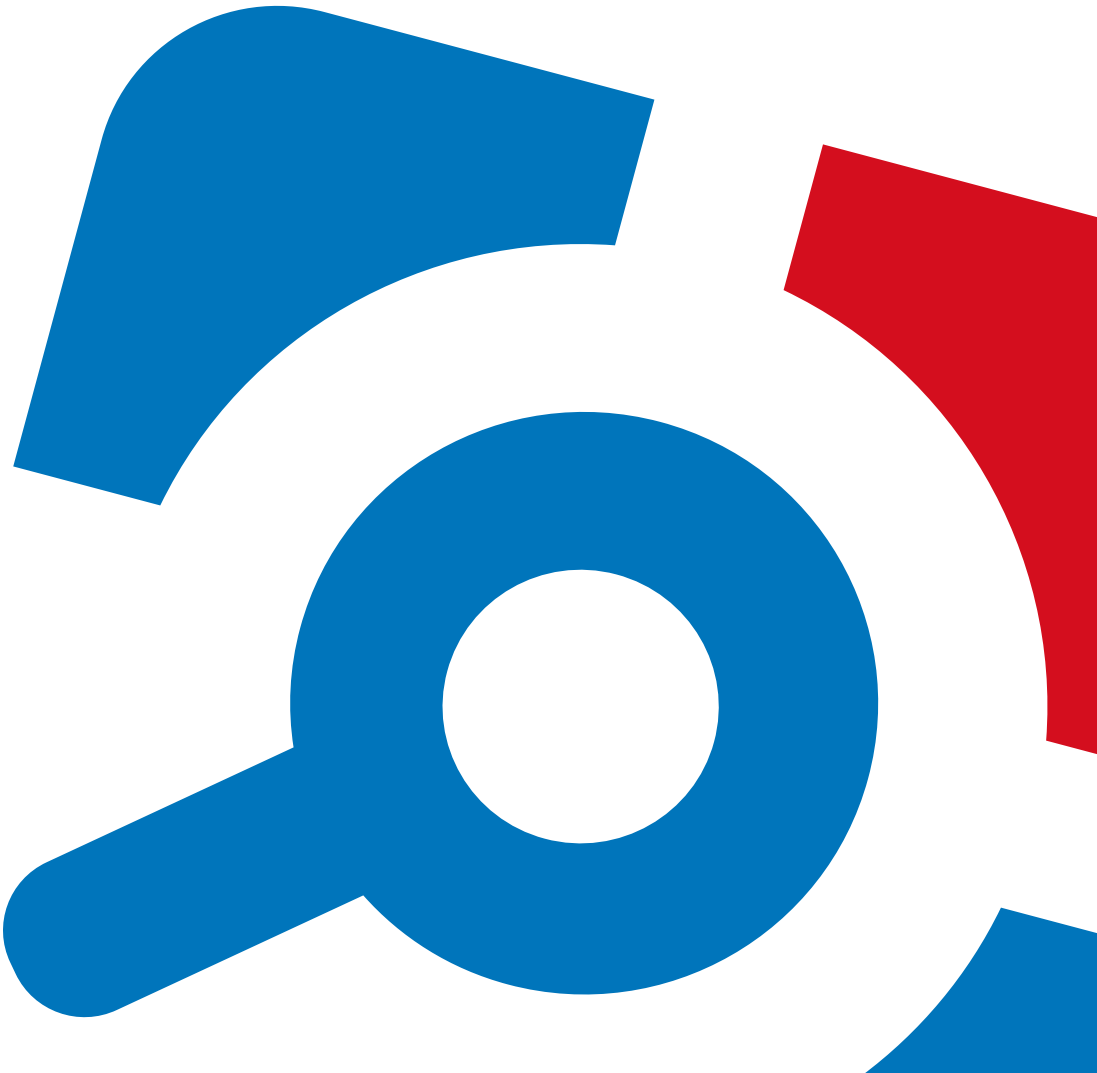
netwrix

Netwrix Auditor

Intelligence Guide

Version: 9.0
4/28/2017



Legal Notice

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

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

Disclaimers

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

Table of Contents

1. Introduction

This guide describes Intelligence features that help enable complete visibility in your environment. The guide is intended for Netwrix Auditor users (both Reviewers and Global administrators) who want to take advantage of searching and filtering of audit data in the easy-to-use searching interface, generating system-specific and overview reports, etc.

After reading this guide you will be able to:

- Investigate incidents and browse your audit data with Google-like interactive search
- Generate reports and add filters
- Subscribe to important reports you want to receive on a regular basis
- Create alerts to stay notified on actions critical to your organization security

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

1.1. Netwrix Auditor Overview

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

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

Major benefits:

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

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

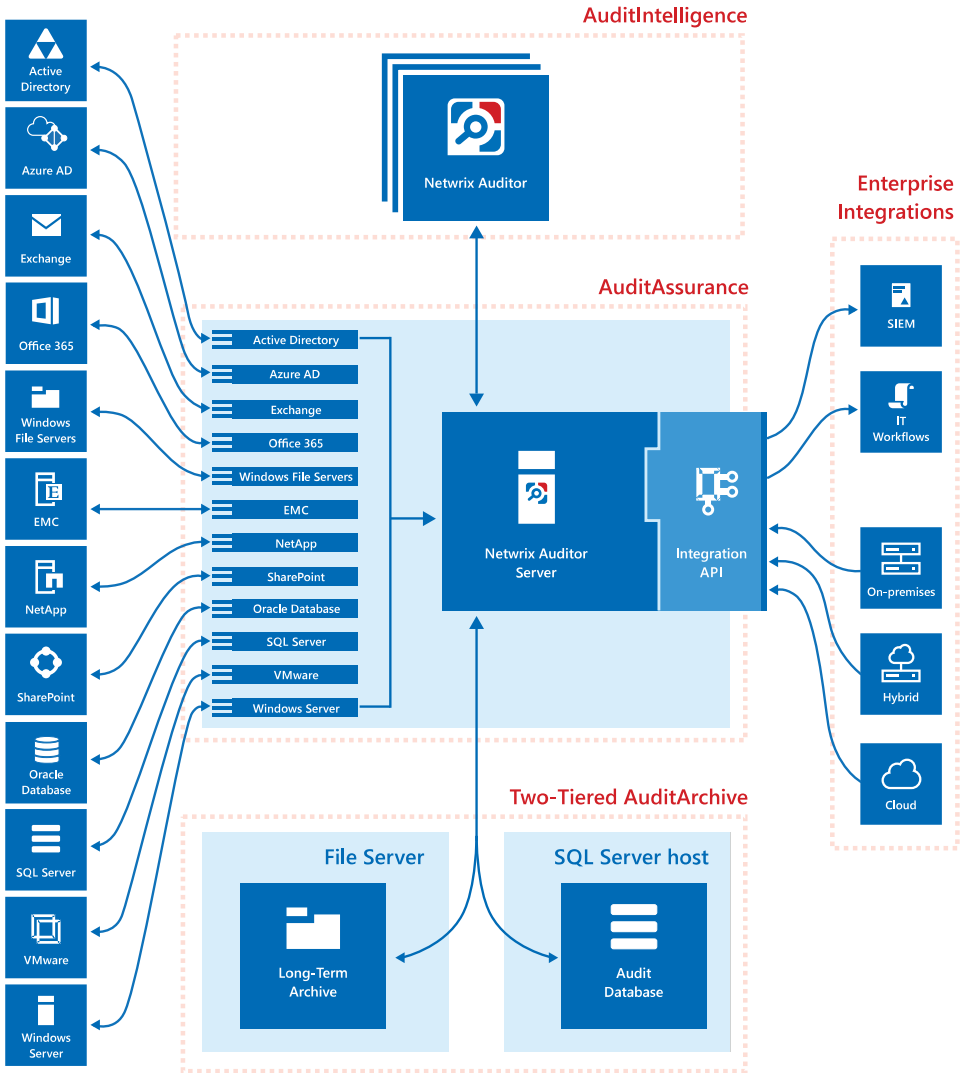
Application	Features
Netwrix Auditor for Active Directory	Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It

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

Application	Features
	attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for Oracle Database	Netwrix Auditor for Oracle Database detects and reports on all changes made to your Oracle Database instance configuration, privileges and security settings, including database objects and directories, user accounts, audit policies, sensitive data, and triggers. The product also reports on failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on read access and changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration, database content, and logon activity.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows–based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. With a stand-alone Event Log Manager tool, Netwrix Auditor collects Windows event logs from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log data. In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

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



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

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

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

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

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

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

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

1.3. Product Editions

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

Netwrix Auditor Standard Edition can be evaluated for 20 days. During this period you have free, unlimited access to all features and functions. After the evaluation license expires, the product will prompt you to supply a commercial license. Alternatively, you can switch to Free Community Edition.

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

When running Free Community Edition, at any time you can upgrade to Standard Edition, simply by supplying a commercial license in **Settings** → **Licenses**.

Refer to a table below to compare product editions.

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

Feature	Free Community Edition	Standard Edition
Support plan	Forum support only	Full
Automatic audit configuration	+	+
Data sources		
Active Directory (including Group Policy and Logon Activity)	One domain	Unlimited
Azure AD	One Office 365 tenant	Unlimited
Exchange	One domain	Unlimited
EMC	One server or one file share, or one IP range, or one OU	Unlimited
NetApp	One server or one file share, or one IP range, or one OU	Unlimited
Windows File Servers	One server or one file share, or one IP range, or one OU	Unlimited
Office 365 (including Exchange Online, SharePoint Online, and OneDrive for Business)	One Office 365 tenant	Unlimited
Oracle Database	One Oracle Database instance	Unlimited
SharePoint	One SharePoint farm	Unlimited
SQL Server	One SQL Server instance	Unlimited
VMware	One VMware Virtual Center	Unlimited
Windows Server	One server or IP range or one Active Directory container	Unlimited
Netwrix Auditor tools		
Netwrix Auditor Object Restore for Active Directory	–	+

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

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

2. Launch the Product

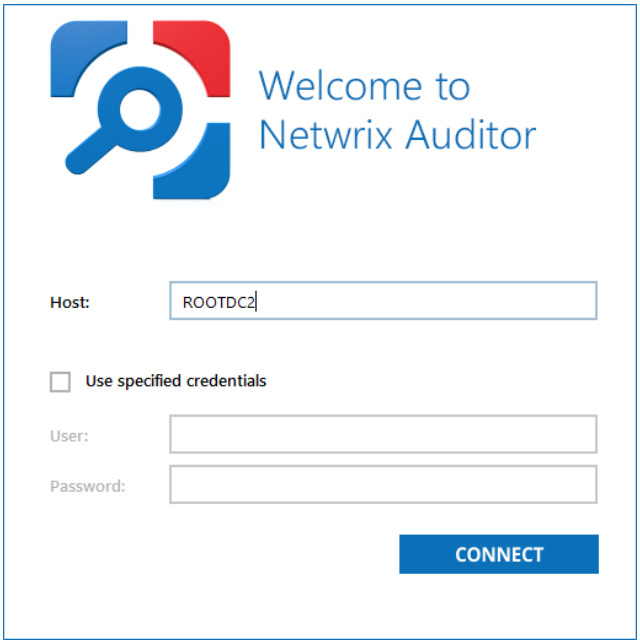
To start using Netwrix Auditor

1. Navigate to **Start** → **Netwrix Auditor**.
2. Log into the product.

   NOTE: This step is required if Netwrix Auditor is installed remotely (not on computer that hosts Netwrix Auditor Server).

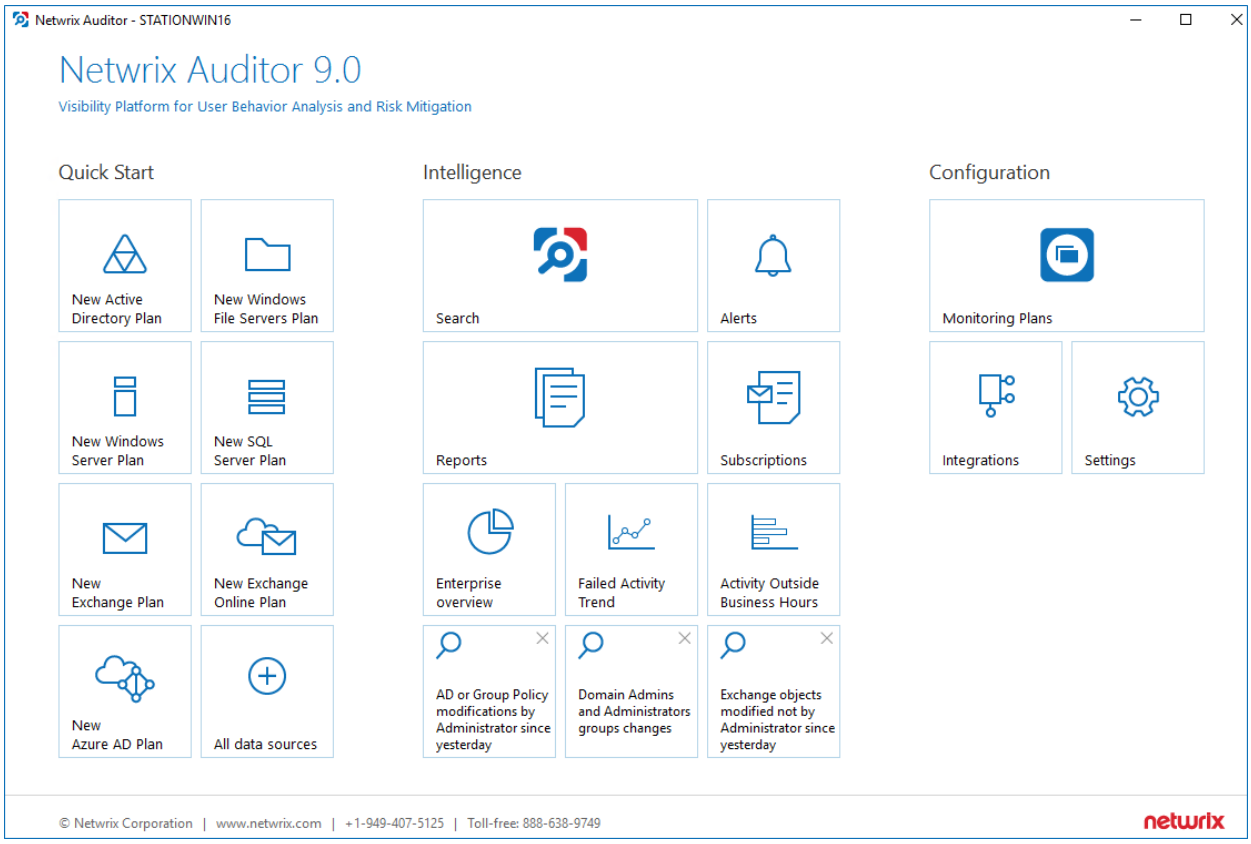
   You can configure a single Netwrix Auditor client to work with several Netwrix Auditor Servers. To switch to another server, reopen the Netwrix Auditor client and provide another host name (e.g., rootdc2, WKSWin12r2.enterprise.local).

   For your convenience, the **Host** field is prepopulated with your computer name. By default, you can log in with your Windows credentials by simply clicking **Connect**. Select **Use specified credentials** if you want to log in as another user.

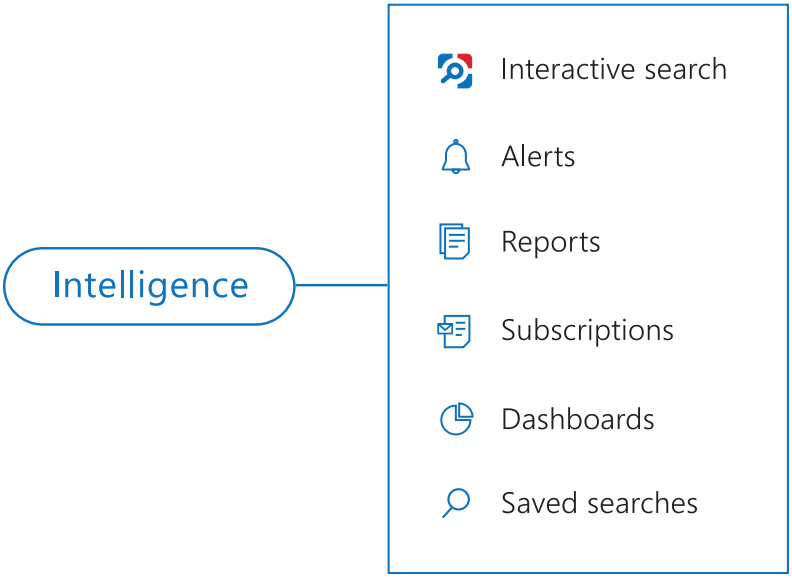


   NOTE: Make sure you have sufficient permissions to access the product. If you cannot log into Netwrix Auditor with your Windows credentials, contact your Netwrix Auditor administrator.

After logging into Netwrix Auditor, you will see the following window:



Take a closer look at the **Intelligence** section. It contains everything you need to enable complete visibility in your environment.



Review the following for additional information:

- Interactive Search
- Alerts
- Reports and Report Packs

- Subscriptions
- Overview Dashboards
- Saved Searches

3. Interactive Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient interactive search interface enables you to investigate incidents and browse data collected across the entire IT infrastructure. When running a search, you are not limited to a certain data source, change type, or object name. You can create flexible searches that provide you with precise results on *who* changed *what*, and *when* and *where* each change was made.

NOTE: To review intelligence data, you must be assigned the Global administrator or Global reviewer role in the product. The users assigned the Reviewer role on a certain plan or folder have a limited access to data—only within a delegated scope. See Netwrix Auditor Administration Guide for more information.

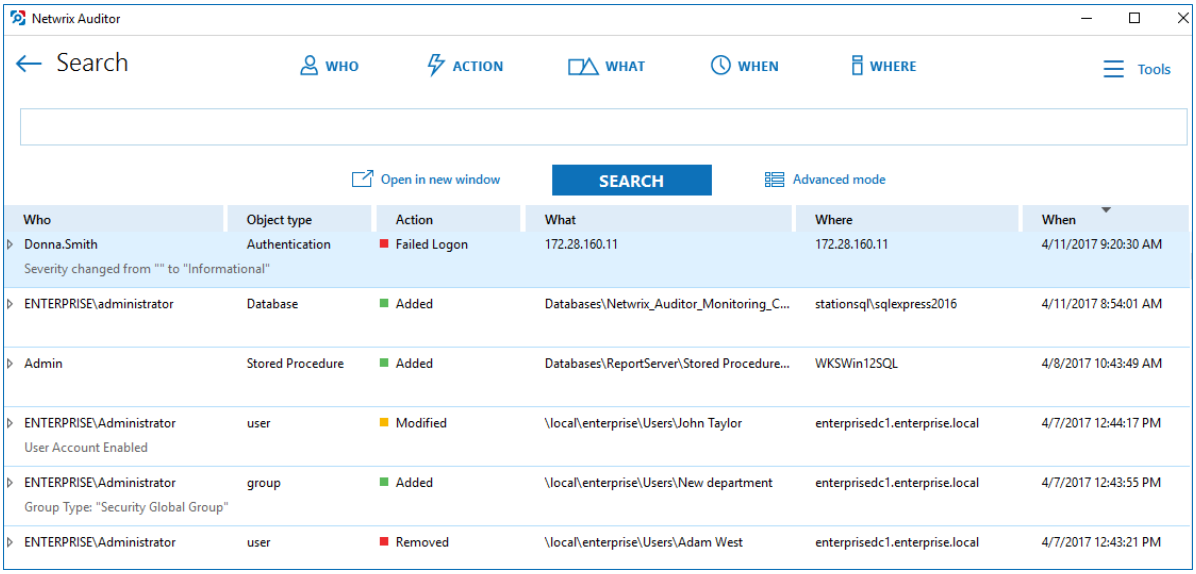
This functionality is currently available for the following data sources:

- Active Directory
- Azure AD
- Exchange
- Exchange Online
- File Servers (Windows File Servers, EMC, and NetApp)
- Oracle Database
- SharePoint
- SharePoint Online
- SQL Server
- VMware
- Windows Server
- Group Policy
- Logon Activity
- User Activity (Video)
- and Netwrix API—data imported to the Audit Database from other sources using Netwrix Auditor Integration API

NOTE: Netwrix Auditor shows only the top 2,000 entries in the search results.

To browse your audit data

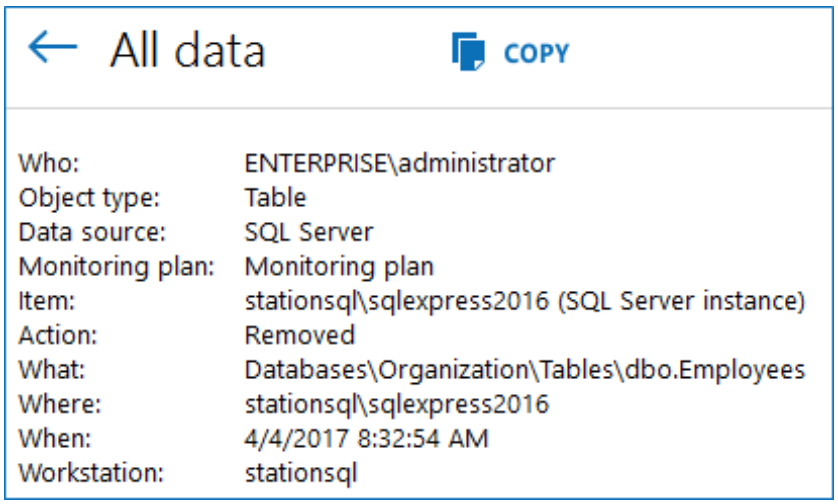
1. On the main Netwrix Auditor page, navigate to **Search**.
2. Do one of the following:
   - Click **Search** to see all audit data stored in the Audit Database. Once the data is retrieved, you can exclude certain entries from the results. See Include and Exclude Data for more information.



   - Add filters to the **Search** field before you click **Search**. In this case, only data matching your search criteria will be displayed. See Apply Filters for more information.

3. Review the search results and see details for each particular change or watch a video recording.
   - Click on a column to sort results by this column (e.g., by date or by account name).
   - Double-click an entry to see details specific to this change (the before and after values, the start and end date, etc.). Click **Read more...** to see all information regarding this change and copy it if necessary. In case of User Activity entries, click the **Show video...** link below the entry. Review

details and play a video by clicking **Show Video**.



NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Netwrix Auditor Global administrator to import that data from the Long-Term Archive.

4. Save or share the search results if desired. See Save Your Search and Share Results for more information.
5. By default, each search opens in the same window and overwrites the previous search results. Click **Open in new window** to compare several searches.

3.1. Apply Filters

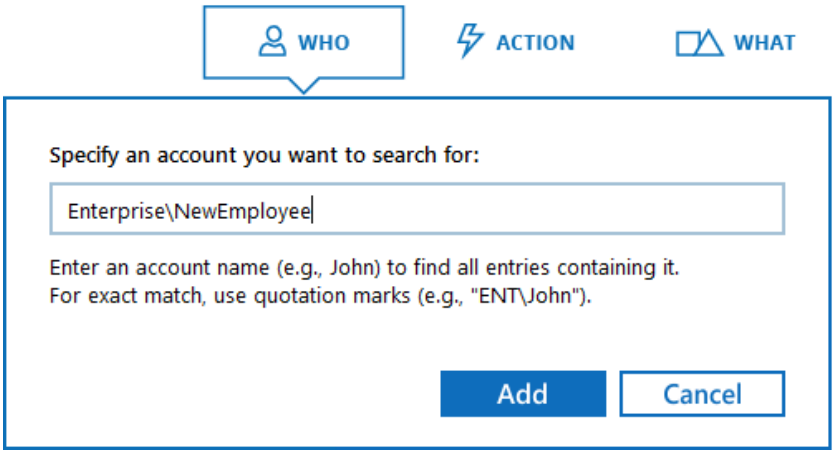
Filters are used to narrow your search results. To create a unique set of filters, you can:

- Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., **Who***: Administrator* AND **Action***: Added*).
- Specify several values in the same filter to search for any of them (e.g., **Action***: Modified* OR **Action***: Removed*). To do this, select a filter again and specify a new value.

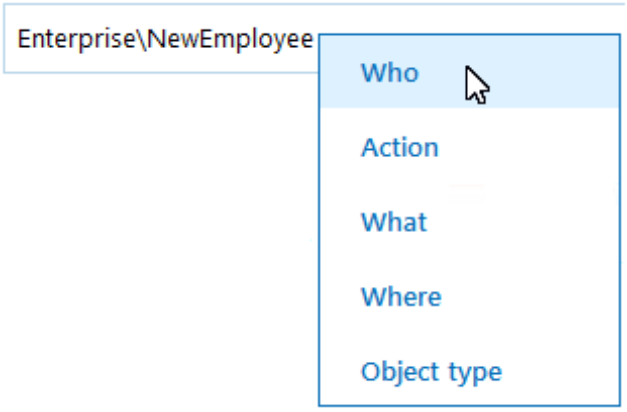
NOTE: Spaces do not separate values, so the whole expression will be included in your search as a single value. For example, if you want to search for any of three names, do not enter *Anna Mark Bill* but instead create a separate filter entry for each name.

To add a filter to your search

1. Click a filter icon and provide a value you want to search for.



Alternatively, you can type a value directly into the **Search** field. To further restrict your search, right-click the value and select a filter from the pop-up menu. You can also leave it as it is to search across all columns (everywhere—**Who**, **What**, **Where**, **Action**, etc.) except those for which filters are explicitly specified.



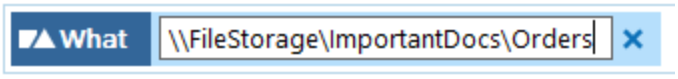
2. Click **Search** to apply your filters. By default, all entries that contain the filter value are shown. For an exact match, use quotation marks. See Apply Additional Filters for more information on additional filters and match types.

Filter	Description
 WHO	Specify an account name (e.g., *John*) to find all entries containing it (e.g., *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*, *John@domain.com*). For an exact match, use quotation marks and provide a user name in Domain\User or UPN format (e.g., *"Domain1\John"* or *"John@domain.com"*) .

Filter	Description
 ACTION	Select an action type from the list (Added, Removed, Modified, Read). For additional actions, navigate to **Advanced mode**. See Apply Additional Filters for more information.
 WHAT	Specify an object name (e.g., *Policy*) to find all entries containing it (e.g., *HiSecPolicy*, *\\FileSserver\Share\NewFolder\NewPolicy.docx* , *http://sharepoint/sites/collection1/Lists/Policy*). **NOTE:** Netwrix Auditor searches across all data sources. For an exact match, use quotation marks and provide an object name in the format that is typical for your data source (e.g., "*HiSecPolicy*").
 WHEN	Specify a timeframe or provide a custom date range. Netwrix Auditor allows you to see changes that occurred today, yesterday, in the last 7 or 30 days, or within the specified date range.
 WHERE	Specify a resource name (e.g., *Enterprise*) to find all entries containing it (e.g., *Enterprise-SQL*, *FileStorage.enterprise.local*). The resource name can be a FQDN or NETBIOS server name, Active Directory domain or container, SQL Server instance, SharePoint farm, VMware host, etc. **NOTE:** Netwrix Auditor searches across all data sources. For an exact match, use quotation marks and provide a resource name in the format that is typical for your data source (e.g., *"Enterprise-SQL"*).

To modify a filter value

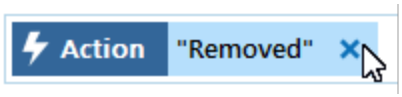
- Double-click it and type a new value.



NOTE: The **When** filter cannot be modified in the Search field. Delete it and add a new value, or navigate to the **Advanced** mode to edit it.

To remove a filter

- Click the **Close** icon next to the filter.



3.2. Advanced Mode

Netwrix Auditor provides an advanced set of filters and match type operators that enable you to customize your searches even more precisely.

Switch to **Advanced mode** to review your current search in details and modify it if necessary. Click Add to add a new filter to your search.

Review the following for additional information:

- Apply Additional Filters
- Change Match Types

3.2.1. Apply Additional Filters

Expand the **Filter** list to find additional filters or filter values. The most commonly used filters are described in Apply Filters. Review the following for additional information:

Filter	Description	Example
Action	Limits your search to the selected actions only. Specify an action from the **Value** list or type it yourself. The **Action** filter in the **Advanced mode** contains actions besides those available in basic mode (added, modified, removed, and read). Reported actions vary depending on the data source and object type. See Netwrix Auditor Administration Guide for more information. • Added • Add (Failed Attempt) • Removed • Remove (Failed Attempt)	You are investigating suspicious user activity. You have already identified the intruder and now you want to see if any files were deleted or moved, and emails sent. Since you are interested in specific actions only, set the **Action** filter to **Removed**, **Moved**, and **Sent**.

Filter	Description	Example
	• Modified • Read • Moved • Renamed • Checked in • Discard check out • Failed Logon • Copied • Activated • Modify (Failed Attempt) • Read (Failed Attempt) • Move (Failed Attempt) • Rename (Failed Attempt) • Checked out • Successful Logon • Logoff • Sent	
Object type	Limits your search to objects of a specific type only. Specify an object type from the **Value** list or type it yourself. This filter modifies the **What** filter. The value list is prepopulated with the most frequent object types.	You noticed that some domain policies were changed and you want to investigate this issue. Your **What** filter is set to *Policy*, and so you keep receiving search results such as *HiSecPolicy*, *\\FS\Share\NewPolicy.docx* , *http://corp/sites/col1/Lists/Policy*. These entries correspond to different object types and data sources. Since you are looking for GPOs only, select **GroupPolicy** from the **Value** list.
Data source	Limits your search to the selected data source only. Specify a data source from the **Value** list or type it yourself.	You are investigating suspicious user activity. A user specified in the **Who** filter made a lot of changes across your IT infrastructure, so the search results became difficult to review. Since you are only interested in the way this user's activity could affect your Active Directory domain and Exchange organization, set the **Data source** filter to **Active Directory** and **Exchange** to limit

Filter	Description	Example
		the search results.
Monitoring plan	Limits your search to the selected plan only. Specify the name from the **Value** list or type it yourself.	You are investigating suspicious user activity. A user specified in the **Who** filter made a lot of changes across your IT infrastructure, so the search results became difficult to review. Since you are only interested in the way this user's activity could affect file shares audited within a single plan, set the **Monitoring plan** filter to *"My servers"* to limit the search results.
Item	Limits your search to the selected item only. This filter can be helpful if have several items of the same type in your monitoring plan (e.g., two Active Directory domains). Specify the name from the **Value** list or type it yourself.	Your monitoring plan is configured to track domains and includes your secured corporate domain and a domain for temporary employees. You are investigating who logged in your secured corporate domain outside business hours. You can set the **Item** filter to this domain name to limit the search results and exclude logons to computers from a less important domain.
Details	Limits your search results to entries that contain the specified information in the **Details** column. The **Details** column normally contains data specific to your target, e.g., assigned permissions, before and after values, start and end dates. This filter can be helpful when you are looking for a unique entry.	You discovered that a registry key was updated to *"242464"*. Now you want to investigate who made the change and what the value was before. You can set the **Details** filter to *242464* to find this change faster.
Before	Limits your search results to entries that contain the specified before value in the **Details** column.	You are investigating an incident in which the SAM- account- name attribute was changed for an account in your Active Directory domain. You can set the **Before** filter to the

Filter	Description	Example
		previous name (e.g., *John2000*) to find the new name faster.
After	Limits your search results to entries that contain the specified after value in the **Details** column.	You are investigating a security incident and want to know who enabled a local Administrator account on your Windows Server. You can set the **After** filter to this account's current state (e.g., *Enabled*) to find this change faster.
Everywhere	Limits your search results to entries that contain the specified value in any column.	You are investigating a security incident. You have already identified the intruder (e.g., *BadActor*) and now you want to see all actions made by intruder's account or with it. Since the intruder can be the actor (Who), the object (What), or can even show up in details, set the **Everywhere** filter to intruder's name.

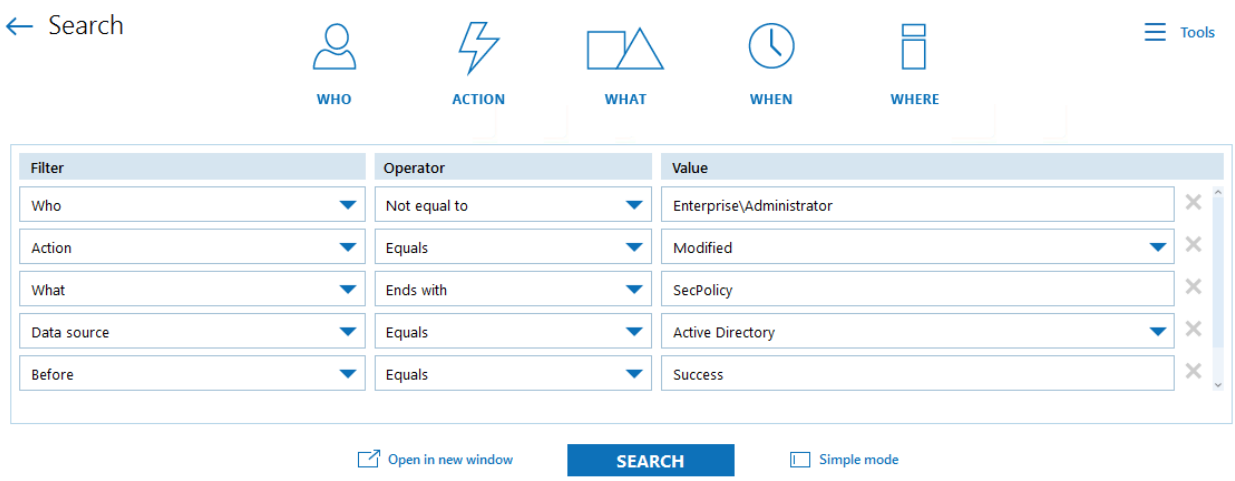
3.2.2. Change Match Types

By default, the **Contains** match type is used when adding most filters in the **Search** field. In the **Advanced mode**, you can customize your search by modifying match types for the filters you have already selected.

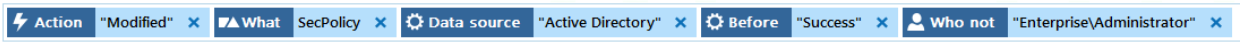
Operator	Description	Example
Contains	This broad match operator shows all entries that include a value specified in the filter.	Set the **Who** filter to **contains** *John*, to get the following results: *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*, *John@domain.com*.
Equals	This exact match operator shows all entries with the exact value specified. Make sure to provide a full object name or path. **NOTE:** To apply this operator when adding filters in the **Search**	Use this operator if you want to get precise results, e.g., *\\FS\Share\NewPolicy.docx*.

Operator	Description	Example
	field in the **Simple** mode, provide a value in quotation marks (e.g., *"Domain1\John"*).	
Not equal to	This negative exact match operator shows all entries except those with the exact value specified. **NOTE:** In the **Search** field in the **Simple** mode, this operator appears as **not**, e.g., **Who not** for the **Who** filter.	Set the **Who** filter to **not equal to** *Domain1\John* to exclude the exact user specified and find all changes performed by other users, e.g., *Domain1\Johnson, Domain2\John*.
Starts with	This operator shows all entries that start with the exact value specified.	Set the **Who** filter to **starts with** *Domain1\John* to find all changes performed by *Domain1\John*, *Domain1\Johnson*, and *Domain1\Johnny*.
Ends with	This operator shows all entries that end with the exact value specified.	Set the **Who** filter to **ends with** *John* to find all changes performed by *Domain1\John*, *Domain2\Dr.John*, *Domain3\John*.
Does not contain	This negative broad match operator shows all entries except those that contain the value specified. **NOTE:** In the **Search** field in the **Simple** mode, this operator appears as **not**, e.g., **Who not** for the **Who** filter.	Set the **Who** filter to **does not contain** *John* to exclude the following users: *Domain1\John*, *Domain2\Johnson*, and *Johnny@domain.com*.

To review the search with advanced filters and operators applied, use the **Advanced mode**.



The image below represents the same search filters as they are shown in the **Search** field in the **Simple** mode.



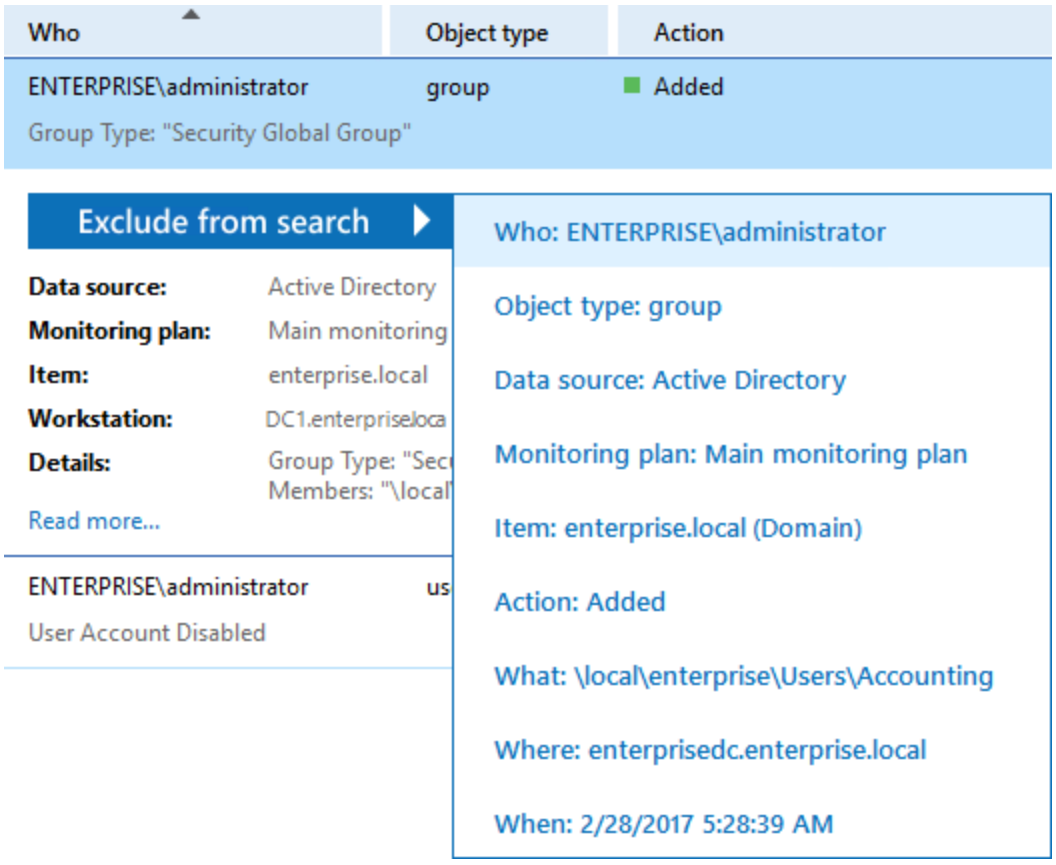
3.3. Include and Exclude Data

Having reviewed the search results, you can proceed with your investigation by excluding or including data. Excluding a filter value is helpful if you want to skip it in your search results (e.g., a service account or trusted user account). On the other hand, including a filter value ensures that only the entries containing it will be shown (e.g., a suspicious user or potentially violated folder).

To include or exclude data

1. Review your search results and locate an entry with data you want to exclude or include.
2. Double-click this entry to review details.
3. Select **Exclude from search** or **Include to search** and specify a filter value from the list.
4. Click **Search** to update the search results.

Your exclusions and inclusions will automatically be added to the search filters, limiting the amount of data shown in the results pane.



3.4. Save Your Search and Share Results

After browsing your audit data, navigate to **Tools** to save your search and share the search results. Review the following for additional information:

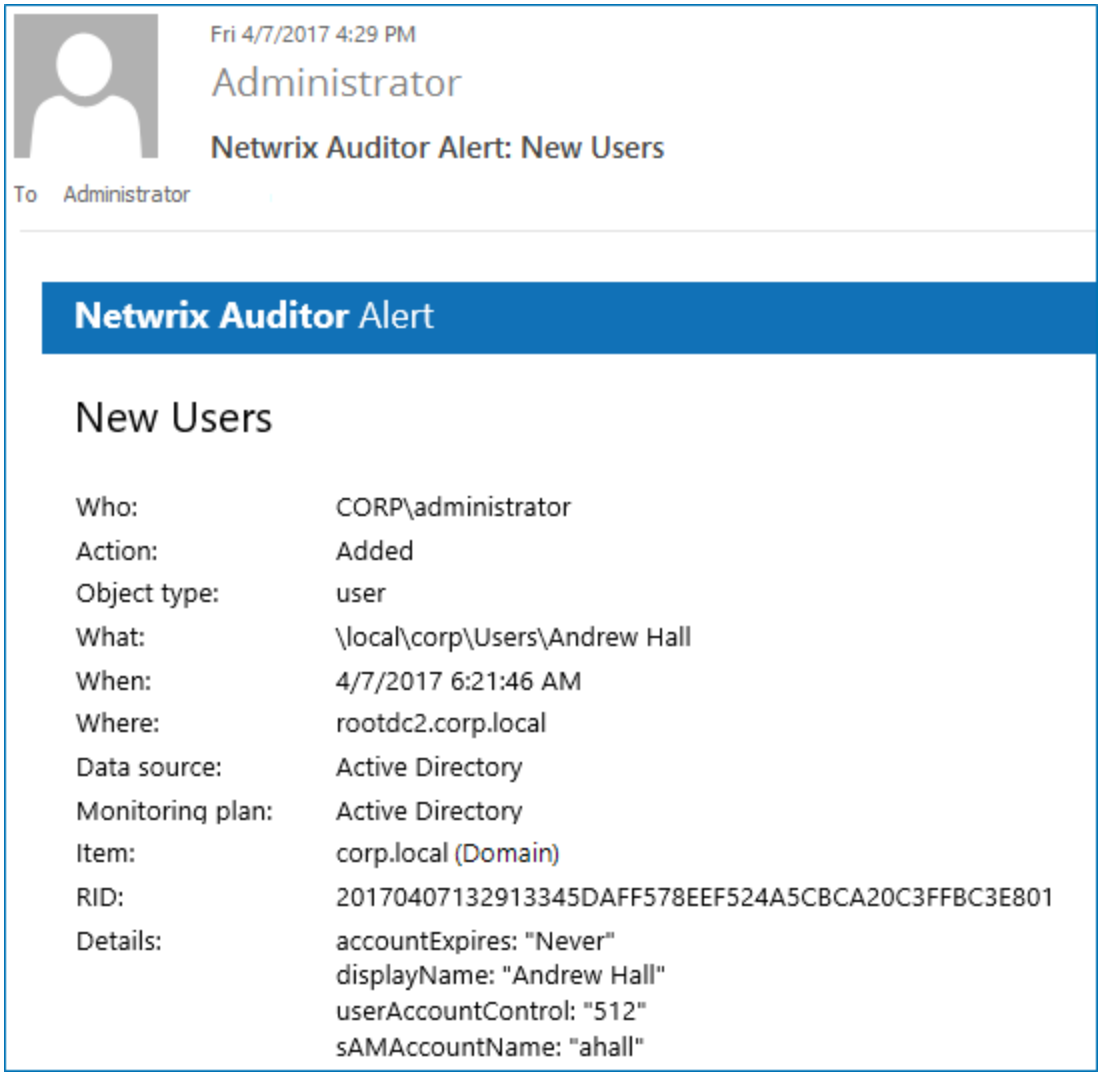
Use...	To...
Copy search	Copy the search filters that are currently applied to your search. This can be helpful if you want to share your search with a colleague (e.g., by pasting it in an email) or you want to modify a saved search with your current filters.
Paste search	Paste the search filters you copied before. These can be filters copied from a previous search or those someone shared with you.
Save search	Refer to Saved Searches for detailed instructions on how to save searches you want to run on a regular basis.
Create alert	Create an alert with the same set of filters you have just specified for your search. See Create Alerts for more information.
Export data	Save your search results as a pdf or csv file.

Use...	To...
	When saving search results to a file, you are not limited to the top 2,000 entries; all audit data relevant to your search will be exported. **NOTE:** Using csv files is recommended when exporting large amount of data (e.g., changes made by a newly retired employee during the last 8 months).

4. Alerts

If you want to be notified about suspicious activity, you can configure alerts that will be triggered by specific events. Alerts are sent after the specified action has been detected. Alerts are helpful if you want to be notified about actions critical to your organization security and have to mitigate risks once the suspicious action occurs.

The example alert is triggered when a new user is created in the monitored domain.



4.1. Create Alerts

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

To...	Do...
Enable/ disable an existing alert	1. Navigate to the **Intelligence** section and click the **Alerts** tile. 2. Select an alert from the list. 3. Select **On** or **Off** in the **Status** column.
Modify an existing alert	1. Navigate to the **Intelligence** section and click the **Alerts** tile. 2. Select an alert from the list and click in the right pane.
Create a new alert	See To create new custom alert for more information.
Remove an alert	1. Navigate to the **Intelligence** section and click the **Alerts** tile. 2. Select an alert from the list and click in the right pane.

NOTE: To create new alerts and modify existing alerts, you must be assigned the Global administrator or Global reviewer role in the product. See Netwrix Auditor Administration Guide for more information.

To create new custom alert

1. On the main Netwrix Auditor page, navigate to the **Intelligence** section and click the **Alerts** tile.

   NOTE: You can also create new alert directly from the interactive search results. Navigate to **Tools** and select **Create alert** to add a new alert with the same set of filters as your search.

2. In the **All Alerts** window, click **Add Alert**. Configure the following:

Option	Description
General	Specify a name and enter the description for the new alert. **NOTE:** Make sure that the **Send alert when the action occurs** option is enabled. Otherwise, the new alert will be disabled.
Recipients	Select alert recipients. Click **Add Recipient** and select alert delivery type: • **Email** — Specify the email address where notifications will be delivered. You can add as many recipients as necessary. **NOTE:** It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

Option	Description
	• **SMS-enabled email**—Netwrix uses the sms gateway technology to deliver notifications to a phone number assigned to a dedicated email address. Specify email address to receive SMS notifications. **NOTE:** Make sure that your carrier supports sms to email gateway technology.
Filters	Apply a set of filters to narrow events that trigger a new alert. Alerts use the same interface and logic as intelligence search. • **Filter**—Select general type of filter (e.g., "*Who*", "*Data Source*", "*Monitoring plan*", etc.) • **Operator**—Configure match types for selected filter (e.g., "*Equals*", "*Does not contain*", etc.) • **Value**—Specify filter value. Refer to Interactive Search for detailed instructions on how to create and modify filters.
Thresholds	If necessary, enable threshold to trigger the new alert. In this case, a single alert will be sent instead of many alerts. This can be helpful when Netwrix Auditor detects many activity records matching the filters you specified. Slide the switch under the **Send alert when the threshold is exceeded** option and configure the following: • **Limit alerting to activity records with the same...**—Select a filter in the drop-down list (e.g., who). Note that, Netwrix Auditor will search for activity records with the same value in the filter you selected. • **Send alert for <...> activity records within <...> seconds**—Select a number of changes that occurred in a given period (in seconds). For example, you want to receive an alert on suspicious activity. You select "*Action*" in the **Limit alerting to activity records with the same** list and specify a number of actions to be considered an unexpected behavior: *1000* changes in *60* seconds. When the selected threshold exceeded, an alert will be delivered to the specified recipients: one for every 1000 removals in 60 seconds, one for every 1000 failed removals in 60 seconds. So you can easily discover what is going on in your IT infrastructure.

4.2. Predefined Alerts

For your convenience, Netwrix provides you with a set of predefined alerts that are commonly used for IT infrastructure monitoring. The out-of-box alerts include those that help you detect suspicious activity and inform you on critical changes to your environment. The alerts contain pre-configured filters and in most case you only need to enable an alert and select who will receive notifications.

To enable predefined alert

1. Navigate to the **Intelligence** section and click the **Alerts** tile.
2. Select an alert in the list and enable it using the slider in the **Status** column.
3. Double-click the selected alert or click  and specify alert recipient. Refer to Create Alerts for detailed instructions on how to configure alerts.
4. Review and update filters. For some alerts you should provide filter values, such as group name or user.

NOTE: You can also create a custom alert based on predefined alert configuration. To do it, select an alert in the list and click **Copy alert** at the bottom of Netwrix Auditor client.

5. Reports and Report Packs

5.1. Manage Reports

Netwrix Auditor provides a variety of reports for each data source that help you keep track of all changes in your IT infrastructure and validate compliance with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

NOTE: To review intelligence data, you must be assigned the Global administrator or Global reviewer role in the product. The users assigned the Reviewer role on a certain plan or folder have a limited access to data—only within a delegated scope. See Netwrix Auditor Administration Guide for more information.

5.1.1. Understand Report Types

In Netwrix Auditor, the following report types are available:

- **Enterprise Overview**—Dashboards that provide quick access to important statistics across the audited IT infrastructure. They allow you to see the activity trends by date, user, object type, server or audited IT system, and drill through to detailed reports for further analysis. The **Enterprise** dashboard aggregates the information on changes from all data sources and provides a centralized overview. System-specific dashboards reflect all changes across all monitoring plans where audit of this target system is enabled. See Overview Dashboards for more information.
- **Organization Level reports**—High-level reports that aggregate data from all data sources and monitoring plans. They list all activity that occurred across the audited IT infrastructure. **Enterprise Overview** provides bird's eye view of changes and activity from all data sources and provides a centralized overview. See Organization Level Reports for more information.
- **Overview diagrams**—System-specific diagram reports that aggregate audit data for an auditing system. They provide a high-level overview of changes within a selected time period. Overviews consist of four charts, showing the activity trends by date, user, object type or server, and drill through to detailed reports for further analysis. See Overview Dashboards for more information.
- **Change and activity reports**—System-specific reports that aggregate audit data for a specific data source within specified monitoring plans. These reports show detailed data on changes and activity and provide grouping, sorting and filtering capabilities. Each report has a different set of filters allowing you to manage collected data in the most convenient way. See Change and Activity Reports for more information.
- **State-in-time reports**—System-specific reports that aggregate data for a specific data source within a specified individual monitoring plan and allow reviewing the point-in-time state of the data source. These reports are based on daily snapshots and help you paint a picture of your system configuration at a specific moment in time. See State–in–Time Reports for more information.

- **Changes with Video reports**—Windows server-based reports that provide video recordings of user activity on audited computers. See Reports with Video for more information.
- **Changes with Review Status reports**—Both system-specific and overview reports that can be used in the basic change management process. These reports allow setting a review status for each change and providing comments. See Reports with Review Status for more information.

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

5.1.2. View Reports

To view reports in Netwrix Auditor

- Navigate to **Reports** and select a report you are interested in and click **View**.

The table below lists report folders available in Netwrix Auditor:

Folder	Reports
Organization Level reports	Contains a set of reports and dashboards that provide a general overview of your entire IT infrastructure. The folder also includes a special report that helps you review activity records supplied via Integration API.
User Behavior and Blind Spot Analysis	Contains a set of reports that help you identify vulnerabilities in your IT infrastructure.

Active Directory	Contains a set of reports on Active Directory and Group Policy changes and state-in-time configuration. Includes the following subfolders:
	• **Active Directory Changes** with:
	  • Overview diagram
	  • Change reports
	  • Changes with review status
	• **Active Directory State-in-Time** with state-in-time reports
	• **Group Policy Changes** with:
	  • Change reports
	  • Changes with review status
	• **Group Policy State-in-Time** with state-in-time reports
	• **Logon Activity** with activity reports

Folder	Reports
Azure AD	Contains a set of reports on Azure Active Directory changes and user activity. Use these reports to track changes in your organization's Active Directory in the cloud, ensure its health, and prevent unauthorized activity. Includes the following reports: • Overview diagram • Change and activity reports
Exchange	Contains a set of reports on Exchange Server changes and non-owner mailbox access. Use these reports to track changes in your Exchange organization, ensure its health, and prevent unauthorized activity. Includes the following reports: • Overview diagram • Change and activity reports • Changes with review status
Exchange Online	Contains a set of reports on Exchange Online changes and non-owner mailbox access. Use these reports to track changes in your Exchange Online organization, ensure its health, and prevent unauthorized activity. Includes the following reports: • Overview diagram for Office 365 • Change and activity reports

File Servers including Windows file servers, EMC and NetApp	Contains a set of reports on file server changes, activities, and state-in-time configuration. Includes the following subfolders:
	• **File Servers Activity** with:
	  • Overview diagram
	  • Change and activity reports
	• **File Servers State-in-Time** with state-in-time reports

Oracle Database	Contains a set of reports on Oracle Database changes and logon activity. Includes the following reports: • Overview diagram • Change and activity reports
SharePoint	Contains a set of reports on SharePoint changes and read access, including changes to content, configuration and access permissions.

Folder	Reports
	Includes the following reports: • Overview diagram • Change and activity reports • Changes with review status
SharePoint Online	Contains a set of reports on SharePoint Online activity and changes, including changes to content and configuration. In addition to SharePoint Online, these reports highlight OneDrive for Business changes. Includes the following reports: • Overview diagram for Office 365 • Change and activity reports
SQL Server	Contains a set of reports on SQL Server changes, including changes to content and configuration, and logon activity. Includes the following reports: • Overview diagram • Change and activity reports
VMware	Contains a set of reports on VMware changes. These reports can be used to prevent potentially harmful actions and changes that may affect the entire virtual infrastructure and lead to data loss. Includes the following reports: • Overview diagram • Change reports

Windows Server	Contains a set of reports on Windows infrastructure including reports on Windows configuration changes, event logs and user activity. Includes the following subfolders:
	• **Windows Server Changes** with:
	  • Overview diagram
	  • Change reports
	  • Changes with review status
	• **User Activity (Video)** with reports with video
	• **Event Log** with change reports, including a syslog change report, the **Netwrix Auditor System Health** report and **IIS** change

Folder	Reports
	reports. **NOTE:** **Netwrix Auditor System Health** is a special report designed for reviewing Netwrix Auditor health status (successful and failed data collections, warnings, errors, etc.)
Compliance folders: • **FERPA Compliance** • **CJIS Compliance** • **FISMA/NIST Compliance** • **GLBA Compliance** • **HIPAA Compliance** • **ISO/IEC 27001 Compliance** • **NERC CIP Compliance** • **PCI DSS Compliance** • **SOX Compliance** • **GDPR Compliance**	For your convenience, contains reports mentioned above but grouped by corresponding international standards and regulations: • **FERPA** • **CJIS** • **FISMA/NIST SP800-53 rev4** • **GLBA** • **HIPAA** • **ISO/IEC 27001** • **NERC** • **PCI DSS v3.2** • **SOX** • **GDPR** **NOTE:** Click **Compliance** above the list of reports to see reports grouped by compliance standards only. See Compliance Report Packs for more information.

To view reports in a web browser

- Open a web browser and type the Report Manager URL (found under **Settings** → **Audit Database**). In the page that opens, navigate to the report you want to generate and click the report name. You can modify the report filters and click **View Report** to apply them.

5.1.3. Leverage Filtering Capabilities

Report filters allow you to display changes matching certain criteria. For example, you can filter changes by audited domain or object type. Filtering does not delete changes, but modifies the report view allowing you to see changes you are interested in. Filters can be found in the upper part of the **Preview Report** page.

To apply filters

1. Navigate to **Reports** and generate a report.
2. Apply filters to the report and click **View Report**. For example, you can update report timeframe, select specific values for *Who* and *Where*, apply sorting, etc.

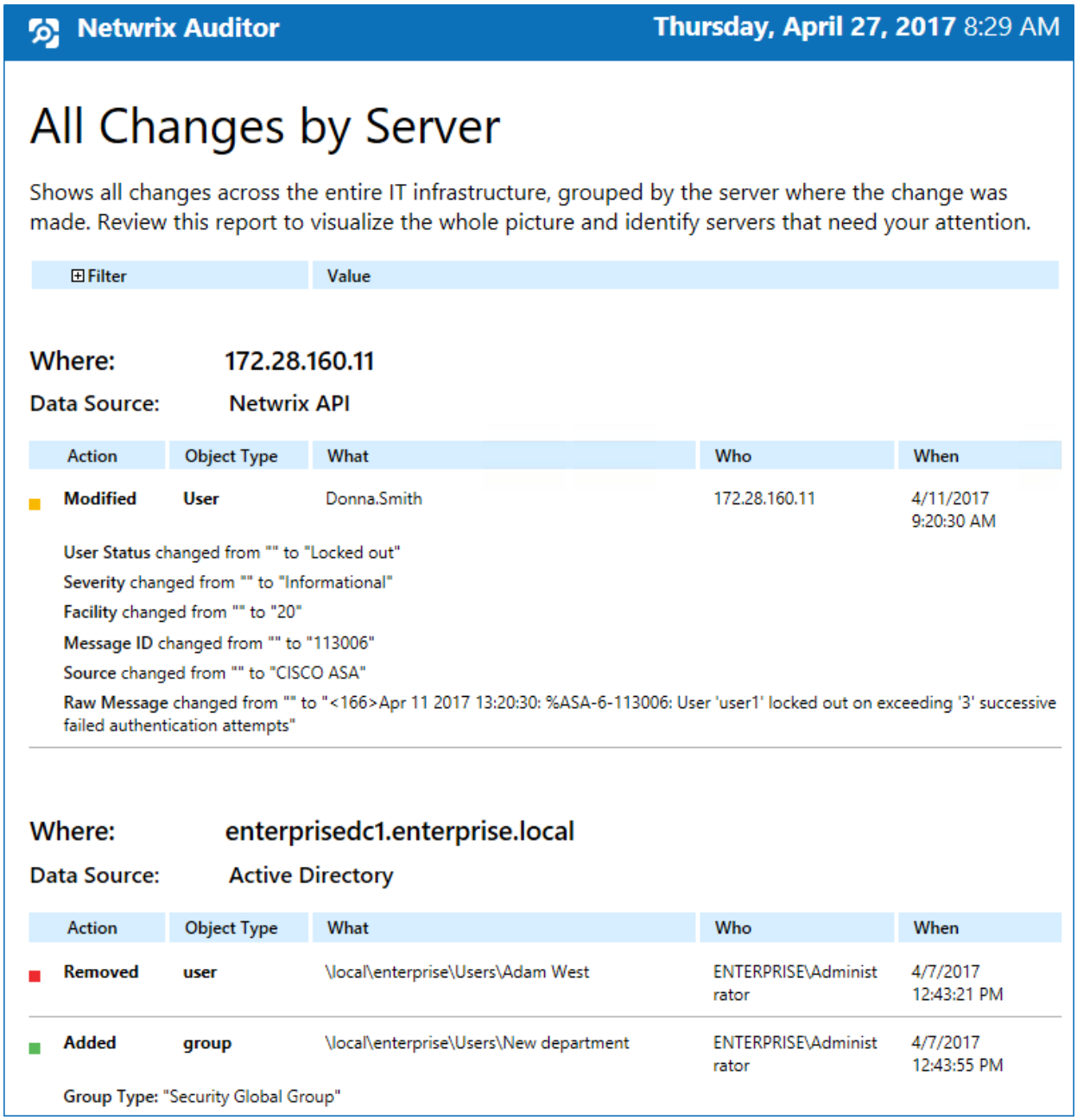
Wildcards are supported. For example, type *%admin%* in the **Who (domain\user)** field if you want to view changes made by users with the name containing "administrator" (e.g., *enterprise\administrator, corp\administrator, sqladmin*).

Do not use % in the exclusive filters (e.g., *Who (Exclude domain\user)*). Otherwise, you will receive an empty report.

NOTE: *escape_characters* are not supported.

The example below applies to the **All Changes by Server** report and shows the before and after views of the report. The filters may vary slightly depending on the data source and report type.

The report without filtering:



Netwrix Auditor Thursday, April 27, 2017 8:29 AM

All Changes by Server

Shows all changes across the entire IT infrastructure, grouped by the server where the change was made. Review this report to visualize the whole picture and identify servers that need your attention.

⊞Filter	Value

Where: 172.28.160.11

Data Source: Netwrix API

Action	Object Type	What	Who	When
Modified	**User**	Donna.Smith	172.28.160.11	4/11/2017 9:20:30 AM

User Status changed from "" to "Locked out"

Severity changed from "" to "Informational"

Facility changed from "" to "20"

Message ID changed from "" to "113006"

Source changed from "" to "CISCO ASA"

Raw Message changed from "" to "<166>Apr 11 2017 13:20:30: %ASA-6-113006: User 'user1' locked out on exceeding '3' successive failed authentication attempts"

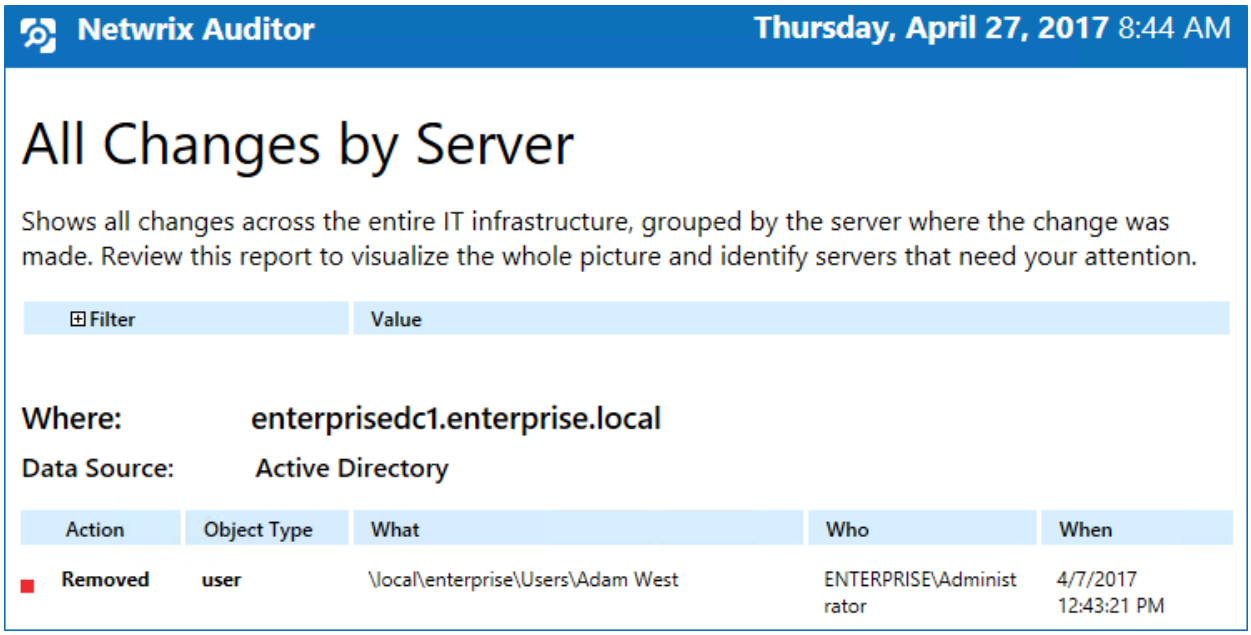
Where: enterprisedc1.enterprise.local

Data Source: Active Directory

Action	Object Type	What	Who	When
Removed	**user**	\local\enterprise\Users\Adam West	ENTERPRISE\Administrator	4/7/2017 12:43:21 PM
Added	**group**	\local\enterprise\Users\New department	ENTERPRISE\Administrator	4/7/2017 12:43:55 PM

Group Type: "Security Global Group"

The report below displays changes made by enterprise\administrator (the Who filter is set to "enterprise\administrator") that affected users (the Object type is set to "user") across all data sources, records are sorted by the action.


Netwrix Auditor Thursday, April 27, 2017 8:44 AM

All Changes by Server

Shows all changes across the entire IT infrastructure, grouped by the server where the change was made. Review this report to visualize the whole picture and identify servers that need your attention.

Filter	Value

Where: enterprisedc1.enterprise.local

Data Source: Active Directory

Action	Object Type	What	Who	When
Removed	user	\local\enterprise\Users\Adam West	ENTERPRISE\Administrator	4/7/2017 12:43:21 PM

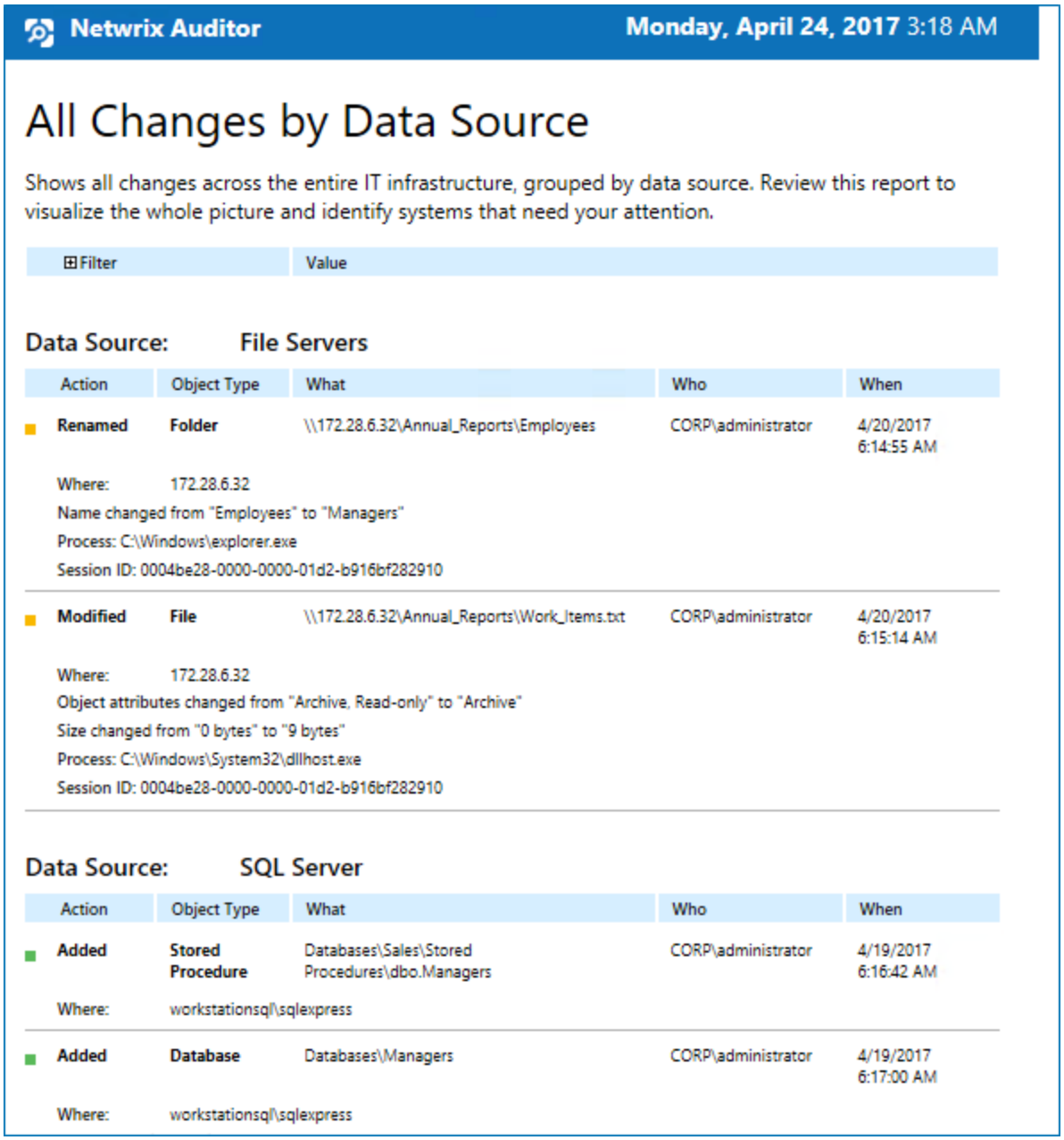
5.2. Organization Level Reports

Organization Level reports aggregate data on all monitoring plans and list changes and activity that occurred across all data sources.

NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Netwrix Auditor Global administrator to import that data from the Long-Term Archive.

Organization Level reports can be found in the **Organization Level Reports** folder under the **Reports** node.



Netwrix Auditor — Monday, April 24, 2017 3:18 AM

All Changes by Data Source

Shows all changes across the entire IT infrastructure, grouped by data source. Review this report to visualize the whole picture and identify systems that need your attention.

Filter	Value

Data Source: File Servers

Action	Object Type	What	Who	When
Renamed	Folder	\\172.28.6.32\Annual_Reports\Employees	CORP\administrator	4/20/2017 6:14:55 AM
Where:	172.28.6.32			
Name changed from "Employees" to "Managers"				
Process: C:\Windows\explorer.exe				
Session ID: 0004be28-0000-0000-01d2-b916bf282910				
Modified	File	\\172.28.6.32\Annual_Reports\Work_Items.txt	CORP\administrator	4/20/2017 6:15:14 AM
Where:	172.28.6.32			
Object attributes changed from "Archive, Read-only" to "Archive"				
Size changed from "0 bytes" to "9 bytes"				
Process: C:\Windows\System32\dllhost.exe				
Session ID: 0004be28-0000-0000-01d2-b916bf282910				

Data Source: SQL Server

Action	Object Type	What	Who	When
Added	Stored Procedure	Databases\Sales\Stored Procedures\dbo.Managers	CORP\administrator	4/19/2017 6:16:42 AM
Where:	workstationsql\sqlexpress			
Added	Database	Databases\Managers	CORP\administrator	4/19/2017 6:17:00 AM
Where:	workstationsql\sqlexpress			

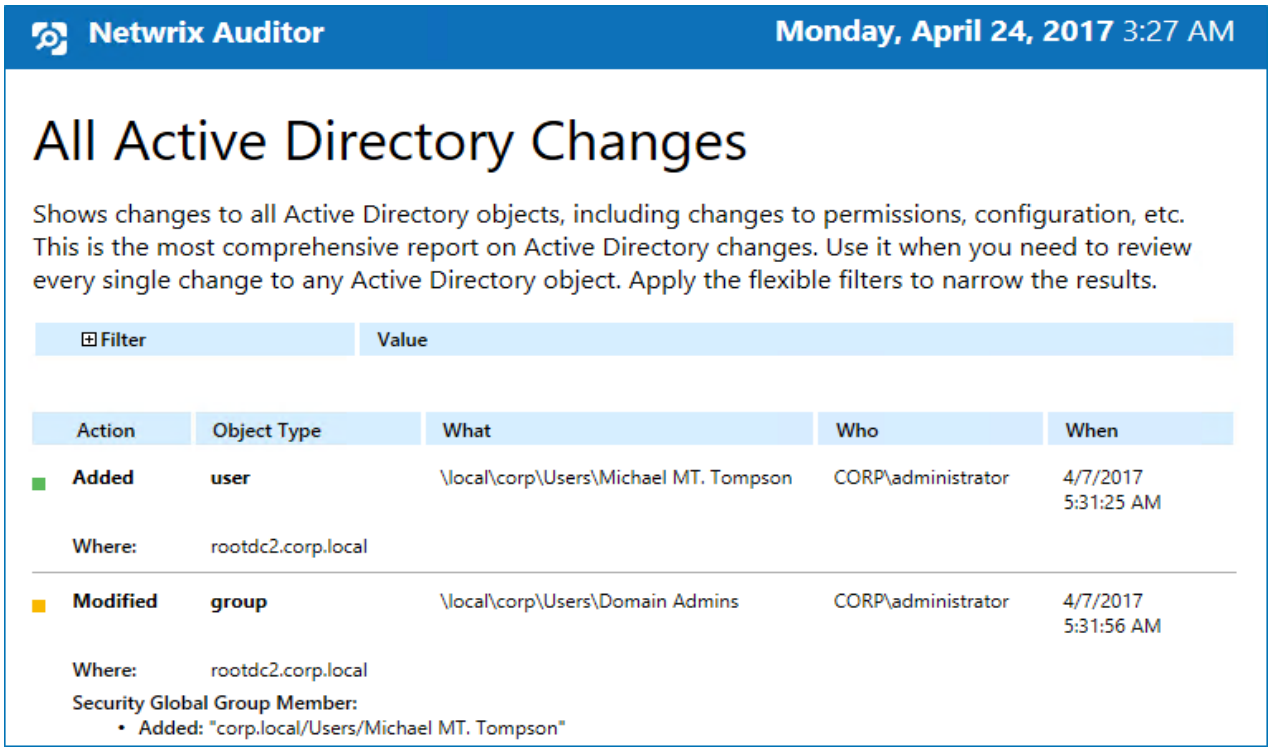
NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

5.3. Change and Activity Reports

Change and activity reports provide information on changes to different aspects of the audited environment. Depending on the data source, navigate to one of the following locations:

Data source	Report location
Active Directory	**Active Directory** → **Active Directory Changes**
Azure AD	**Azure AD**
Group Policy	**Active Directory** → **Group Policy Changes**
Exchange	**Exchange**
Exchange Online	**Exchange Online**
File Servers	**File Servers** → **File Servers Activity**
Oracle Database	**Oracle Database**
SharePoint	**SharePoint**
SharePoint Online	**SharePoint Online**
SQL Server	**SQL Server**
VMware	**VMware**
Windows Server	**Windows Server** → **Windows Server Changes**
Event Log	**Windows Server** → **Event Log**
IIS	**Windows Server**→ **Event Log**
Logon Activity	**Active Directory** → **Logon Activity**
Integration API	**Organization Level Reports**

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.


Netwrix Auditor Monday, April 24, 2017 3:27 AM

All Active Directory Changes

Shows changes to all Active Directory objects, including changes to permissions, configuration, etc. This is the most comprehensive report on Active Directory changes. Use it when you need to review every single change to any Active Directory object. Apply the flexible filters to narrow the results.

Filter	Value

Action	Object Type	What	Who	When
Added	user	\local\corp\Users\Michael MT. Tompson	CORP\administrator	4/7/2017 5:31:25 AM
Where:	rootdc2.corp.local			
Modified	group	\local\corp\Users\Domain Admins	CORP\administrator	4/7/2017 5:31:56 AM
Where:	rootdc2.corp.local			

Security Global Group Member:
- Added: "corp.local/Users/Michael MT. Tompson"

NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

5.4. State–in–Time Reports

The state-in-time reports functionality allows generating reports on the system's state at a specific moment of time in addition to change and activity reports. State-in-time reports are based on the daily configuration snapshots, and reflect a particular aspect of the audited environment.

This functionality is currently available for the following data sources:

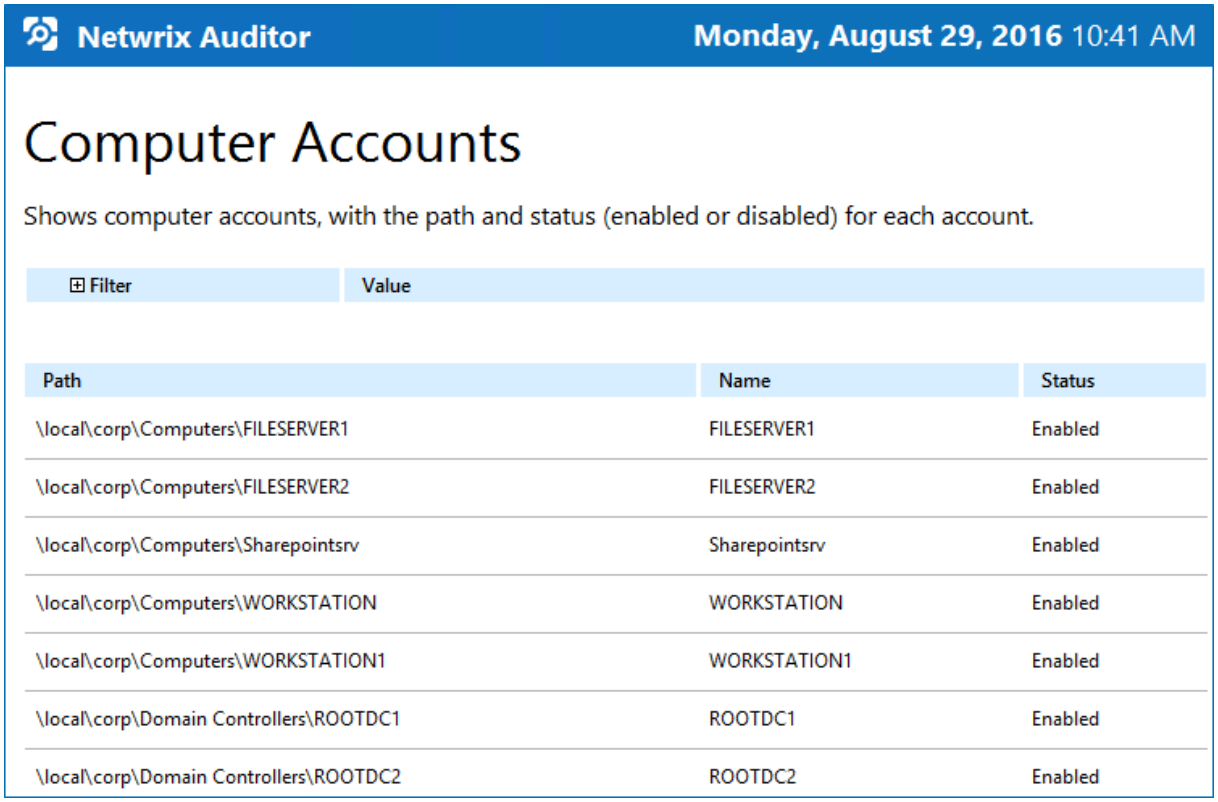
- Active Directory
- File Servers
- Group Policy

The state-in-time reports are found under the **Reports** node. Depending on the data source, navigate to one of the following locations:

Data source	Report location
Active Directory	**Active Directory** → **Active Directory State-in-Time**
Group Policy	**Active Directory** → **Group Policy State-in-Time**

Data source	Report location
File Servers	**File Servers** → **File Servers State-in-Time**

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

By default, state-in-time reports reflect the current state of the data source. If you want to generate a report to assess your system at a particular moment in the past, you can select the corresponding snapshot from the **Snapshot Date** filter.

NOTE: To be able to generate reports based on different snapshots, ask your Netwrix Auditor Global administrator to import historical snapshots to the Audit Database, otherwise only the **Current Session** option is available in the drop-down list.

When auditing file servers, changes to both access and audit permissions are tracked. To exclude information on access permissions, contact your Netwrix Auditor Global administrator or Configurator of this plan.

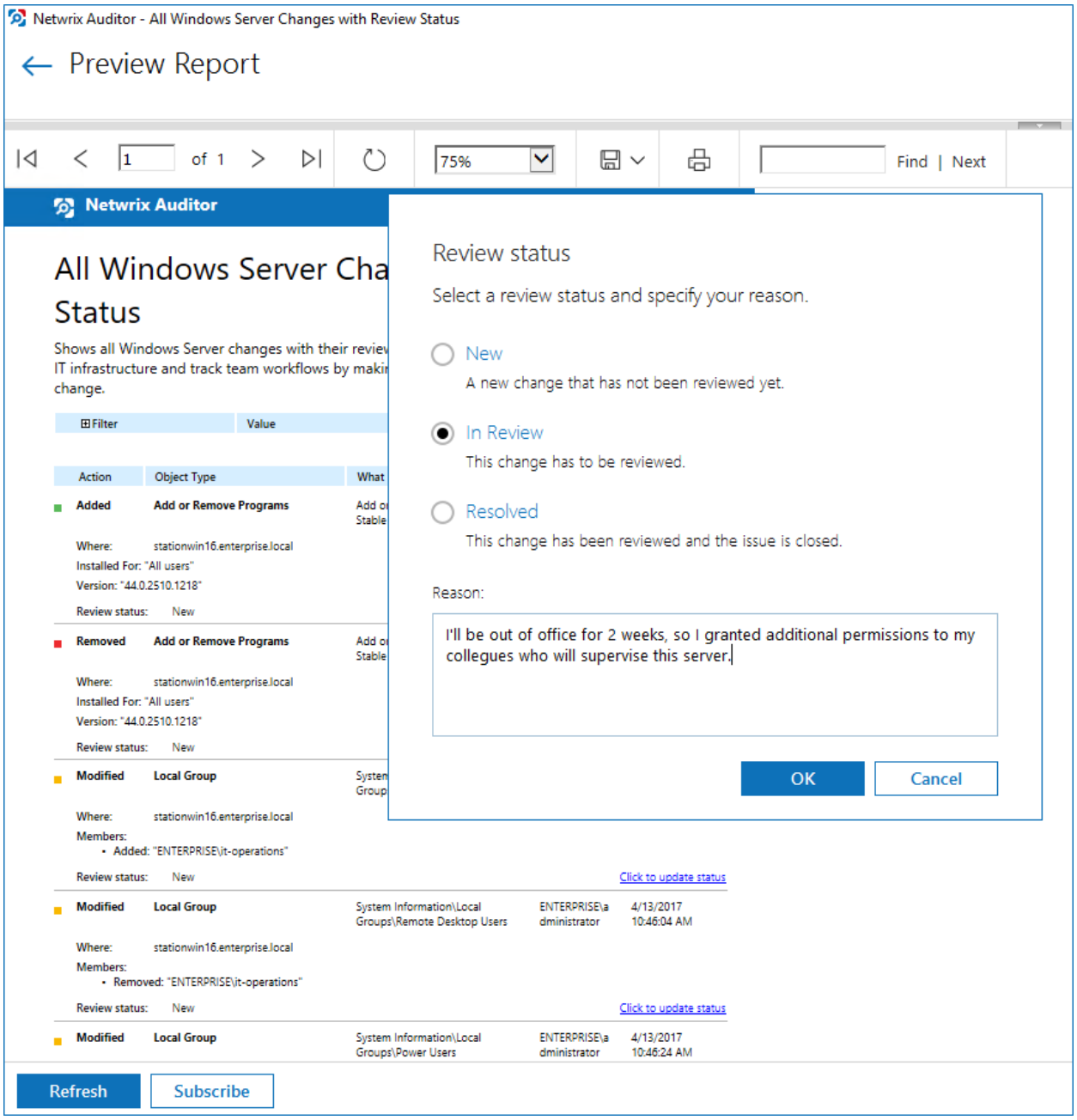
5.5. Reports with Review Status

Change management is one of the critical processes for many companies referring to such areas as requesting, planning, implementing, and evaluating changes to various systems. Netwrix Auditor allows facilitating the change auditing process by providing the change monitoring and reporting capabilities. Additionally, you can track team workflows by making notes on the review status or reasons for each change.

Data source	Report location
Entire IT infrastructure	**Organization Level Reports**
Active Directory	**Active Directory** → **Active Directory Changes** → **All Active Directory Changes with Review Status**
Exchange	**Exchange** → **All Exchange Server Changes with Review Status**
SharePoint	**SharePoint** → **All SharePoint Changes with Review Status**
Windows Server	**Windows Server** → **Windows Server Changes** → **All Windows Server Changes with Review Status**
Group Policy	**Active Directory** → **Group Policy Changes** → **All Group Policy Changes with Review Status**

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.

They list all changes to the monitored environment that are assigned the **New** status by default. If a change seems unauthorized, or requires further analysis, you can click the **Click to update status** link, set its status to **In Review** and provide a reason. Once the change has been approved of, or rolled back, you can set its status to **Resolved**.



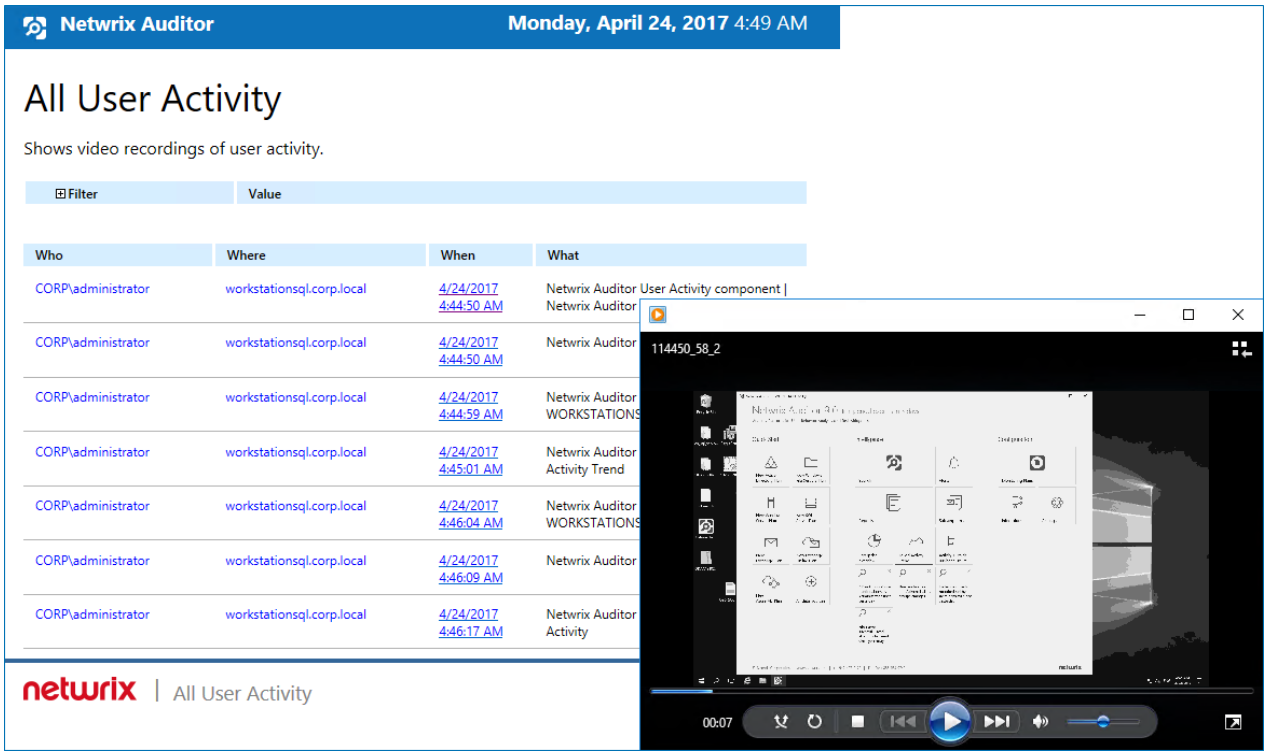
NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

5.6. Reports with Video

Netwrix Auditor can be configured to capture video of user activity on the monitored computers that helps analyze and control changes made there. When you click a link, a video player opens and playback of the recorded user activity starts, showing launched applications, actions, etc.

To view reports with video, navigate to **Windows Server** → **User Activity**.

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

To play a video

1. Navigate to **Reports** → **Windows Server** → **User Activity**. Select any report and click **View**.
2. Click a link in the When column.

NOTE: To open User Activity report for the selected user or server, you can also click the link in the **Who** and **Where** columns of the **All Users Activity** report.

5.7. Compliance Report Packs

For your convenience, besides grouping by data source the reports are grouped by compliance standards. Netwrix Auditor provides out-of-box reports that allow validating compliance with different standards and regulations, including but not limited to:

- **FERPA**
- **FISMA/NIST SP800-53 rev4**

- **GDPR**
- **GLBA**
- **HIPAA**
- **ISO/IEC 27001**
- **NERC**
- **PCI DSS v3.2**
- **SOX**
- **CJIS**

You can find **Compliance** folders under the **Reports** node by clicking **Compliance** or you can scroll down the **All reports** list. Each compliance folder provides overview on a selected standard, to read it, click on the folder name. Click **Read More** to learn more about mapping between these standards and Netwrix Auditor reports.

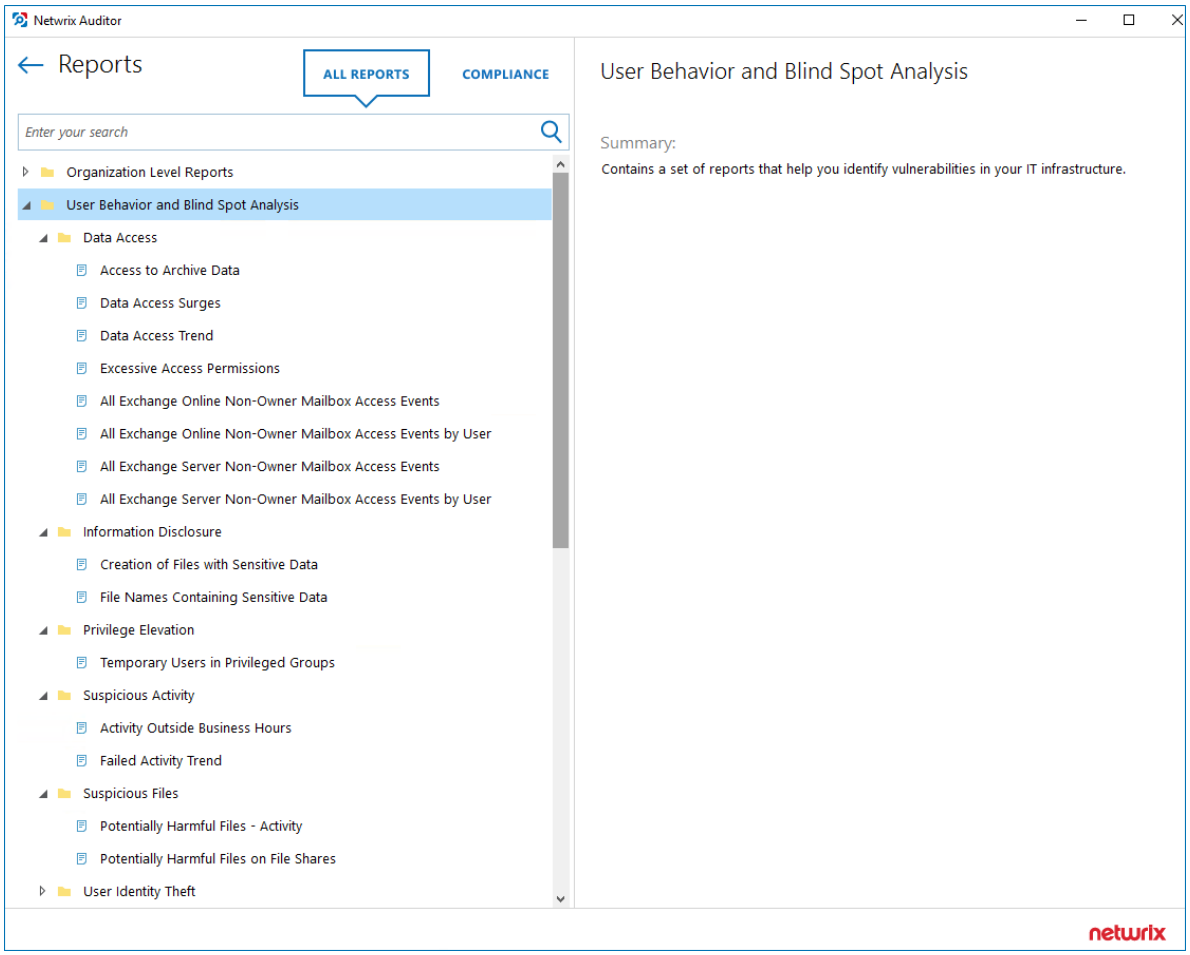
NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.

5.8. User Behavior and Blind Spot Analysis Report Pack

Netwrix Auditor takes a step forward as a visibility and governance platform and introduces report packs that help you enable control over changes, configurations and access in hybrid cloud IT environments. Netwrix Auditor report packs provide security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

The **User Behavior and Blind Spot Analysis** report pack contains a set of smart reports that help you identify vulnerabilities and easily answer questions such as:

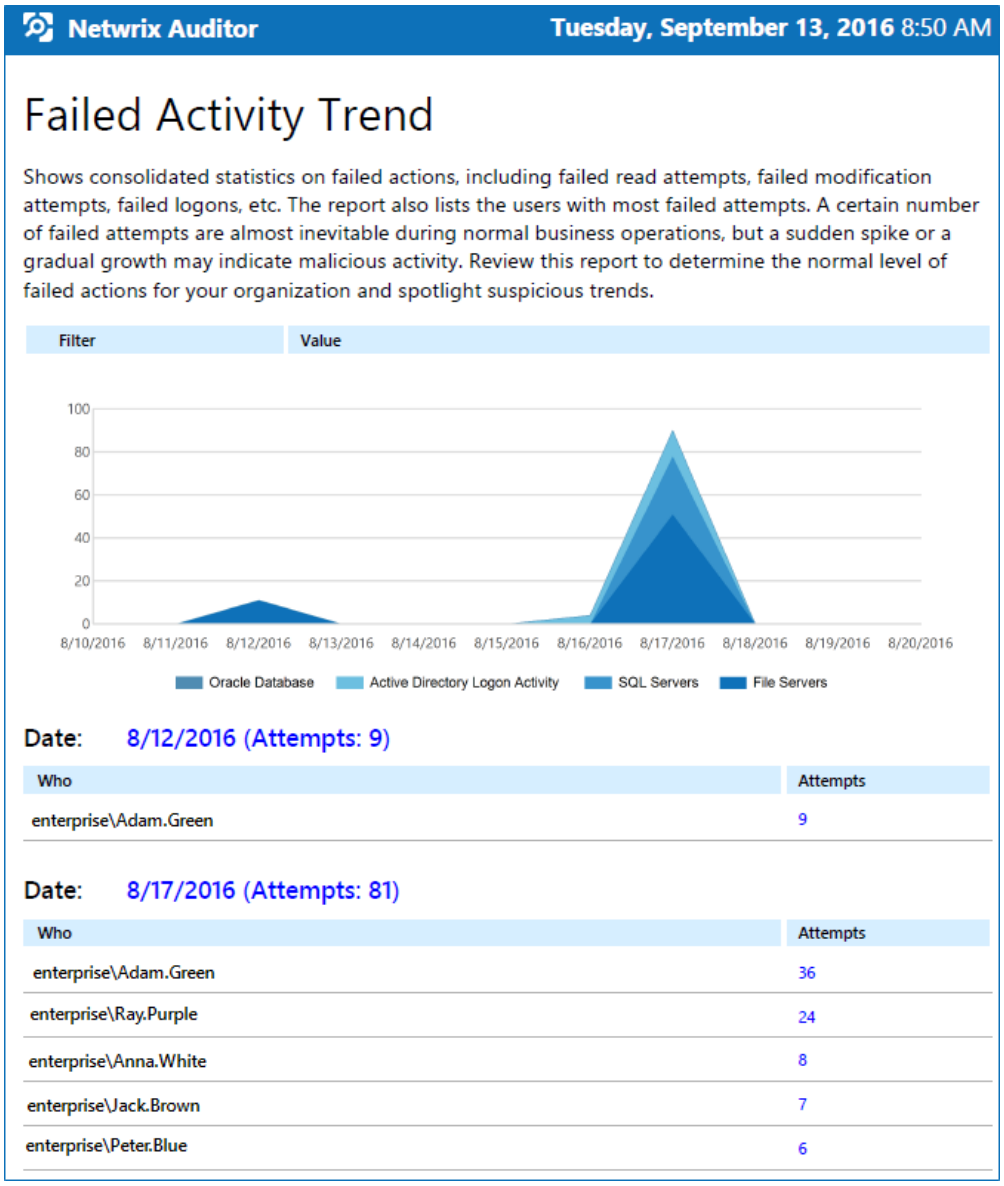
- Has there been any abnormal access to sensitive data?
- Is anyone accessing stale data?
- Have there been any unusual spikes in failed activity?
- Who is active outside of business hours and what are they doing?
- Has anyone put harmful files on corporate data storage?
- Are there any files likely to contain credentials, Social Security numbers, PHI or other sensitive data?



Analytics reports can be found in the **User Behavior and Blind Spot Analysis** folder under the **Reports** node.

NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Netwrix Auditor Global administrator to import that data from the Long-Term Archive.



Netwrix Auditor Tuesday, September 13, 2016 8:50 AM

Failed Activity Trend

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts. A certain number of failed attempts are almost inevitable during normal business operations, but a sudden spike or a gradual growth may indicate malicious activity. Review this report to determine the normal level of failed actions for your organization and spotlight suspicious trends.

Filter	Value

Date: 8/12/2016 (Attempts: 9)

Who	Attempts
enterprise\Adam.Green	9

Date: 8/17/2016 (Attempts: 81)

Who	Attempts
enterprise\Adam.Green	36
enterprise\Ray.Purple	24
enterprise\Anna.White	8
enterprise\Jack.Brown	7
enterprise\Peter.Blue	6

NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

6. Subscriptions

You can configure a report subscription to schedule automatic report generation and delivery. You can also apply various filters to reports, choose output format for your reports, and delivery method.

NOTE: To create new subscriptions and manage existing subscriptions, you must be assigned the Global administrator or Global reviewer role in the product. See Netwrix Auditor Administration Guide for more information.

Review the following for additional information:

- To create a subscription
- To manage subscriptions

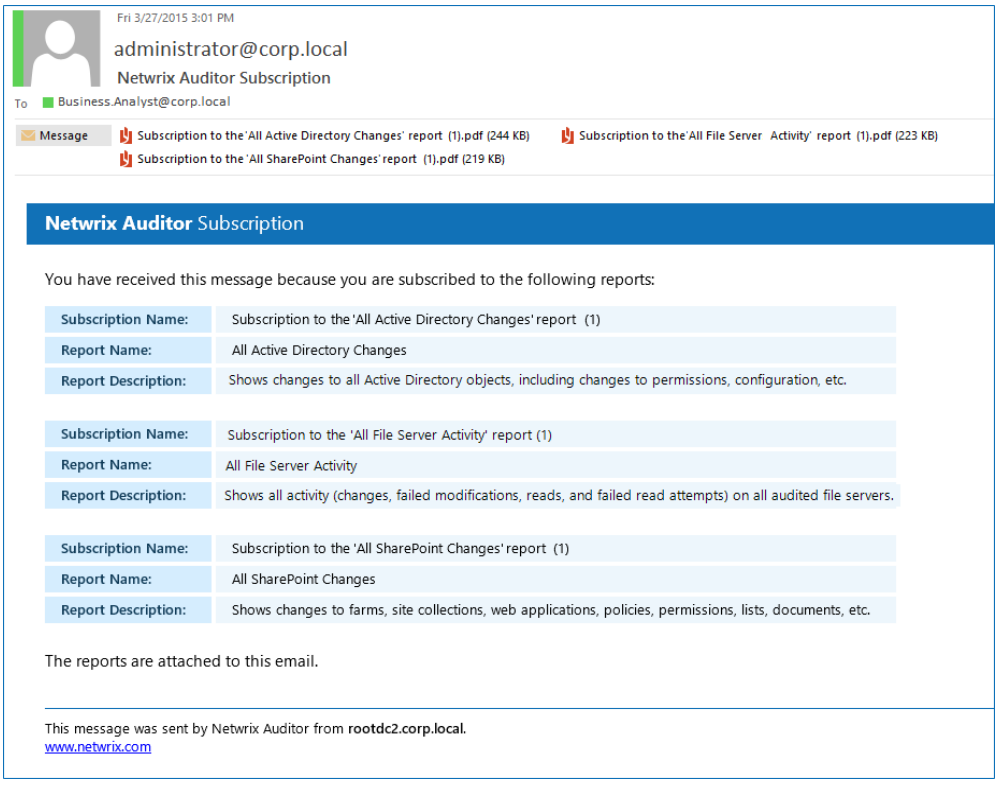
To create a subscription

1. Do one of the following:
   - On the main Netwrix Auditor page, navigate to **Reports**. Specify the report that you want to subscribe to and click **Subscribe**.
   - On the main Netwrix Auditor page, navigate to **Enterprise Overview**. Specify the data source, whose report you want to subscribe to and click **Subscribe**.
2. On the **Subscribe to the 'report_name' report** page, complete the following fields:

Option	Description
Subscription name	Enter the name for the subscription.
Delivery format	Configure reports to be delivered as the pdf, docx, csv or xlsx files.
Send empty reports	Select **Yes** if you want to receive a report even if no changes occurred.
Deliver report to...	Shows the number of recipients selected and allows specifying emails where reports are to be sent. Expand the **Recipients** list and click **Add** to add more recipients.
Every...	Allows specifying report delivery schedule (daily, certain days of week, a certain day of a certain month). **NOTE:** By default, the product emails reports daily at 8.00 am.

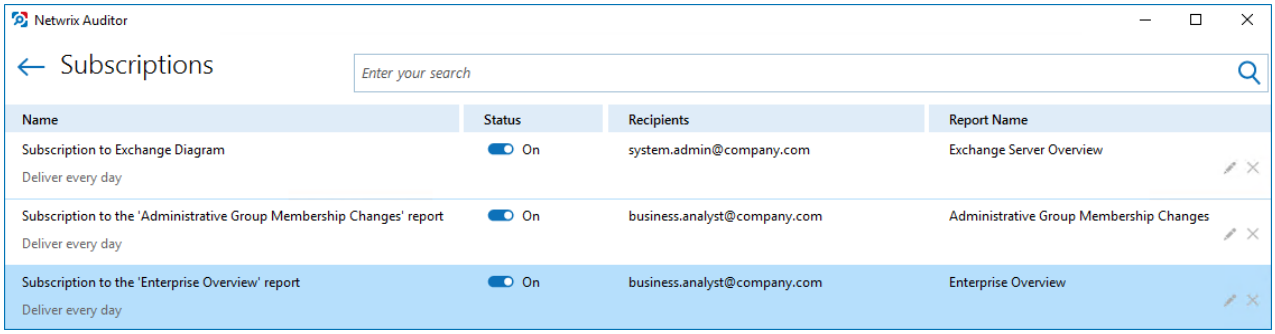
Option	Description
Attach report to email / Upload report to file server	Select report delivery method: • **Attach report to email**—Select this option to receive reports as email attachments. • **Upload report to file server**—Select this option to save reports on the selected file server. Click **Browse** to select a folder on the computer that hosts Netwrix Auditor Server or specify a UNC path to a shared network resource. **NOTE:** Make sure that the recipients have sufficient rights to access it and the Long-Term Archive service account has sufficient rights to upload reports. See Netwrix Auditor Installation and Configuration Guide for more information.
Filters	Specify the report filters, which vary depending on the selected report.

NOTE: Subscription emails may vary slightly depending on reports delivery method.



To manage subscriptions

- On the main Netwrix Auditor page, navigate to **Subscriptions** to review a list of your subscriptions.



The table below provides instructions on how to manage your subscriptions.

To...	Do...
Browse subscriptions	Type the target subscription name in the search bar in the upper part of the **Subscriptions** window and click the **Search** icon to review results.
Enable or disable subscriptions	Select a subscription and check or clear the **Enabled** checkbox in the **Status** column.
Modify subscriptions	Click icon next to the selected subscription. Edit the subscription parameters and save your changes.
Remove subscriptions	Click icon next to the selected subscription.

7. Overview Dashboards

Overview dashboards offer a bird's eye view of your IT infrastructure. They allow you to see activity trends by date, user, object type, server or data source, and drill down to detailed reports for further analysis.

The **Enterprise Overview** diagram aggregates data on all monitoring plans and all data sources, while system-specific diagrams provide quick access to important statistics within one data source.

NOTE: To review intelligence data, you must be assigned the Global administrator or Global reviewer role in the product. The users assigned the Reviewer role on a certain plan or folder have a limited access to data—only within a delegated scope. See Netwrix Auditor Administration Guide for more information.

The current version of Netwrix Auditor contains the following diagrams:

- Enterprise (aggregates data on all data sources listed below)
- Active Directory
- Azure AD
- Exchange
- File Servers (includes Windows File Servers, EMC, and NetApp)
- Office 365 (includes Exchange Online and SharePoint Online)
- Oracle Database
- SharePoint
- SQL Server
- VMware
- Windows Server

NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Netwrix Auditor Global administrator to import that data from the Long-Term Archive.

All diagrams provide the drill-down functionality, which means that by clicking on a segment, you will be redirected to a report with the corresponding filtering and grouping of data that renders the next level of detail.

To review the Enterprise Overview diagram

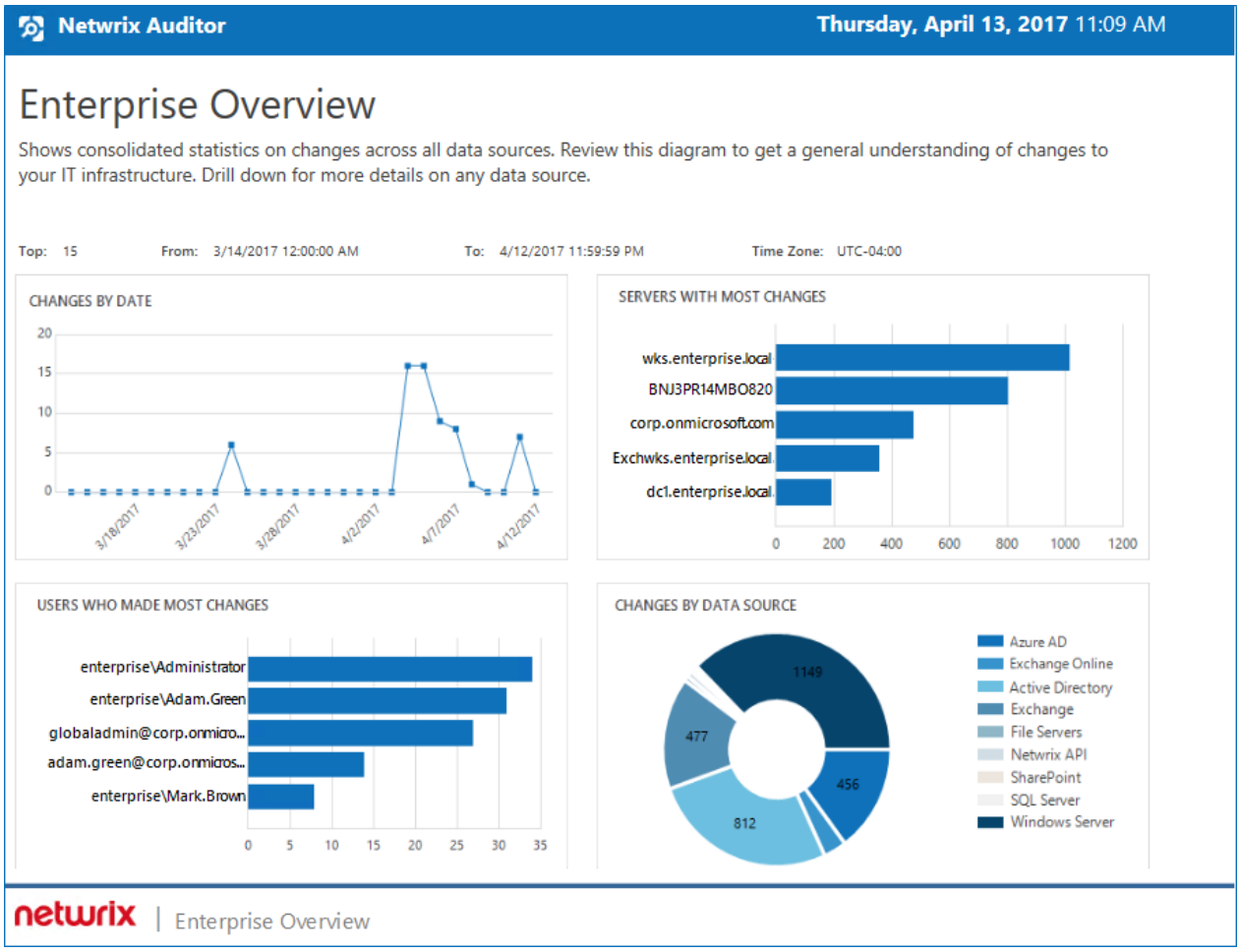
- On the main Netwrix Auditor page, click the **Enterprise Overview** tile.

To review the data source-specific diagrams

- Navigate to **Reports** and select one of the following locations:

Title	Location
Enterprise Overview	**Organization Level Reports**
Active Directory Overview	**Active Directory** → **Active Directory Changes**
Azure AD Overview	**Azure AD**
Exchange Overview	**Exchange**
Office 365 Overview	**Exchange Online** **SharePoint Online**
File Servers Overview	**File Servers** → **File Servers Activity**
Oracle Database Overview	**Oracle Database**
SharePoint Overview	**SharePoint**
SQL Server Overview	**SQL Server**
VMware Overview	**VMware**
Windows Server Overview	**Windows Server** → **Windows Server Changes**

NOTE: The example below applies to **Enterprise Overview**.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Leverage Filtering Capabilities for more information. You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

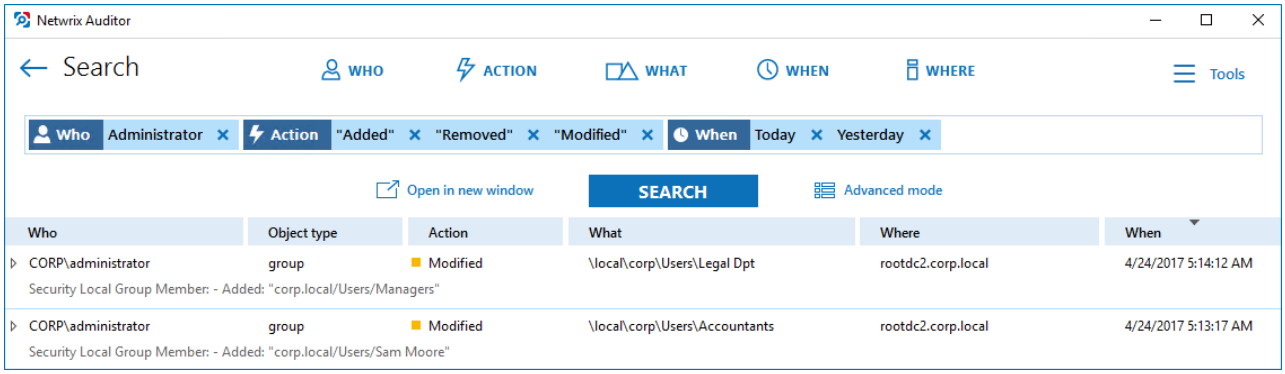
8. Saved Searches

Netwrix Auditor allows you to save your favorite searches to access them instantly. For your convenience, the product provides predefined searches for some popular usage scenarios. Refer to Interactive Search for detailed instructions on how to create searches.

Moreover, saved searches are shared between all Netwrix Auditor clients that have access to the same Netwrix Auditor Server (the main component responsible for collecting and processing audit data).

You can save your custom searches or use one of predefined saved searches. Predefined searches can be found in the **Intelligence** section. Click the search tile to run this search.

NOTE: The example saved search results apply to **AD or Group Policy modifications by admin yesterday**. Other saved search results generated by Netwrix Auditor may vary depending on the data source and applied filters.



Review the following for additional information:

- To save a custom search
- To modify a saved search
- To delete a saved search

To save a custom search

1. On the main Netwrix Auditor page, navigate to **Search**.
2. Apply filters and click **Search**.

   NOTE: Refer to Interactive Search for detailed instructions on how to apply filters and search audit data.

3. Navigate to **Tools** and select **Save Search**.
4. In the **Specify a name for your saved search** dialog, specify a name. Make sure to specify a unique name.

To modify a saved search

1. On the main Netwrix Auditor page, navigate to **Intelligence** section.
2. Select one of the searches and click its tile to open search results.
3. Modify filters and click **Search**.

   NOTE: Refer to Interactive Search for detailed instructions on how to apply filters when searching audit data.
4. Navigate to **Tools** and select **Save Search**.
5. In the **Specify a name for your saved search** dialog, specify a name. Netwrix Auditor automatically offers a previously used search name so that this saved search will be overwritten. If you want to save both searches, specify a unique name for a modified search.

To delete a saved search

- In the **Intelligence** section, select a saved search and click ✕ on its tile.

9. Troubleshoot Issues

This section provides instructions on how to troubleshoot issues that you may encounter while using Netwrix Auditor. Review the following for additional information:

Issue	Reason and solution
I cannot connect/logon to Netwrix Auditor.	1. You may have insufficient permissions. Contact your Netwrix Auditor Global administrator to make sure that your account is delegated control of the product. 2. You are trying to connect to a remote Netwrix Auditor Server specified by its IP address while the NTLM authentication is disabled. Try specifying a server by its name (e.g., EnterpriseWKS).
I do not receive any results while searching audit data or generating reports, or I am sure that some data is missing.	1. No changes were detected. 2. You do not have sufficient permissions to review intelligence data. Contact your Global administrator. 3. Review your filter settings and make sure that your filters are properly configured. Try modifying your search. 4. You are looking for changes that occurred more than 180 days ago. These changes are no longer available for reporting and running searches. Ask your Netwrix Auditor Global administrator to import audit data for a required date range from the Long-Term Archive. 5. Data collection for this monitoring plan might not have been launched two times yet or there was no data collection after this change; therefore, audit data has not been written to the Audit Database yet. 6. Some settings in Netwrix Auditor are configured incorrectly. Contact your Netwrix Auditor administrator to make sure that: • The monitoring plan you want to audit is properly configured, and the monitoring is enabled for each data source individually. • Audit Database settings are properly configured for each data source individually and **Disable security intelligence and make data available only in activity summaries** is cleared.

Issue	Reason and solution
	NOTE: Netwrix recommends to store all audit data on the same default SQL Server instance.
"No plans found" text in the Monitoring plan field.	Contact your Netwrix Auditor Global administrator or Configurator to make sure that the monitoring plans exist and are properly configured.
I see a blank window instead of a report.	Contact your Netwrix Auditor Global administrator to make sure that you are granted sufficient permissions on the Report Server.
I configured report subscription to be uploaded to a file server, but cannot find it / cannot access it.	Subscriptions can be uploaded either to a file share (e.g., *filestorage**reports*) or to a folder on the computer where Netwrix Auditor Server is installed. To access these reports, you must be granted the **Read** permission.

Index

T