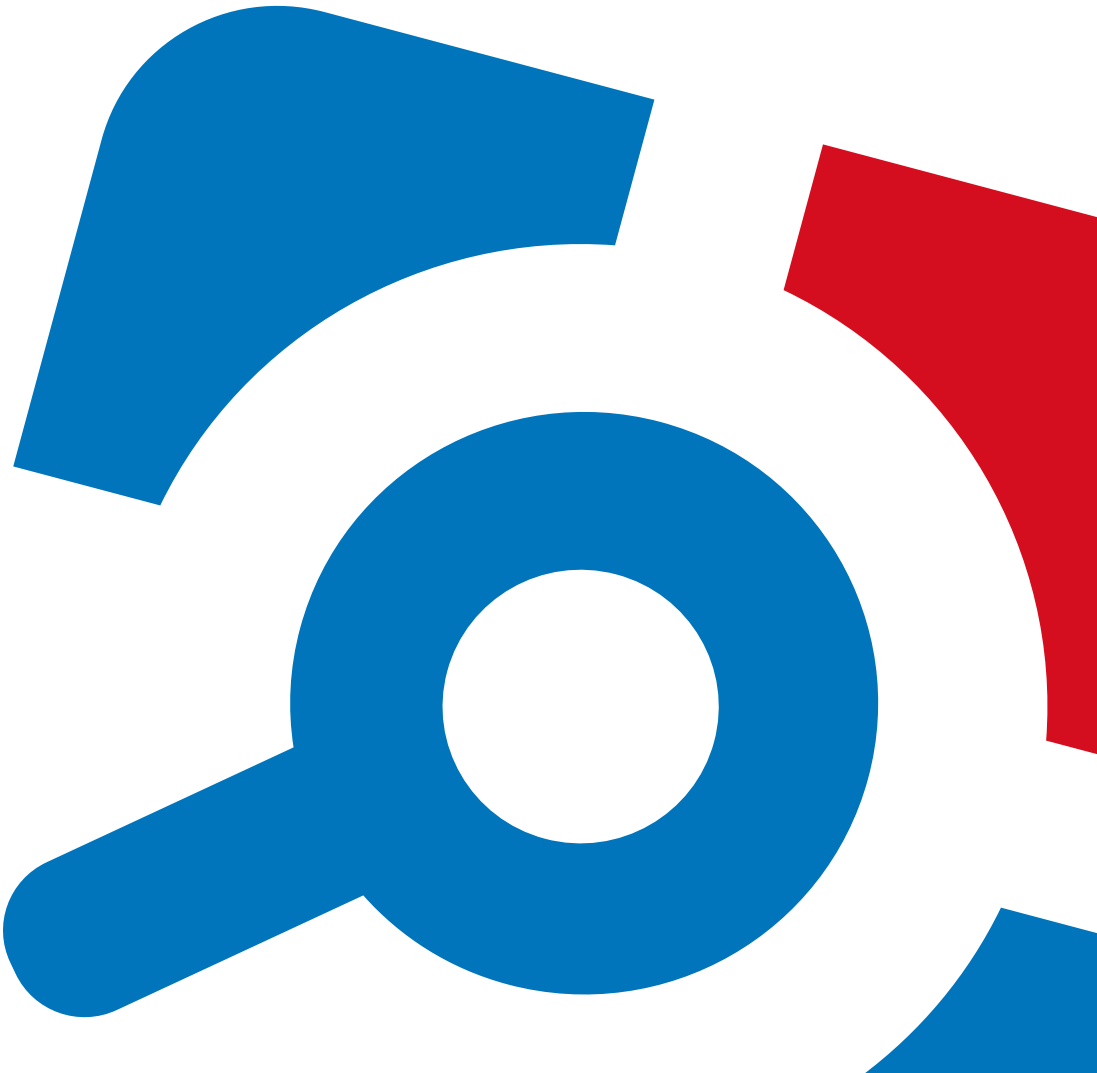
netwrix

Netwrix Auditor

User Guide

Version: 8.0
5/17/2016



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 users 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 AuditIntelligence search
- Generate reports and add filters
- Subscribe to important reports you want to receive on a regular basis

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.

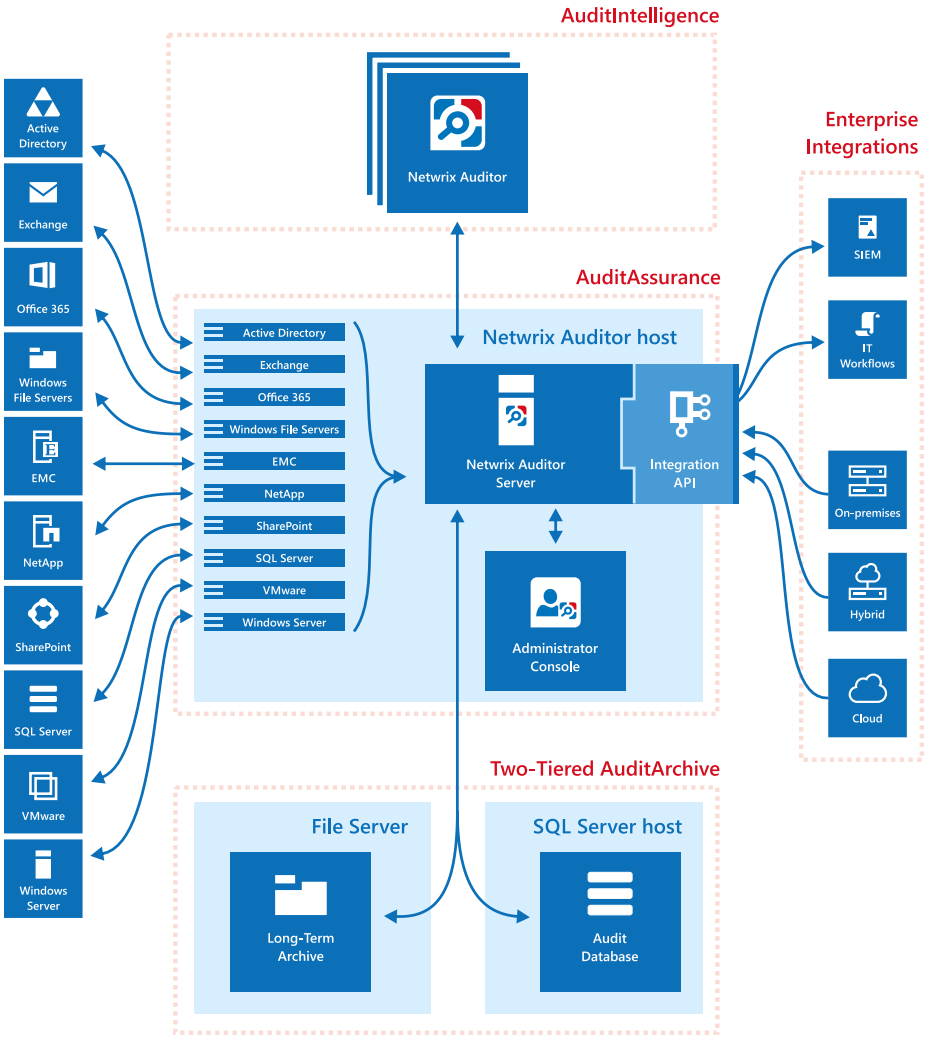
- **Predefined reports and diagrams:** Netwrix Auditor includes more than 150 predefined reports and diagrams. Reports can be exported to a range of formats, including PDF and XLS, and stakeholders can subscribe to reports to stay informed automatically by email.
- **AuditArchive™:** Netwrix Auditor's 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.

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

Application	Features
	access attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7- modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for 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

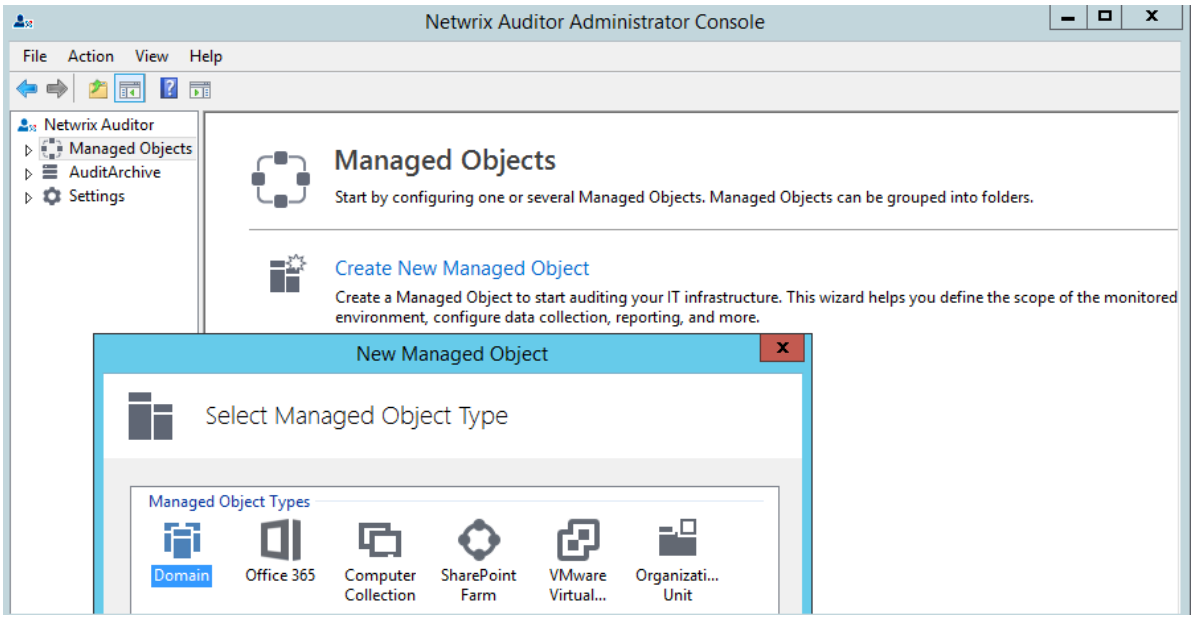
A user who installed Netwrix Auditor Administrator Console is referred to as Netwrix Auditor administrator.

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.

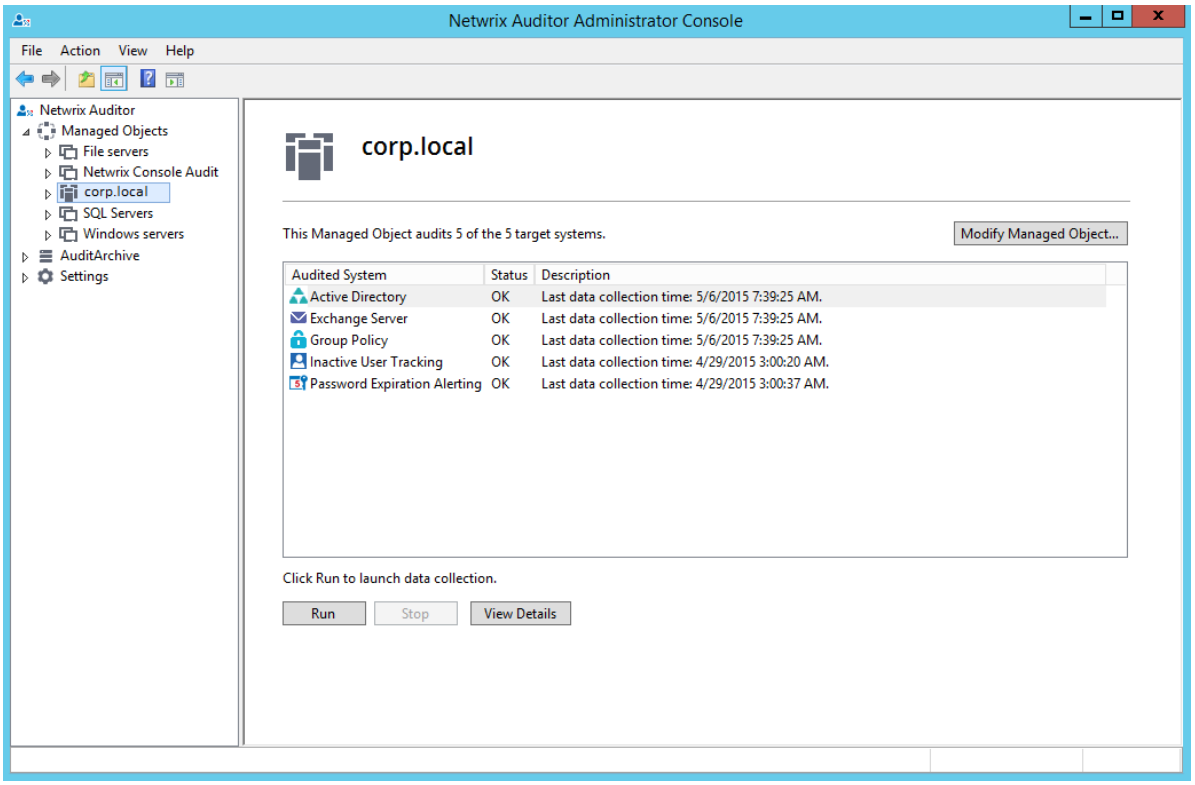
See Netwrix Auditor Installation and Configuration Guide for more information.

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.



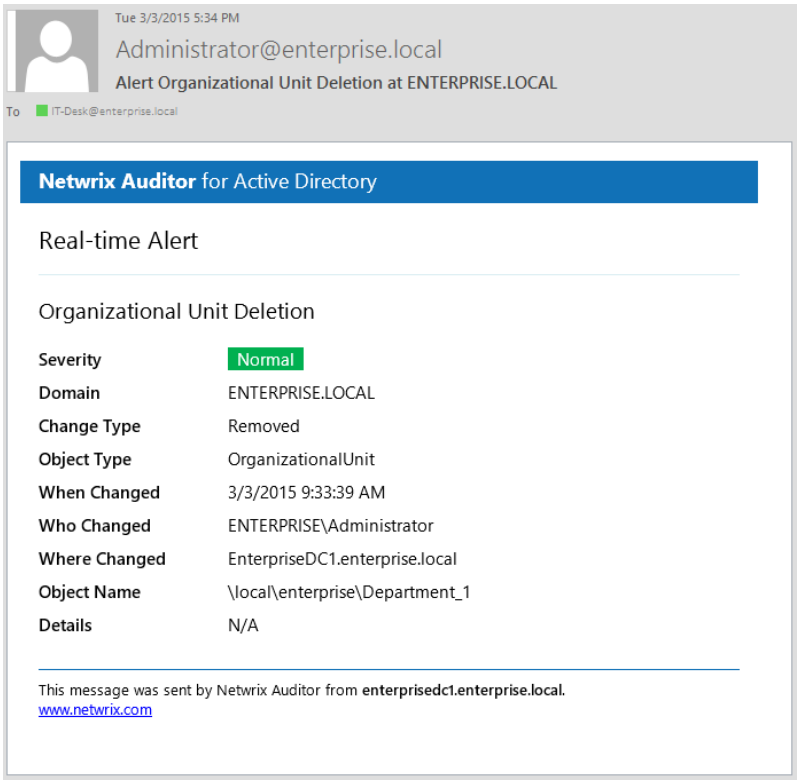
2. The administrator configures the **Audit Database** settings (SQL Server and SSRS settings).
3. Netwrix Auditor audits IT infrastructure and collects data on changes and state-in-time configuration snapshots.



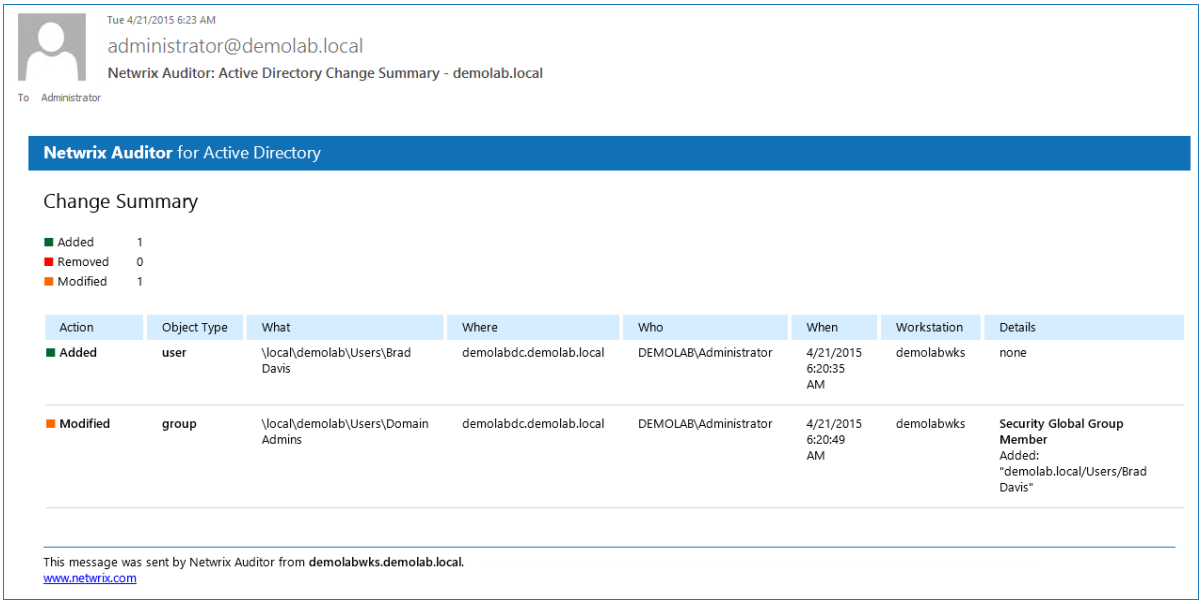
NOTE: Collected audit data is written to the AuditArchive that includes both the file-based Long-Term Archive and the short-term SQL Server-based Audit Database.

4. For some audited systems, the administrator can configure alerts to be triggered if some critical

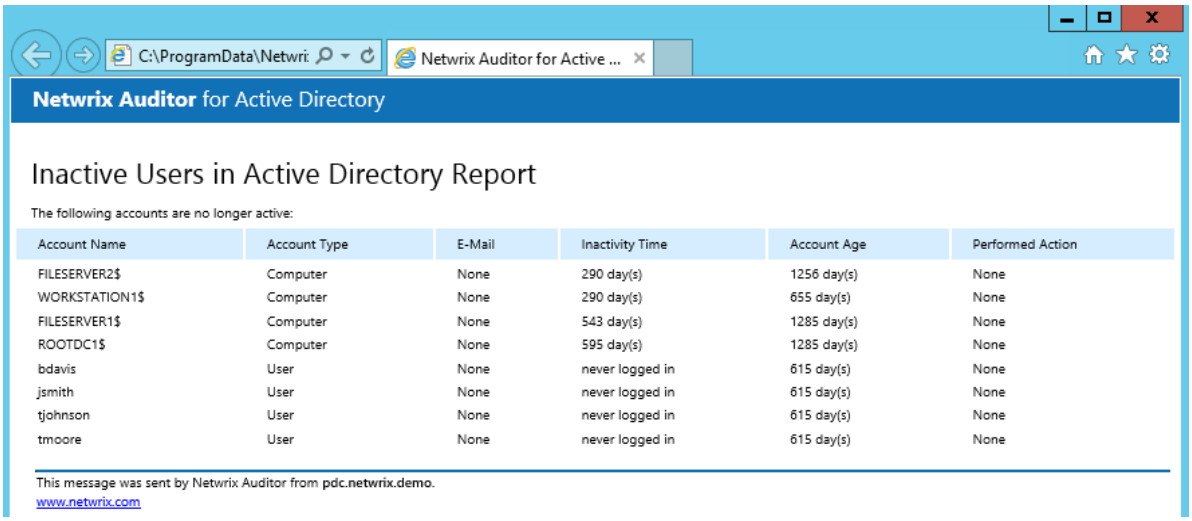
event is detected. In this case an email notification is sent immediately to the specified recipients.



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.



6. The administrator can generate ad-hoc reports to detect inactive users and expiring passwords.



See Netwrix Auditor Administrator's Guide 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.

2. Launch the Product

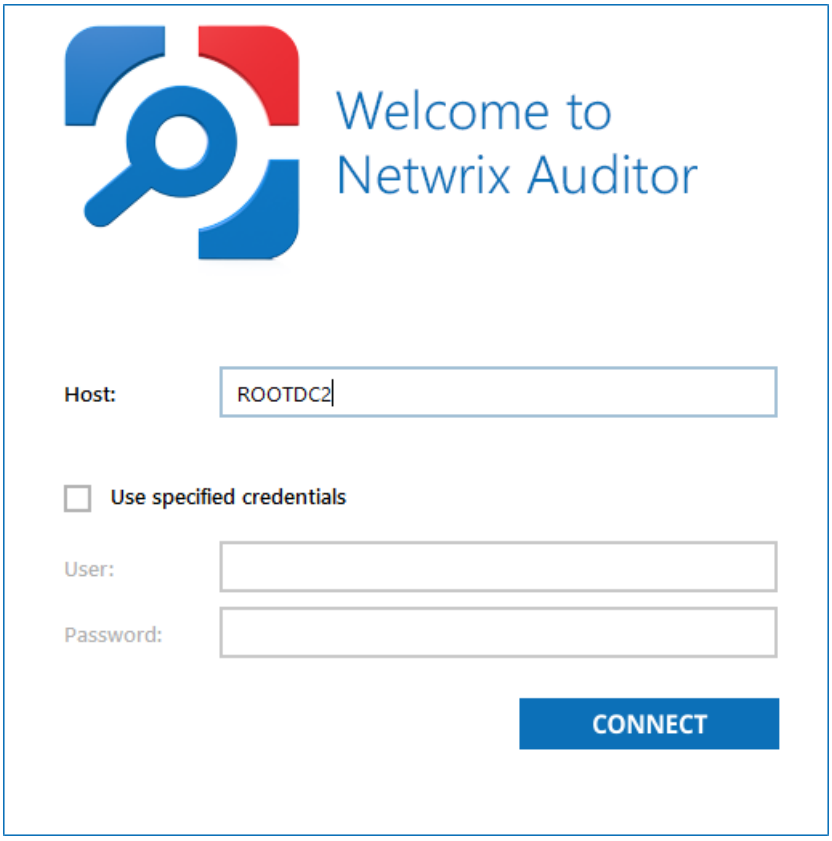
To start using Netwrix Auditor

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

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

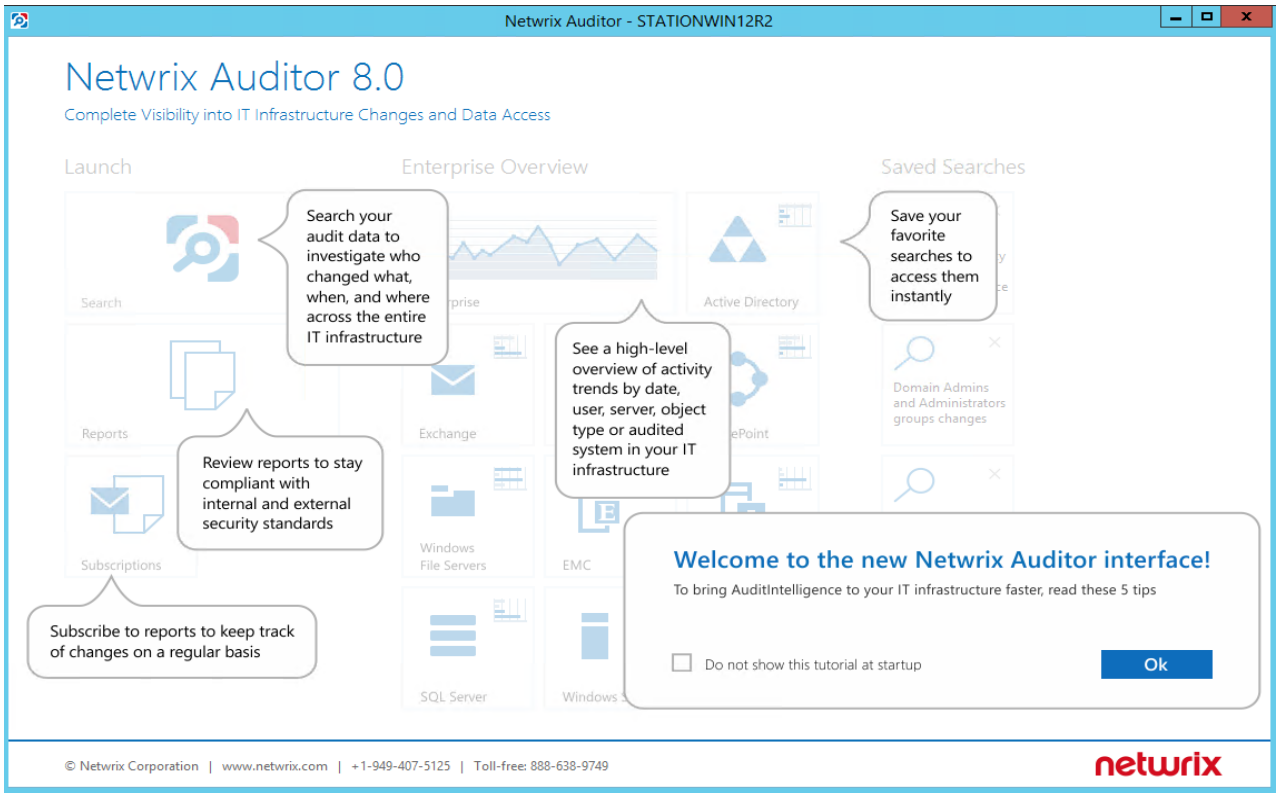
   You can configure a single Netwrix Auditor client to work with several Netwrix Auditor Servers. To switch to another server, reopen the Netwrix Auditor client and provide another host name (e.g., rootdc2, WKSWin12r2.enterprise.local).

   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:



Read these tips to get started faster. Review the following for additional information:

- AuditIntelligence Search
- Reports
- Subscriptions
- Enterprise Overview
- Saved Searches

3. AuditIntelligence Search

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

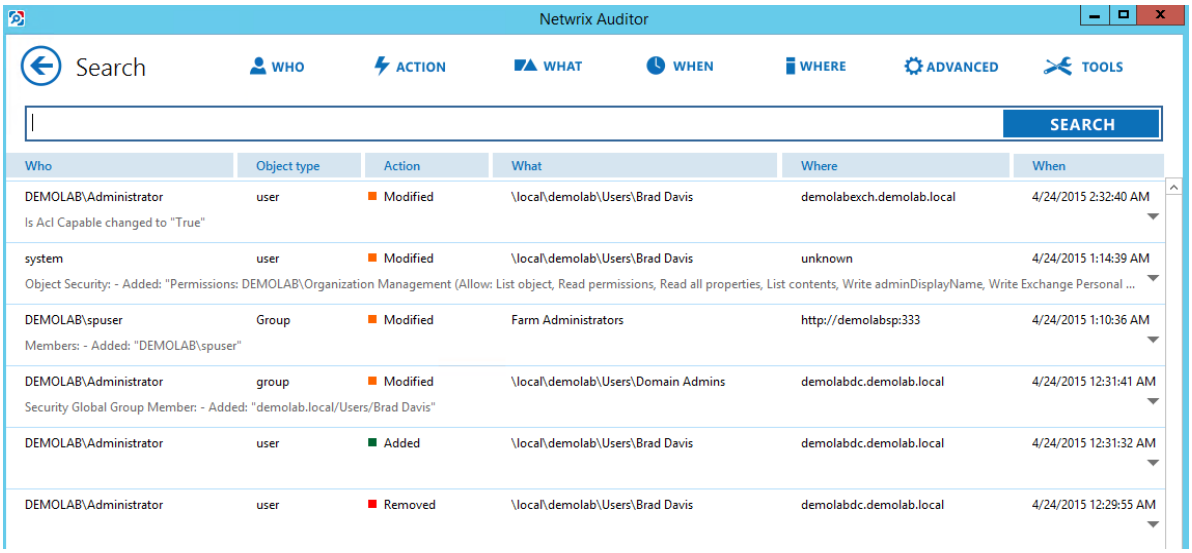
This functionality is currently available for the following audited systems:

- Active Directory
- Exchange
- Exchange Online (Office 365)
- File Servers (Windows File Servers, EMC, and NetApp)
- SharePoint
- 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.

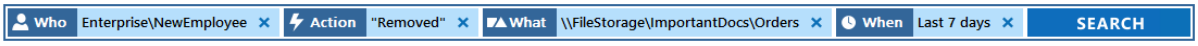
NOTE: Netwrix Auditor shows only the top 2,000 entries in the search results.

To browse your audit data

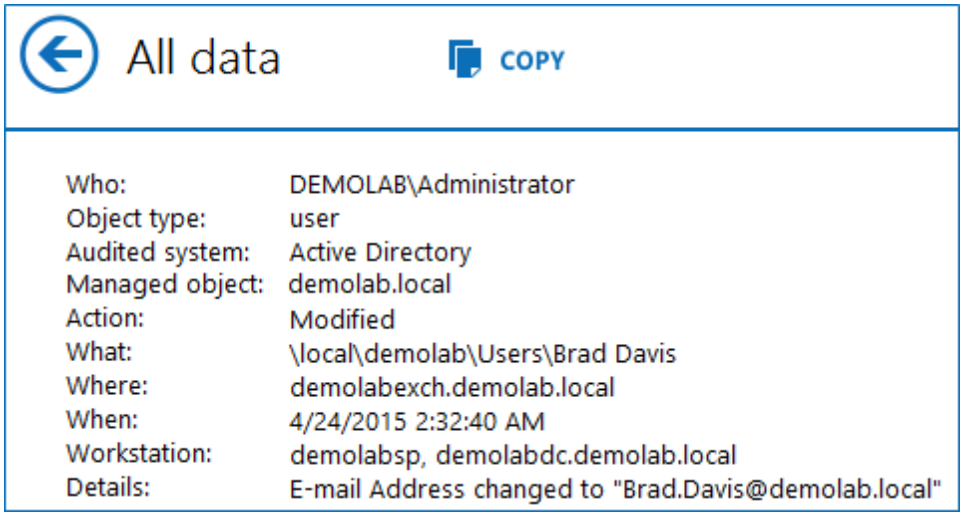
1. On the main Netwrix Auditor page, navigate to **Search**.
2. Do one of the following:
    - Click **Search** to see all audit data stored in the Audit Database. Once the data is retrieved, you can exclude certain entries from the results. See Include and Exclude Data for more information.



- 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**.



   - Click **Show video...** below the User Activity entry to to see all information regarding this change and copy it if necessary. For User Activity entries, watch 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 VMware infrastructure in reports and search results), contact your Netwrix Auditor administrator. The administrator must verify that the Audit Database settings are configured in Netwrix Auditor Administrator Console and that audit data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running AuditIntelligence 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 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.

3.1. Apply Filters

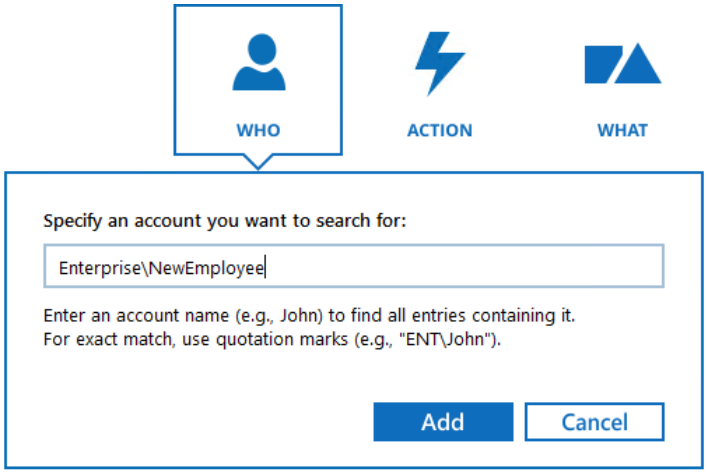
Filters are used to narrow your search results. To create a unique set of filters, you can:

- 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.

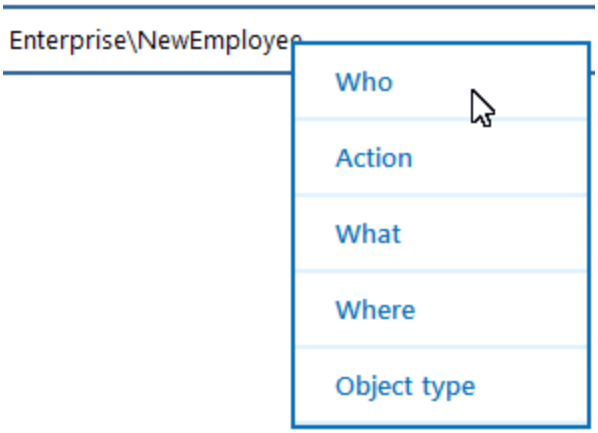
NOTE: Spaces do not separate values, so the whole expression will be included in your search as a single value. For example, if you want to search for any of three names, do not enter *Anna Mark Bill* but instead create a separate filter entry for each name.

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 (**Who**, **What**, **Where**, **Action**, etc.) except those for which filters are explicitly specified.



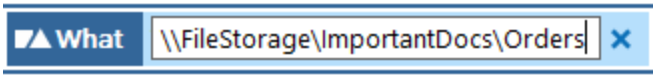
2. Click **Search** to apply your filters. By default, all entries that contain the filter value are shown. For an exact match, use quotation marks. See Advanced View for more information on additional filters and match types.

Filter	Description
WHO	Specify an account name (e.g., *John*) to find all entries containing it (e.g., *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*). For an exact match, use quotation marks and provide a user name in Domain\User format (e.g., *"Domain1\John"*) .
ACTION	Select an action type from the list (Added, Removed, Modified, Read). For additional actions, navigate to **Advanced**. See Advanced View 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 audited systems. For an exact match, use quotation marks and provide an object name in the format that is typical for your audited system (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.

Filter	Description
WHERE	Specify a resource name (e.g., *Enterprise*) to find all entries containing it (e.g., *Enterprise-SQL*, *FileStorage.enterprise.local*). The resource name can be a FQDN or NETBIOS server name, Active Directory domain or container, SQL Server instance, SharePoint farm, VMware host, etc. **NOTE:** Netwrix Auditor searches across all audited systems. For an exact match, use quotation marks and provide a resource name in the format that is typical for your audited system (e.g., *"Enterprise-SQL"*).

To modify a filter value

- Double-click it and type a new value.



NOTE: The **When** filter cannot be modified. Delete it and add a new value.

To remove a filter

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

3.2. Advanced View

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

Navigate to **Advanced** to review your current search in the **Advanced** view 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. Review the following for additional information:

Filter	Description	Example
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.	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://sharepoint/sites/col1/Lists/Policy* . These entries correspond to different object types and audited systems. Since you are looking for GPOs only, select **GroupPolicy** from the **Value** list.
Audited system	Limits your search to the selected audited system only. Specify an audited system 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 **Audited system** filter to **Active Directory** and **Exchange** to limit the search results.
Managed object	Limits your search to the selected Managed Object 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 Managed Object, set the **Managed Object** filter to *"My Computer Collection"* to limit the search results.
Details	Limits your search results to entries that contain the specified information in the **Details** column.	You discovered that a registry key was updated to *"242464"*. Now you want to investigate who made the change and

Filter	Description	Example
	The **Details** column normally contains data specific to your audited system, 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.	what the value was before. You can set the **Details** filter to *242464* to find this change faster.
Before	Limits your search results to entries that contain the specified before value in the **Details** column.	You are investigating an incident in which the SAM-account-name attribute was changed for an account in your Active Directory domain. You can set the **Before** filter to the previous name (e.g., *John2000*) to find the new name faster.
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.

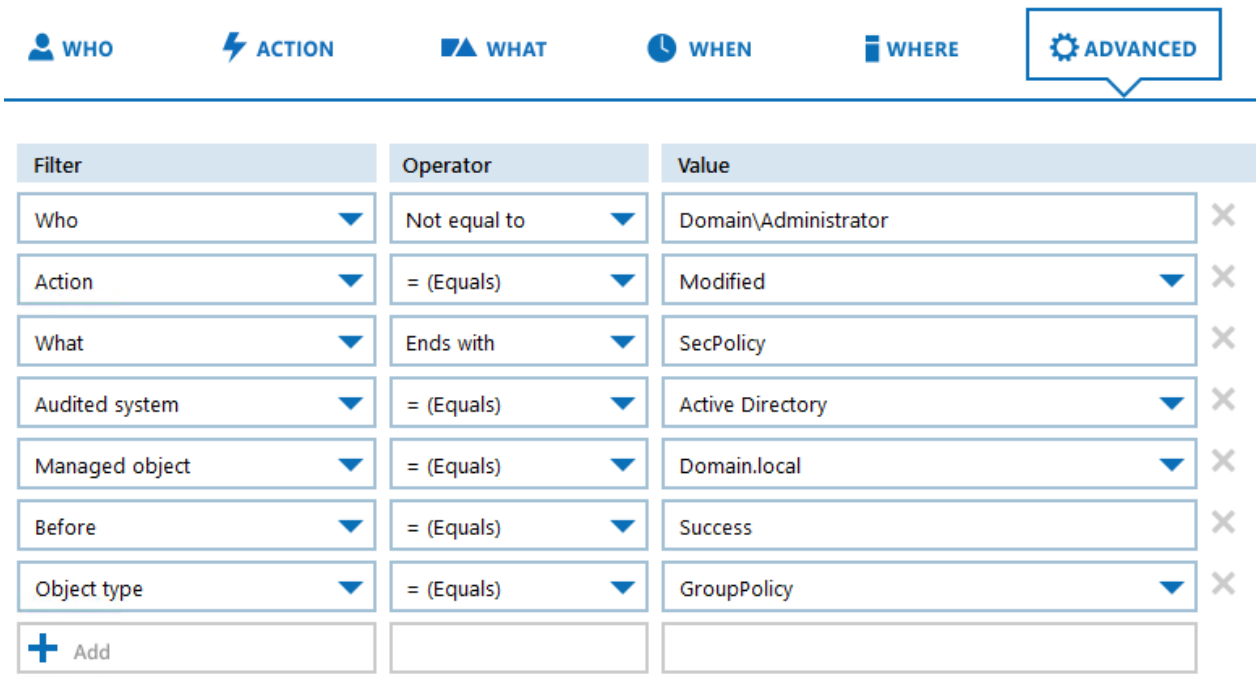
3.2.2. Change Match Types

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

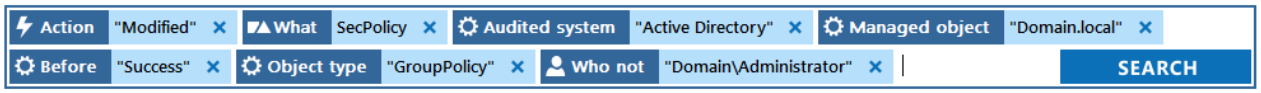
Operator	Description	Example
Contains	This broad match operator shows all entries that include a value specified in the filter.	Set the **Who** filter to **contains** *John*, to get the following results: *Domain1\John*, *Domain1\Johnson*, *Domain2\Johnny*.
Equals	This exact match operator shows all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

Operator	Description	Example
	NOTE: To apply this operator when adding filters in the **Search** field, 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, this operator appears as **Who not**.	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, this operator appears as **Who not**.	Set the **Who** filter to **does not contain** *John* to exclude the following users, *Domain1\John*, *Domain2\Johnson*, and *Domain3\Johnny*.

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



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



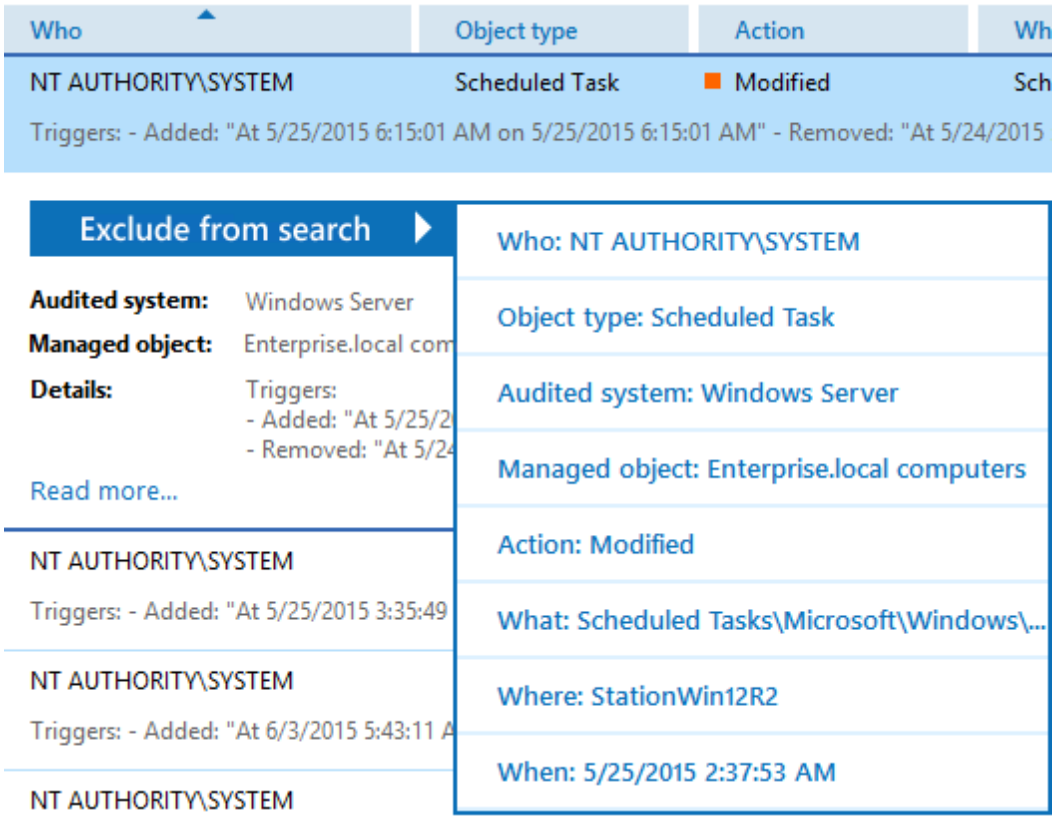
3.3. Include and Exclude Data

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.
Export data	Save your search results as a pdf or csv file. 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. Reports

4.1. 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.).

NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your VMware infrastructure in reports and search results), contact your Netwrix Auditor administrator. The administrator must verify that the Audit Database settings are configured in Netwrix Auditor Administrator Console and that audit data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running AuditIntelligence 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 administrator to import that data from the Long-Term Archive.

4.1.1. Report Types

In Netwrix Auditor, 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. 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 Enterprise Overview for more information.
- **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. See Change and Activity Reports for more information.
- **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. See State–in–Time Reports for more information.

- **Changes with Video**—Provide video recordings of user activity on audited computers. See Reports with Video for more information.
- **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. 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 AuditIntelligence Search for more information. You can also order custom report templates from Netwrix.

4.1.2. 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 that provide a general overview of your entire 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 change reports.

Exchange	Contains a set of reports on Exchange Server changes. Use these reports to track changes in your Exchange organization and ensure its health and security. Includes the following reports:

Folder	Reports
	• Overview diagram • Change and activity reports • Changes with review status
Exchange Online	Contains a set of reports on Exchange Online changes. Use these reports to track changes in your Exchange Online organization and ensure its health and security. Includes the following reports: • Overview diagram • 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
	NOTE: The following reports can be generated for Windows file servers only: Account Permissions, Object Permissions by Object, and Excessive Access Permissions.

SharePoint	Contains a set of reports on SharePoint changes, including changes to content, configuration and access permissions. Includes the following reports: • Overview diagram • Change and activity reports • Changes with review status
SQL Server	Contains a set of reports on SQL Server changes. Includes the following reports: • Overview diagram • Change 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

Folder	Reports
	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 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: • **FISMA/NIST Compliance** • **HIPAA Compliance** • **ISO/IEC 27001 Compliance** • **PCI DSS v3.0 Compliance** • **SOX Compliance**	For your convenience, contains reports mentioned above but grouped by corresponding international standards and regulations: • **FISMA/NIST SP800-53 rev4** • **HIPAA** • **ISO/IEC 27001** • **PCI DSS v3.0** • **SOX** **NOTE:** Click **Compliance** above the list of reports to see reports grouped by compliance standards only. See Compliance Reports for more information.

To view reports in a web browser

1. Open a web browser and type the Report Manager URL. 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.

4.1.3. Customize Report with Filters

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

To apply filters

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

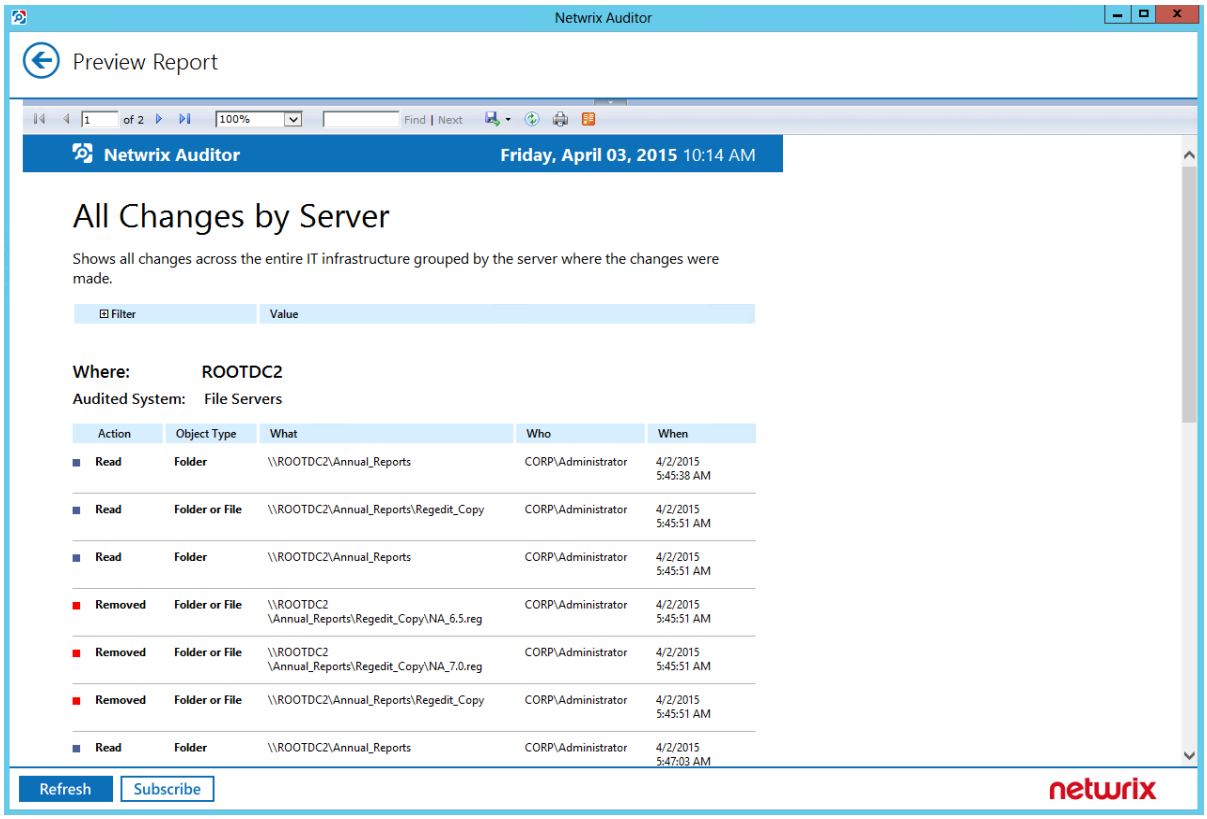
Wildcards are supported. For example, type *%corp\administrator%* in the in the **Who domain\user** field if you want to view changes made by the **corp\administrator** user only .

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

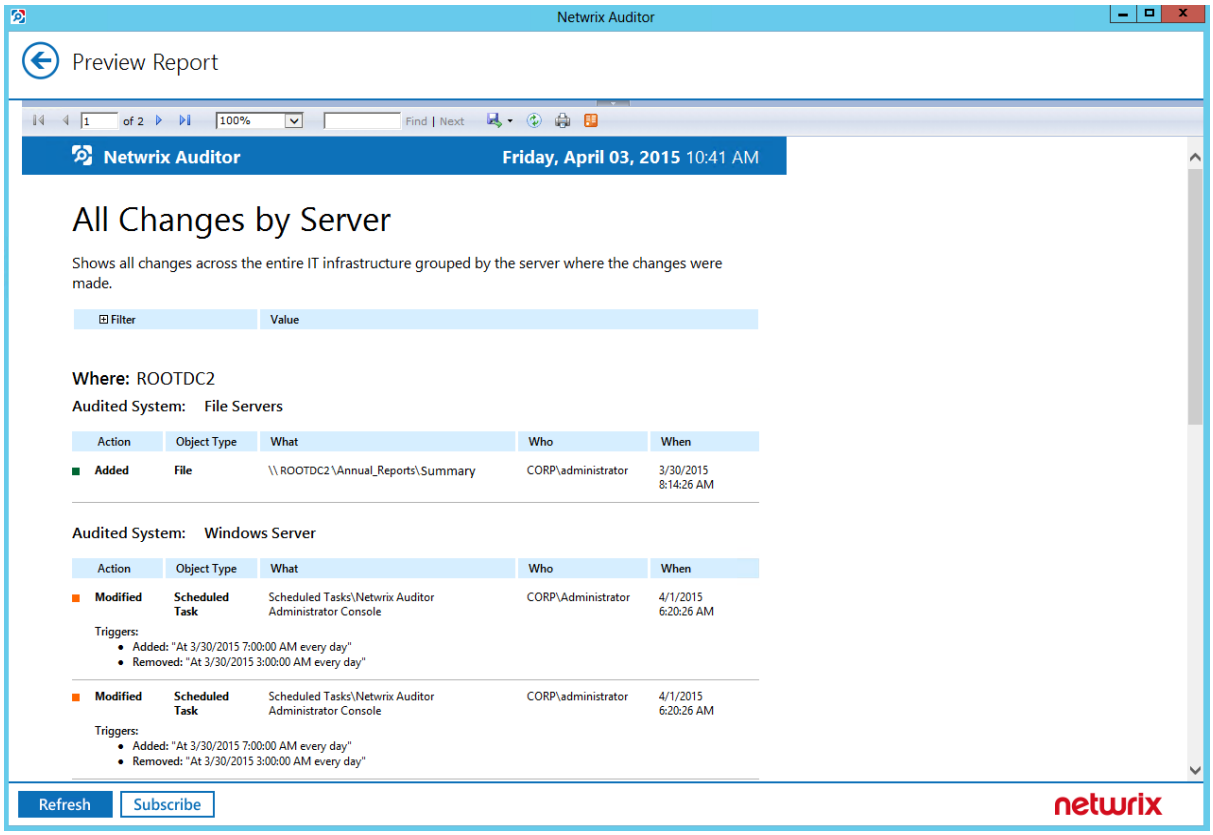
NOTE: *escape_characters* are not supported.

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 audited system and report type.

The report without filtering:



The report below displays changes for all audited systems made by the **CORP\Administrator** user on the **ROOTDC2** domain controller for a month sorted by the action type.



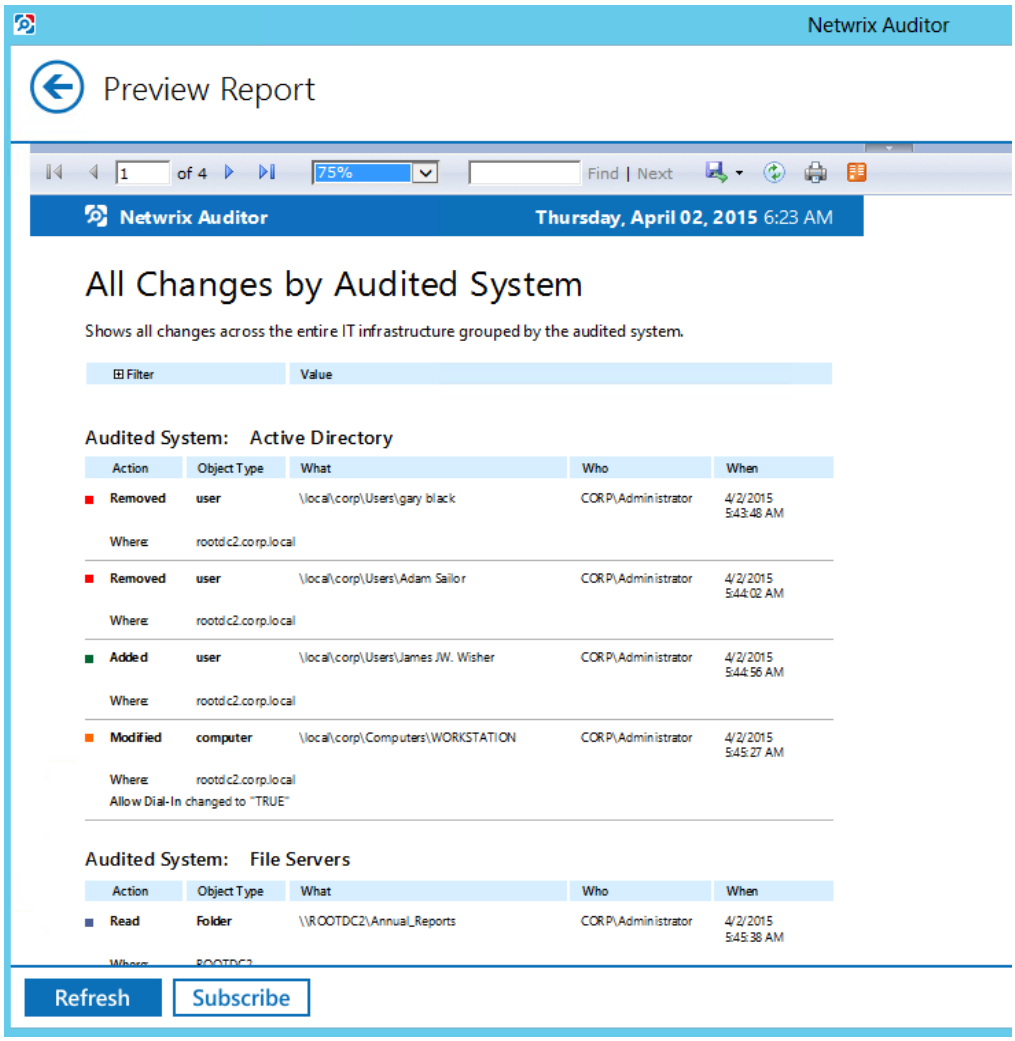
4.2. Organization Level Reports

Organization Level reports aggregate data on all Managed Objects and list changes that occurred across all audited systems.

NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your VMware infrastructure in reports and search results), contact your Netwrix Auditor administrator. The administrator must verify that the Audit Database settings are configured in Netwrix Auditor Administrator Console and that audit data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running AuditIntelligence 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 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.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Customize Report with Filters 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.

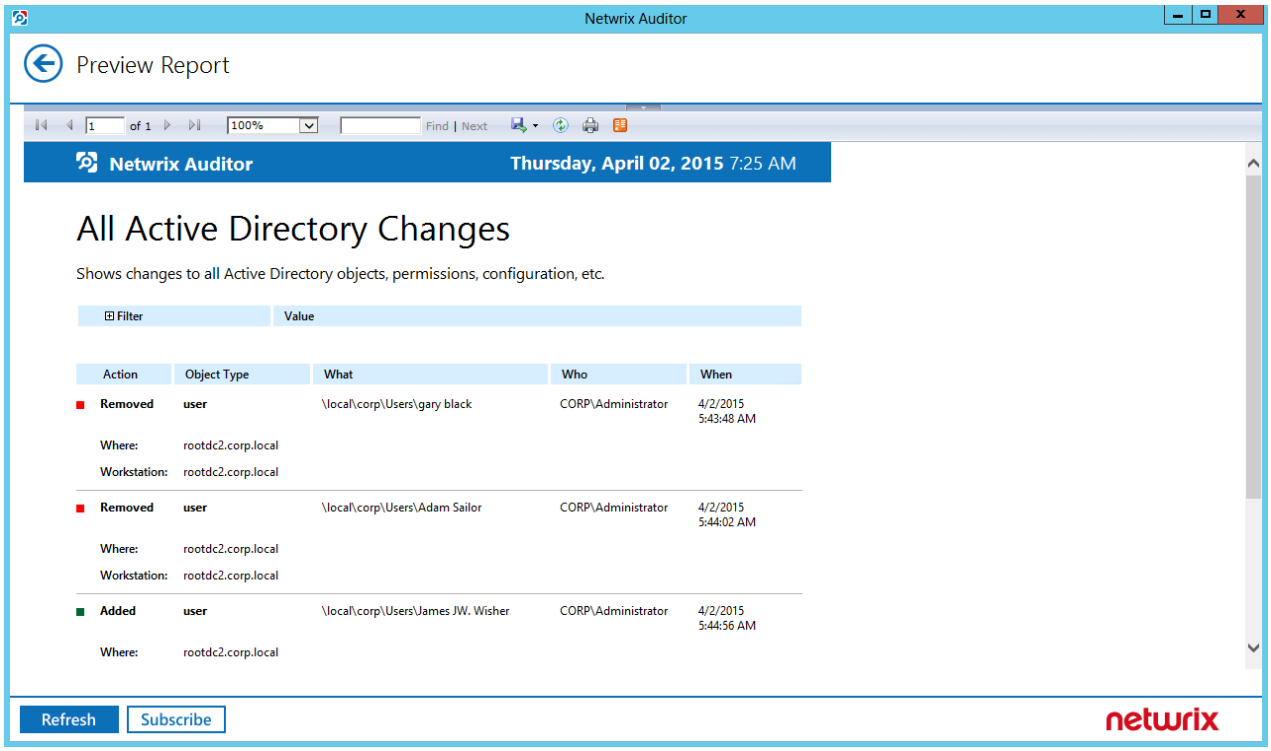
4.3. Change and Activity Reports

Change reports provide information on changes to different aspects of the audited environment. Some audited systems provide activity reports as well. Some audited

Depending on the audited system, navigate to one of the following locations:

Audited system	Report location
Active Directory	**Active Directory** → **Active Directory Changes**
Group Policy	**Active Directory** → **Group Policy Changes**
Exchange	**Exchange**
Exchange Online	**Exchange Online**
File Servers	**File Servers** → **File Servers Activity**
SharePoint	**SharePoint**
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**

NOTE: Select a Managed Object you want to generate a report for in the report filters. Contact your Netwrix Auditor administrator to learn more about auditing scope for each Managed Object.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Customize Report with Filters 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.

4.4. State–in–Time Reports

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

This functionality is currently available for the following audited systems:

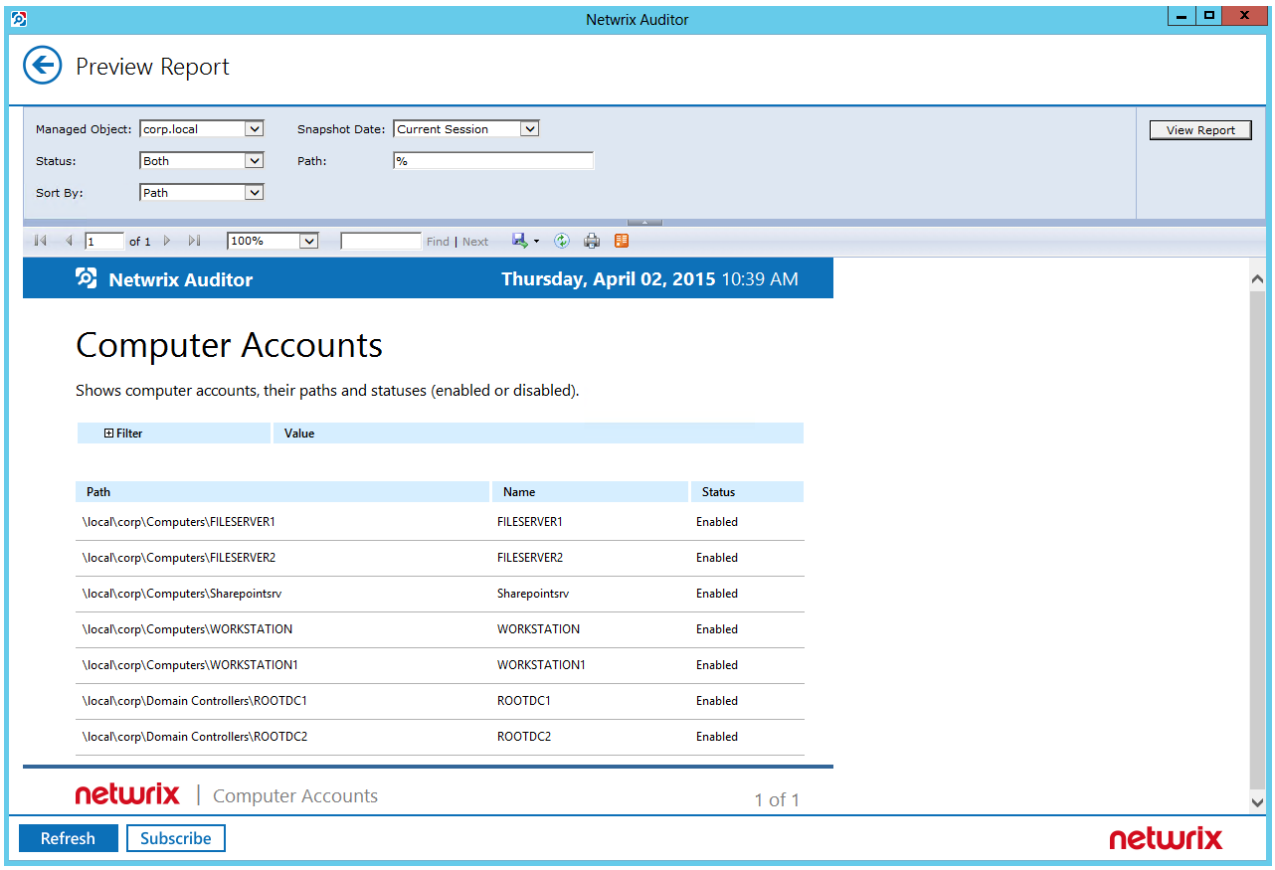
- Active Directory
- File Servers
- Group Policy

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

Audited system	Report location
Active Directory	**Active Directory** → **Active Directory State-in-Time**

Audited system	Report location
Group Policy	**Active Directory** → **Group Policy State-in-Time**
File Servers	**File Servers** → **File Servers State-in-Time** **NOTE:** The following reports can be generated for Windows file servers only: Account Permissions, Object Permissions by Object, and Excessive Access Permissions.

NOTE: Select a Managed Object you want to generate a report for in the report filters. Contact your Netwrix Auditor administrator to learn more about auditing scope for each Managed Object.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Customize Report with Filters 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 audited system. 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 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 administrator.

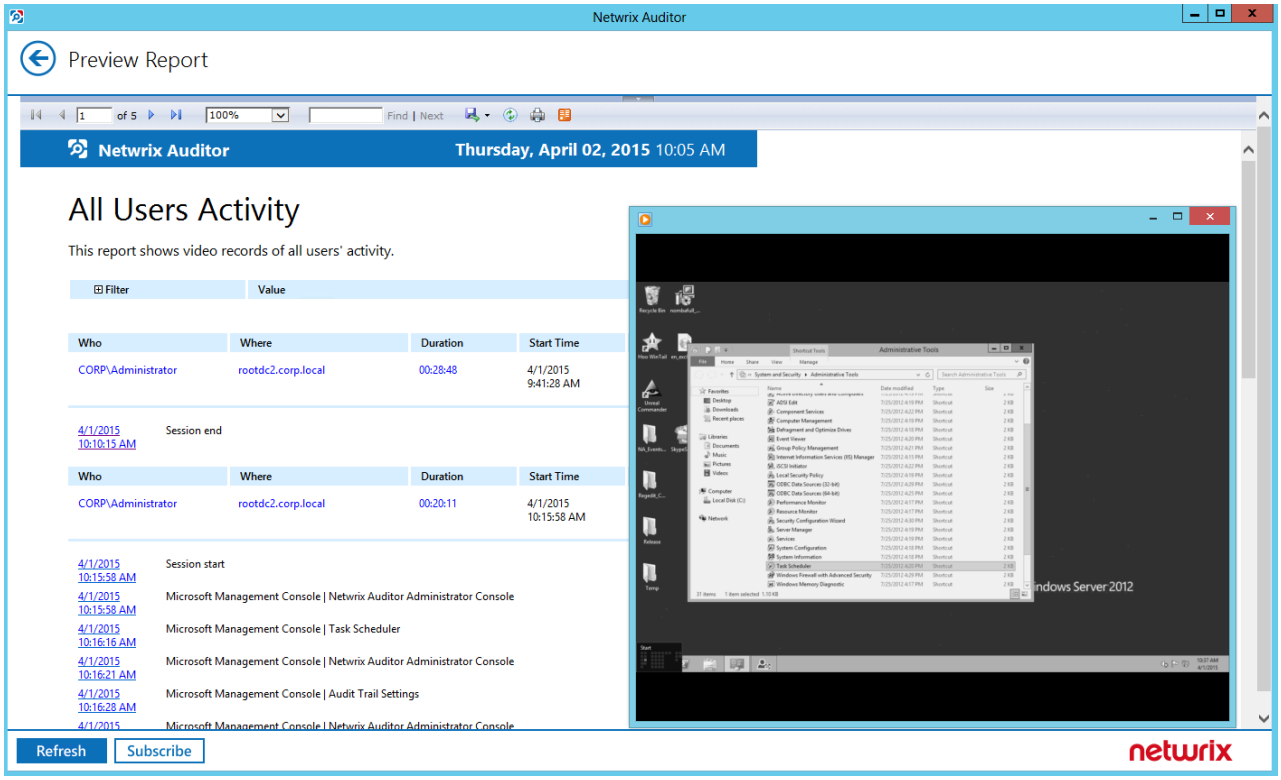
4.5. Reports with Video

Netwrix Auditor can be configured to capture video of user activity on the audited 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.

NOTE: To configure users activity auditing, navigate to Netwrix Auditor Administrator Console or contact your Netwrix Auditor administrator.

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

NOTE: Select a Managed Object you want to generate a report for in the report filters. Contact your Netwrix Auditor administrator to learn more about auditing scope for each Managed Object.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Customize Report with Filters 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.

You can playback an entire user session or specific activities in your IT infrastructure.

To playback...	Do...
Entire user session	1. Navigate to **Reports** → **Windows Server** → **User Activity**. Select any report and click **View**. 2. Select a user session you want to playback and click the link in the **Duration** column.
Specific action	1. Navigate to **Reports** → **Windows Server** → **User Activity**. Select any report and click **View**. 2. Select a user session and click a link to an action under the session.

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.

4.6. 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 review and assign such properties as a review status and reason for each change made to the audited systems.

This functionality is currently available for the following audited systems:

- Active Directory
- Exchange
- SharePoint
- Windows Server
- Group Policy

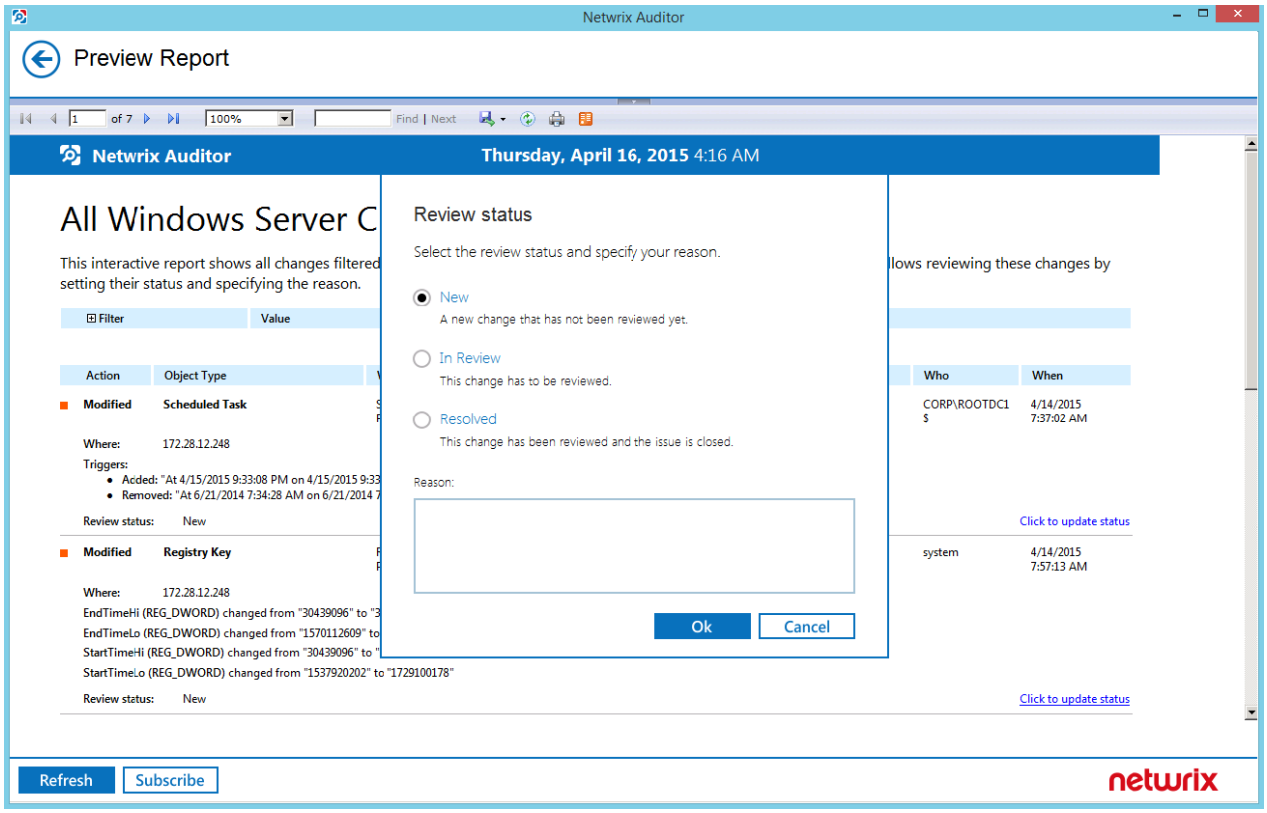
The reports with review status can be found under the **Reports** node for the selected audited system. Depending on the audited system, navigate to one of the following locations:

Audited system	Report location
Active Directory	**Active Directory** → **Active Directory Changes** → **All Active Directory Changes with Review Status**

Audited system	Report location
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: Select a Managed Object you want to generate a report for in the report filters. Contact your Netwrix Auditor administrator to learn more about auditing scope for each Managed Object.

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 Customize Report with Filters 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.

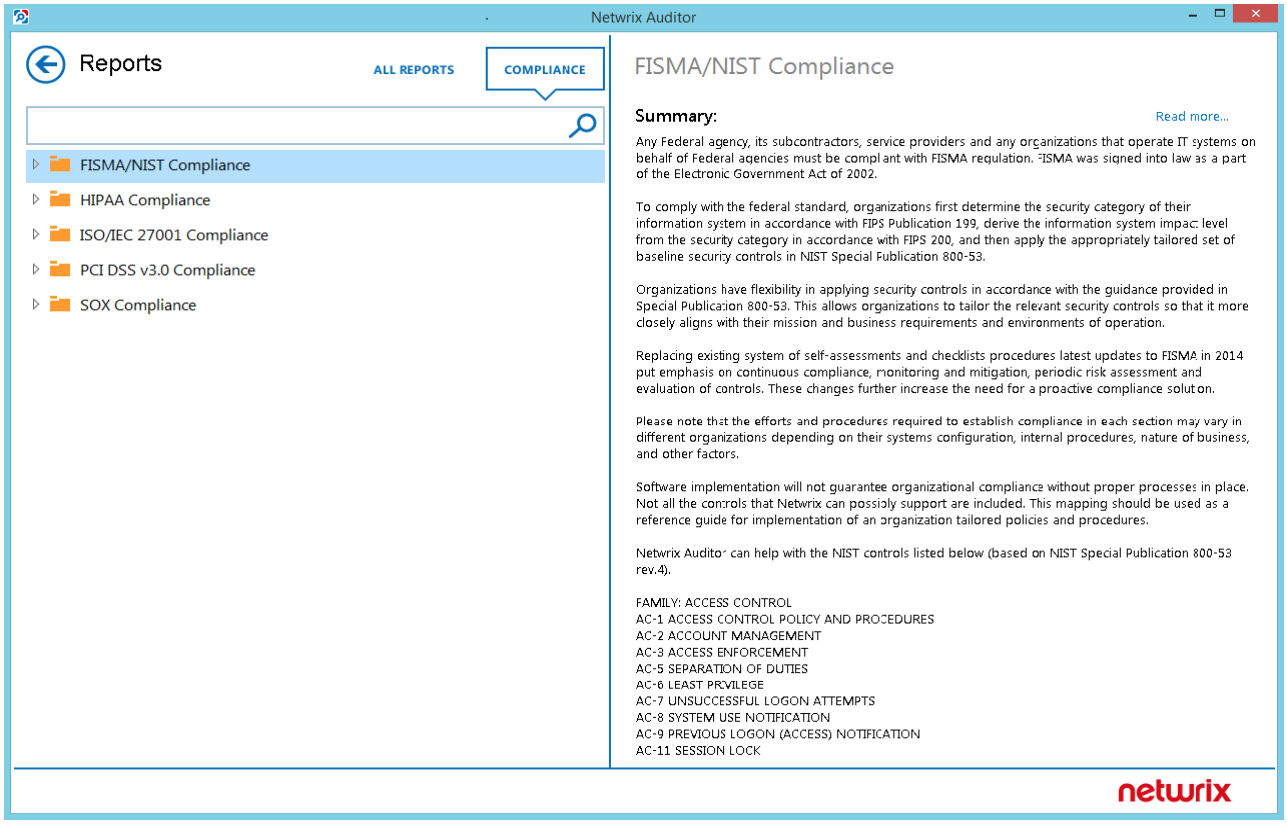
4.7. Compliance Reports

For your convenience, besides grouping by audited system 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:

- **FISMA/NIST SP800-53 rev4**
- **HIPAA**
- **ISO/IEC 27001**
- **PCI DSS v3.0**
- **SOX**

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: Select a Managed Object you want to generate a report for in the report filters. Contact your Netwrix Auditor administrator to learn more about auditing scope for each Managed Object.



5. Subscriptions

In the Netwrix Auditor client, 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.

Review the following for additional information:

- To create a subscription
- To manage subscriptions

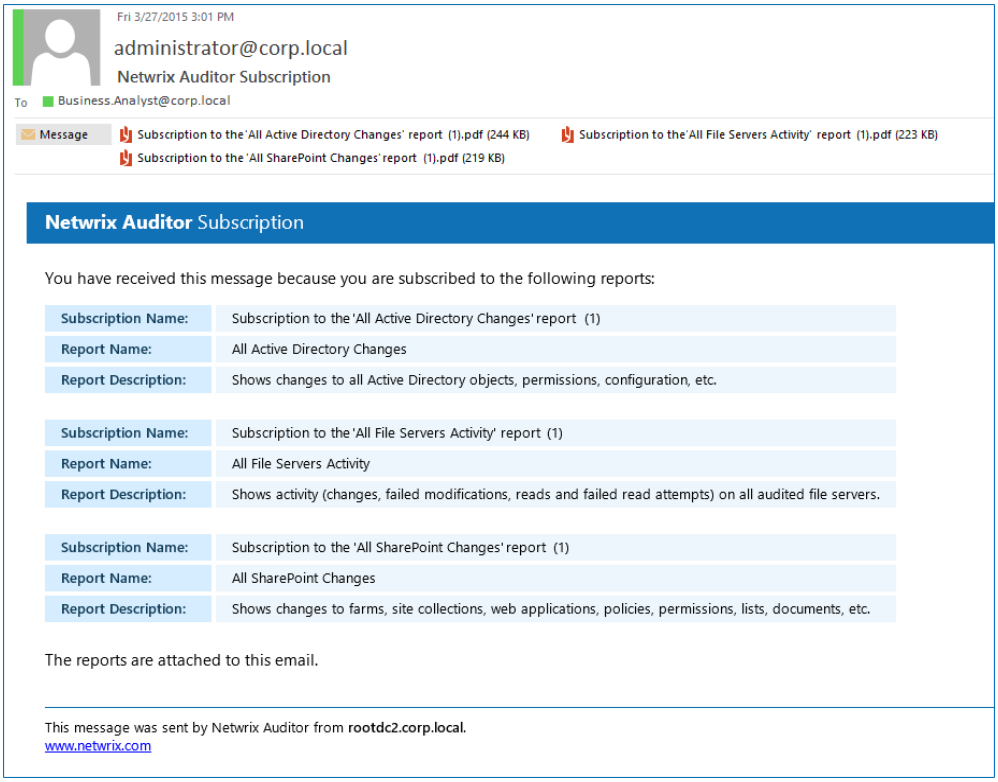
To create a subscription

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 audited system, 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.
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.

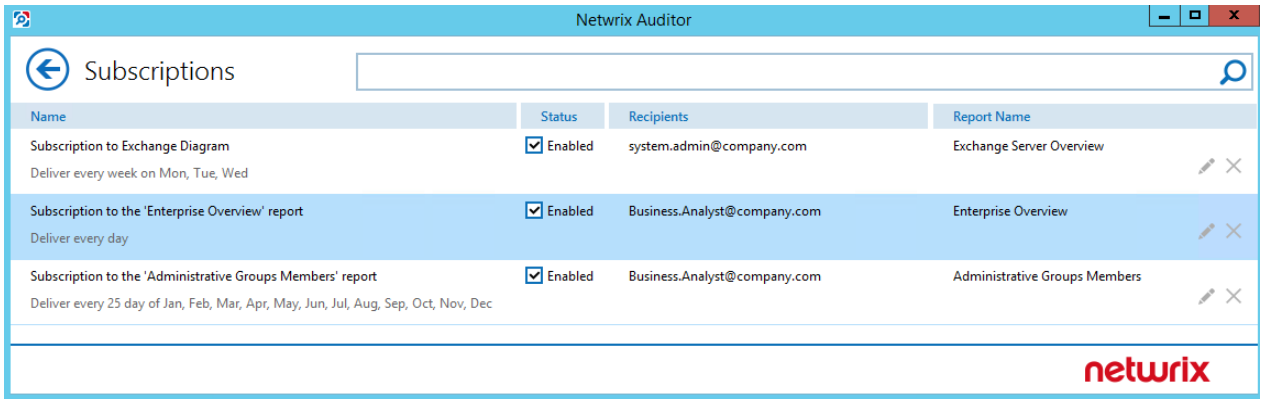
Option	Description
	• **Upload report to file server**—Select this option to save reports on the selected file server. Click **Browse** to select a folder on Netwrix Auditor host (computer where Netwrix Auditor Administrator Console is installed) or specify a UNC path to a shared network resource. **NOTE:** Make sure that your network resource is reachable and you have sufficient rights to access it.
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.

6. Enterprise Overview

Enterprise Overview provide a high-level overview of activity trends by date, user, server, object type or audited system in your IT infrastructure. They allow you to see the activity trends by date, user, object type, server or audited IT system, and drill through to detailed reports for further analysis. The **Enterprise** diagram aggregates data on all Managed Objects and all audited systems, while system-specific diagrams provide quick access to important statistics within one audited system.

The current version of Netwrix Auditor contains the following diagrams:

- Enterprise (aggregates data on all audited systems listed below)
- Active Directory
- Exchange
- File Servers (Windows File Servers, EMC, and NetApp)
- Office 365 (Exchange Online)
- 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 VMware infrastructure in reports and search results), contact your Netwrix Auditor administrator. The administrator must verify that the Audit Database settings are configured in Netwrix Auditor Administrator Console and that audit data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running AuditIntelligence 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 administrator to import that data from the Long-Term Archive.

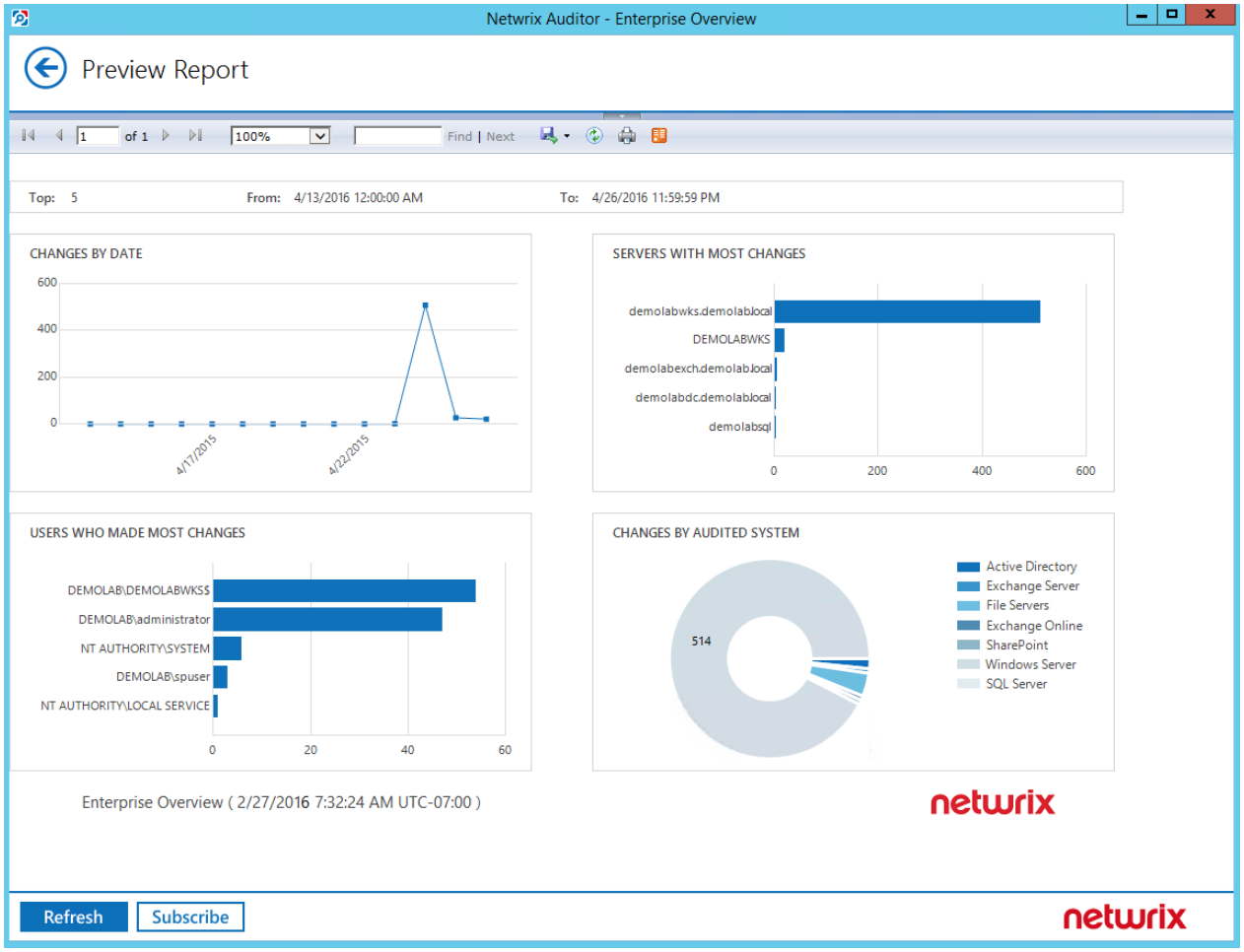
All diagrams provide the drill-down functionality, which means that by clicking on a segment, you will be redirected to a report with the corresponding filtering and grouping of data that renders the next level of detail.

To review a diagram

- On the main Netwrix Auditor page, navigate to the **Enterprise Overview** section. Click a tile to open a corresponding diagram.
- Navigate to **Reports** and select one of the following locations:

Title	Location
Enterprise	**Organization Level Reports**
Active Directory Overview	**Active Directory** → **Active Directory Changes**
Exchange Overview	**Exchange**
Exchange Online Overview	**Exchange Online**
File Servers Overview	**File Servers** → **File Servers Activity**
SharePoint Overview	**SharePoint**
SQL Server Overview	**SQL Server**
VMware Overview	**VMware**
Windows Server Overview	**Windows Server** → **Windows Server Changes**

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



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See Customize Report with Filters for more information.

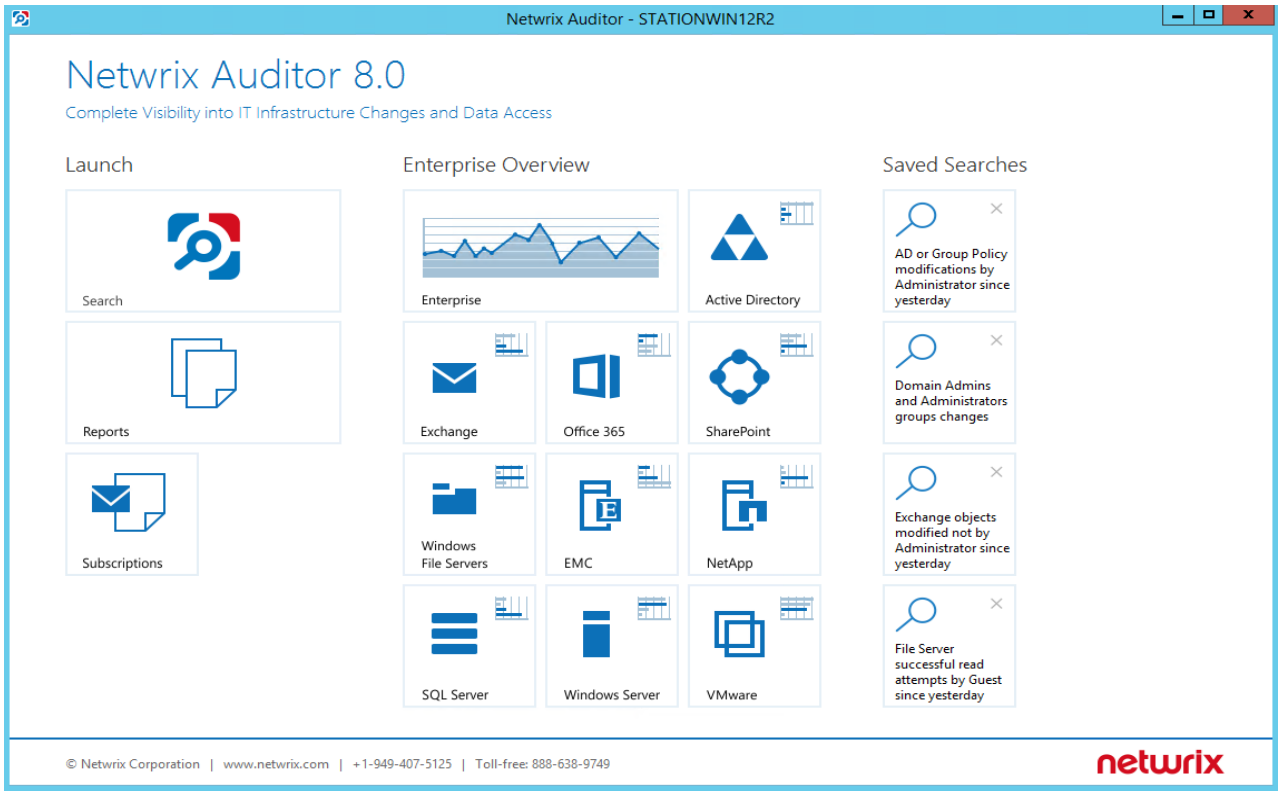
You can also create a subscription to any report you want to receive on a regular basis. See Subscriptions for more information.

7. Saved Searches

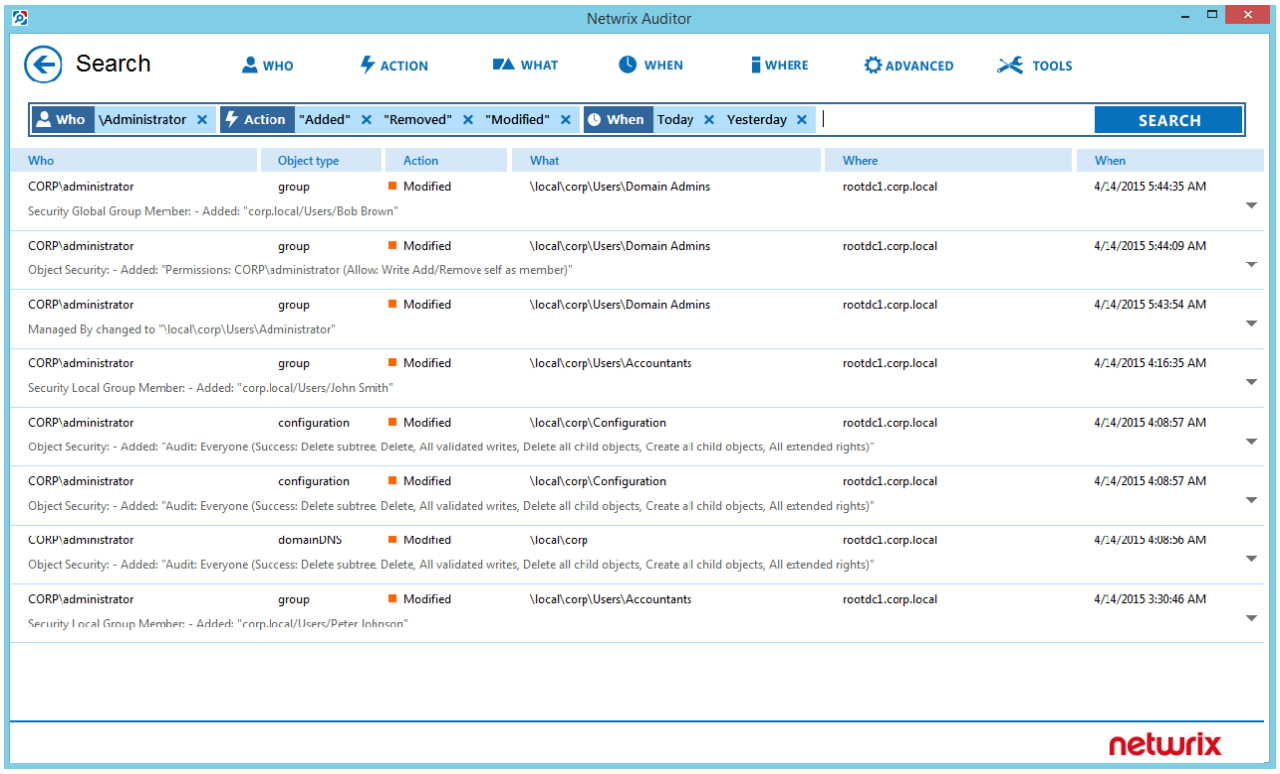
Netwrix Auditor allows you to save your favorite searches to access them instantly. For your convenience, the product provides predefined searches for some popular usage scenarios. Refer to AuditIntelligence Search for detailed instructions on how to create searches.

Moreover, saved searches are shared between all Netwrix Auditor clients that have access to the same Netwrix Auditor Server (an internal component responsible for collecting and processing audit data that is installed with Netwrix Auditor Administrator Console).

You can save your custom searches or use one of predefined saved searches. Predefined searches can be found in the **Saved Searches** 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 audited system 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 AuditIntelligence 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 **Saved Searches**.
2. Select one of the searches and click its tile to open search results.
3. Modify filters and click **Search**.

NOTE: Refer to AuditIntelligence 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.

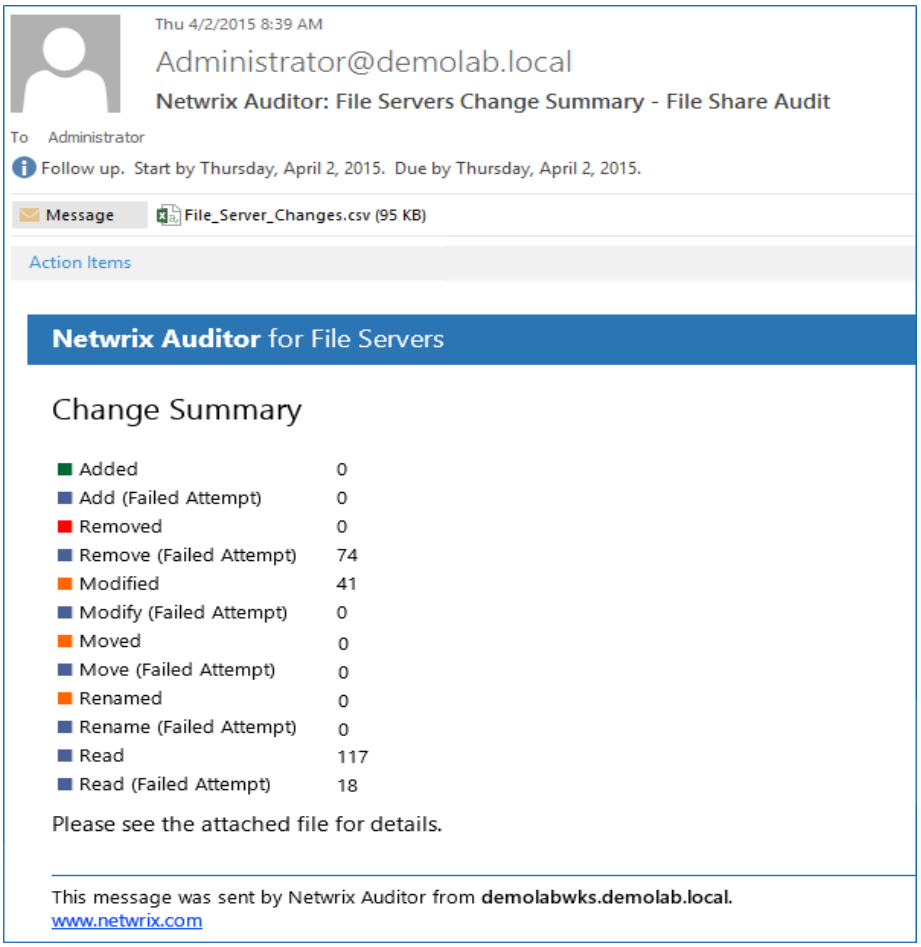
To delete a saved search

- In the **Saved Searches** section, click × on the search tile.

8. Investigate Incidents with Netwrix Auditor: Usage Example

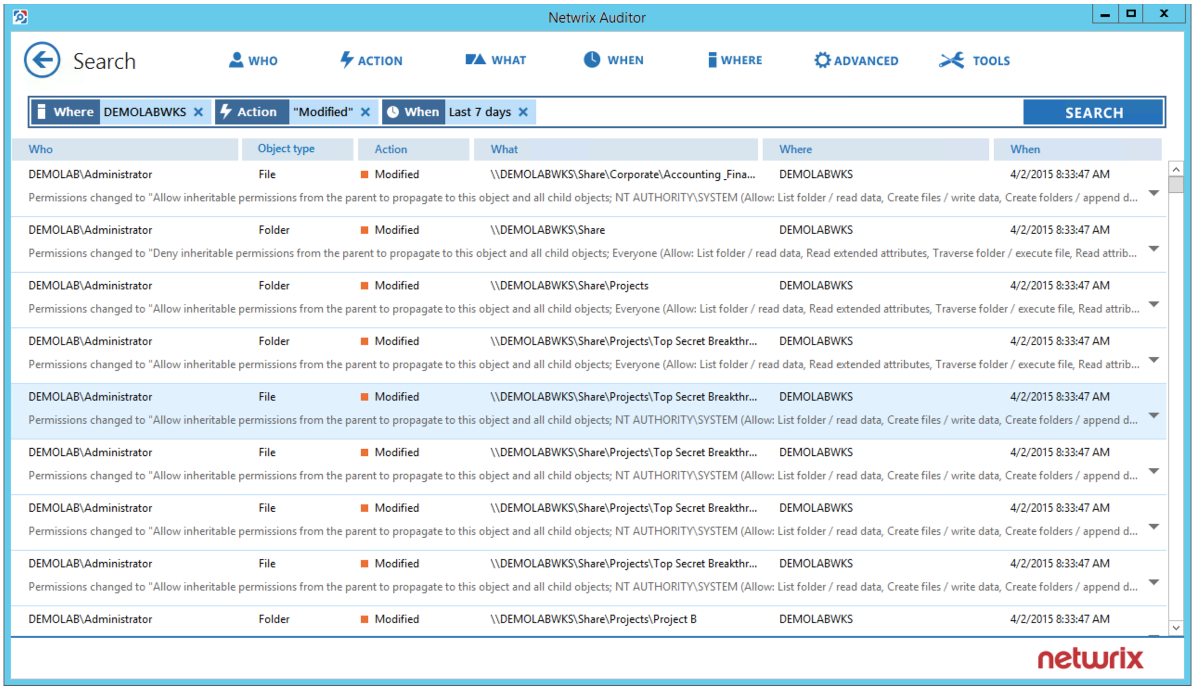
This topic presents an example how you can achieve complete visibility with AuditIntelligence provided by Netwrix Auditor. Refer to AuditIntelligence Search for detailed instructions on how to create data searches.

1. Imagine, when reviewing a daily Change Summary you noticed unusual activity on your file server.



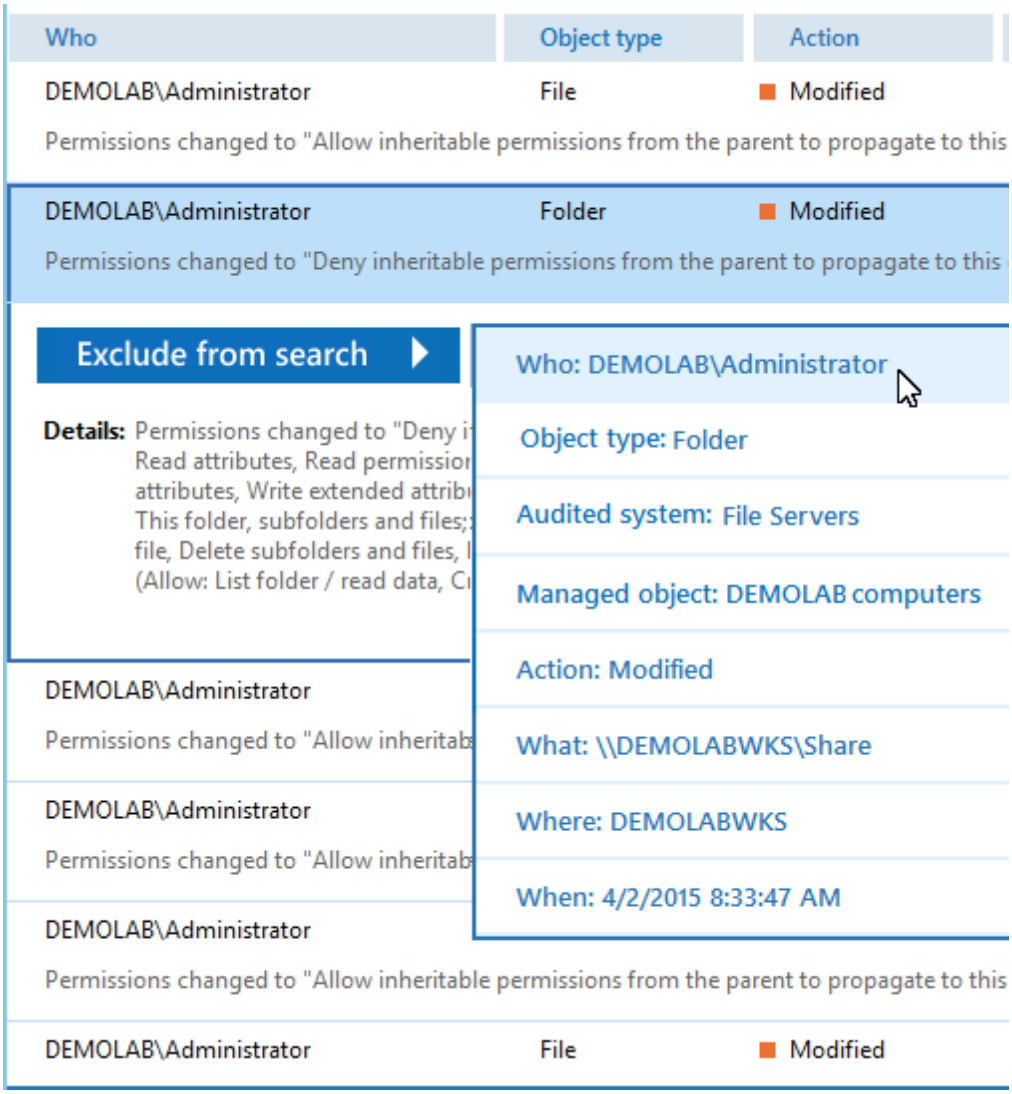
   In a Change Summary you can see 41 modifications, 18 failed read attempts, and 74 failed remove attempts—and this looks suspicious as if someone unauthorized tried to do something with your file share. Your next step is to start investigating this activity.

2. In Netwrix Auditor, you navigate to **Search** to check all modifications that occurred on your file server (**DEMOLABWKS**) within last 7 days.

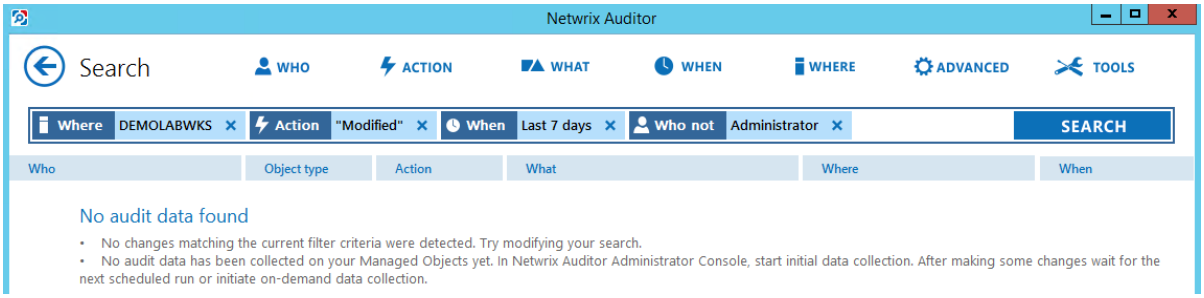


As you see, most of these changes were made by **Administrator**, that is considered to be expected behavior.

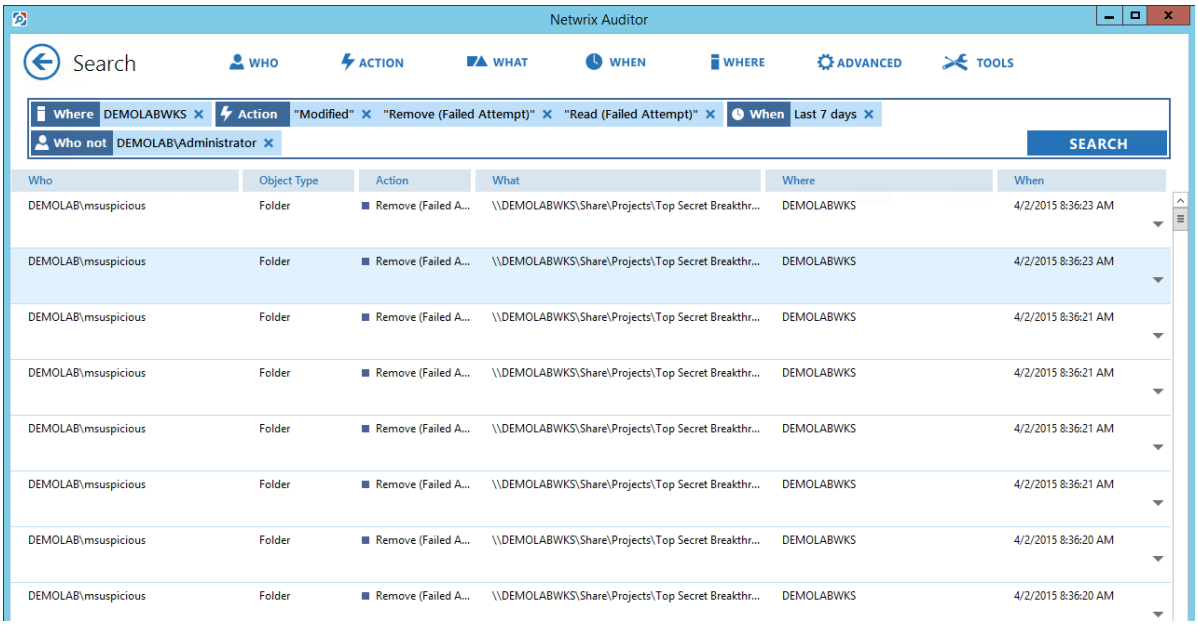
3. You exclude **DEMOLAB\Administrator** from search results.



4. After you click **Search**, you get no results. It means that **Administrator** was the only person who modified files on your file server.

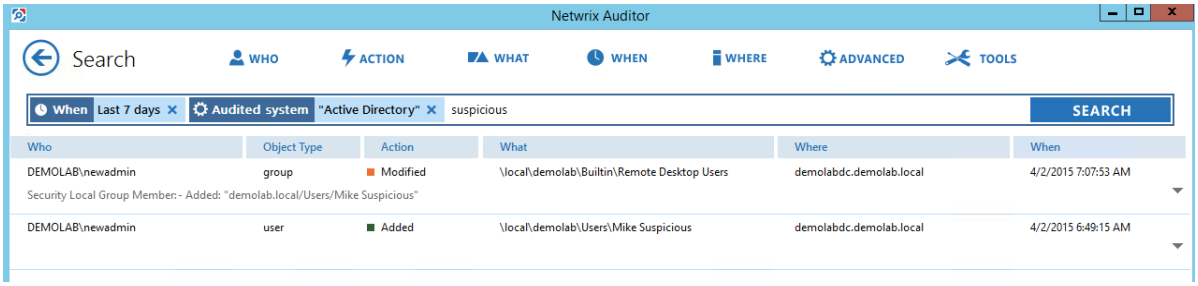


5. The next step in investigating suspicious activity is to find a user who tried to read and remove files, but failed to do it. You navigate to **Advanced** view and add the following filters to your search: set **Action** to **Equals Remove (Failed Attempt)** and **Action** to **Equals Read (Failed Attempt)**. Click **Search** again to update search results.



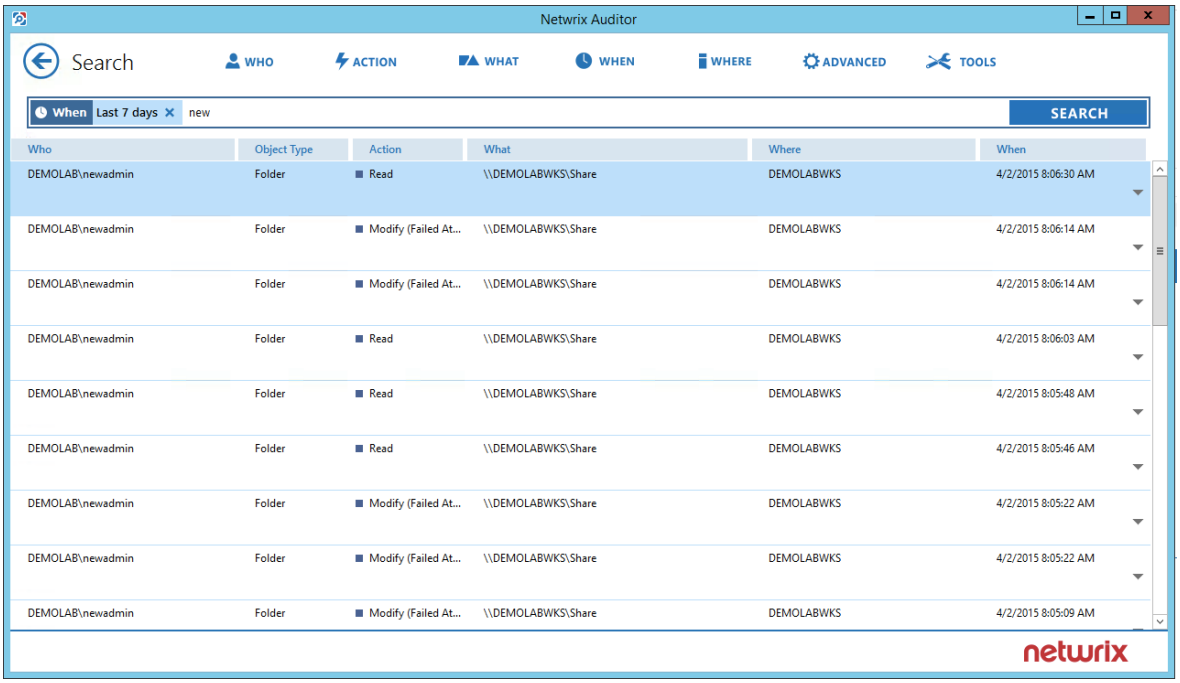
You can see that the **msuspicious** user tried to read and remove files over and over again.

6. As you have not heard about the **msuspicious** user before, you want to find out how could this user appear in your Active Directory domain. You type *suspicious* in the **Search** field and update search results.



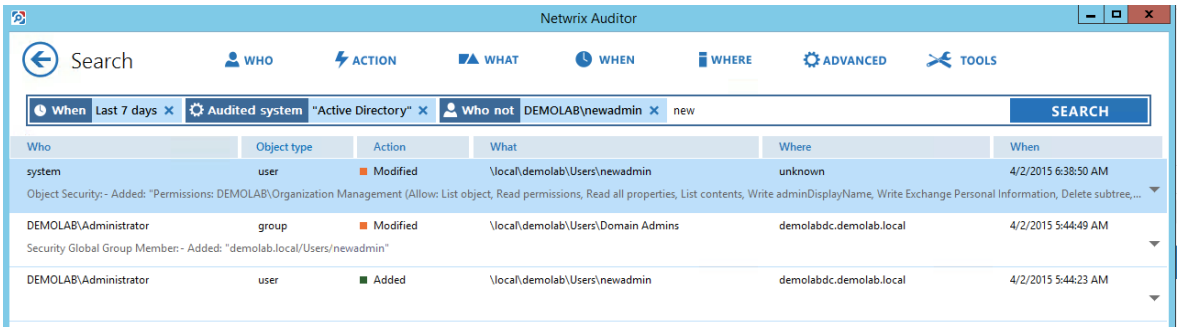
You see that the **newadmin** user created **msuspicious** and added him to the **Remote Desktop Users** group. What do you know about **newadmin**?

7. Run a new search looking for anything to do with **newadmin**.



You can see a lot of changes performed by **newadmin**, you still do not know the way he appeared in your Active Directory domain.

8. You update your search in the **Advanced** view. Set **Audited system** to **Equals Active Directory**, **Who** to **Does not contain DEMOLAB\newadmin** and click **Search**.



In search results, you see that **DEMOLAB\Administrator** created the **newadmin** user, added it to the **Domain Admins** group and granted some special permissions. After that, **newadmin** created a new "suspicious" user who tried to read and remove important files from the audited file server.

Netwrix Auditor with AuditIntelligence brings complete visibility in your IT infrastructure!

9. Additional Options Available in Netwrix Auditor

The Netwrix Auditor client provides quick access to all changes across your IT infrastructure in the easy–to–use search interface, allows generating system–specific and overview reports, etc. If you want to track your IT infrastructure changes whenever possible, try the following options available in Netwrix Auditor Administrator Console:

- Change Summaries
- Real-Time Alerts
- Additional Reports Available in Netwrix Auditor Administrator Console

NOTE: To configure this functionality, contact your Netwrix Auditor administrator.

See Netwrix Auditor Workflow for more information on Netwrix Auditor workflow and features, including functionality provided by Netwrix Auditor Administrator Console.

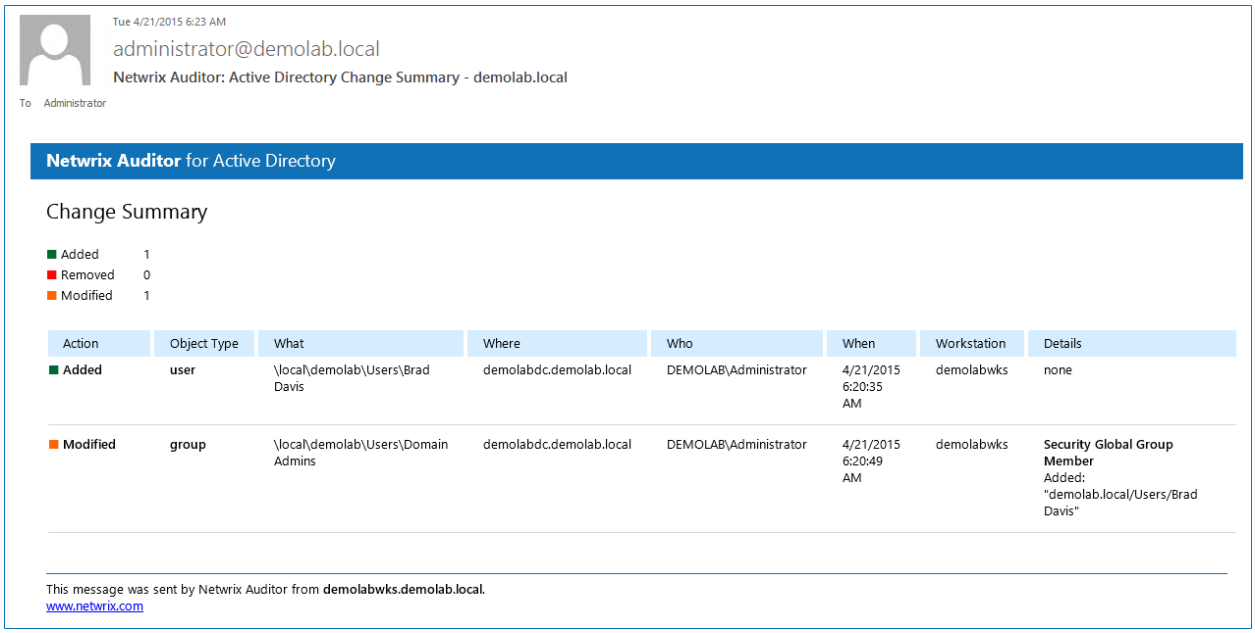
9.1. Change Summaries

After auditing has been configured in Netwrix Auditor Administrator Console, the product starts collecting data on your IT infrastructure. A notification email—a Change Summary—is sent to dedicated recipients and lists all changes that occurred since the last Change Summary delivery. By default, a Change Summary delivery is scheduled once a day at 3.00 AM, but it can also be initialized on-demand by Netwrix Auditor administrator in Netwrix Auditor Administrator Console.

If you want Change Summaries to be delivered to your email address, ask your Netwrix Auditor administrator to configure them for you.

Netwrix Auditor sends a separate Change Summary per each audited system within a Managed Object.

NOTE: The Change Summary example below 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:

Column	Description
Action	Shows the type of action that was performed on the object.
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.
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.

9.2. Real-Time Alerts

Real-time alert is an email notification triggered by a specific event and sent immediately to dedicated recipients. If you want to be notified immediately about changes to certain objects across your IT infrastructure, ask your Netwrix Auditor administrator to configure real-time alerts for you.

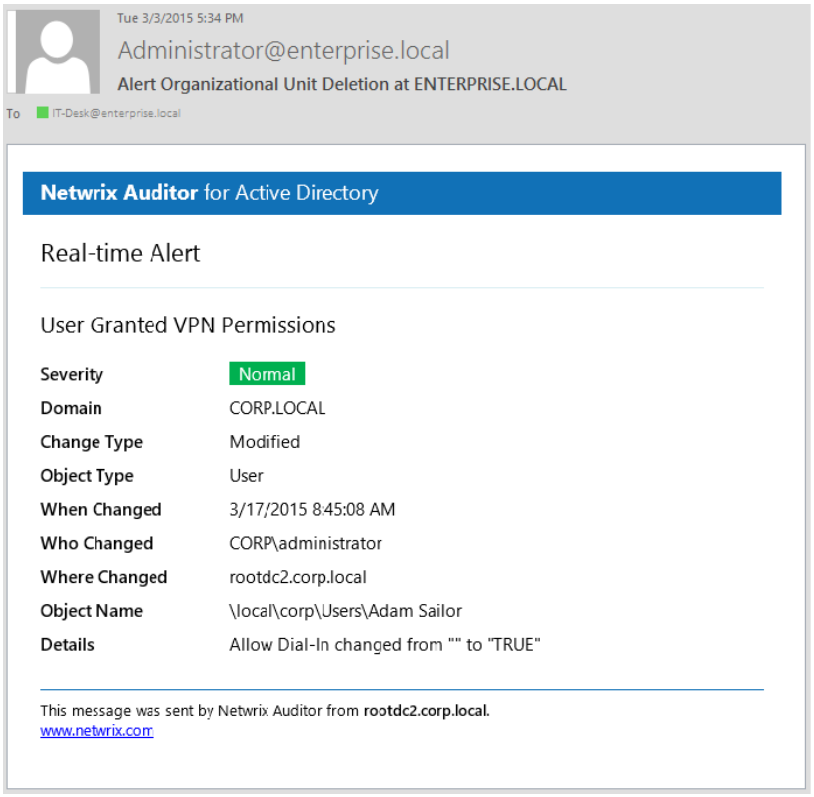
Real-time alerts are available for:

- Active Directory
- Event Log

If a specified event is detected in your IT infrastructure, an email notification will be sent to the recipients.

Netwrix Auditor provides predefined real-time alerts and allows Netwrix Auditor administrator to create custom alerts (e.g., alerts on User Account Lockout, User Granted VPN Permissions).

NOTE: The real-time alert example below applies to Active Directory. Other real-time alerts generated and delivered by Netwrix Auditor may vary slightly depending on the audited system.



9.3. Additional Reports Available in Netwrix Auditor Administrator Console

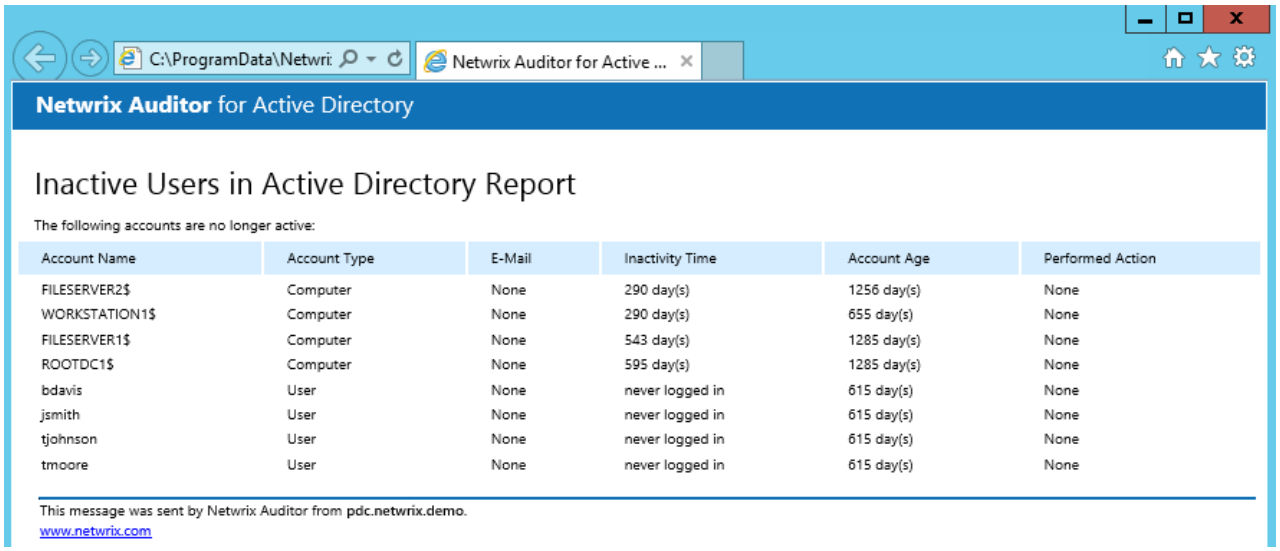
In Netwrix Auditor Administrator Console, administrator can generate additional reports to review inactive users and expiring passwords.

Review the following for additional information:

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

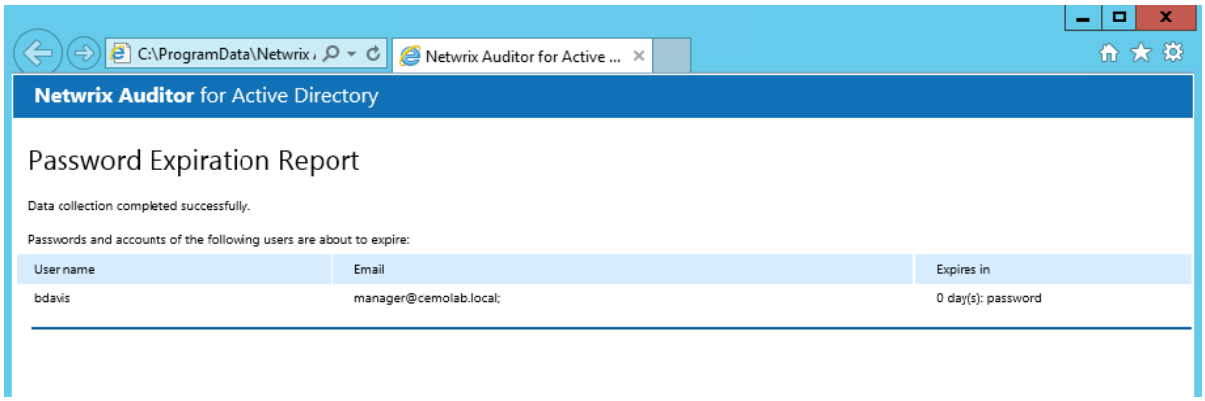
9.3.1. Inactive Users Ad-hoc Report

Administrator 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.



9.3.2. Password Expiration Ad-hoc Report

Administrator can schedule daily emails listing users with expiring passwords. This report can be also generated on demand and reviewed in a web browser.



10. 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 administrator to make sure that your account belongs to the **Netwrix Auditor Client Users** security group. 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. Review your filter settings and make sure that your filters are properly configured. Try modifying your search. 3. 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 administrator to import audit data for a required date range from the Long-Term Archive. 4. Data collection for this Managed Object 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. 5. Some settings in Netwrix Auditor Administrator Console are configured incorrectly. Contact your Netwrix Auditor administrator to make sure that: • The Managed Object you want to audit is properly configured, and the **Enable <Audited_ System> audit** checkbox is selected for each audited system individually. • Audit Database settings are properly configured for each audited system individually and **Make audit data available via summary emails only** is cleared. **NOTE:** Netwrix recommends to store all audit data on the same default SQL Server instance.

Issue	Reason and solution
"NO MANAGED OBJECTS FOUND" text in the **Managed Object** field.	Contact your Netwrix Auditor administrator to make sure that the Managed Object you want to audit exists and is properly configured.
I see a blank window instead of a report.	Contact your Netwrix Auditor 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 a Netwrix Auditor host (computer where Netwrix Auditor Administrator Console is installed). To access these reports, you must be granted the **Read** permission.

Index

T

U

W