

# 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.

© 2016 Netwrix Corporation.

All rights reserved.

# Table of Contents

1. Introduction .....	5
1.1. Netwrix Auditor Overview .....	5
1.2. How It Works .....	7
1.3. Netwrix Auditor Workflow .....	9
2. Launch the Product .....	13
3. AuditIntelligence Search .....	15
3.1. Apply Filters .....	17
3.2. Advanced View .....	19
3.2.1. Apply Additional Filters .....	19
3.2.2. Change Match Types .....	21
3.3. Include and Exclude Data .....	23
3.4. Save Your Search and Share Results .....	24
4. Reports .....	25
4.1. Reports Available in Netwrix Auditor .....	25
4.1.1. Report Types .....	25
4.1.2. View Reports .....	26
4.1.3. Customize Report with Filters .....	29
4.2. Organization Level Reports .....	31
4.3. Change and Activity Reports .....	32
4.4. State-in-Time Reports .....	33
4.5. Reports with Video .....	35
4.6. Reports with Review Status .....	36
4.7. Compliance Reports .....	38
5. Subscriptions .....	39
6. Enterprise Overview .....	42
7. Saved Searches .....	45
8. Investigate Incidents with Netwrix Auditor: Usage Example .....	48
9. Additional Options Available in Netwrix Auditor .....	53

9.1. Change Summaries .....	53
9.2. Real-Time Alerts .....	54
9.3. Additional Reports Available in Netwrix Auditor Administrator Console .....	55
9.3.1. Inactive Users Ad-hoc Report .....	56
9.3.2. Password Expiration Ad-hoc Report .....	56
10. Troubleshoot Issues .....	57
Index .....	59

# 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.

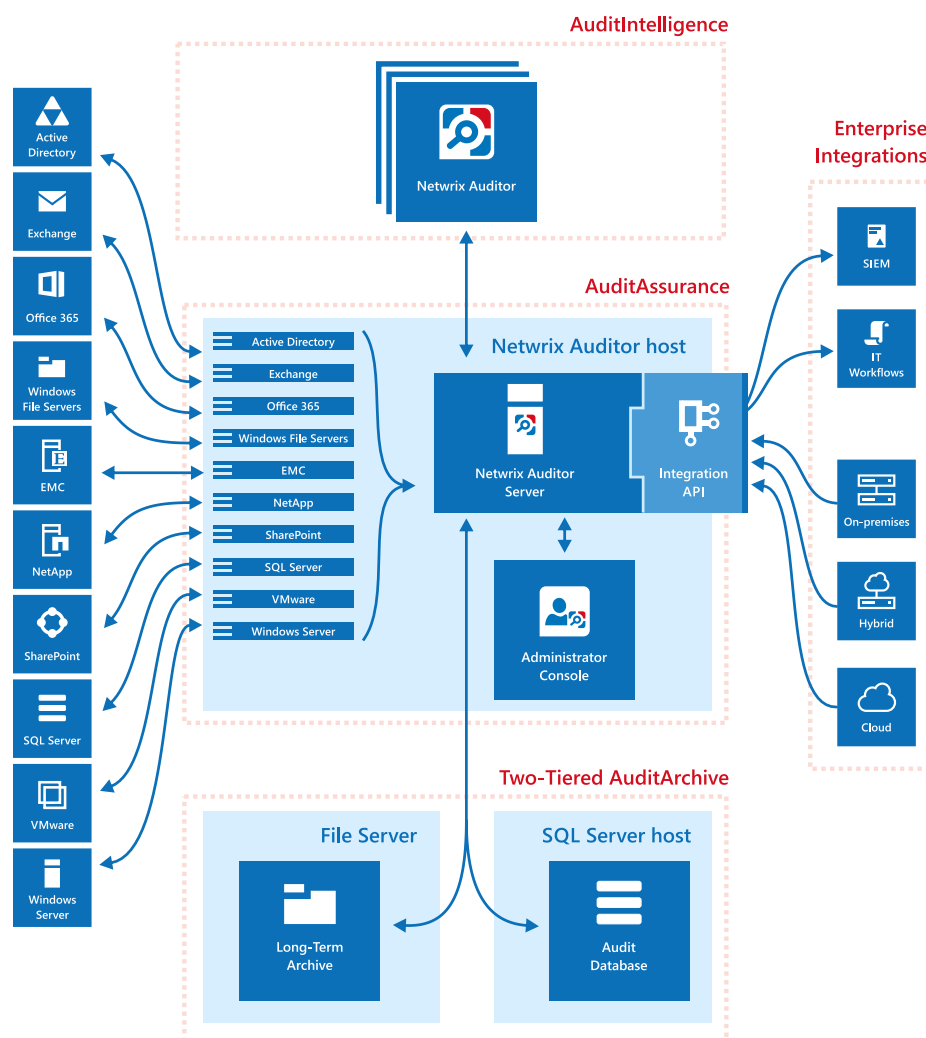
- **Predefined reports and diagrams:** Netwrix Auditor includes more than 150 predefined reports and diagrams. Reports can be exported to a range of formats, including PDF and XLS, and stakeholders can subscribe to reports to stay informed automatically by email.
- **AuditArchive™:** Netwrix Auditor's 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	<p>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.</p> <p>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.</p>
Netwrix Auditor for Exchange	<p>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.</p>
Netwrix Auditor for Office 365	<p>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.</p>
Netwrix Auditor for Windows File Servers	<p>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.</p>
Netwrix Auditor for EMC	<p>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</p>

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	<p>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.</p> <p>In addition, Netwrix Auditor for Windows Server can be configured to capture a video of users' activity on the audited computers.</p>

## 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*

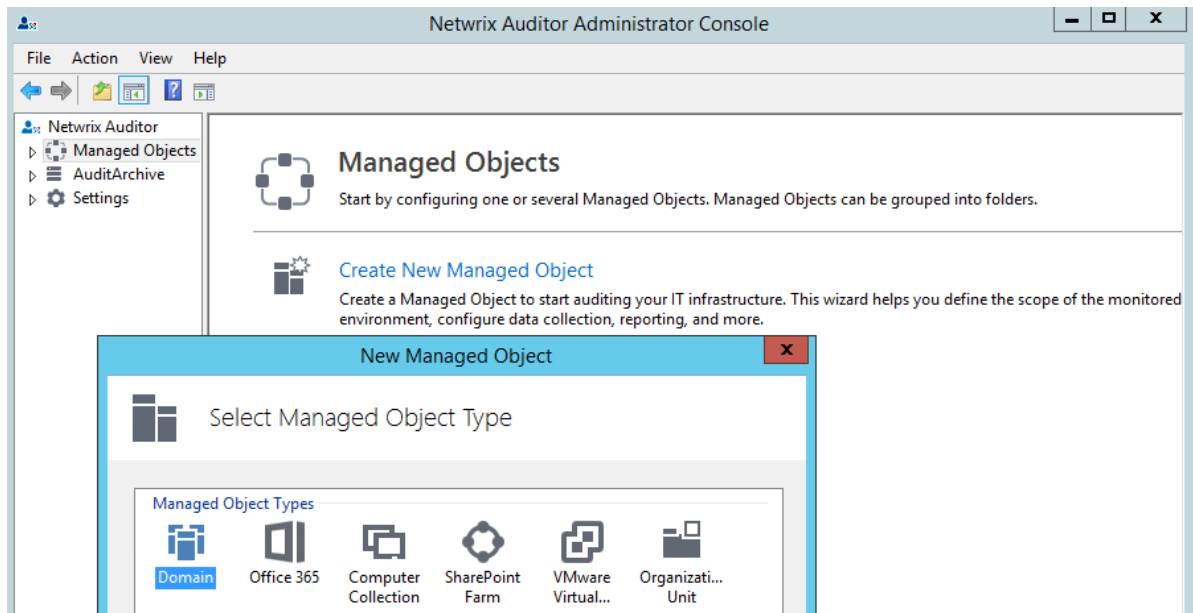
A user who installed Netwrix Auditor Administrator Console is referred to as Netwrix Auditor administrator.

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.

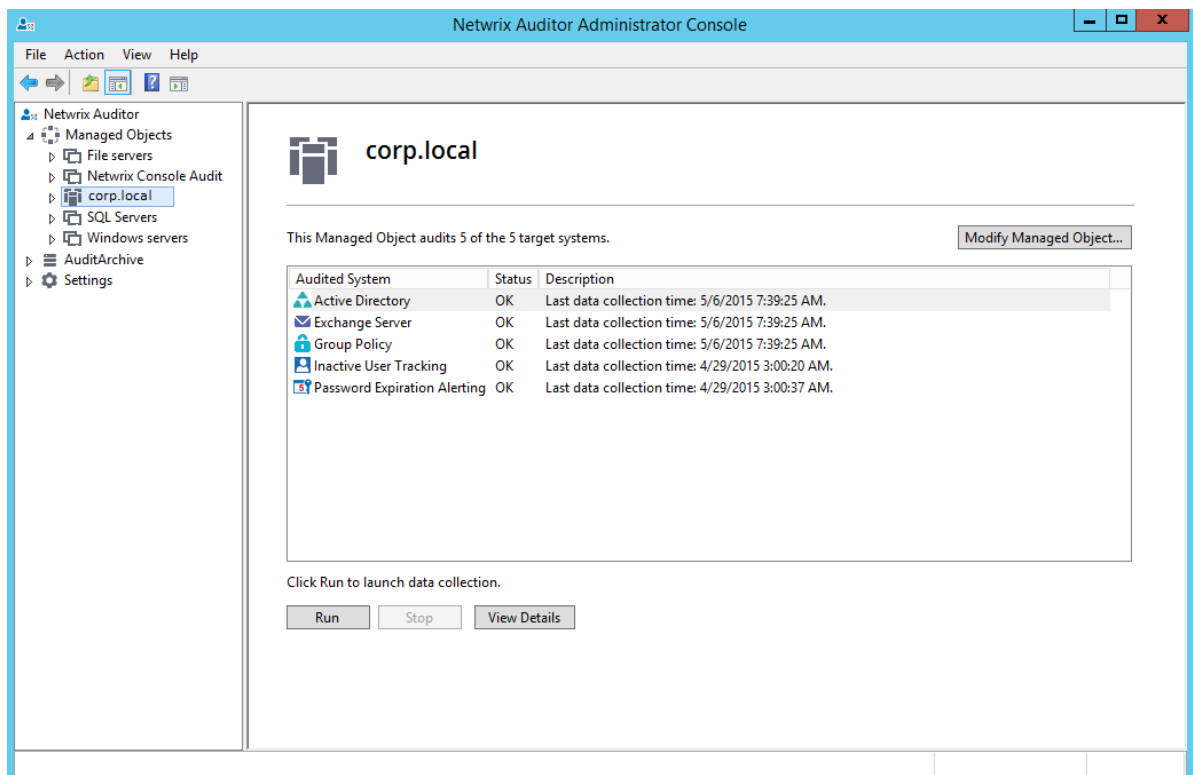
See [Netwrix Auditor Installation and Configuration Guide](#) for more information.

### *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.



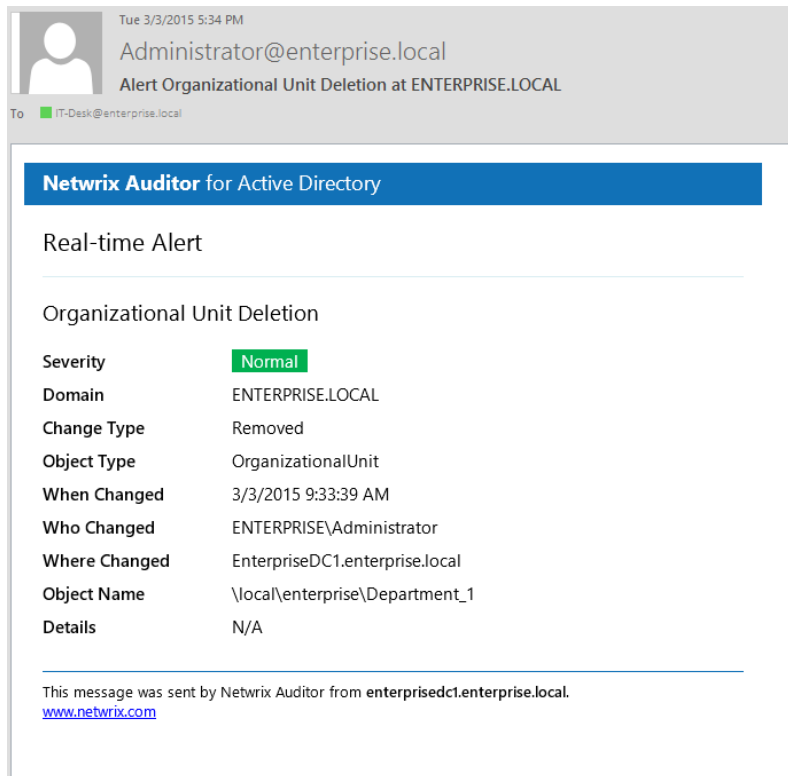
2. The administrator configures the **Audit Database** settings (SQL Server and SSRS settings).
3. Netwrix Auditor audits IT infrastructure and collects data on changes and state-in-time configuration snapshots.



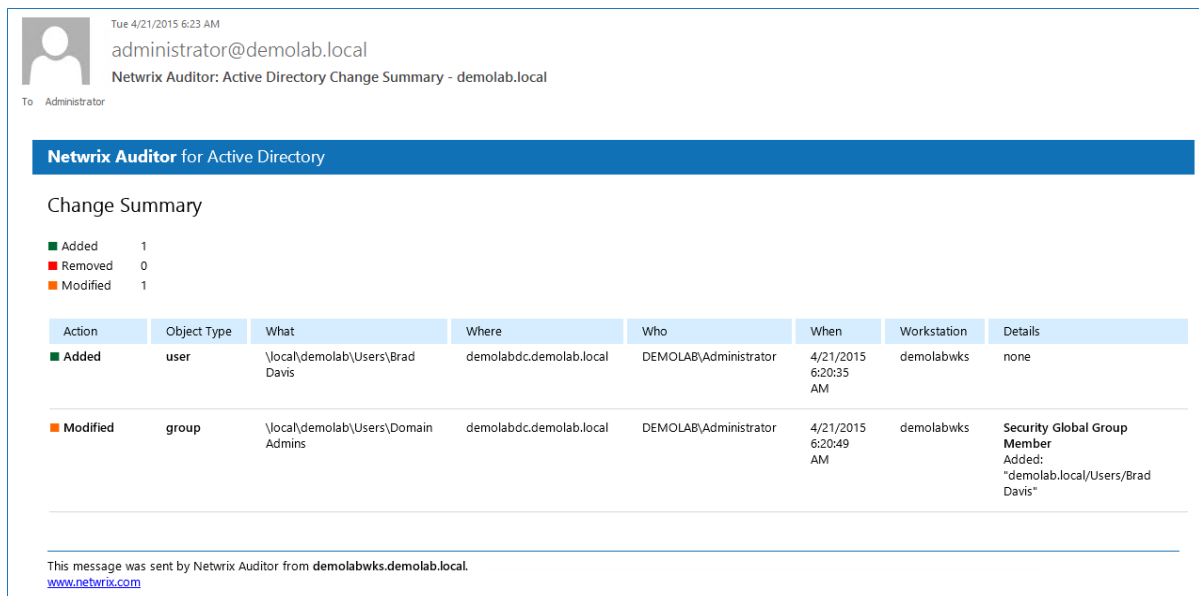
**NOTE:** Collected audit data is written to the AuditArchive that includes both the file-based Long-Term Archive and the short-term SQL Server-based Audit Database.

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

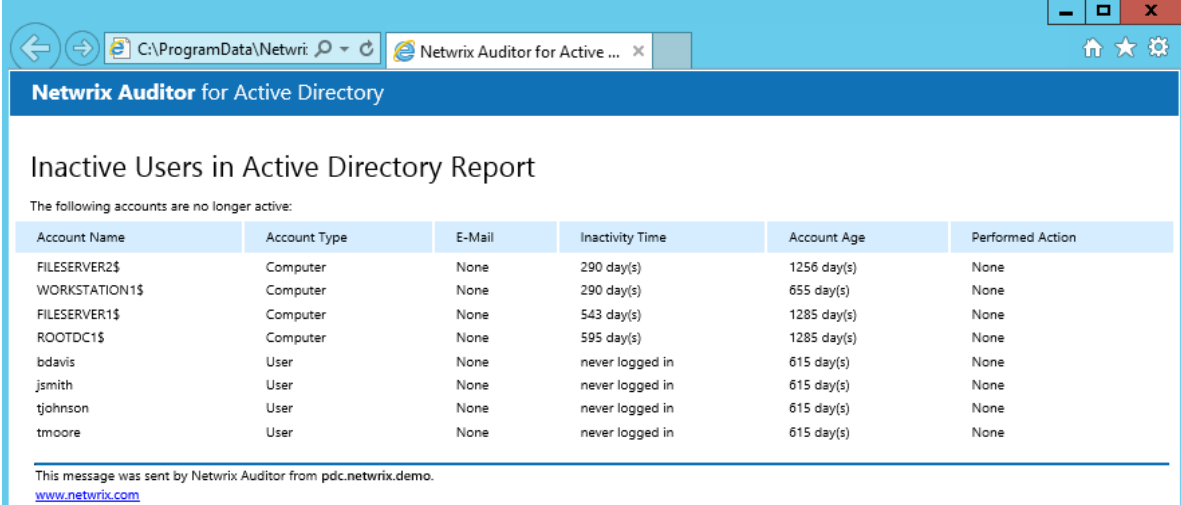
event is detected. In this case an email notification is sent immediately to the specified recipients.



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.



The screenshot shows a web browser window with the title 'Netwrix Auditor for Active Directory'. The main content area displays a report titled 'Inactive Users in Active Directory Report'. Below the title, it states 'The following accounts are no longer active:'. A table follows, listing inactive accounts with columns for Account Name, Account Type, E-Mail, Inactivity Time, Account Age, and Performed Action. The table lists eight accounts: FILESERVER2\$, WORKSTATION1\$, FILESERVER1\$, ROOTDC1\$, bdavis, jsmith, tjohnson, and tmoore. The first four are computers, and the last four are users. All users have 'never logged in' as their inactivity time. At the bottom, a footer note states 'This message was sent by Netwrix Auditor from pdc.netwrix.demo.' and includes the website 'www.netwrix.com'.

Account Name	Account Type	E-Mail	Inactivity Time	Account Age	Performed Action
FILESERVER2\$	Computer	None	290 day(s)	1256 day(s)	None
WORKSTATION1\$	Computer	None	290 day(s)	655 day(s)	None
FILESERVER1\$	Computer	None	543 day(s)	1285 day(s)	None
ROOTDC1\$	Computer	None	595 day(s)	1285 day(s)	None
bdavis	User	None	never logged in	615 day(s)	None
jsmith	User	None	never logged in	615 day(s)	None
tjohnson	User	None	never logged in	615 day(s)	None
tmoore	User	None	never logged in	615 day(s)	None

This message was sent by Netwrix Auditor from pdc.netwrix.demo.  
[www.netwrix.com](http://www.netwrix.com)

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

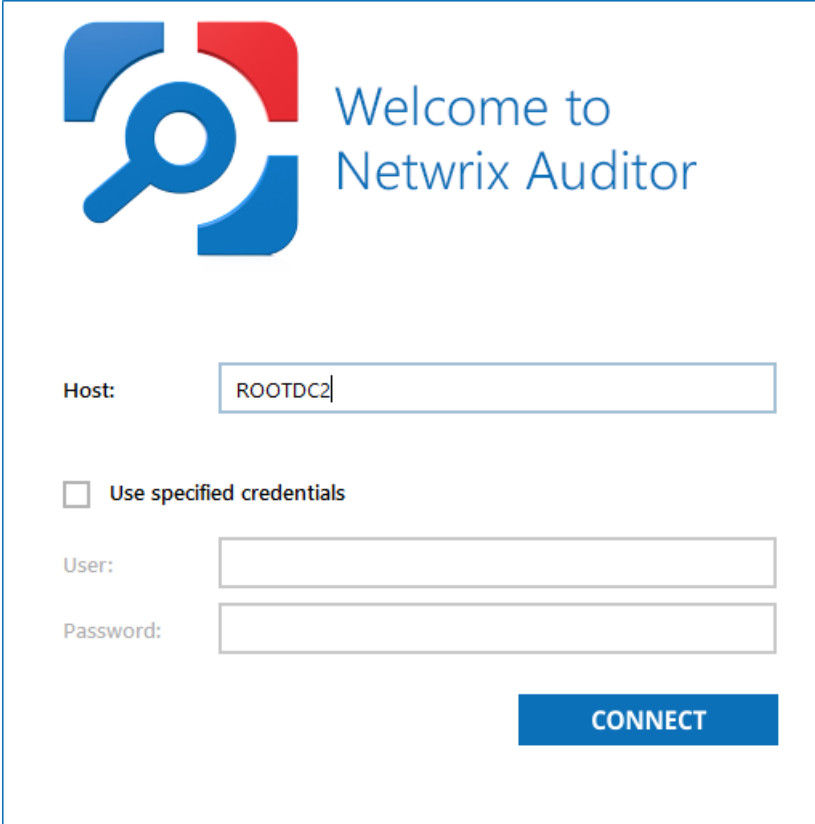
### *To start using Netwrix Auditor*

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.

The image shows the Netwrix Auditor login window. It features a logo on the top left consisting of a blue magnifying glass over a red and blue square. To the right of the logo, the text "Welcome to Netwrix Auditor" is displayed in a blue sans-serif font. Below the logo and text, there is a "Host:" label followed by a text input field containing "ROOTDC2". Underneath this, there is a checkbox labeled "Use specified credentials". Below the checkbox, there are two more text input fields, one labeled "User:" and one labeled "Password:". At the bottom right of the window is a blue button with the word "CONNECT" in white capital letters.

Welcome to  
Netwrix Auditor

Host:

☐ Use specified credentials

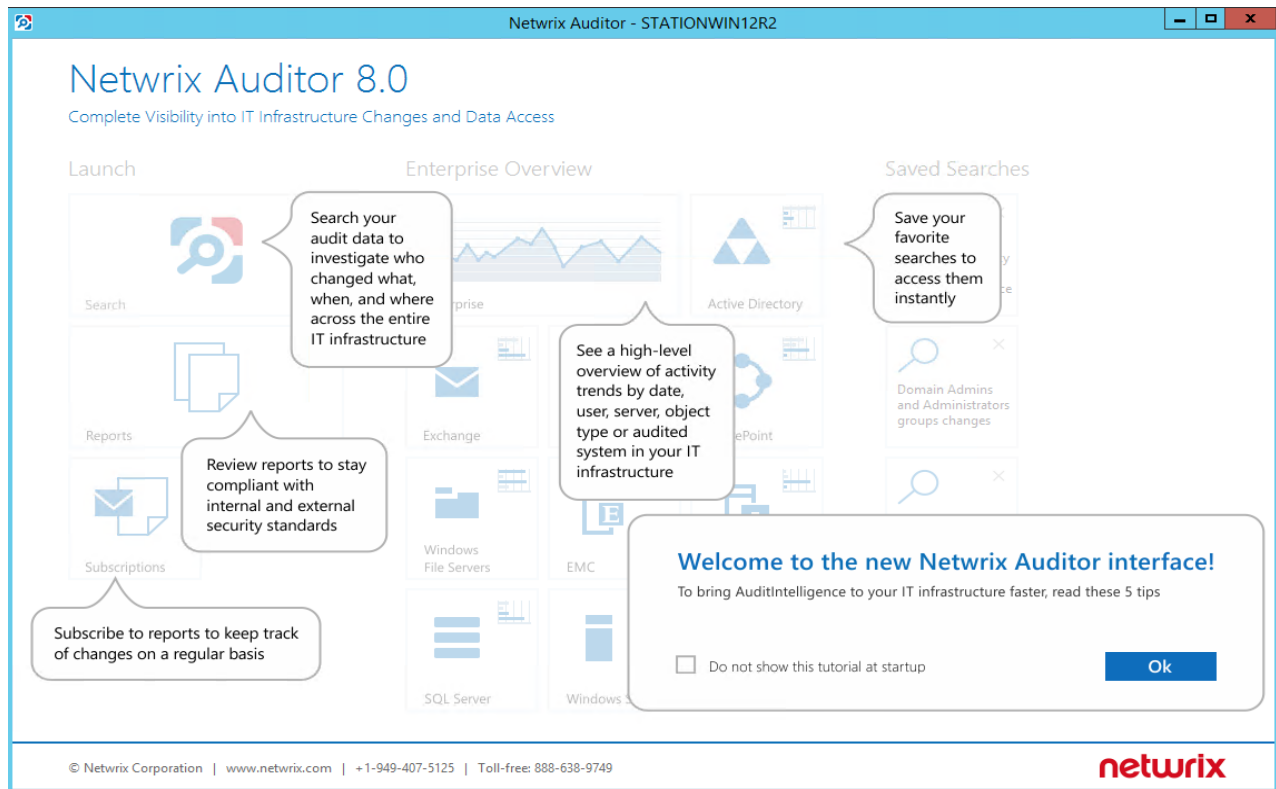
User:

Password:

**CONNECT**

**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*.

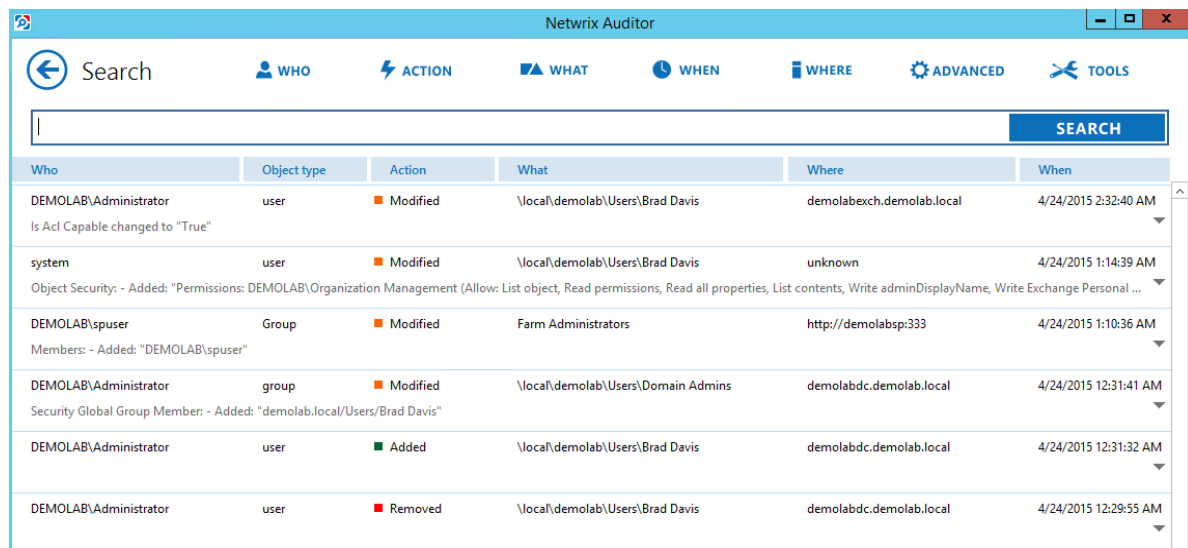
This functionality is currently available for the following audited systems:

- 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.

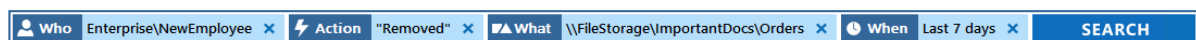
### *To browse your audit data*

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.



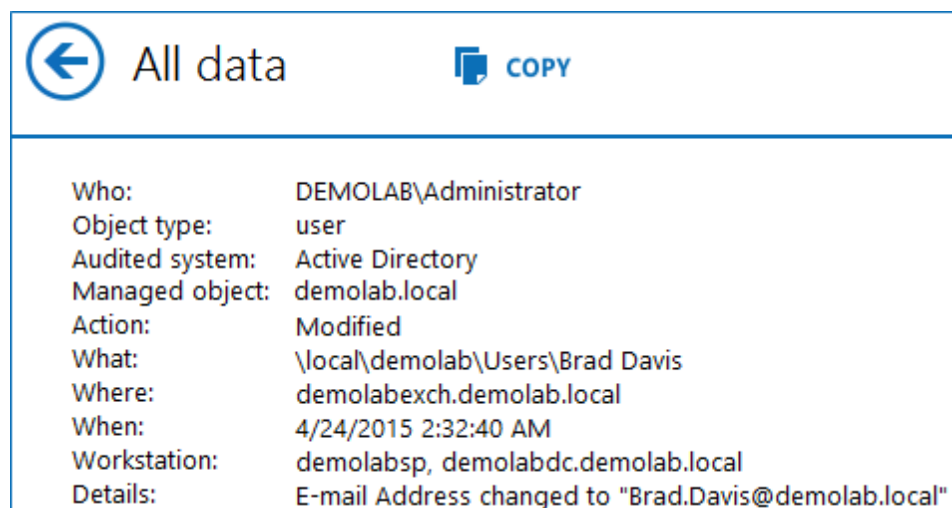
Who	Object type	Action	What	Where	When
DEMOLAB\Administrator Is Acl Capable changed to "True"	user	Modified	\\local\demolab\Users\Brad Davis	demolabexch.demolab.local	4/24/2015 2:32:40 AM
system Object Security: - Added: "Permissions: DEMOLAB\Organization Management (Allow: List object, Read permissions, Read all properties, List contents, Write adminDisplayName, Write Exchange Personal ..."	user	Modified	\\local\demolab\Users\Brad Davis	unknown	4/24/2015 1:14:39 AM
DEMOLAB\spuser Members: - Added: "DEMOLAB\spuser"	Group	Modified	Farm Administrators	http://demolabsp:333	4/24/2015 1:10:36 AM
DEMOLAB\Administrator Security Global Group Member: - Added: "demolab.local/Users/Brad Davis"	group	Modified	\\local\demolab\Users\Domain Admins	demolabdc.demolab.local	4/24/2015 12:31:41 AM
DEMOLAB\Administrator	user	Added	\\local\demolab\Users\Brad Davis	demolabdc.demolab.local	4/24/2015 12:31:32 AM
DEMOLAB\Administrator	user	Removed	\\local\demolab\Users\Brad Davis	demolabdc.demolab.local	4/24/2015 12:29:55 AM

- 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**.



All data	
Who:	DEMOLAB\Administrator
Object type:	user
Audited system:	Active Directory
Managed object:	demolab.local
Action:	Modified
What:	\\local\demolab\Users\Brad Davis
Where:	demolabexch.demolab.local
When:	4/24/2015 2:32:40 AM
Workstation:	demolabsp, demolabdc.demolab.local
Details:	E-mail Address changed to "Brad.Davis@demolab.local"

- Click **Show video...** below the User Activity entry 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

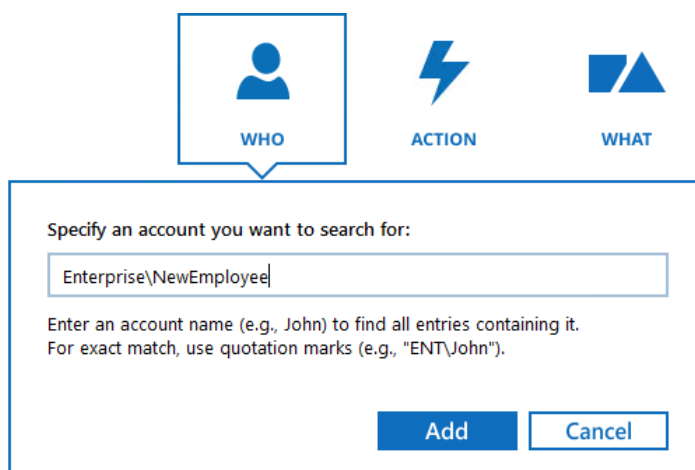
Filters are used to narrow your search results. To create a unique set of filters, you can:

- 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.



WHO ACTION WHAT

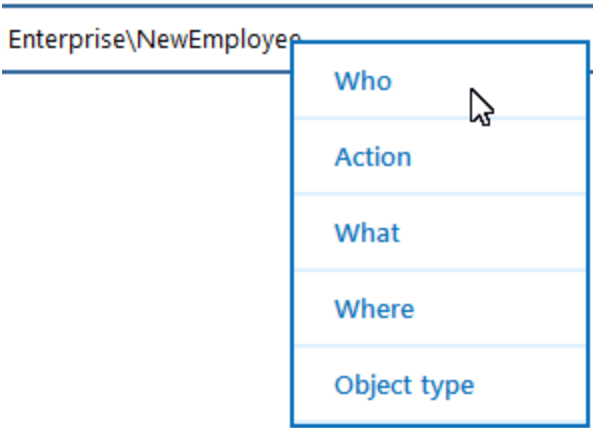
Specify an account you want to search for:

Enterprise\NewEmployee





Enter an account name (e.g., John) to find all entries containing it.  
For exact match, use quotation marks (e.g., "ENT\John").


Add Cancel

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.



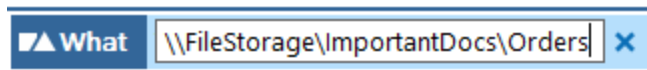
- 2. Click **Search** to apply your filters. By default, all entries that contain the filter value are shown. For an exact match, use quotation marks. See [Advanced View](#) for more information on additional filters and match types.

Filter	Description
 <b>WHO</b>	<p>Specify an account name (e.g., <i>John</i>) to find all entries containing it (e.g., <i>Domain1\John</i>, <i>Domain1\Johnson</i>, <i>Domain2\Johnny</i>).</p> <p>For an exact match, use quotation marks and provide a user name in Domain\User format (e.g., "<i>Domain1\John</i>").</p>
 <b>ACTION</b>	<p>Select an action type from the list (Added, Removed, Modified, Read).</p> <p>For additional actions, navigate to <b>Advanced</b>. See <a href="#">Advanced View</a> for more information.</p>
 <b>WHAT</b>	<p>Specify an object name (e.g., <i>Policy</i>) to find all entries containing it (e.g., <i>HiSecPolicy</i>, <i>\\FileSserver\Share\NewFolder\NewPolicy.docx</i>, <i>http://sharepoint/sites/collection1/Lists/Policy</i>).</p> <p><b>NOTE:</b> Netwrix Auditor searches across all audited systems.</p> <p>For an exact match, use quotation marks and provide an object name in the format that is typical for your audited system (e.g., "<i>HiSecPolicy</i>").</p>
 <b>WHEN</b>	<p>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.</p>

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

#### To modify a filter value

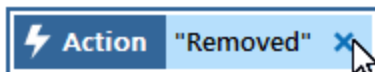
- Double-click it and type a new value.



**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	<p>Limits your search to objects of a specific type only.</p> <p>Specify an object type from the <b>Value</b> list or type it yourself. This filter modifies the <b>What</b> filter.</p>	<p>You noticed that some domain policies were changed and you want to investigate this issue.</p> <p>Your <b>What</b> filter is set to <i>Policy</i>, and so you keep receiving search results such as <i>HiSecPolicy</i>,  <i>\\FS\Share\NewPolicy.docx</i>,  <i>http://sharepoint/sites/col1/Lists/Policy</i>. These entries correspond to different object types and audited systems.</p> <p>Since you are looking for GPOs only, select <b>GroupPolicy</b> from the <b>Value</b> list.</p>
Audited system	<p>Limits your search to the selected audited system only.</p> <p>Specify an audited system from the <b>Value</b> list or type it yourself.</p>	<p>You are investigating suspicious user activity. A user specified in the <b>Who</b> filter made a lot of changes across your IT infrastructure, so the search results became difficult to review.</p> <p>Since you are only interested in the way this user's activity could affect your Active Directory domain and Exchange organization, set the <b>Audited system</b> filter to <b>Active Directory</b> and <b>Exchange</b> to limit the search results.</p>
Managed object	<p>Limits your search to the selected Managed Object only.</p> <p>Specify the name from the <b>Value</b> list or type it yourself.</p>	<p>You are investigating suspicious user activity. A user specified in the <b>Who</b> filter made a lot of changes across your IT infrastructure, so the search results became difficult to review.</p> <p>Since you are only interested in the way this user's activity could affect file shares audited within a single Managed Object, set the <b>Managed Object</b> filter to <i>"My Computer Collection"</i> to limit the search results.</p>
Details	<p>Limits your search results to entries that contain the specified information in the <b>Details</b> column.</p>	<p>You discovered that a registry key was updated to <i>"242464"</i>. Now you want to investigate who made the change and</p>

Filter	Description	Example
	<p>The <b>Details</b> column normally contains data specific to your audited system, e.g., assigned permissions, before and after values, start and end dates.</p> <p>This filter can be helpful when you are looking for a unique entry.</p>	<p>what the value was before.</p> <p>You can set the <b>Details</b> filter to <i>242464</i> to find this change faster.</p>
Before	Limits your search results to entries that contain the specified before value in the <b>Details</b> column.	<p>You are investigating an incident in which the SAM-account-name attribute was changed for an account in your Active Directory domain.</p> <p>You can set the <b>Before</b> filter to the previous name (e.g., <i>John2000</i>) to find the new name faster.</p>
After	Limits your search results to entries that contain the specified after value in the <b>Details</b> column.	<p>You are investigating a security incident and want to know who enabled a local Administrator account on your Windows Server.</p> <p>You can set the <b>After</b> filter to this account's current state (e.g., <i>Enabled</i>) to find this change faster.</p>

### 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 <b>Who</b> filter to <b>contains</b> <i>John</i> , to get the following results: <i>Domain1\John</i> , <i>Domain1\Johnson</i> , <i>Domain2\Johnny</i> .
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., <i>\\FS\Share\NewPolicy.docx</i> .

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

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

WHO
ACTION
WHAT
WHEN
WHERE

ADVANCED

Filter	Operator	Value	
Who ▼	Not equal to ▼	Domain\Administrator	✕
Action ▼	= (Equals) ▼	Modified ▼	✕
What ▼	Ends with ▼	SecPolicy	✕
Audited system ▼	= (Equals) ▼	Active Directory ▼	✕
Managed object ▼	= (Equals) ▼	Domain.local ▼	✕
Before ▼	= (Equals) ▼	Success	✕
Object type ▼	= (Equals) ▼	GroupPolicy ▼	✕
+ Add			

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

⚡ Action

"Modified" ✕

⚙️ What

SecPolicy ✕

⚙️ Audited system

"Active Directory" ✕

⚙️ Managed object

"Domain.local" ✕

⚙️ Before

"Success" ✕

⚙️ Object type

"GroupPolicy" ✕

👤 Who not

"Domain\Administrator" ✕

SEARCH

## 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.

Who	Object type	Action	When
NT AUTHORITY\SYSTEM	Scheduled Task	Modified	Scheduled Task
Triggers: - Added: "At 5/25/2015 6:15:01 AM on 5/25/2015 6:15:01 AM" - Removed: "At 5/24/2015 6:15:01 AM on 5/24/2015 6:15:01 AM"			

Exclude from search

**Audited system:** Windows Server

**Managed object:** Enterprise.local computers

**Details:** Triggers:  
- Added: "At 5/25/2015 6:15:01 AM on 5/25/2015 6:15:01 AM"  
- Removed: "At 5/24/2015 6:15:01 AM on 5/24/2015 6:15:01 AM"

[Read more...](#)

Who: NT AUTHORITY\SYSTEM
Object type: Scheduled Task
Audited system: Windows Server
Managed object: Enterprise.local computers
Action: Modified
What: Scheduled Tasks\Microsoft\Windows\...
Where: StationWin12R2
When: 5/25/2015 2:37:53 AM

NT AUTHORITY\SYSTEM	Triggers: - Added: "At 5/25/2015 3:35:49 AM on 5/25/2015 3:35:49 AM" - Removed: "At 5/24/2015 3:35:49 AM on 5/24/2015 3:35:49 AM"
NT AUTHORITY\SYSTEM	Triggers: - Added: "At 6/3/2015 5:43:11 AM on 6/3/2015 5:43:11 AM" - Removed: "At 5/24/2015 5:43:11 AM on 5/24/2015 5:43:11 AM"
NT AUTHORITY\SYSTEM	

## 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 <a href="#">Saved Searches</a> for detailed instructions on how to save searches you want to run on a regular basis.
Export data	<p>Save your search results as a pdf or csv file.</p> <p>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.</p>

**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
<b>Organization Level reports</b>	Contains a set of reports that provide a general overview of your entire IT infrastructure.
<b>Active Directory</b>	<p>Contains a set of reports on Active Directory and Group Policy changes and state-in-time configuration. Includes the following subfolders:</p> <ul style="list-style-type: none"> <li>• <b>Active Directory Changes</b> with: <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change reports</li> <li>• Changes with review status</li> </ul> </li> <li>• <b>Active Directory State-in-Time</b> with state-in-time reports</li> <li>• <b>Group Policy Changes</b> with: <ul style="list-style-type: none"> <li>• Change reports</li> <li>• Changes with review status</li> </ul> </li> <li>• <b>Group Policy State-in-Time</b> with state-in-time reports</li> <li>• <b>Logon Activity</b> with change reports.</li> </ul>
<b>Exchange</b>	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
	<ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change and activity reports</li> <li>• Changes with review status</li> </ul>
<b>Exchange Online</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change and activity reports</li> </ul>
<b>File Servers</b> including Windows file servers, EMC and NetApp	<p>Contains a set of reports on file server changes, activities, and state-in-time configuration. Includes the following subfolders:</p> <ul style="list-style-type: none"> <li>• <b>File Servers Activity</b> with: <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change and activity reports</li> </ul> </li> <li>• <b>File Servers State-in-Time</b> with state-in-time reports</li> </ul> <p><b>NOTE:</b> The following reports can be generated for Windows file servers only: Account Permissions, Object Permissions by Object, and Excessive Access Permissions.</p>
<b>SharePoint</b>	<p>Contains a set of reports on SharePoint changes, including changes to content, configuration and access permissions. Includes the following reports:</p> <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change and activity reports</li> <li>• Changes with review status</li> </ul>
<b>SQL Server</b>	<p>Contains a set of reports on SQL Server changes. Includes the following reports:</p> <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change reports</li> </ul>
<b>VMware</b>	<p>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</p>

Folder	Reports
	<p>the following reports:</p> <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change reports</li> </ul>
<b>Windows Server</b>	<p>Contains a set of reports on Windows infrastructure including reports on Windows configuration changes, event logs and user activity. Includes the following subfolders:</p> <ul style="list-style-type: none"> <li>• <b>Windows Server Changes</b> with: <ul style="list-style-type: none"> <li>• Overview diagram</li> <li>• Change reports</li> <li>• Changes with review status</li> </ul> </li> <li>• <b>User Activity (Video)</b> with reports with video</li> <li>• <b>Event Log</b> with change reports, including a syslog change report, the <b>Netwrix Auditor System Health</b> report and IIS change reports.</li> </ul> <p><b>NOTE:</b> <b>Netwrix Auditor System Health</b> is a special report designed for reviewing Netwrix Auditor health status (successful and failed data collections, warnings, errors, etc.)</p>
<p><b>Compliance folders:</b></p> <ul style="list-style-type: none"> <li>• FISMA/NIST Compliance</li> <li>• HIPAA Compliance</li> <li>• ISO/IEC 27001 Compliance</li> <li>• PCI DSS v3.0 Compliance</li> <li>• SOX Compliance</li> </ul>	<p>For your convenience, contains reports mentioned above but grouped by corresponding international standards and regulations:</p> <ul style="list-style-type: none"> <li>• FISMA/NIST SP800-53 rev4</li> <li>• HIPAA</li> <li>• ISO/IEC 27001</li> <li>• PCI DSS v3.0</li> <li>• SOX</li> </ul> <p><b>NOTE:</b> Click <b>Compliance</b> above the list of reports to see reports grouped by compliance standards only.</p> <p>See <a href="#">Compliance Reports</a> for more information.</p>

### *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 **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:

**Netwrix Auditor** Friday, April 03, 2015 10:14 AM

## All Changes by Server

Shows all changes across the entire IT infrastructure grouped by the server where the changes were made.

Filter Value

**Where:** ROOTDC2  
**Audited System:** File Servers

Action	Object Type	What	Who	When
Read	Folder	\\ROOTDC2\Annual_Reports	CORP\Administrator	4/2/2015 5:45:38 AM
Read	Folder or File	\\ROOTDC2\Annual_Reports\Regedit_Copy	CORP\Administrator	4/2/2015 5:45:51 AM
Read	Folder	\\ROOTDC2\Annual_Reports	CORP\Administrator	4/2/2015 5:45:51 AM
Removed	Folder or File	\\ROOTDC2\Annual_Reports\Regedit_Copy\NA_6.5.reg	CORP\Administrator	4/2/2015 5:45:51 AM
Removed	Folder or File	\\ROOTDC2\Annual_Reports\Regedit_Copy\NA_7.0.reg	CORP\Administrator	4/2/2015 5:45:51 AM
Removed	Folder or File	\\ROOTDC2\Annual_Reports\Regedit_Copy	CORP\Administrator	4/2/2015 5:45:51 AM
Read	Folder	\\ROOTDC2\Annual_Reports	CORP\Administrator	4/2/2015 5:47:03 AM

Refresh Subscribe

netwrix

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.

**Netwrix Auditor** Friday, April 03, 2015 10:41 AM

## All Changes by Server

Shows all changes across the entire IT infrastructure grouped by the server where the changes were made.

Filter Value

**Where:** ROOTDC2  
**Audited System:** File Servers

Action	Object Type	What	Who	When
Added	File	\\ROOTDC2\Annual_Reports\Summary	CORP\Administrator	3/30/2015 8:14:26 AM

**Audited System:** Windows Server

Action	Object Type	What	Who	When
Modified	Scheduled Task	Scheduled Tasks\Netwrix Auditor Administrator Console	CORP\Administrator	4/1/2015 6:20:26 AM

Triggers:

- Added: "At 3/30/2015 7:00:00 AM every day"
- Removed: "At 3/30/2015 3:00:00 AM every day"

Action	Object Type	What	Who	When
Modified	Scheduled Task	Scheduled Tasks\Netwrix Auditor Administrator Console	CORP\Administrator	4/1/2015 6:20:26 AM

Triggers:

- Added: "At 3/30/2015 7:00:00 AM every day"
- Removed: "At 3/30/2015 3:00:00 AM every day"

Refresh Subscribe

netwrix

## 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.

The screenshot displays the Netwrix Auditor web interface. At the top, a blue header bar contains the Netwrix Auditor logo and the text 'Netwrix Auditor'. Below this is a 'Preview Report' section with a back arrow icon. A navigation bar shows '1 of 4' pages, a '75%' zoom level, and search controls. A status bar indicates 'Thursday, April 02, 2015 6:23 AM'.

The main content area is titled 'All Changes by Audited System' with a subtitle 'Shows all changes across the entire IT infrastructure grouped by the audited system.' Below this is a 'Filter' and 'Value' section.

The first section is 'Audited System: Active Directory'. It contains a table with the following data:

Action	Object Type	What	Who	When
Removed	user	\\local\corp\Users\gary.black	CORP\Administrator	4/2/2015 5:43:48 AM
Where: rootd.c2.corp.local				
Removed	user	\\local\corp\Users\Adam.Sailor	CORP\Administrator	4/2/2015 5:44:02 AM
Where: rootd.c2.corp.local				
Added	user	\\local\corp\Users\James.J.W. Wisher	CORP\Administrator	4/2/2015 5:44:56 AM
Where: rootd.c2.corp.local				
Modified	computer	\\local\corp\Computers\WORKSTATION	CORP\Administrator	4/2/2015 5:45:27 AM
Where: rootd.c2.corp.local Allow Dial-In changed to "TRUE"				

The second section is 'Audited System: File Servers'. It contains a table with the following data:

Action	Object Type	What	Who	When
Read	Folder	\\ROOTDC2\Annual_Reports	CORP\Administrator	4/2/2015 5:45:38 AM
Where: ROOTDC2				

At the bottom of the interface are 'Refresh' and 'Subscribe' buttons.

**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

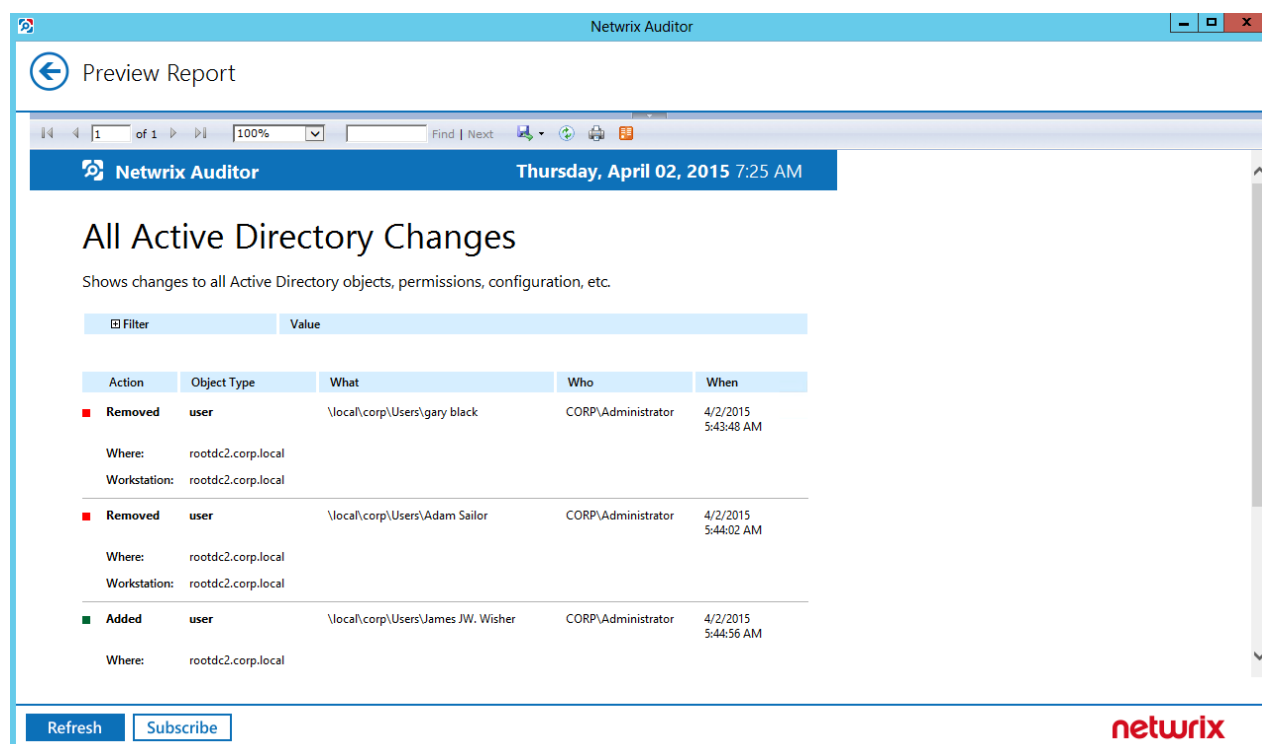
Change reports provide information on changes to different aspects of the audited environment. Some audited systems provide activity reports as well. Some audited

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.

The screenshot shows the 'Preview Report' window in Netwrix Auditor. The title bar says 'Netwrix Auditor'. The main header area includes a back arrow and 'Preview Report'. Below this is a filter section with 'Managed Object' set to 'corp.local', 'Snapshot Date' set to 'Current Session', 'Status' set to 'Both', and 'Path' set to '%'. A 'View Report' button is on the right. Below the filter section is a toolbar with navigation icons and a search bar. The main content area has a blue header with the Netwrix Auditor logo and the date 'Thursday, April 02, 2015 10:39 AM'. The report title is 'Computer Accounts', followed by a description: 'Shows computer accounts, their paths and statuses (enabled or disabled)'. Below this is a table with columns 'Path', 'Name', and 'Status'. The table lists several computer accounts, all with a status of 'Enabled'. At the bottom, there is a footer with the Netwrix logo, the text 'Computer Accounts', and '1 of 1'. There are also 'Refresh' and 'Subscribe' buttons, and the Netwrix logo on the right.

Path	Name	Status
\\local\\corp\\Computers\\FILESERVER1	FILESERVER1	Enabled
\\local\\corp\\Computers\\FILESERVER2	FILESERVER2	Enabled
\\local\\corp\\Computers\\Sharepointsrv	Sharepointsrv	Enabled
\\local\\corp\\Computers\\WORKSTATION	WORKSTATION	Enabled
\\local\\corp\\Computers\\WORKSTATION1	WORKSTATION1	Enabled
\\local\\corp\\Domain Controllers\\ROOTDC1	ROOTDC1	Enabled
\\local\\corp\\Domain Controllers\\ROOTDC2	ROOTDC2	Enabled

**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.

The screenshot displays the Netwrix Auditor 'Preview Report' window. The main content area is titled 'All Users Activity' and includes a sub-header 'This report shows video records of all users' activity.' Below this, there is a table with columns 'Who', 'Where', 'Duration', and 'Start Time'. The table shows two entries for 'CORP\Administrator' on 'rootdc2.corp.local'.

Who	Where	Duration	Start Time
CORP\Administrator	rootdc2.corp.local	00:28:48	4/1/2015 9:41:28 AM
4/1/2015 10:10:15 AM Session end			
Who	Where	Duration	Start Time
CORP\Administrator	rootdc2.corp.local	00:20:11	4/1/2015 10:15:38 AM
4/1/2015 10:15:58 AM Session start			
4/1/2015 10:15:58 AM Microsoft Management Console   Netwrix Auditor Administrator Console			
4/1/2015 10:16:16 AM Microsoft Management Console   Task Scheduler			
4/1/2015 10:16:21 AM Microsoft Management Console   Netwrix Auditor Administrator Console			
4/1/2015 10:16:28 AM Microsoft Management Console   Audit Trail Settings			
4/1/2015 Microsoft Management Console   Netwrix Auditor Administrator Console			

At the bottom of the report preview, there are 'Refresh' and 'Subscribe' buttons. To the right of the report, a video player is embedded, showing a Windows Server 2012 desktop environment with various administrative tools open.

**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	<ol style="list-style-type: none"> <li>1. Navigate to <b>Reports</b> → <b>Windows Server</b> → <b>User Activity</b>. Select any report and click <b>View</b>.</li> <li>2. Select a user session you want to playback and click the link in the <b>Duration</b> column.</li> </ol>
Specific action	<ol style="list-style-type: none"> <li>1. Navigate to <b>Reports</b> → <b>Windows Server</b> → <b>User Activity</b>. Select any report and click <b>View</b>.</li> <li>2. Select a user session and click a link to an action under the session.</li> </ol>

**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

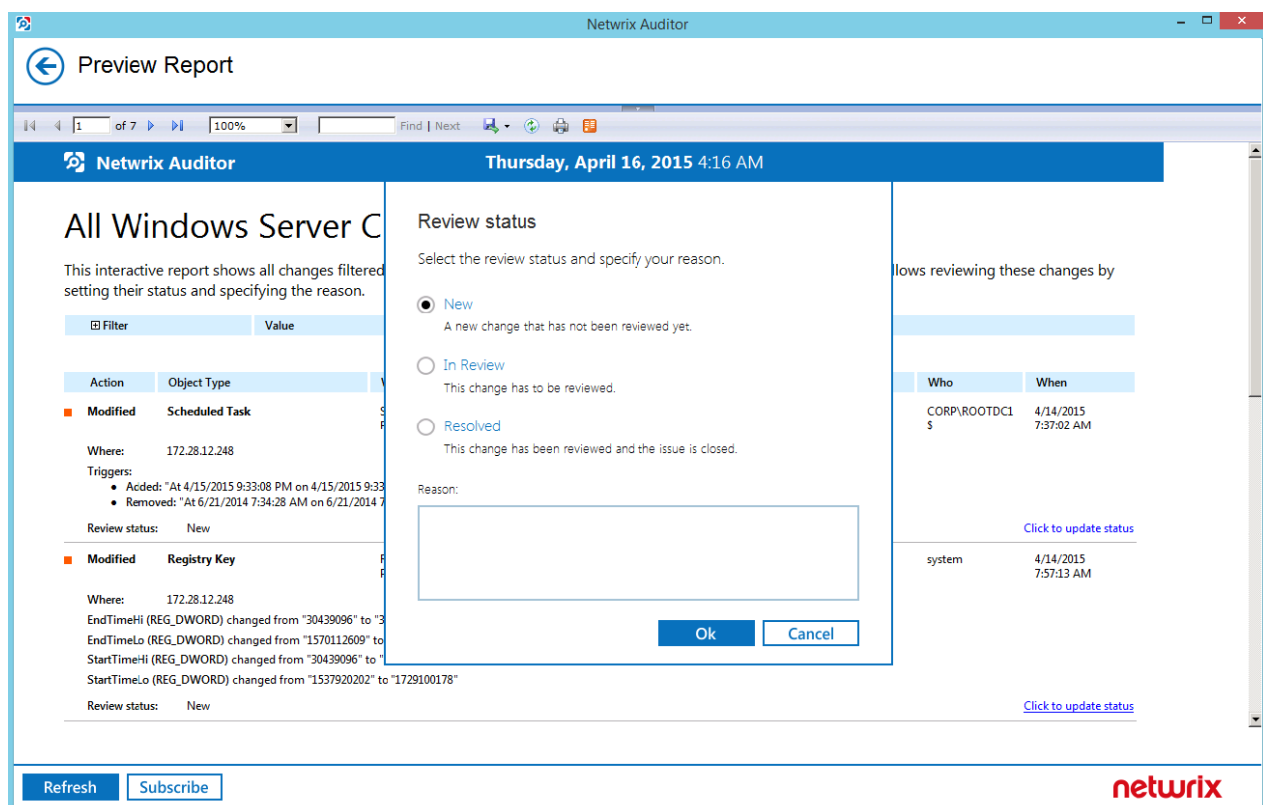
The reports with review status can be found under the **Reports** node for the selected audited system. Depending on the audited system, navigate to one of the following locations:

Audited system	Report location
Active Directory	<b>Active Directory</b> → <b>Active Directory Changes</b> → <b>All Active Directory Changes with Review Status</b>

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.

The screenshot displays the Netwrix Auditor web interface. On the left, a sidebar shows the 'Reports' section with a 'COMPLIANCE' tab selected. Below the tab, a list of compliance folders is shown: FISMA/NIST Compliance, HIPAA Compliance, ISO/IEC 27001 Compliance, PCI DSS v3.0 Compliance, and SOX Compliance. The 'FISMA/NIST Compliance' folder is selected and expanded. The main content area displays the 'FISMA/NIST Compliance' report. It includes a 'Summary' section with a 'Read more...' link. The summary text states: 'Any Federal agency, its subcontractors, service providers and any organizations that operate IT systems on behalf of Federal agencies must be compliant with FISMA regulation. FISMA was signed into law as a part of the Electronic Government Act of 2002.' Below this, it explains that organizations first determine the security category of their information system in accordance with FIPS Publication 199, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53. It also mentions that organizations have flexibility in applying security controls in accordance with the guidance provided in Special Publication 800-53. The report further states that replacing existing system of self-assessments and checklists procedures latest updates to FISMA in 2014 put emphasis on continuous compliance, monitoring and mitigation, periodic risk assessment and evaluation of controls. These changes further increase the need for a proactive compliance solution. A note mentions that the efforts and procedures required to establish compliance in each section may vary in different organizations depending on their systems configuration, internal procedures, nature of business, and other factors. It also states that software implementation will not guarantee organizational compliance without proper processes in place. Not all the controls that Netwrix can possibly support are included. This mapping should be used as a reference guide for implementation of an organization tailored policies and procedures. The report concludes by stating that Netwrix Auditor can help with the NIST controls listed below (based on NIST Special Publication 800-53 rev.4). The list of controls includes: FAMILY: ACCESS CONTROL, AC-1 ACCESS CONTROL POLICY AND PROCEDURES, AC-2 ACCOUNT MANAGEMENT, AC-3 ACCESS ENFORCEMENT, AC-5 SEPARATION OF DUTIES, AC-6 LEAST PRIVILEGE, AC-7 UNSUCCESSFUL LOGON ATTEMPTS, AC-8 SYSTEM USE NOTIFICATION, AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION, and AC-11 SESSION LOCK.

## 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](#)

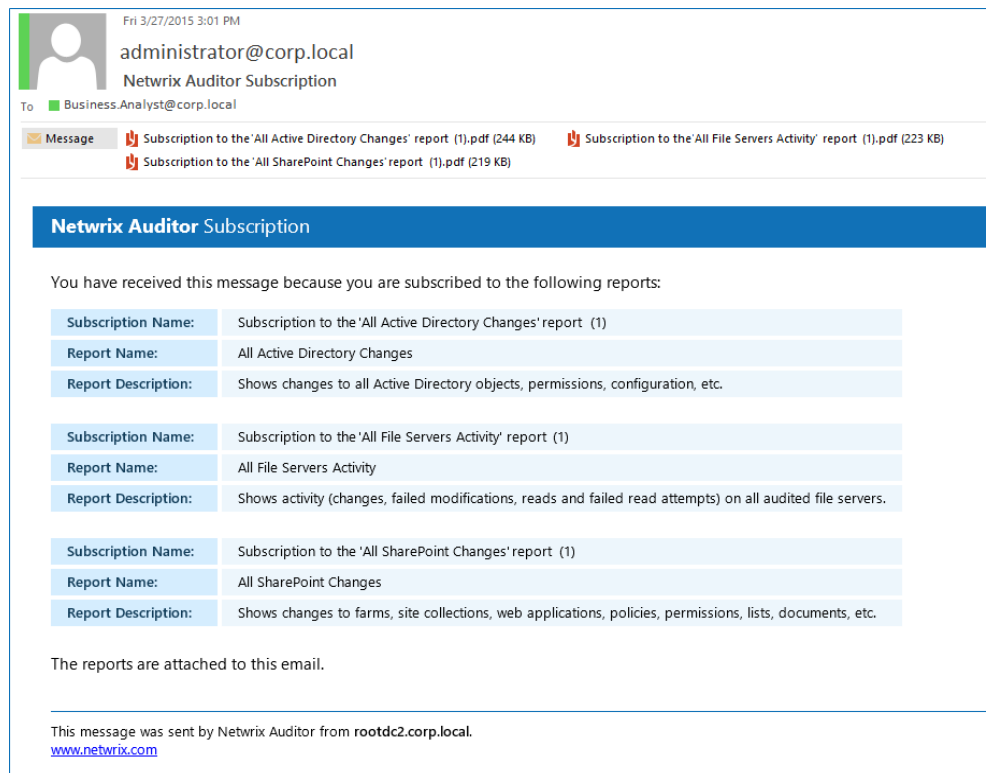
### *To create a subscription*

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 <b>Yes</b> 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 <b>Recipients</b> list and click <b>Add</b> to add more recipients.
Every...	Allows specifying report delivery schedule (daily, certain days of week, a certain day of a certain month).  <b>NOTE:</b> By default, the product emails reports daily at 8.00 am.
Attach report to email / Upload report to file server	Select report delivery method: <ul style="list-style-type: none"><li>• <b>Attach report to email</b>—Select this option to receive reports as email attachments.</li></ul>

Option	Description
	<ul style="list-style-type: none"> <li>• <b>Upload report to file server</b>—Select this option to save reports on the selected file server. Click <b>Browse</b> 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.</li> </ul> <p><b>NOTE:</b> Make sure that your network resource is reachable and you have sufficient rights to access it.</p>
Filters	Specify the report filters, which vary depending on the selected report.

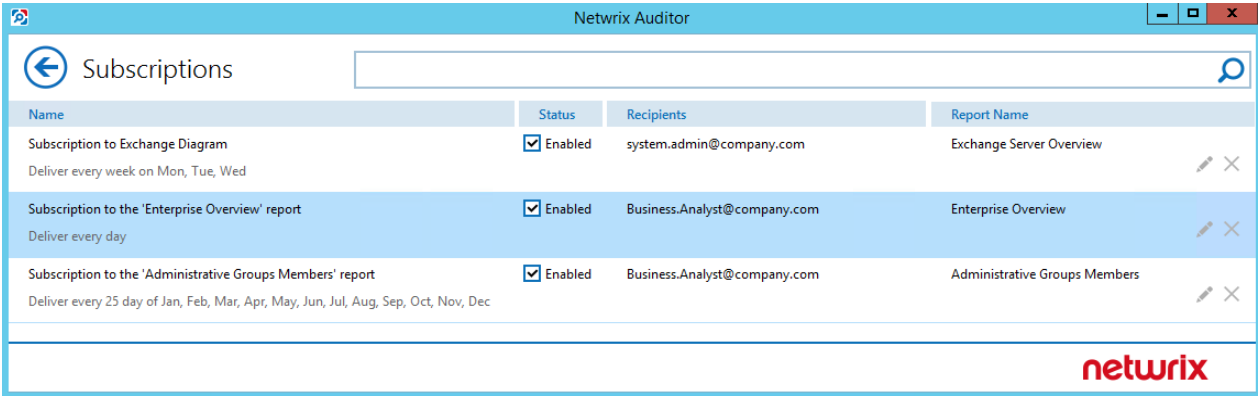
**NOTE:** Subscription emails may vary slightly depending on reports delivery method.





### 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 <b>Subscriptions</b> window and click the <b>Search</b> icon to review results.
Enable or disable subscriptions	Select a subscription and check or clear the <b>Enabled</b> checkbox in the <b>Status</b> 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.

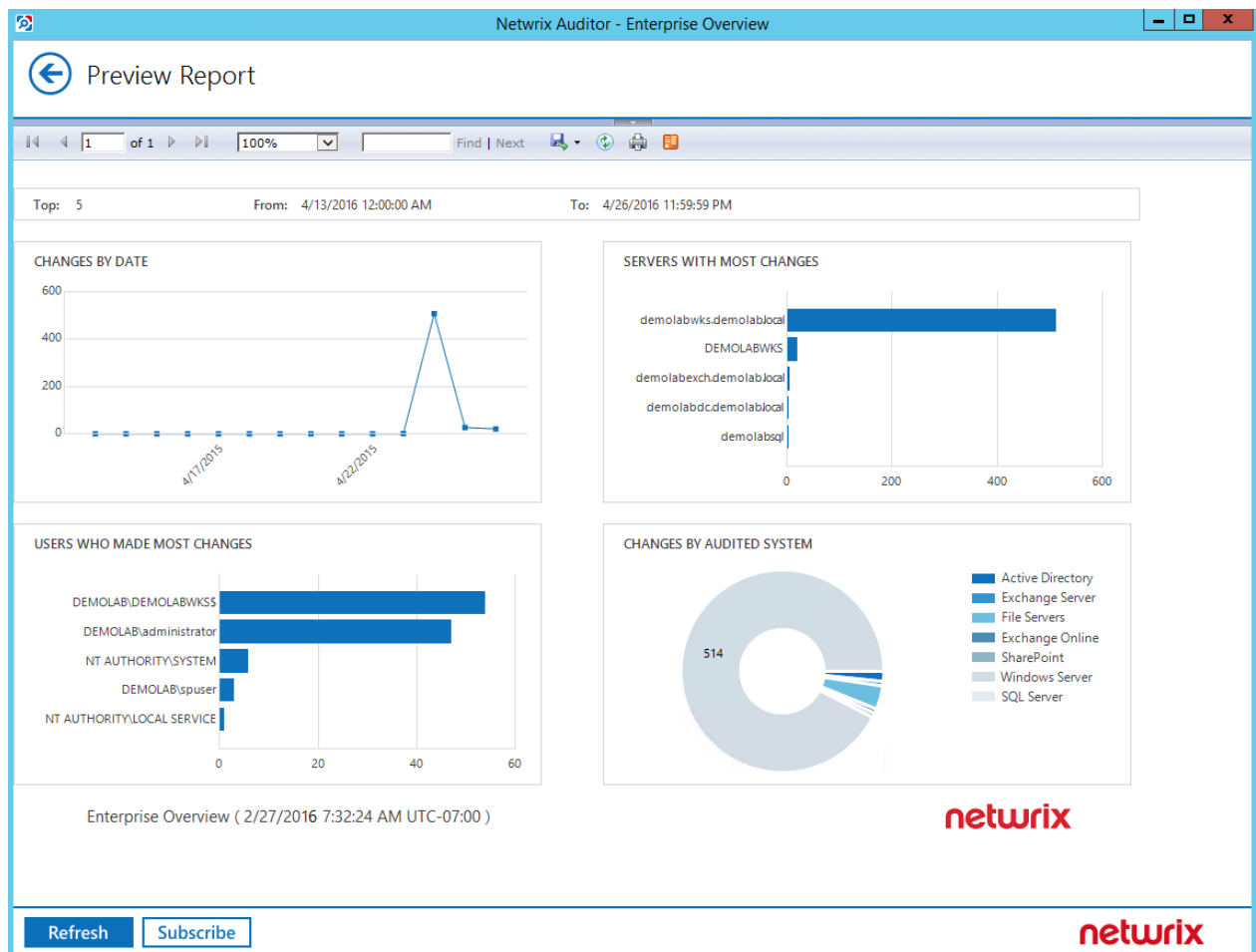
All diagrams provide the drill-down functionality, which means that by clicking on a segment, you will be redirected to a report with the corresponding filtering and grouping of data that renders the next level of detail.

### *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.

Netwrix Auditor					
Search	WHO	ACTION	WHAT	WHEN	WHERE
Who	Object type	Action	What	Where	When
CORP\administrator	group	Modified	\\local\corp\Users\Domain Admins	rootdc1.corp.local	4/24/2015 5:44:35 AM
Security Global Group Member - Added: "corp.local\Users\Bob Brown"					
CORP\administrator	group	Modified	\\local\corp\Users\Domain Admins	rootdc1.corp.local	4/24/2015 5:44:09 AM
Object Security: - Added: "Permissions: CORP\administrator (Allow: Write Add/Remove self as member)"					
CORP\administrator	group	Modified	\\local\corp\Users\Domain Admins	rootdc1.corp.local	4/24/2015 5:43:54 AM
Managed By changed to "local\corp\Users\Administrator"					
CORP\administrator	group	Modified	\\local\corp\Users\Accountants	rootdc1.corp.local	4/24/2015 4:16:35 AM
Security Local Group Member - Added: "corp.local\Users\John Smith"					
CORP\administrator	configuration	Modified	\\local\corp\Configuration	rootdc1.corp.local	4/24/2015 4:08:57 AM
Object Security: - Added: "Audit: Everyone (Success: Delete subtree. Delete, All validated writes, Delete all child objects, Create all child objects, All extended rights)"					
CORP\administrator	configuration	Modified	\\local\corp\Configuration	rootdc1.corp.local	4/24/2015 4:08:57 AM
Object Security: - Added: "Audit: Everyone (Success: Delete subtree. Delete, All validated writes, Delete all child objects, Create all child objects, All extended rights)"					
CORP\administrator	domainUNs	Modified	\\local\corp	rootdc1.corp.local	4/24/2015 4:08:56 AM
Object Security: - Added: "Audit: Everyone (Success: Delete subtree. Delete, All validated writes, Delete all child objects, Create all child objects, All extended rights)"					
CORP\administrator	group	Modified	\\local\corp\Users\Accountants	rootdc1.corp.local	4/24/2015 3:30:46 AM
Security Local Group Member - Added: "corp.local\Users\Peter Johnson"					

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

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

**NOTE:** Refer to [Audit Intelligence Search](#) for detailed instructions on how to apply filters and search audit data.

- Navigate to **Tools** and select **Save Search**.
- 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

- On the main Netwrix Auditor page, navigate to **Saved Searches**.
- Select one of the searches and click its tile to open search results.
- 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.

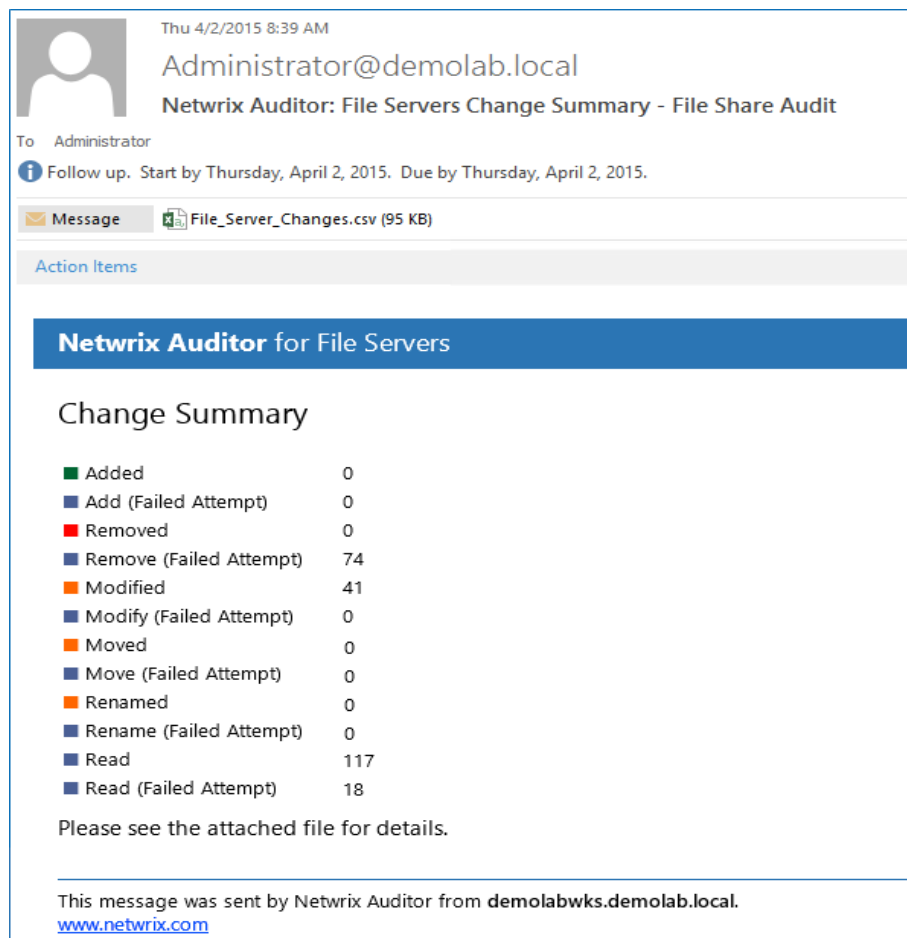
*To delete a saved search*

- 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.



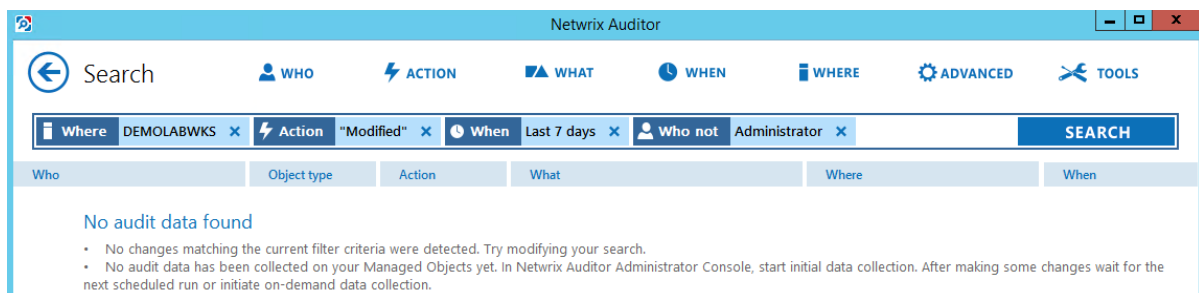
Netrix Auditor						
Search	WHO	ACTION	WHAT	WHEN	WHERE	ADVANCED TOOLS
Where	DEMOLABWKS	Action	"Modified"	When	Last 7 days	SEARCH
Who	Object type	Action	What	Where	When	
DEMOLAB\Administrator	File	Modified	\\DEMOLABWKS\Share\Corporate\Accounting_Fina...	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; NT AUTHORITY\SYSTEM (Allow: List folder / read data, Create files / write data, Create folders / append d...
DEMOLAB\Administrator	Folder	Modified	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Deny inheritable permissions from the parent to propagate to this object and all child objects; Everyone (Allow: List folder / read data, Read extended attributes, Traverse folder / execute file, Read attrib...
DEMOLAB\Administrator	Folder	Modified	\\DEMOLABWKS\Share\Projects	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; Everyone (Allow: List folder / read data, Read extended attributes, Traverse folder / execute file, Read attrib...
DEMOLAB\Administrator	Folder	Modified	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; Everyone (Allow: List folder / read data, Read extended attributes, Traverse folder / execute file, Read attrib...
DEMOLAB\Administrator	File	Modified	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; NT AUTHORITY\SYSTEM (Allow: List folder / read data, Create files / write data, Create folders / append d...
DEMOLAB\Administrator	File	Modified	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; NT AUTHORITY\SYSTEM (Allow: List folder / read data, Create files / write data, Create folders / append d...
DEMOLAB\Administrator	File	Modified	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; NT AUTHORITY\SYSTEM (Allow: List folder / read data, Create files / write data, Create folders / append d...
DEMOLAB\Administrator	File	Modified	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:33:47 AM	Permissions changed to "Allow inheritable permissions from the parent to propagate to this object and all child objects; NT AUTHORITY\SYSTEM (Allow: List folder / read data, Create files / write data, Create folders / append d...
DEMOLAB\Administrator	Folder	Modified	\\DEMOLABWKS\Share\Projects\Project B	DEMOLABWKS	4/2/2015 8:33:47 AM	

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

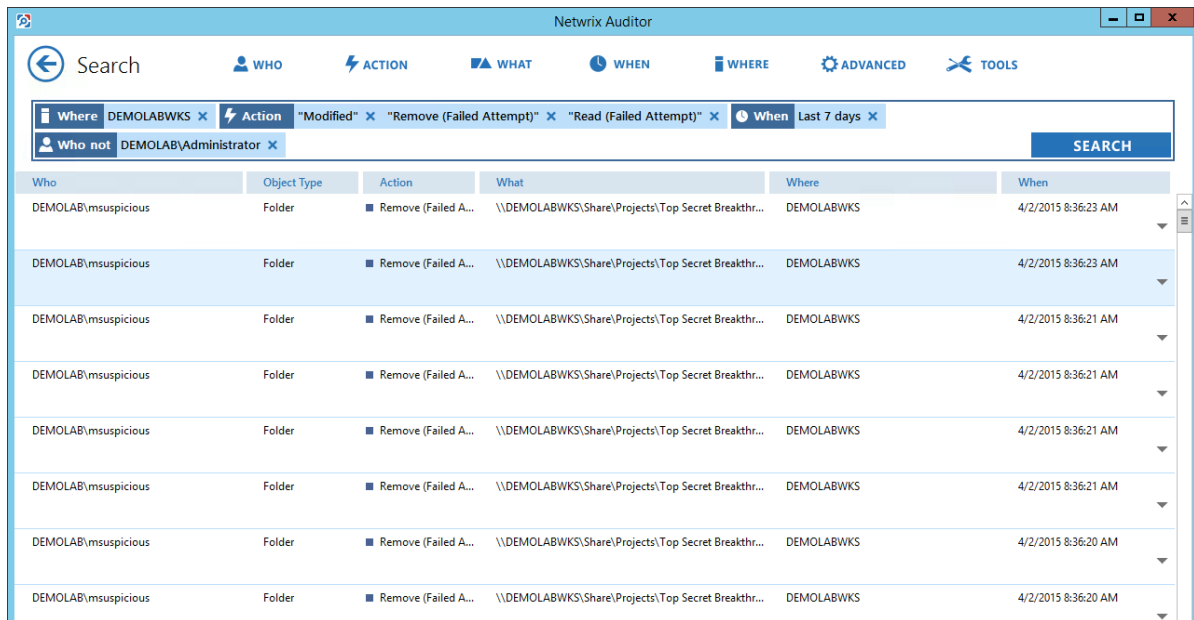
- You exclude **DEMOLAB\Administrator** from search results.

Who	Object type	Action
DEMOLAB\Administrator	File	Modified
Permissions changed to "Allow inheritable permissions from the parent to propagate to this		
DEMOLAB\Administrator	Folder	Modified
Permissions changed to "Deny inheritable permissions from the parent to propagate to this		
<div> <div>Exclude from search ▶</div> <div> <p><b>Details:</b> Permissions changed to "Deny i Read attributes, Read permission attributes, Write extended attrib This folder, subfolders and files; file, Delete subfolders and files, l (Allow: List folder / read data, C</p> </div> </div>		
DEMOLAB\Administrator		
Permissions changed to "Allow inheritab		
DEMOLAB\Administrator		
Permissions changed to "Allow inheritab		
DEMOLAB\Administrator		
Permissions changed to "Allow inheritable permissions from the parent to propagate to this		
DEMOLAB\Administrator	File	Modified

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.

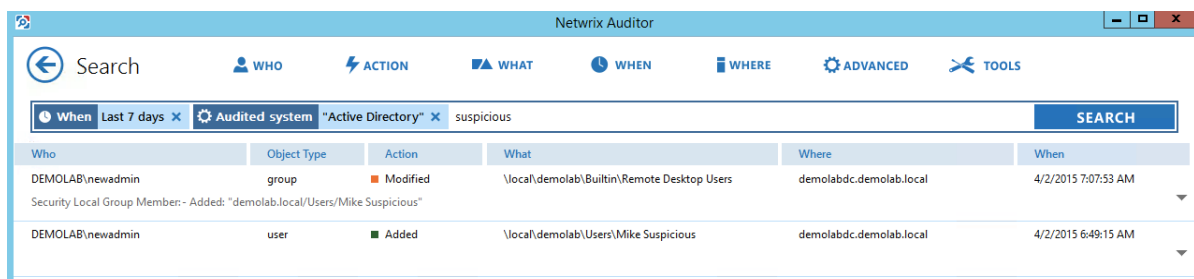


The screenshot shows the Netwrix Auditor interface with a search filter for 'Who not DEMOLAB\Administrator'. The search results table lists multiple failed actions performed by the 'msuspicious' user on a folder at 'DEMOLABWKS'.

Who	Object Type	Action	What	Where	When
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:23 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:23 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:21 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:21 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:21 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:21 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:20 AM
DEMOLAB\msuspicious	Folder	Remove (Failed A...	\\DEMOLABWKS\Share\Projects\Top Secret Breakthr...	DEMOLABWKS	4/2/2015 8:36:20 AM

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

- 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.

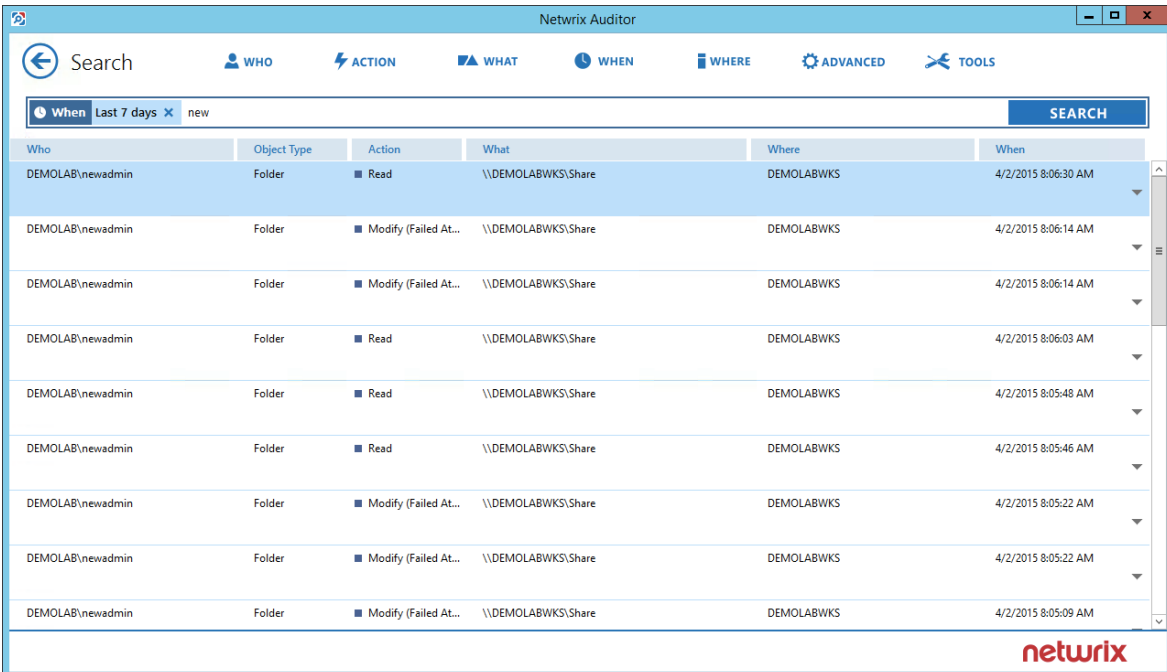


The screenshot shows the Netwrix Auditor interface with a search filter for 'Audited system "Active Directory" suspicious'. The search results table shows the creation of the 'msuspicious' user by the 'newadmin' user.

Who	Object Type	Action	What	Where	When
DEMOLAB\newadmin	group	Modified	\\local\demolab\Builtin\Remote Desktop Users	demolabdc.demolab.local	4/2/2015 7:07:53 AM
Security Local Group Member - Added: "demolab.local/Users/Mike Suspicious"					
DEMOLAB\newadmin	user	Added	\\local\demolab\Users\Mike Suspicious	demolabdc.demolab.local	4/2/2015 6:49:15 AM

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

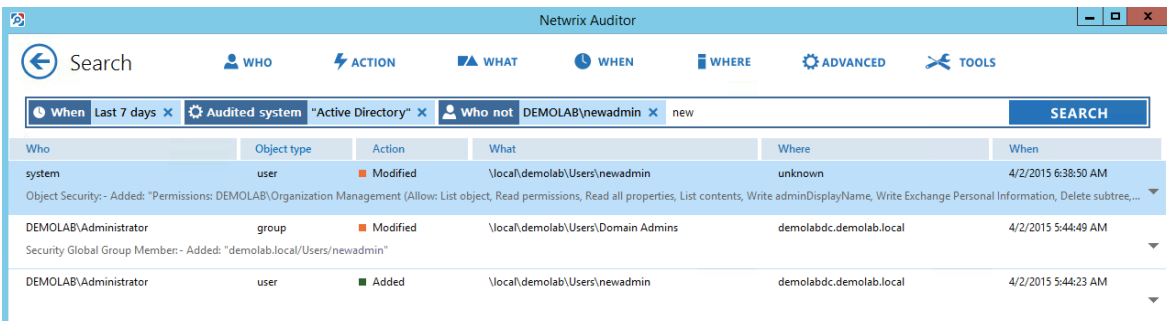
- Run a new search looking for anything to do with **newadmin**.



Who	Object Type	Action	What	Where	When
DEMOLAB\newadmin	Folder	Read	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:06:30 AM
DEMOLAB\newadmin	Folder	Modify (Failed At...	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:06:14 AM
DEMOLAB\newadmin	Folder	Modify (Failed At...	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:06:14 AM
DEMOLAB\newadmin	Folder	Read	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:06:03 AM
DEMOLAB\newadmin	Folder	Read	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:05:48 AM
DEMOLAB\newadmin	Folder	Read	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:05:46 AM
DEMOLAB\newadmin	Folder	Modify (Failed At...	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:05:22 AM
DEMOLAB\newadmin	Folder	Modify (Failed At...	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:05:22 AM
DEMOLAB\newadmin	Folder	Modify (Failed At...	\\DEMOLABWKS\Share	DEMOLABWKS	4/2/2015 8:05:09 AM

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**.



Who	Object type	Action	What	Where	When
system	user	Modified	\\local\demolab\Users\newadmin	unknown	4/2/2015 6:38:50 AM
DEMOLAB\Administrator	group	Modified	\\local\demolab\Users\Domain Admins	demolabdc.demolab.local	4/2/2015 5:44:49 AM
DEMOLAB\Administrator	user	Added	\\local\demolab\Users\newadmin	demolabdc.demolab.local	4/2/2015 5:44:23 AM

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	<b>Security Global Group Member</b> Added: "demolab.local/Users/Brad Davis"

This message was sent by Netwrix Auditor from demolabwks.demolab.local.  
[www.netwrix.com](http://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.

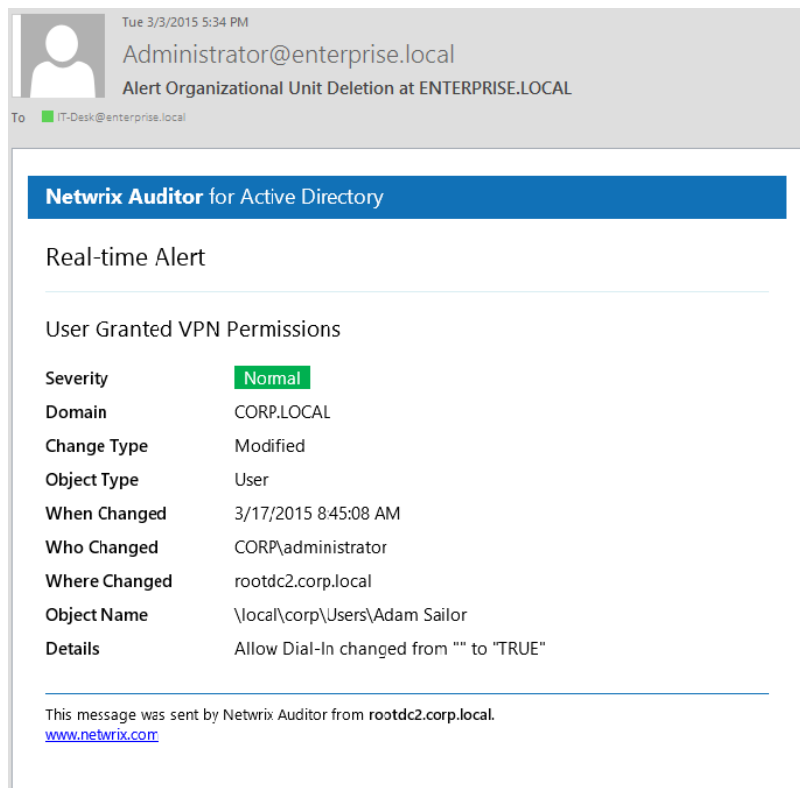
Real-time alerts are available for:

- 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

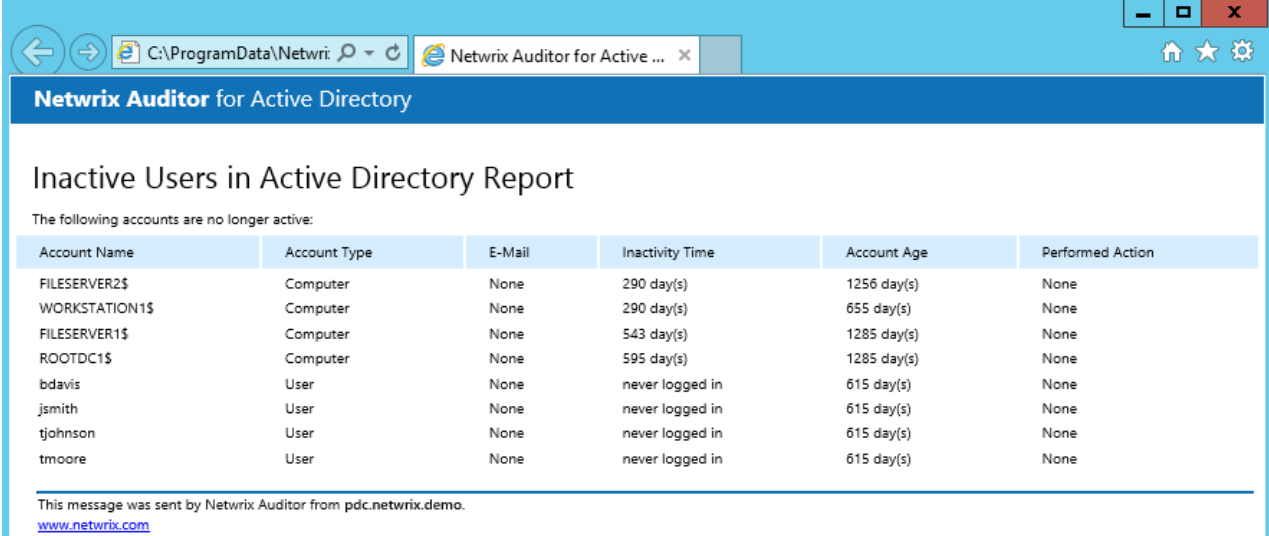
In Netwrix Auditor Administrator Console, administrator can generate additional reports to review inactive users and expiring passwords.

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.



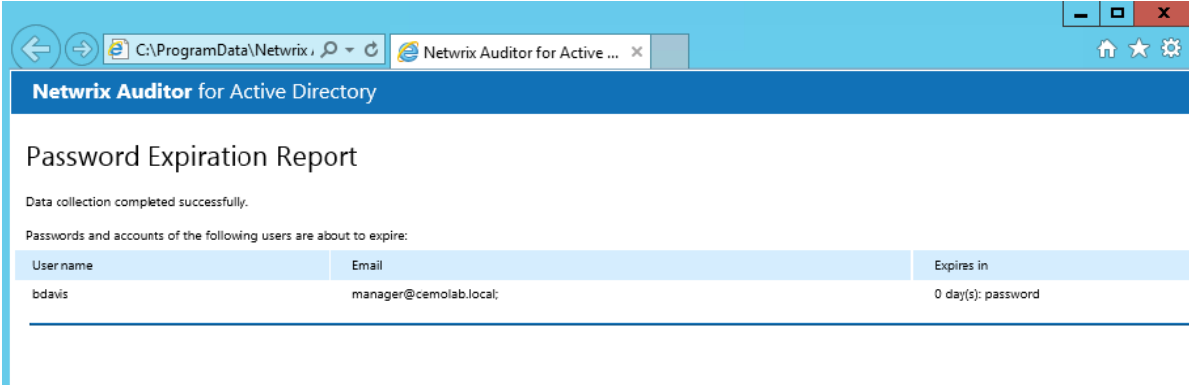
The screenshot shows a web browser window with the address bar displaying 'C:\ProgramData\Netwrix...' and the title 'Netwrix Auditor for Active ...'. The page title is 'Netwrix Auditor for Active Directory'. The main heading is 'Inactive Users in Active Directory Report'. Below the heading, a message states: 'The following accounts are no longer active:'. A table follows with the following data:

Account Name	Account Type	E-Mail	Inactivity Time	Account Age	Performed Action
FILESERVER2\$	Computer	None	290 day(s)	1256 day(s)	None
WORKSTATION1\$	Computer	None	290 day(s)	655 day(s)	None
FILESERVER1\$	Computer	None	543 day(s)	1285 day(s)	None
ROOTDC1\$	Computer	None	595 day(s)	1285 day(s)	None
bdavis	User	None	never logged in	615 day(s)	None
jsmith	User	None	never logged in	615 day(s)	None
tjohnson	User	None	never logged in	615 day(s)	None
tmoore	User	None	never logged in	615 day(s)	None

At the bottom, a message states: 'This message was sent by Netwrix Auditor from pdc.netwrix.demo. [www.netwrix.com](http://www.netwrix.com)'.

### 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.



The screenshot shows a web browser window with the address bar displaying 'C:\ProgramData\Netwrix...' and the title 'Netwrix Auditor for Active ...'. The page title is 'Netwrix Auditor for Active Directory'. The main heading is 'Password Expiration Report'. Below the heading, a message states: 'Data collection completed successfully.'. Another message states: 'Passwords and accounts of the following users are about to expire:'. A table follows with the following data:

User name	Email	Expires in
bdavis	manager@cemolab.local;	0 day(s); password



# 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.	<ol style="list-style-type: none"> <li>1. You may have insufficient permissions. Contact your Netwrix Auditor administrator to make sure that your account belongs to the <b>Netwrix Auditor Client Users</b> security group.</li> <li>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).</li> </ol>
I do not receive any results while searching audit data or generating reports, or I am sure that some data is missing.	<ol style="list-style-type: none"> <li>1. No changes were detected.</li> <li>2. Review your filter settings and make sure that your filters are properly configured. Try modifying your search.</li> <li>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.</li> <li>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.</li> <li>5. Some settings in Netwrix Auditor Administrator Console are configured incorrectly. Contact your Netwrix Auditor administrator to make sure that: <ul style="list-style-type: none"> <li>• The Managed Object you want to audit is properly configured, and the <b>Enable &lt;Audited_System&gt; audit</b> checkbox is selected for each audited system individually.</li> <li>• Audit Database settings are properly configured for each audited system individually and <b>Make audit data available via summary emails only</b> is cleared.</li> </ul> </li> </ol>

**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 <b>Managed Object</b> 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., <code>\\filestorage\reports</code> ) 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 <b>Read</b> permission.

# Index

## A

Additional options 53-54

    Change Summary 53

AuditIntelligence

    Enterprise Overview 42

    Reports 25

    Search 15

## B

Browse audit data 15

## C

Change Summary 53

## D

Diagrams 42

## E

Enterprise Overview 42

## H

How it works 7

## L

Launch 13

## N

Netwrix Auditor Administrator Console 7, 53-54

Netwrix Auditor client 7

## O

Overview 5

## R

Real-Time Alerts 54

## Reports

Ad-hoc 56

Change management 26

Change reports 25, 32

Change Review Status reports 26

Changes with video 26

Compliance 38

Filtering 29

Organization Level reports 25, 31

Overview diagrams 42

Overview reports 25

Reports with review status 36

Reports with video 35

SSRS-based Reports 25

State-in-Time Reports 25, 33

Subscriptions 39

## S

Saved Searches 45

## Search

Advanced 19

Browse data 15

Copy and paste 24

Example 48

Export data 24

Filters 17

Include and exclude data 23

Match types 21

More filters 19

Save 45

Subscriptions 39

**T**

Troubleshooting 57

**U**

Usage Example 48

**W**

Workflow 9