobjlist_ecr.txt	Contains a list of human-readable names of object classes to be excluded from change reports.	`Classname`
		For example:
		`exchangeAdminService`
		`msExchMessageDeliveryConfig`
		`Exchange_DSAccessDC`

omitpathlist_ecr.txt	Contains a list of AD paths to be excluded from change reports.	`Path`
		For example:
		`*\Microsoft Exchange System Objects\SystemMailbox*`

omitproplist_ecr.txt	Contains a list of object types and properties to be	`object_type.property_name`

File	Description	Syntax

	excluded from change reports.	**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 Change 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 2013 to be excluded from data collection.	`FQDN_server_name`
		For example:
		`mailserver01.ent.local`

omitstorelist_ecr.txt	Contains a list of classes and attributes names to be excluded from Exchange snapshots.	`object_type.property_name`
		NOTE: If there is no separator (.) between an object type and a property, the whole entry is treated as an object type.
		For example:
		`Exchange_ Server.AdministrativeGroup`
		`Exchange_ Server.AdministrativeNote`
		`Exchange_Server.CreationTime`

propnames_ecr2007.txt	Contains a list of human-readable names for object	`classname.attrname= intelligiblename`

File	Description	Syntax
	classes and attributes of Exchange 2007 to be displayed in change reports.	For example: `msExchMDBAvailabilityGroup= Database Availability Group`

To exclude users or mailboxes from the Mailbox Access auditing scope

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

1. Navigate to the *%Netwrix Auditor installation folder%\Non-owner Mailbox Access Reporter for Exchange* folder.
2. Edit **mailboxestoexclude.txt**, **userstoexclude.txt**, or **agentomitusers.txt** files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - Lines that start with the # sign are treated as comments and are ignored.

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

File	Description
	affect reports and snapshots only if **Use Core Service to collect detailed audit data** is enabled.

10.7.3. Exclude Data from Exchange Online Auditing Scope

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

To exclude data from Exchange Online Auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Exchange Online Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported. You can use * for cmdlets and their parameters.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax

omitlist.txt	The file contains a list of changes performed by cmdlets. To exclude a change from reports, search results and change 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`

File	Description	Syntax

omitpathlist.txt	Contains a list of paths to be excluded from reports, search results and change summaries.	`path`
		For example:
		`SystemMailbox{*}`
		`DiscoverySearchMailbox{*}`
		`FederatedEmail.*`
		NOTE: You can use a wildcard (*) to replace any number of characters in the path.

omituserlist.txt	Contains a list of user names to be excluded from reports, search results and change summaries.	`domain\user`
		For example:
		`Enterprise\analyst`
		`email address`
		For example:
		`analyst@Enterprise.onmicrosoft.com`

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

10.7.4. Exclude Data from File Servers Auditing Scope

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

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

1. Navigate to the *%Netwrix Auditor installation folder%\File Server Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:

- Each entry must be a separate line.
- Wildcards (*, ?) are supported. For example, you can use * for a class name to specify an attribute for all classes.
- Lines that start with the # sign are treated as comments and are ignored.
- A backslash (\) must be put in front of (*), (?) and (,) if they are a part of an entry value.

File	Description	Syntax

omitcollectlist.txt	Contains a list of objects to be excluded from being audited.	`Managed Object name,server name,resource path`
		
		NOTE: Wildcards are not supported for the **Server Name** field. To disable filtering for this field, specify an empty string.
		
		For example:
		`*,,\\\\*\\System Volume Information*`

omiterrors.txt	Contains a list of errors/warnings to be omitted from logging to the Netwrix Auditor System Health event log.	`Managed Object 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 Change Summary emails. In this case audit data is still being collected.	`Managed Object name,Change Type,who changed,resource 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:
		`*,,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	`Managed Object name,Change Type,who changed,resource 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.

File	Description	Syntax
	audit data is still being collected.	For example: `*,,*,*,\\\\productionserver1.corp.local\\builds\\*,Attributes`

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

10.7.5. Exclude Data from SharePoint Auditing Scope

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

To exclude data from SharePoint auditing scope

1. Navigate to the *%ProgramData%\Netwrix Auditor\Netwrix Auditor for SharePoint\Configuration\<Managed_Object_GUID* folder.

   NOTE: If you have several Managed Objects for auditing SharePoint farms, configure omitlists for each Managed Object separately.

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

File	Description	Syntax
omitscstorelist.txt	Contains a list of site collections to be excluded from audit data collection.	`http(s)://URL` **NOTE:** Enter the root web site URLs. If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for

File	Description	Syntax
		different zones, you can use any of these URLs to specify a child site collection. For example: `https://siteColl*`

omitwastorelist.txt	Contains a list of web applications to be excluded from audit data collection.	`http(s)://URL`
		NOTE: Enter the root web site URLs. If you have alternate access mapping configured in your SharePoint farm, and one web application has different URLs for different zones, you can use any of these URLs.
		For example:
		`http://webApplication1:3333/`

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

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

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

10.7.6. Exclude Data from SQL Server Auditing Scope

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

To exclude data from the SQL Server auditing scope

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

File	Description	Syntax

omitobjlist.txt	Contains a list of object types to be excluded from Change Summaries and reports.	`object_type_name`
		For example:
		`Database`
		`Column`

omitpathlist.txt	Contains a list of resource paths to the objects to be excluded from Change Summaries and reports. In this case data is still being collected and saved to the AuditArchive.	`Server_instance:resource_path` where`resource_path` is shown in the **What** column in the reports. For example, to exclude information about databases whose names start with "tmp" on the SQL Server instance "PROD.SQL2012": `PROD.SQL2012:Databases\tmp*`.
omitproplist.txt	Contains a list of attributes to be excluded from being audited and stored to the AuditArchive.	`object_type_name.property_name.attribute_name` where: • `object_ type_ name` — Can be found in the found in the **Object Type** column in change reports. • `property_name`—Can be found in the **Details** column (property name is bold). • `attribute_name`—Can be found

File	Description	Syntax
		in the **Details** column (attribute name is not bold). If an object does not have an attribute name, use the ***** character. For example to exclude information about the **Size** attribute of the **Database File** property in all databases: `Database.Database File.Size`.
omitstorelist.txt	Contains a list of objects you want to exclude from being stored to the AuditArchive.	`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).	`server\instance name`

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

propnames.txt	Contains a list of human-readable names for object types and properties to be displayed in the change reports.	`object_type_name.property_name=friendlyname`
		For example:
		`*.Date modified=Modification Time`

10.7.7. Exclude Data from VMware Auditing Scope

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

To exclude data from VMware auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\VMware Auditing* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - A wildcard (*) is supported. For example, you can use * for a class name to specify an attribute for all classes.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
omitproplist.txt	Contains a list of object types and properties to be excluded from change reports.	`object_type.property_name` **NOTE:** If there is no separator (.) between an object type and a property, the whole entry is treated as an object type. For example, to exclude the **config.flags.monitorType** property from reports, add the following line: `*.config.flags.monitorType`.
hidepropvalues.txt	Contains a list of object types and properties to be excluded from the reports when the property is set to certain value.	`object_type.property_name=property_value:object_type.hidden_property` For example, to exclude the **config.cpuAllocation.shares.level** property when it equals to *"Low"*, add the following line: `*.config.cpuAllocation.shares.level=low:*.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`.

10.7.8. Exclude Data from Windows Server Auditing Scope

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

To exclude data from the Windows Server auditing scope

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

File	Description	Syntax

omitcollectlist.txt	Contains a list of objects and their properties to be excluded from being audited.
	
	NOTE: If you want to restart auditing these objects, remove them from the omitcollectlist.txt and run data collection at least twice.
		`Managed Object 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.	`Managed Object Name,server name,error text`
		
		For example:
		
		`*,productionserver1.corp.local,*Access is denied*`

omitreportlist.txts	Contains a list of objects to be excluded from reports and Change Summary emails. In this case audit data is still being collected.	`Managed Object name,who,where,object type,what,property name`
		
		For example:
		
		`*,CORP\\jsmith,*,*,*,*`

File	Description	Syntax

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.	`Managed Object name,who,where,object type,what,property name`
		For example:
		`*,*,*,Scheduled task,Scheduled Tasks\\User_Feed_ Synchronization*,*`

10.7.9. Exclude Data from Event Log Auditing Scope

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

To exclude data from the Event Log auditing scope

1. Navigate to the *%Netwrix Auditor installation folder%\Event Log Management* folder.
2. Edit the *.txt files, based on the following guidelines:
   - Each entry must be a separate line.
   - Wildcards (* and ?) are supported.
   - Lines that start with the # sign are treated as comments and are ignored.

File	Description	Syntax
OmitErrorsList.txt	Contains a list of data collection errors and warnings to be excluded from the Netwrix Auditor System Health event log.	`Error text`

omitServerList.txt	Contains a list of server names or servers IP addresses to be excluded from processing.	`ip address` or `server name`
		For example:
		`192.168.3.*`

10.7.10. Exclude Data from Group Policy Auditing Scope

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

To exclude data from the Group Policy Auditing scope

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

File	Description	Syntax
omitobjlist_gp.txt	The file contains a list of the Group Policy Object (GPO) names to be excluded from change reports.	`<object name>` For example, to exclude changes to the Default Domain Policy GPO, add the following line: `Default Domain Policy`.
omitproplist_gp.txt	The file contains a list of the Group Policy Object settings to be excluded from change reports.	`<settingname>` For example, to exclude data on changes made to the Maximum password length setting, add the following line: `Maximum password length`.
omituserlist_gp	The file contains a list of user names to be excluded from change reports.	`<domain\user>` For example, to exclude changes made by the user “usertest” in the domain “domaintest”, add the following line: `domaintest\usertest`.

10.7.11. Exclude Data from Inactive Users Auditing Scope

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

To exclude data from the Inactive Users auditing scope

1. Navigate to the *%ProgramData%\Netwrix Auditor\Inactive Users Tracker* folder.
2. Edit the *.txt files, based on the following guidelines:

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

File	Description	Syntax
filter.txt	Contains a list of accounts to be excluded from processing.	`Username`
omitdclist.txt	Contains a list of domain controllers to be excluded from processing. Netwrix Auditor skips all automated deactivation actions for inactive accounts (disable, move, delete) even if one domain controller is unavailable during scheduled task execution. Add the unavailable domain controllers to this file to ensure Netwrix Auditor functions properly.	`Full DNS name` or `NetBIOS name` **NOTE:** IP addresses are not supported.

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

10.7.12. Exclude Data from Logon Activity Auditing Scope

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

To exclude data from the Logon Activity auditing scope

1. Navigate to *%ProgramData%\Netwrix Auditor\NLA\Settings\<your_Managed_Object_GUID>*.

   NOTE: If you have several Managed Objects for auditing Logon Activity, configure omitlist for each Managed Object separately.

2. Edit the **Settings.cfg** file based on the following guidelines:

- Each entry must be a separate line.
- Wildcards (* and ?) are supported. A backslash (\) must be put in front of (*) and (?) if they are a part of an entry value.
- Lines that start with <!-- are treated as comments and are ignored.

Configuration String	Description	Syntax

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

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

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

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

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

Symbol	XML entity
&	**&**
e.g., Ally **&** Sons	e.g., Ally **&** Sons
"	**"**
e.g., Domain1\Users\"Stars"	e.g., Domain1\Users**"**Stars**"**
'	**'**
e.g., Domain1\Users\O'Hara	e.g., Domain1\Users\O**'**Hara
<	**<**
e.g., CompanyDC<100	e.g., CompanyDC**<**100
>	**>**
e.g., ID>500	e.g., ID**>**500

10.7.13. Exclude Data from Password Expiration Auditing Scope

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

To exclude data from the Password Expiration Alerting auditing scope

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

File	Description	Syntax

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

10.8. 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 audited systems:

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

10.8.1. Registry Keys for Auditing Active Directory

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Change 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 Change Summary footer: • 0—Display errors • 1—Do not display errors

Registry key (REG_DWORD type)	Description / Value
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 Change Summary must display the attributes whose values were modified and then restored between data collections: • 0—These attributes are not displayed • 1—These attributes are displayed as "modified and reverted back"
ShortEmailSubjects	Defines whether to contract the email subjects: • 0—No • 1—Yes
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes **NOTE:** Even if this key is set to *"0"*, the security log backups will not be deleted regardless of the value of the **CleanAutoBackupLogs** key.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter\<Managed Object Name>	
CollectLogsMaxThreads	Defines the number of Domain Controllers to simultaneously start log collection on.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Management Console\Database settings	
SqlOperationTimeout	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).
timeout	Defines the Audit Database connection timeout (in seconds).

10.8.2. Registry Keys for Auditing Exchange

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
IgnoreAuditCheckResultError	Defines whether audit check errors should be displayed in the Change 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 Change Summary footer: • 0—Display errors • 1—Do not display errors
LogonResolveOptions	Defines what will be shown in the Workstation field: • 2—MAC address • 4—FQDN or IP address (set by default) • 6—Both
ShortEmailSubjects	Defines whether to contract the email subjects (e.g., Netwrix Auditor: Change 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

Registry key (REG_DWORD type)	Description / Value
	not be deleted regardless of the value of the **CleanAutoBackupLogs** key.
ShowReportFooter	Defines whether to display the footer in the Change Summary email: • 0—No • 1—Yes
ShowReportGeneratorServer	Defines whether to display the report generation server in the Change Summary footer: • 0—No • 1—Yes
ShowSummaryInFooter	Defines whether to display the summary in the Change Summary footer: • 0—No • 1—Yes
ShowSummaryInHeader	Defines whether to display the summary in the Change Summary header: • 0—No • 1—Yes
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter\<Managed Object 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 Managed Object: • 0—No • 1—Yes

Registry key (REG_DWORD type)	Description / Value
SqlOperationTimeout	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).
timeout	Defines the Audit Database connection timeout (in seconds).

10.8.3. Registry Keys for Auditing File Servers

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

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

10.8.4. Registry Keys for Auditing Windows Server

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

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

Registry key (REG_DWORD type)	Description / Value
	• 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.

10.8.5. Registry Keys for Auditing Event Log

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager\<Managed Object Name>\Database Settings	
ConnectionTimeout	Defines SQL database connection timeout (in seconds).
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager\<Managed Object Name>\ElmDbOptions	
BatchTimeOut	Defines batch writing timeout (in seconds).
DeadLockErrorCount	Defines the number of write attempts to a SQL database.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Netwrix Auditor\Event Log Manager	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
ProcessBackupLogs	Defines whether to process security log backups: • 0—No • 1—Yes

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.
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

10.8.6. Registry Keys for Auditing Group Policy

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter	
CleanAutoBackupLogs	Defines the retention period for the security log backups: • 0—Backups are never deleted from Domain controllers • [X]— Backups are deleted after [X] hours
GPOBackup	Defines whether to backup GPOs during data collection: • 0—No • 1—Yes
GPOBackupDays	Defines the backup frequency: • 0—Backup always • X—Once in X days **NOTE:** GPOBackup must be set to *"1"*.

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

Registry key (REG_DWORD type)	Description / Value
	• 0—No • 1—Yes
ShowSummaryInFooter	Defines whether to display the summary in the Change Summary footer: • 0—No • 1—Yes
ShowSummaryInHeader	Defines whether to display the summary in the Change Summary header: • 0—No • 1—Yes
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\AD Change Reporter\<Managed Object Name>	
CollectLogsMaxThreads	Defines the number of Domain Controllers to simultaneously start log collection on.
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\ AD Change Reporter\<Managed Object Name>\Database settings	
SessionImportDays	Defines the frequency of a full snapshot upload: • X—Once in X days
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Management Console\Database settings	
overwrite_datasource	Defines whether to overwrite the database connection settings (stored in the reports data source) if they differ from the SQL server settings specified when configuring the Managed Object: • 0—No • 1—Yes
SqlOperationTimeout	Defines the timeout for executing SQL queries such as data selection, insertion or deletion (in seconds).
timeout	Defines the Audit Database connection timeout (in seconds).

10.8.7. Registry Keys for Auditing Password Expiration

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

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

10.8.8. Registry Keys for Auditing Inactive Users

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

Registry key (REG_DWORD type)	Description / Value
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netwrix Auditor\Inactive Users Tracker	
HideEmailAdditionalInfo	Defines whether to show or hide the header and footer in emails sent to managers (emails sent to administrators always have default header and footer): • 0—Show • Any other number—Hide
RandomPasswordLength	Defines the length of a random password to be set for inactive user.
WriteEventLog	Defines whether to write events to the Application Log: • 0—No • 1—Yes

10.8.9. Registry Keys for Auditing Logon Activity

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

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

10.9. Enable Integration with Third-Party SIEM Solutions

If your organization is already using a third-party Security Information and Event Management (SIEM) solution, Netwrix Auditor can help protect these investments by integrating with major SIEM systems. Netwrix Auditor allows you to manage audit data in your usual way, but with improved performance and increased reliability of the collected audit data.

When auditing Active Directory, Exchange, File Servers, and Group Policy, Netwrix Auditor can integrate with all major SIEM solutions, including:

- Microsoft System Center Operations Manager (SCOM) 2007 R2 and 2012
- RSA enVision®
- Arc-Sight® Logger™
- Novell® Sentinel™
- NetIQ® Security Manager™
- IBM Tivoli® Security Information
- Event Manager™
- and many others.

When integration with SIEM products is enabled, a custom Windows event log called **Netwrix Auditor** is created. This event log will generate events for each detected change. You can configure custom processing rules, alerts and reports in your SIEM solution to track these events.

10.9.1. Enable Integration

1. In Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name**. Depending on the audited system you want to integrate with SIEM solution, select a corresponding node: **Active Directory**, **Exchange**, **File Servers** or **Group Policy**.
2. In the right pane, select **Configure** next to **Advanced Options/Advanced Settings**.
3. In the **Advanced Options** dialog that opens, select **Third-party SIEM products** to integrate the product with a SIEM solution.
4. Customize your solution to use the **Netwrix Auditor** event log and create rules to trigger alerts on certain events. Review the Netwrix event types and their structure below.

10.9.2. Netwrix Audit Events

Property	Audit event
Source	• Netwrix Auditor for Active Directory—Corresponds to auditing Active Directory and Group Policy. • Netwrix Auditor for Exchange—Corresponds to auditing Exchange. • Netwrix Auditor for File Servers—Corresponds to auditing file servers.
Category	Audit (id=1)
Level	Success Audit / Failure Audit
ID	1001 – 1008

To review event properties

1. On the computer where Netwrix Auditor Administrator Console is installed, navigate to **Start** → **Administrative Tools** → **Event Viewer**.
2. In the right pane, locate the **Netwrix Auditor** event log and double-click it.
3. Double-click an event.
4. In the **Event Properties** dialog, select one of the following tabs:
   - The **Event Properties General** tab shows the event description in the upper grid and the general properties information below the grid.
   - The **Details** tab shows the event details.

The table below provides a description of the audit events sorted by their ID.

ID	Name	Description	Change type string in description	Change detail string in description	Applies to the following audited systems:
1001	Add	Object added	Added	—	• Active Directory • Exchange • File Servers • Group Policy
1002	Remove	Object removed	Removed	—	• Active Directory • Exchange • File Servers • Group Policy
1003	Modify	Single-valued string was modified. Empty values reported as empty quoted strings in description templates	Modified	<attribute > changed from "<old value>" to "<new value>"	• Active Directory • Exchange • File Servers • Group Policy
1004	Modify by Events	Information extracted from Windows Event Log. (e.g., user account enabled/disabled, account locked/unlocked)	Modified	<attribute >	• Active Directory • Exchange
1005	Value Added	Value was added to the multi- valued attribute (e. g., a new member was added to a group)	Modified	<attribute>: Added: "<new value>"	• Active Directory • Exchange • File Servers
1006	Value Removed	Value was removed from the multi-valued attribute, (e. g., a member was removed from a group)	Modified	<attribute >: Removed: "<old value>"	• Active Directory • Exchange • File servers
1007	Modified and	Attribute was modified and then rolled back to	Modified	<attribute >: Modified and	• Active Directory • Exchange

ID	Name	Description	Change type string in description	Change detail string in description	Applies to the following audited systems:
	Reverted Back	its previous value. Intermediate values are unknown.		Reverted back	
1008	Access	Access to file system objects (e.g., successful or failure file reads; failure attempts to access a folder or share)	Read	—	• File Servers

NOTE: (when auditing Group Policy) The Add/Remove events (Event ID 1001 or 1002) are generated only when a Group Policy object is added or removed. Changes to policy settings are always displayed as the Modified event (ID 1003).

The table below provides a description of the insertion strings that are displayed in the **Details** tab of the **Event Properties** dialog:

String	Generic content	Active Directory	Exchange	Group Policy	File Servers
1	Managed Object	Domain	Domain	Domain	Computer Collection
2	When detected (local)	-//-	-//-	-//-	-//-
3	When detected (UTC)	-//-	-//-	-//-	-//-
4	When changed (local)	-//-	-//-	-//-	-//-
5	When changed (UTC)	-//-	-//-	-//-	-//-
6	The name of the user who	-//-	-//-	-//-	-//-

String	Generic content	Active Directory	Exchange	Group Policy	File Servers
	made the change (DOMAIN\user)				
7	Object type	AD object type (computer/ user/ group, etc.)	AD object type (computer/user/group, etc.)	"Policy"	File / folder / share
8	Object path	AD path: *\local\amdom\ Users\testUser1*	AD path: *\local\amdom\ Users\testUser1*	*\zone\domain\ GPO Display Name\Path*	*\\server\ share\ folder\file*
9	The name of the server where Netwrix Auditor is installed	-//-	-//-	-//-	-//-
10	The server where the change was made (DC, file server, etc.)	-//-	-//-	-//-	-//-
11	Custom field	Depends on type. The Active Directory specific events have the following custom field values: • Distribution Domain Local Group • Distribution Global Group • Distribution	Schema-based name, e.g., msExchExchangeServer	GPO Display Name	n/a

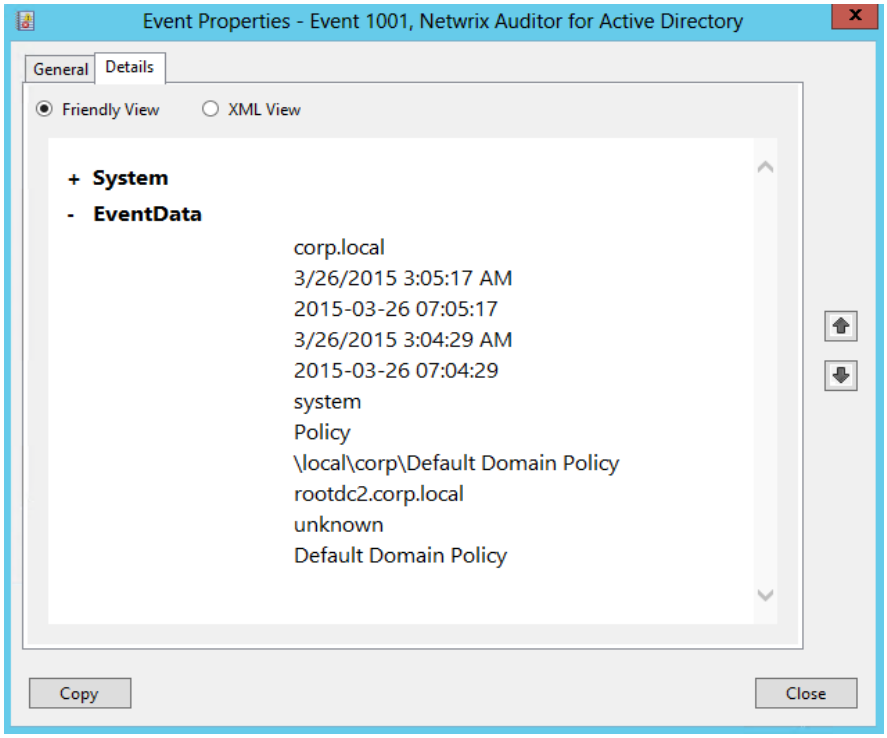
String	Generic content	Active Directory	Exchange	Group Policy	File Servers
		Universal Group • Security Domain Local Group • Security Global Group • Universal Security Group			
12	Internal name of the attribute that was changed	-//-	-//-	GPO setting attribute name (currently is equivalent to [13])	-//-
13	Display name of the attribute that was changed	-//-	-//-	Friendly attribute name (GPO setting attribute name)	n/a
14	The previous value of the attribute (or removed values if a multi-valued attribute). Can be empty.	-//-	-//-	-//-	-//-
15	The current value of the attribute (or added values	-//-	-//-	-//-	-//-

String	Generic content	Active Directory	Exchange	Group Policy	File Servers
	if a multi-valued attribute). Can be empty.				
16	Object GUID	AD object GUID	AD object GUID	Group Policy object GUID	n/a
17	Custom field	n/a	n/a	Group Policy Change Type: 1 - policy added, 2 - policy removed, 3- policy modified	n/a

NOTE:

- Local time is written in the default locale format (for example 03/16/2011 6:37:43 PM)
- UTC value is written the SQL date format (MM-DD-YYYY hh:mm:ss)

Review the event example:



10.10. 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 Administrator Console) or its IP address.
   - `user_name`—Replace with a Netwrix Auditor user who wants to log in.

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

   ```
   "C:\Program Files (x86)\Netwrix Auditor\Audit Intelligence\Audit
   Intelligence.exe" /s:host.corp.local /u:corp\analyst /specify_creds
   ```

5. Click **Apply**.

You can create as many shortcuts with different parameters as needed. When you click the shortcut, the product will start with pre-populated connection details.

10.11. Customize Branding

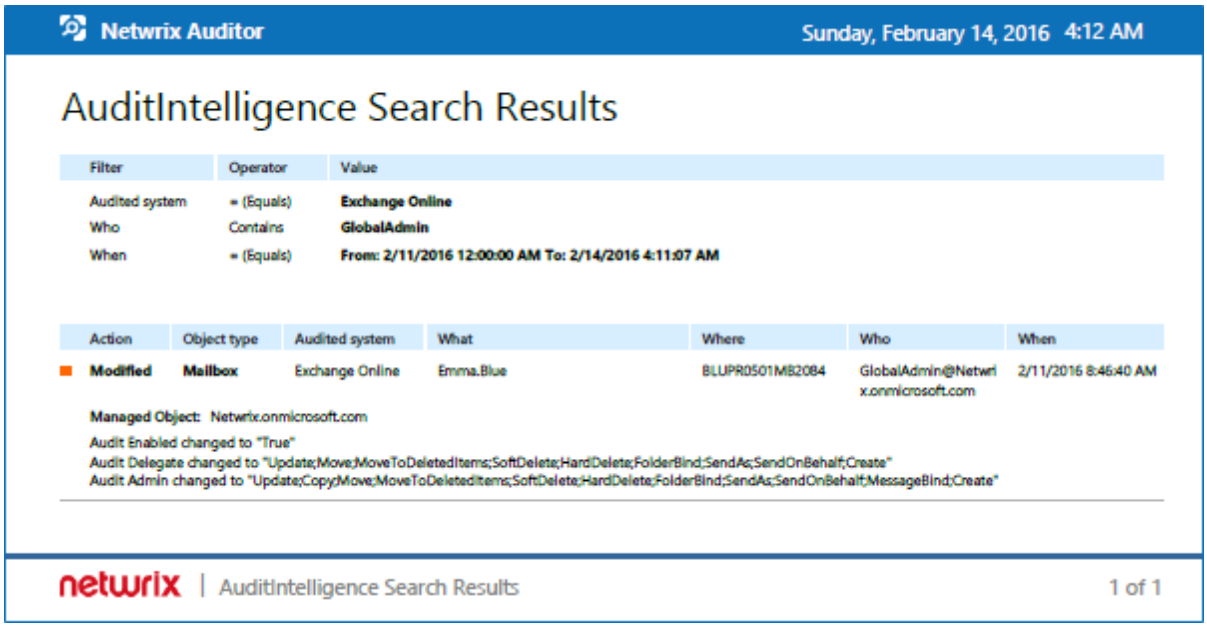
Netwrix Auditor allows customizing look and feel of your reports and exported search results—you can skip Netwrix logo, add your company logo and title. Nonetheless, users are not empowered to customize layout or color scheme.

Review the following for additional information:

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

10.11.1. Customize Branding in Exported Search Results

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



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

To customize branding

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

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

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

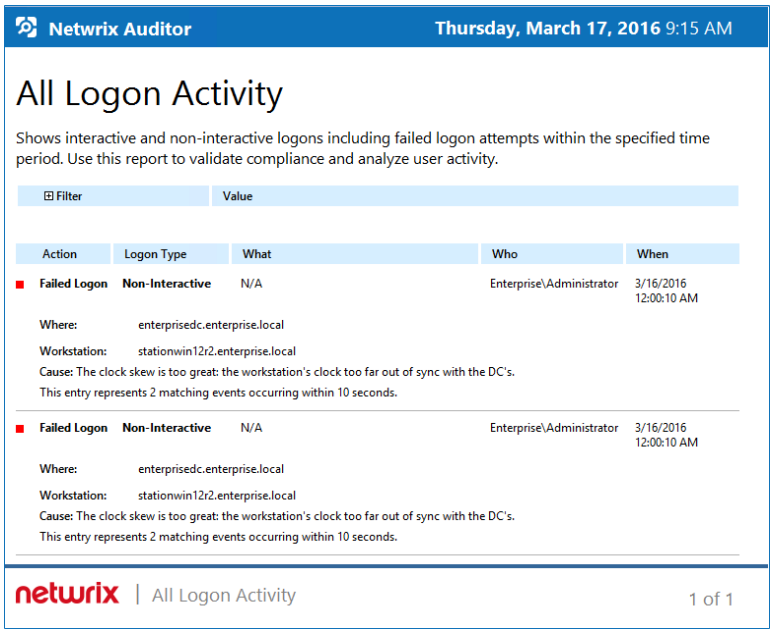
To..	Do..
Enable branding	In the "enabled" section, replace "False" with "True".
Add your company name in the header	In the "header_title" section, type your company name instead of "Replace with your company title". In this case "Netwrix Auditor" will no longer appear in pdf output.
Add your company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

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

Symbol	XML entity
& e.g., Ally **&** Sons	**&** e.g., Ally **&** Sons
" e.g., Domain1\Users\"Stars"	**"** e.g., Domain1\Users**"**Stars**"**
' e.g., Domain1\Users\O'Hara	**'** e.g., Domain1\Users\O**'**Hara
< e.g., CompanyDC<100	**<** e.g., CompanyDC**<**100
> e.g., ID>500	**>** e.g., ID**>**500

10.11.2. 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

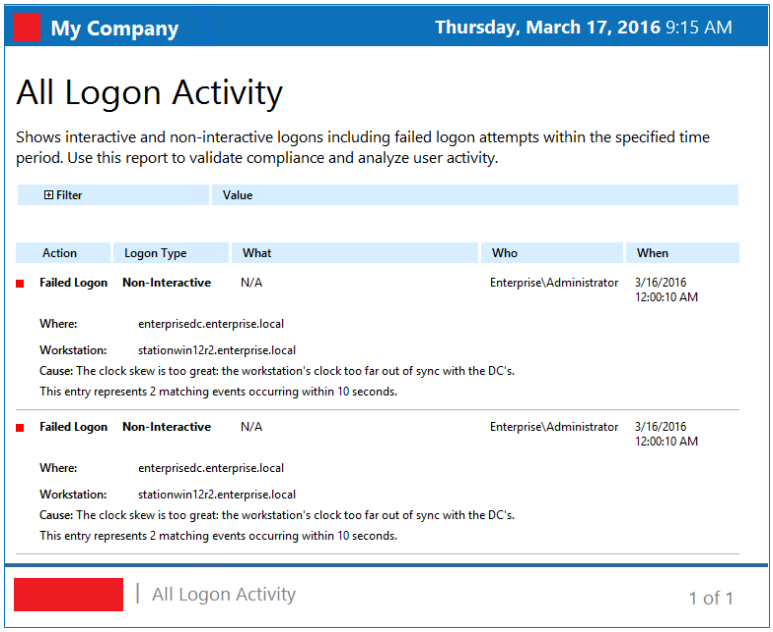
1. Navigate to the script location.
2. Right-click a script and select **Edit**. **Windows PowerShell ISE** will start.
3. Review the script and provide parameters.

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.

Parameter	Description
	By default, local unnamed instance is selected.
DBName	By default, the database responsible for Netwrix Auditor look and feel is **Netwrix_CommonDB**. If you renamed this database, provide a new name.
HeaderImageFullPath	Defines a full path to the png image with the new report header (product logo). Supported size: 21x21px (WxH).
FooterImageFullPath	Defines a full path to the png image with the new report footer (logo). Supported size: 105x22px (WxH).
HeaderText	Defines text in the report header. Max length: 21 characters.
FooterURL	Defines URL that opens on clicking the report logo in the footer.

4. Click (**Run Script**). The user who runs the script is granted the **db_owner** role on the **Netwrix_CommonDB** database.

After running the script, start the Netwrix Auditor client and generate a report. The branding will be updated.



To restore original look and feel

1. Navigate to the script location.
2. Right-click a script and select **Edit**. **Windows PowerShell ISE** will start.

3. Run the script as it is. The user who runs the script must be granted the **db_owner** role on the **Common_DB** database in a local unnamed SQL Server configured as default for Netwrix Auditor.

11. Appendix

11.1. Audited Object Types and Components

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

- Object Types and Attributes Audited in Active Directory
- Object Types and Attributes Audited on File Servers
- Object Types and Attributes Audited on SharePoint
- Object and Data Types Audited on SQL Server
- Object Types and Attributes Audited on VMware
- Components and Settings Audited on Windows Server
- Actions Captured When Auditing Mailbox Access

11.1.1. Object Types and Attributes Audited in Active Directory

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

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

NOTE: Review the following limitations:

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

11.1.2. Object Types and Attributes Audited on File Servers

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

NOTE: For the attributes marked with asterisk (*) *who* and *when* changed are not reported.

Object type	Attributes
File	• Attributes • Security • Size • Date Created • Date Modified
Folder	• Security • Attributes • Date Created • Date Modified
Share	• Share Permissions* • User Limit* • Local Path* • Root Folder Security

11.1.3. Object Types and Attributes Audited on SharePoint

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

NOTE: The attributes marked with * are reported without details, only the fact of change is reported.

The changes to object types marked with ** are reported with the "Not applicable" value in the "Who" and "Workstation" columns.

The changes to object types and attributes marked with *** are reported with the "Not applicable" value in the "Workstation" column.

Read access is reported with the "Not applicable" value in the "Workstation" column.

Object type	Attributes
Group***	• Membership
Permission Level***	• Permissions
Site	• Site URL • Permissions*** • Permission Inheritance***
List	• Permissions*** • Permission Inheritance***
List Item	• Attachments • Permissions*** • Permission Inheritance*** • List Item Properties*
Document	• Document URL • Permissions*** • Permission Inheritance*** • Document Properties* • Content Modifications*
Farm**	• Configuration Database • Configuration Database Server • Version • Managed Account for "Web Application Pool - {name}" • Managed Account for "Service Application Pool - {name}" • Managed Account for "Windows Service - {name}" • Managed Account for "Farm Account" • Managed Accounts
Web Application **	• Web Application URL • Name

Object type	Attributes
	• Port • User Permissions • Alternate Access Mappings • Content Database • Blocked File Extensions
Site Collection**	• Site Collection URL • Content Database • Content Database Server • Site Storage Maximum Limit • Site Storage Warning Limit • Sandboxed Solutions Resource Maximum Quota • Sandboxed Solutions Resource Warning Quota • Quota Template • Lock Status
Server**	• Name
Service**	• Name • Status
Permission Policy Level**	• Name • Grant Permissions • Deny Permissions • Site Collection Permissions
User Policy**	• Display Name • Permissions
Anonymous Policy**	• Zone • Permissions
Farm Solution**	• Name • Status

Object type	Attributes
	• Last Operation Time
Farm Feature**	• Name • Status

11.1.4. Object and Data Types Audited on SQL Server

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

- Audited Object Types
- Audited Data Types

11.1.4.1. Audited Object Types

Object type	Attributes
Application Role	• Date Created • Date Modified • Default Schema • Extended Properties • Id • Name • Owned Schemas
Backup	• Backup name • Description • Device name • logical_device_name • Size • Type
Column	• Allow nulls • ANSI Padding Status • Collation

Object type	Attributes
	• Computed Text • Default Constraint • Full Text • ID • Identity • Identity increment • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale • Primary Key • Rule • Rule Schema • System Type • XML Schema Namespace
Constraints	• Date Created • Date Modified • Definition • ID • Is system named • MS shipped • Name • Published • Schema published
Credential	• Id

Object type	Attributes
	• Identity • Date Created • Date Modified • Name
Database	• Compatibility • Database Size • Database Space Available • Date Created • Date Modified • Extended Properties • File Id • File Group • File Name • Growth • Id • Name • Options • Owner • Permissions • Size • Usage
Database Role	• Date Created • Date Modified • Extended Properties • Id • Name • Owner • Owned Schemas

Object type	Attributes
	• Role Members
Functions	• Date Created • Date Modified • Id • Name • Permissions • Type
Jobs	• Automatically delete job • Category • Date Created • Date Modified • Description • Email notification • Email operator • Enabled • ID • Name • Net send notification • Net send operator • Owner • Page notification • Page operator • Schedules • Write to the Windows Application event log
Job Steps	• ID • Name • On Failure • On Success

Object type	Attributes
	• Output file • Process exit code of a successful command • Retry attempts • Retry interval (minutes) • Step • Type
Jobs Schedules	• Date Created • Date Modified • Enabled • ID • Name • Owner • Schedule Type • Settings
Indexes	• Allow page locks • Name • Primary key • Ignore duplicate values • Unique constraint • Allow row locks • Type • Disabled • Included Columns • Fill factor • Data Space ID • Index Key Columns • Padded • Hypothetical

Object type	Attributes
	• Unique
Keys	• Name • ID • Date Created • Date Modified • MS shipped • Published • Schema published • Disabled • Not for replication • Not trusted • Delete referential action • Update referential action • Is system named
Login	• Date Created • Date Modified • Default Database • Default Language • Disabled • Enforce Password Expiration • Enforce Password Policy • Id • Name • Password Hash • Server Roles
Restore	• Type
Schema	• Date Created

Object type	Attributes
	• Date Modified • Extended Properties • Id • Name • Owner • Permissions
Server Instance	• Ad Hoc Distributed Queries • Affinity I/O Mask • Affinity Mask • Agent XPs • Allow Updates • Awe Enabled • Blocked Process Threshold • C2 Audit Mode • Clr Enabled • Collation • Cost Threshold For Parallelism • Cross Db Ownership Chaining • Cursor Threshold • Database Mail XPs • Date Modified • Default Full-text Language • Default Language • Default Trace Enabled • Disallow Results From Triggers • Fill Factor (%) • Ft Crawl Bandwidth (max) • Ft Crawl Bandwidth (min)

Object type	Attributes
	• Ft Notify Bandwidth (max) • Ft Notify Bandwidth (min) • Id • In-doubt Xact Resolution • Index Create Memory (K) • Lightweight Pooling • Locks • Max Degree Of Parallelism • Max Full-text Crawl Range • Max Server Memory (M) • Max Text Repl Size (B) • Max Worker Threads • Media Retention • Min Memory Per Query (K) • Min Server Memory (M) • Name • Nested Triggers • Network Packet Size (B) • Ole Automation Procedures • Open Objects • Permissions • PH Timeout (s) • Precompute Rank • Priority Boost • Query Wait (s) • Query Governor Cost Limit • Recovery Interval (min) • Remote Admin Connections

Object type	Attributes
	• Remote Login Timeout (s) • Remote Proc Trans • Remote Query Timeout (s) • Remote Access • Replication XPs • Scan For Startup Procs • Server Trigger Recursion • Set Working Set Size • Show Advanced Options • SMO And DMO XPs • SQL Mail XPs • Status • Transform Noise Words • Two Digit Year Cutoff • User Connections • User Instances Enabled • User Instance Timeout • User Options • Web Assistant Procedures • Xp_cmdshell
Server Role	• Date Created • Date Modified • Id • Name • Role Members
Stored Procedure	• ANSI NULLs • Date Created • Date Modified

Object type	Attributes
	• Encrypted • Execute us • FOR replication • Id • Name • Permissions • Quoted Identifier • Recompile • Schema
Table	• ANSI NULLs • Date Created • Date Modified • Filegroup • Id • Name • Partition scheme • Permissions • Schema • Table is partitioned • Table is replicated • Text filegroup
Triggers	**NOTE:** Only DML table triggers are supported. • Date Created • Date Modified • Disabled • ID • Instead of trigger • MS shipped

Object type	Attributes
	• Name • Not for replication
User	• Date Created • Date Modified • Default Schema • Extended Properties • Id • Name • Owned Schemas • Roles
View	• ANSI NULLs • Date Created • Date Modified • Encrypted • Id • Name • Permissions • Quoted Identifier • Schema • Schema bound
View Column	• Allow nulls • ANSI Padding Status • Collation • Computed Text • Default Constraint • Full Text • ID • Identity

Object type	Attributes
	• Identity increment • Identity seed • Is Computed • Length • Name • Not for replication • Numeric precision • Numeric scale • Rule • Rule Schema • System Type • XML Schema Namespace • XML Schema Namespace schema
View Index	• Allow Page Locks • Allow Row Locks • ID • Data Space ID • Disabled • Fill Factor • Hypothetical • Ignore Dup Key • Name • Padindex • Primary Key • Schema Name • Type • Unique • Unique Constraint

Object type	Attributes
	• View Name
View Index Column	• Column ID • ID • Included Column • Index ID • Key Ordinal • Name • Partition Ordinal • Schema Name • Sort Order • View Name

11.1.4.2. Audited Data Types

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

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

11.1.5. Object Types and Attributes Audited on VMware

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

Object type	Attributes
Virtual Machine	• Snapshot Name • Snapshot Description • Current Snapshot • Power State • Guest State • Virtual Machine Name • Guest OS • Guest OS Version • Memory Size (M) • Power Off Type • Suspend Type • Run VMware Tools Scripts After Powering On • Run VMware Tools Scripts After Resuming • Run VMware Tools Scripts Before Powering Off • Run VMware Tools Scripts Before Suspending • Guest Power Management • Disable Acceleration • Enable Logging • Record Debugging Information • Synchronize guest time with host • Check and upgrade Tools • Hyper-threaded Core Sharing • Swap file Location • Hardware Page Table Virtualization • Force BIOS Setup • Power-on Boot Delay • Power On • Advanced Configuration

Object type	Attributes
	• Number of virtual processors • Operation mode of guest OS • Notes • Annotation • ResourcePool • Template • Connected • Connect at power on • VirtualCdrom Device Type • VirtualCdrom Mode • VirtualParallelPort Port • VirtualParallelPort Connection • VirtualSerialPort Connection • VirtualSerialPort Yield CPU on poll • VirtualSerialPort Near End • VirtualSerialPort Far End • VirtualPCNet32 MAC Address Type • VirtualPCNet32 MAC Address • VirtualPCNet32 Wake on LAN • VirtualPCNet32 IP Address • VirtualPCNet32 Network Adapter Name • VirtualPCNet32 Network Adapter Network • VirtualPCNet32 Network Adapter MAC • VirtualFloppy Device Type • VirtualSCSIController Controller Type • VirtualSCSIController Bus Sharing • VirtualSCSIController Bus Number • VirtualDisr Disk Mode

Object type	Attributes
	• VirtualDisr Unit Number • VirtualDisr Capacity(K) • VirtualDisr Share Level • VirtualDisr Datastore
Authorization Manager	• Privilege • Authorization Manager Name
Cluster Resource	• Name • VMware HA • VMware DRS • VMware HA Admission Control • VMware HA Isolation Response • VMware HA Restart Priority • VMware HA Number of host failures allowed • VMware HA Advanced Option • VMware DRS Automation Level • VMware DRS Migration threshold • Swap Policy for Virtual Machines • VMware HA Isolation Response • VMware HA Restart Priority • VMware DRS Power Management • VMware DRS 'Keep Virtual Machines Together' Rule Name • VMware DRS 'Keep Virtual Machines Together' Rule Enabled • VMware DRS 'Keep Virtual Machines Together' Rule Status • VMware DRS 'Keep Virtual Machines Together' Rule Virtual Machine • VMware DRS 'Separate Virtual Machines' Rule Name • VMware DRS 'Separate Virtual Machines' Rule Enabled • VMware DRS 'Separate Virtual Machines' Rule Status • VMware DRS 'Separate Virtual Machines' Rule Virtual Machine

Object type	Attributes
	• VMware DRS Virtual Machine Automation Mode • Available CPU • Available Memory • Available Hosts
Computer Resource	• Name
Datacenter	• Name
Data Store	• Accessible • Name
Folder	• Folder Name
Host System	• Overall Status • Configuration Status • CPU Expandable Reservation • CPU Limit • CPU Reservation • CPU Shares Level • CPU Shares • Memory Expandable Reservation • Memory Limit • Memory Reservation • Memory Shares Level • Memory Shares • Datastore accessible to Host • NTP required • NTP uninstallable • NTP running • NTP policy

Object type	Attributes
	• NTP Servers • Port Group Allow Promiscuous • Port Group MAC Address Changes • Port Group Forged Transmits • Port Group VLAN ID • Port Group Attached uplink adapter • Virtual Switch Allow Promiscuous • Virtual Switch MAC Address Changes • Virtual Switch Forged Transmits • Virtual Switch Number of Ports • Virtual Switch Attached uplink adapter • VMkernel IP Address of port • Service Console IP Address of port
Resource Pool	• Name

11.1.6. Components and Settings Audited on Windows Server

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

- General Computer Settings
- Add / Remove Programs
- Services
- Hardware
- Scheduled Tasks
- Local Users and Groups
- DNS Configuration**
- DNS Resource Records**
- Windows Registry Settings

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

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

Object type	Attributes
General Computer Settings	
Computer Name	• Computer Description • Name • Domain
Environment Variables	• Type • Value
General	• Caption • Organization • Registered User • Serial Number • Service Pack* • Version*
Remote	• Enable Remote Desktop on this computer
Startup and Recovery	• Automatically Restart • Dump File • Dump Type • Overwrite any existing file • Send Alert • System Startup Delay • Write an Event
Add / Remove Programs	
Add or Remove Programs	• Installed For* • Version
Services	
System	• Action in case of failed service startup

Object type	Attributes
Service	• Allow service to interact with desktop • Caption • Created • Deleted • Description Name • Path to executable • Service Account • Service Type • Start Mode
	Hardware
Base Board*	• Hosting Board • Status • Manufacturer • Product • Version • Serial Number
BIOS*	• Manufacturer • Version
Bus*	• Bus Type • Status
Cache Memory*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Purpose • Status
CD-ROM Drive*	• Configuration Manager Error Code • Last Error Description

Object type	Attributes
	• Last Error Code • Media Type • Name • SCSI Bus • SCSI Logical Unit • SCSI Port • SCSI Target ID • Status
Disk Partition*	• Primary Partition • Size (bytes) • Starting offset (bytes)
Display Adapter*	• Adapter RAM (bytes) • Adapter Type • Bits/Pixel • Configuration Manager Error Code • Driver Version • Installed Drivers • Last Error Description • Last Error Code • Refresh Rate • Resolution • Status
DMA*	• Status
Floppy Drive*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status

Object type	Attributes
Hard Drive*	• Bytes/Sector • Configuration Manager Error Code • Interface Type • Last Error Description • Last Error Code • Media Loaded • Media Type • Model • Partitions • SCSI Bus • SCSI Logical Unit • SCSI Port • SCSI Target ID • Sectors/Track • Size (bytes) • Status • Total Cylinders • Total Heads • Total Sectors • Total Tracks • Tracks/Cylinder
IDE*	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Status
Infrared*	• Configuration Manager Error Code • Last Error Description

Object type	Attributes
	• Last Error Code • Status
Keyboard*	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Layout • Name • Status
Logical Disk*	• Description • File System • Size (bytes) • Status
Monitor*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Monitor Type • Status
Network Adapter	• Adapter Type • Configuration Manager Error Code • Default IP Gateway • DHCP Enabled • DHCP Server • DNS Server Search Order • IP Address • Last Error Description • Last Error Code

Object type	Attributes
	• MAC Address • Network Connection Name • Network Connection Status • Service Name • Status
Network Protocol*	• Description • Status
Parallel Ports*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
PCMCIA Controller*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
Physical Memory*	• Capacity (bytes) • Status • Manufacturer • Memory Type • Speed • Part Number • Serial Number
Pointing Device*	• Configuration Manager Error Code • Double Click Threshold • Handedness • Hardware Type • Last Error Description

Object type	Attributes
	• Last Error Code • Number of buttons • Status
Printing	• Comment* • Hidden* • Local* • Location* • Name* • Network* • Port Name* • Printer error information • Published* • Shared* • Share Name* • Status
Processor*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Max Clock Speed (MHz) • Name • Status
SCSI*	• Configuration Manager Error Code • Description • Last Error Description • Last Error Code • Status
Serial Ports*	• Configuration Manager Error Code

Object type	Attributes
	• Last Error Description • Last Error Code • Maximum Bits/Second • Name • Status
Sound Device*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Status
System Driver	• Description • Error Control • Start Mode • Service Type
System Slot*	• Slot Designation • Status
USB Controller*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Name • Status
USB Hub*	• Configuration Manager Error Code • Last Error Description • Last Error Code • Name • Status
	Scheduled Tasks
Scheduled	• Account Name

Object type	Attributes
Task	• Application • Comment • Creator • Enabled • Parameters • Triggers
Local Users and Groups	
Local Group	• Description • Name • Members
Local User	• Description • Disabled/Enabled • Full Name • Name • User cannot change password • Password Never Expires • User must change password at next logon
DNS Configuration**	
DNS Server**	• Address Answer Limit • Allow Update • Auto Cache Update • Auto Config File Zones • Bind Secondaries • Boot Method • Default Aging State • Default No Refresh Interval • Default Refresh Interval

Object type	Attributes
	• Disable Auto Reverse Zones • Disjoint Nets • Ds Available • Ds Polling Interval • Ds Tombstone Interval • EDns Cache Timeout • Enable Directory Partitions • Enable Dns Sec • Enable EDns Probes • Enable Netmask Ordering • Event Log Level • Fail On Load If Bad Zone Data • Forward Delegations • Forwarders • Forwarding Timeout • Is Slave • Listen Addresses • Log File Max Size • Log File Path • Log Level • Loose Wildcarding • Max Cache TTL • Max Negative Cache TTL • Name Check Flag • No Recursion • Recursion Retry • Recursion Timeout • Round Robin

Object type	Attributes
	• Rpc Protocol • Scavenging Interval • Secure Cache Against Pollution • Send Port • Server Addresses
DNS Zone**	• Aging State • Allow update • Auto created • Data file name • Ds integrated • Expires after • Forwarder slave • Forwarder timeout • Master servers • Minimum TTL • No refresh interval • Notify • Notify servers • Owner name • Paused • Primary server • Refresh interval • Responsible person • Retry interval • Reverse • Scavenge servers • Secondary servers • Secure secondaries

Object type	Attributes
	• Shutdown • TTL • User NB stat • Use WINS • Zone type
	DNS Resource Records**
DNS AAAA**	• Container name • IPv6 Address • Owner name • Record class • TTL • Zone type
DNS AFSDB**	• Container name • Owner name • Server name • Server subtype • Record class • TTL • Zone type
DNS ATM A**	• ATM Address • Container name • Format • Owner name • Record class • TTL • Value • Zone type

Object type	Attributes
DNS A**	• Container name • IP Address • Owner name • Record class • TTL • Zone type
DNS CNAME**	• Container name • FQDN for target host • Owner name • Record class • TTL • Zone type
DNS DHCID**	• Container name • DHCID (base 64) • Owner name • Record class • TTL • Zone type
DNS DNAME**	• Container name • FQDN for target domain • Owner name • Record class • TTL • Zone type
DNS DNSKEY**	• Algorithm • Container name • Key type

Object type	Attributes
	• Key (base 64) • Name type • Owner name • Protocol • Record class • Signatory field • TTL • Zone type
DNS DS**	• Algorithm • Container name • Data • DigestType • Key tag • Owner name • Record class • TTL • Zone type
DNS HINFO**	• Container name • CPU type • Operating system • Owner name • Record class • TTL • Zone type
DNS ISDN**	• Container name • ISDN phone number and DDI • ISDN subaddress • Owner name

Object type	Attributes
	• Record class • TTL • Zone type
DNS KEY**	• Algorithm • Container name • Key type • Key (base 64) • Name type • Owner name • Protocol • Record class • Signatory field • TTL • Zone type
DNS MB**	• Container name • Mailbox host • Owner name • Record class • TTL • Zone type
DNS MD**	• Container name • MD host • Owner name • Record class • TTL • Zone type
DNS MF**	• Container name

Object type	Attributes
	• MF host • Owner name • Record class • TTL • Zone type
DNS MG**	• Container name • Member mailbox • Owner name • Record class • TTL • Zone type
DNS MINFO**	• Container name • Error mailbox • Owner name • Responsible mailbox • Record class • TTL • Zone type
DNS MR**	• Container name • Owner name • Replacement mailbox • Record class • TTL • Zone type
DNS MX**	• Container name • FQDN of mail server • Mail server priority

Object type	Attributes
	• Owner name • Record class • TTL • Zone type
DNS NAPTR**	• Container name • Flag string • Order • Owner name • Preference • Record class • Regular expression string • Replacement domain • Service string • TTL • Zone type
DNS NS**	• Container name • Name servers • Owner name • TTL
DNS NXT**	• Container name • Next domain name • Owner name • Record class • Record types • TTL • Zone type
DNS PTR**	• Container name

Object type	Attributes
	• Owner name • PTR domain name • Record class • TTL • Zone type
DNS RP**	• Container name • Mailbox of responsible person • Optional associated text (TXT) record • Owner name • Record class • TTL • Zone type
DNS RRSIG**	• Algorithm • Container name • Key tag • Labels • Original TTL • Owner name • Record class • Signature expiration (GMT) • Signature inception (GMT) • Signature (base 64) • Signer's name • TTL • Type covered • Zone type
DNS RT**	• Container name • Intermediate host

Object type	Attributes
	• Owner name • Preference • Record class • TTL • Zone type
DNS SIG**	• Algorithm • Container name • Key tag • Labels • Original TTL • Owner name • Record class • Signature expiration (GMT) • Signature inception (GMT) • Signature (base 64) • Signer's name • TTL • Type covered • Zone type
DNS SRV**	• Container name • Host offering this service • Owner name • Port number • Priority • Record class • TTL • Weight • Zone type

Object type	Attributes
DNS TEXT**	• Container name • Owner name • Record class • Text • TTL • Zone type
DNS WINS**	• Cache time-out • Container name • Do not replicate this record • Lookup time-out • Owner name • Record class • Wins servers • Zone type
DNS WKS**	• Container name • IP address • Owner name • Protocol • Record class • Services • TTL • Zone type
DNS X25**	• Container name • Owner name • Record • Record class • TTL • X.121 PSDN address

Object type	Attributes
	• Zone type
	Windows Registry Settings
OS Security	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\FileSystem(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\NetworkProvider (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\Print\\Providers\\LanMan Print Services(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\SecurePipeServers (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\Environment(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\SubSystems(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\Memory Management(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\Executive(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\KnownDLLs(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Control\\Windows(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Image File ExecutionOptions(|\\.*)
Security Settings	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\DrWatson (|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Driver Signing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Non-Driver Signing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\MSDTC (|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\NetDDE (|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Microsoft\\Windows\\CurrentVersion\\Policies\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Explorer\\BitBucket(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Group Policy(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Installer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Policies\\System(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\policies\\Network(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\policies\\Ratings(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\policies\\system(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\AEDebug(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\AsrCommands(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Perflib(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\SeCEdit(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Setup\\RecoveryConsole(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)

Object type	Attributes
	\\Policies\\Microsoft\\PCHealth\\ErrorReporting(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Conferencing(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\EventViewer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Messenger\\Client(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\SearchCompanion(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\SystemCertificates\\AuthRoot(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\W32time\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\DCOM(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\IIS(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\Printers(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\Rpc(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows\\DriverSearching(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows\\Group Policy(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows\\Installer(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows\\Internet Connection Wizard(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows\\Network Connections(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Windows\\Registration Wizard Control(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\Peernet(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Policies\\Microsoft\\WindowsFirewall\\ StandardProfile\\IcmpSettings(|\\.*) • HKEY_LOCAL_MACHINE\\System\\Clone(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\Control\\SessionManager(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\WinLogon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\CrashControl (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\FileSystem(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\LSA(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Print\\Providers\\LanManPrint Services\\Servers(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\ProductOptions (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SecurePipeServers\\WinReg(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Control\\SessionManager\\kernel(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\WMI\\Security (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Enum(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Hardware Profiles(|\\.*) • HKEY_USERS\\.DEFAULT\\Software\\ Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer(|\\.*) • HKEY_USERS\\.Default\\Software\\Microsoft\\NetDDE(|\\.*) • HKEY_USERS\\.Default\\Software\\Microsoft\\ SystemCertificates\\Root\\ProtectedRoots(|\\.*)
Patches	• HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\

Object type	Attributes
	Component Based Servicing\\Packages(|\\.*)
Windows Firewall	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\WindowsFirewall\\DomainProfile(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\WindowsFirewall\\StandardProfile(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\cryptography(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\windows\\safer\\codeidentifiers(|\\.*)
Remote Desktop	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Control\\Terminal Server\\WinStations\\RDP-Tcp(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|)\\Policies\\Microsoft\\Windows NT\\Terminal Services(|\\.*)
File Sharing Settings	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\LanmanServer\\Shares(|\\.*)
USB Devices	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\USBSTOR(|\\.*)
Important Services	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Schedule(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WebClient(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WmiApSrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\upnphost(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AFD(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Alerter(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgmt(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\AppMgr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Appmon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\BINLSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\ \Services\\Browser(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Cdrom(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\CiSvc(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Clipsrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\Eventlog\\Application(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\Security (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Eventlog\\System (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Fax(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\HTTPFilter(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\IISADMIN(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\IPSEC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\LanManServer\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9] +\\Services\\LanmanWorkstation\\Parameters(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\LicenseService (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSDTC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MSFtpsvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacFile(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MacPrint(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Messenger(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\MrxSmb(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NTDS(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\NWCWorkstation (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NetBT(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netlogon(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Netman(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NntpSvc(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\NtFrs(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\POP3Svc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RDSessMgr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasAuto(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RasMan(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteAccess (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RemoteRegistry (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Remote_Storage_ Server(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\Services\\Remote_Storage_ User_Link(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\RpcLocator(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SMTPSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMPTRAP(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SNMP(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SharedAccess (|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Spooler(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\SrvcSurg(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TapiSrv(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\Tcpip(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TermService(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\TlntSvr(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\W3SVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\WZCSVC(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\helpsvc(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\ldap(|\\.*) • HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\mnmsrvc(|\\.*)

Object type	Attributes
	• HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet[0-9]+\\ Services\\tftpd(|\\.*)
Startup and autorun	• HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows NT\\CurrentVersion\\IniFileMapping(|\\.*) • HKEY_LOCAL_MACHINE\\SOFTWARE(\\WOW6432NODE|) \\Microsoft\\Windows\\CurrentVersion\\Run(|\\.*)
All other settings	• All keys from HKLM\Software, HKLM\System, HKU\Default that are not covered by the masks of other categories

11.1.7. Actions Captured When Auditing Mailbox Access

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

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

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

11.2. Install ADSI Edit

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

domain controller in the domain you want to start auditing.

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

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

To install ADSI Edit on Windows Server 2012 and above

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

To install ADSI Edit on Windows 7

1. Download and install Remote Server Administration Tools that include ADSI Edit.
2. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **OK**.

To install ADSI Edit on Windows 8 and above

1. Download and install Remote Server Administration Tools.
2. Navigate to **Start** → **Control Panel** → **Programs** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **OK**.

To install GPMC on Windows 8.1

1. Download and install **Remote Server Administrator Tools** that include Group Policy Management Console.
2. Navigate to **Start** → **Control Panel** → **Programs and Features** → **Turn Windows features on or off**.
3. Navigate to **Remote Server Administration Tools** → **Role Administration Tools** and select **AD DS and AD LDS Tools**.
4. Click **OK**.

11.3. Install Microsoft SQL Server

This section provides instructions on how to:

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

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

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

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

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

11.3.1. Install Microsoft SQL Server 2014 Express

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

1. Download SQL Server 2014.
2. Run the installation package and follow the instructions of the wizard until you get to the **Feature Selection** page. On this page, ensure that the **Reporting Services** option is selected under **Instance Features**.
3. Proceed with the wizard until you get to the **Server Configuration** page. On this page, ensure that

the **SQL Server Reporting Services** will run under the **Network Service account**, and its startup type is set to *"Automatic"*.

4. Follow the instructions of the wizard to complete the installation.

11.3.2. Verify Reporting Services Installation

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

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

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

Index