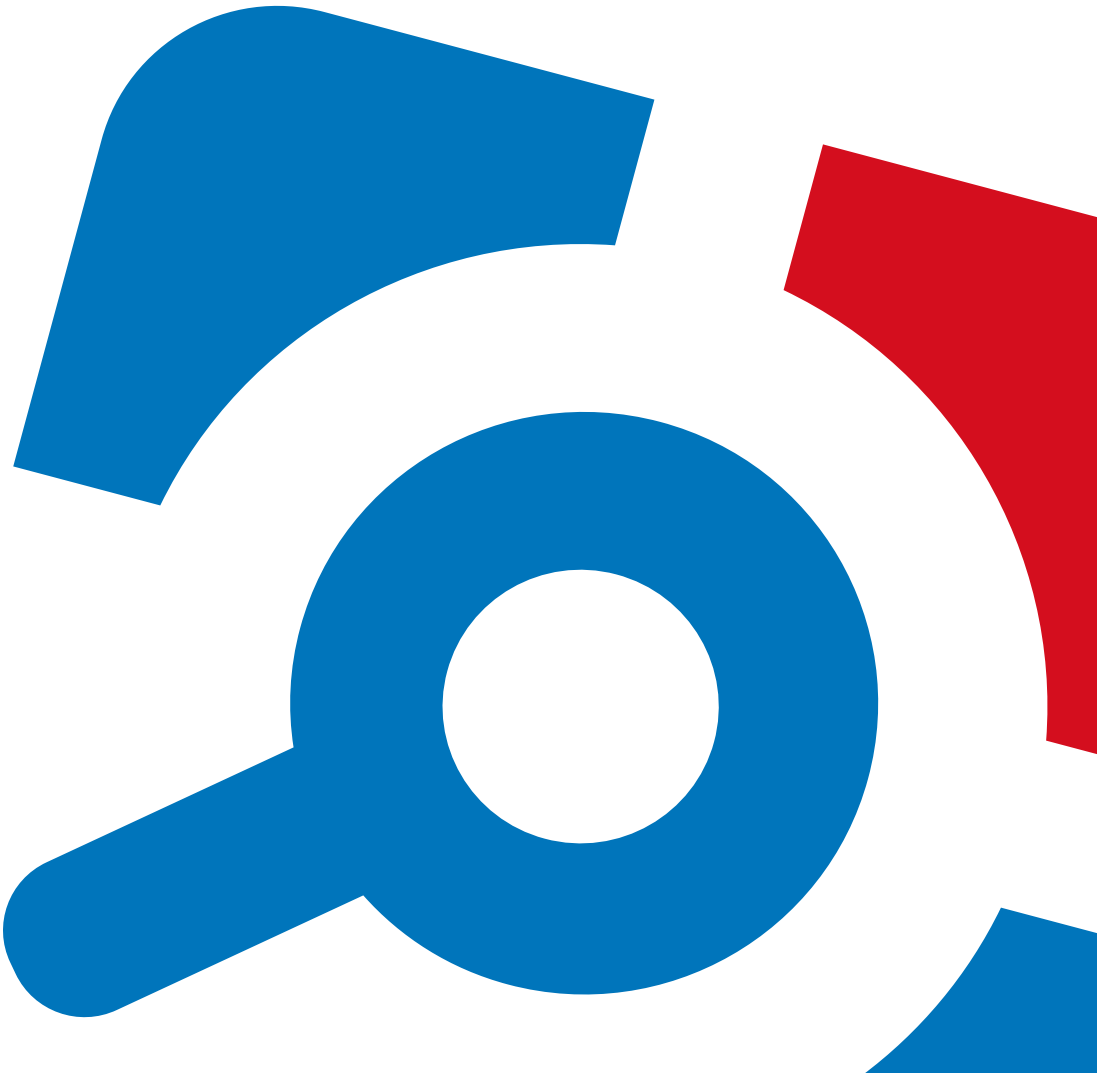
netwrix

Netwrix Auditor for EMC

Quick-Start Guide

Version: 9.6
9/21/2018



Legal Notice

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

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

Disclaimers

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

Table of Contents

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for EMC. It can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Install and configure Netwrix Auditor
- Create a monitoring plan to start auditing EMC appliances
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing EMC appliances with Netwrix Auditor. For advanced installation scenarios and configuration options, as well as for information on various reporting possibilities and other product features, refer to:

- Netwrix Auditor Installation and Configuration Guide
- Netwrix Auditor Administration Guide
- Netwrix Auditor Intelligence Guide

1.1. Netwrix Auditor Overview

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

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

Major benefits:

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

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

Netwrix Auditor for EMC detects and reports on all changes made to EMC VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.

2. Prerequisites and System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed.

To learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs. To learn how to install a license, refer to Licenses.

2.1. Supported Data Sources

The table below lists systems that can be monitored with Netwrix Auditorfor EMC:

Data source	Supported Versions
EMC	• EMC VNX/VNXe/Celerra families (CIFS configuration only) • EMC Isilon 7.2.0.0 – 7.2.0.4, 7.2.1.0 – 7.2.1.2, 8.0.0.0 , 8.1.0.0 (CIFS configuration only) • EMC Unity – for recommendations on setting up the auditing, see this Netwrix Knowledge Base article.

2.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements

2.2.1. Hardware Requirements

Review the hardware requirements for Netwrix Auditor installation.

The metrics provided in this section are valid for clean installation on a server without any additional roles or third part applications installed on it. The use of virtual machine is recommended.

The hardware configuration depends on the size of your monitored environment and the number of activity records processed by the product per day. Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for EMC. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on the Netwrix Auditor hardware requirements.

Hardware component	Starter, evaluation, or small environment
Processor	2 cores
RAM	4 GB
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)
Screen resolution	Minimum 1280 x 1024 Recommended 1920 x 1080 or higher

2.2.2. Software Requirements

The table below lists the software requirements for the Netwrix Auditor installation:

Component	Requirements
Operating system	• Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8.1, and Windows 10 • Windows Server OS: Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2, and Windows Server 2016
.NET Framework	• .NET Framework 3.5 SP1. **NOTE:** To audit VMware vSphere 6.7, .NET Framework 4.5 or 4.6 is required.
Installer	• Windows Installer 3.1 and above

3. Review Components Checklist

To speed up the evaluation process, Netwrix recommends you to ensure that the following services and components are up and running prior to the Netwrix Auditor installation.

Service or component	Recommendations
Network and target systems or servers that work as your data sources	Test connectivity to your data source. Make sure you can access it by its NetBIOS and FQDN name from the computer where you intend to install Netwrix Auditor—use the nslookup command-line tool to look up domain names. Domain controllers must be accessible as well.
SQL Server 2014 with SSRS (optional step)	Although Netwrix Auditor provides a convenient interface for downloading SQL Server 2014 Express right from Netwrix Auditor, it is recommended to deploy SQL Server instance in advance. Test your SQL Server connectivity. **NOTE:** Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor.

Test account	Netwrix recommends you to create a special account with extensive privileges. This account should have sufficient permissions to:
	• Collect audit data. See Configure Data Collecting Account for more information.
	• Access data stored in the SQL Server instance:
	  • The account must be assigned the **Database owner (db_owner)** role and the **dbcreator** server role.
	  • The account must be assigned the **Content Manager** role on the SSRS Home folder.
	• Make test changes in your environment.

3.1. Configure Data Collecting Account

This service account is specified on the monitoring plan creation and is used to collect audit data from the data source items. To ensure successful data collection, Netwrix recommends creating a special service account in advance. The account must comply with the following requirements depending on the data source.

NOTE: The information in this section is outside the quick-start guide scope and is provided for reference only. See Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to configure your Data Processing Account.

Data source	Rights and permissions
EMC Isilon	*On the target server:* • A member of the local **Administrators** group • The **Read** permissions on the audited shared folders
EMC VNX/VNXe	*On the target server:* • The **Read** share permissions on to the audited shared folders • A member of the local **Administrators** group

4. Configure EMC Storages for Monitoring

4.1. Configure EMC VNX/VNXe for Monitoring

To collect comprehensive audit data, you must configure your file shares for monitoring. The configuration includes several manual and automatically performed steps:

- Automatically when creating a monitoring plan—partially. Only audit settings for file shares will be configured.
- Manually.
  - Configure Security Event Log Maximum Size to avoid overwriting of the security logs; it is recommended to set security log size to a maximum (4GB).
  - Configure Audit Object Access Policy. Set the **Audit object access** policy set to *"Success"* and *"Failure"* in the Group Policy of the OU where your EMC VNX/VNXe/Celerra appliance belongs to.

  To configure EMC Unity storage system audit, take the steps described in this Netwrix Knowledge Base article.

4.1.1. Configure Security Event Log Maximum Size

1. On your file server, create a new file system where the security log will be stored.
2. Mount this file system on a mount point, e.g., **/events**.
3. Make sure that it is accessible via the **\\<file_server_name>\C$\events** UNC path.
4. On the computer where Netwrix Auditor Server is installed, open **Registry Editor**: navigate to **Start → Run** and type *"regedit"*.
5. Navigate to **File → Connect Network Registry** and specify the file server name.
6. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security** and set the **File** value to *"C:\events\security.evt"*.
7. Set the **MaxSize** value to *"4 000 000 000 (decimal)"*.
8. Restart the corresponding Data Mover for the changes to take effect.

4.1.2. Configure Audit Object Access Policy

NOTE: Netwrix recommends you to avoid linking a GPO to the top level of the domain due to the potential impact. Instead, create a new organization unit for your file servers within your domain and assign

GPO there. For detailed instructions on how to create a new OU, refer to the following Microsoft article: Create a New Organizational Unit.

1. Open the **Group Policy Management** console on any domain controller in the target domain: navigate to **Start → Windows Administrative Tools** (Windows Server 2016) or **Administrative Tools** (Windows 2012 R2 and below) → **Group Policy Management.**
2. In the left pane, navigate to **Forest: <forest_name> → Domains → <domain_name>**, right-click **<OU_name>** and select **Create a GPO in this domain and Link it here**.
3. Enter the name for the new GPO.
4. Right-click the newly created GPO and select **Edit**.
5. In the **Group Policy Management Editor** dialog, expand the **Computer Configuration** node on the left and navigate to **Policies → Windows Settings → Security Settings → Local Policies → Audit Policy.**

Policy Subnode	Policy Name	Audit Events
Audit Policy	**Audit object access**	*"Success"* and *"Failure"*

6. Navigate to **Start → Run** and type *"cmd"*. Input the `gpupdate /force` command and press **Enter**. The group policy will be updated.

NOTE: You can configure advanced audit policy to narrow the range of events tracked and recorded by the product, thus preventing your AuditArchive and the Security event log from overfilling. See Netwrix Auditor Installation and Configuration Guide for more information.

4.2. Configure EMC Isilon in Normal and Enterprise Modes

You can configure your cluster for monitoring in one of the following ways:

- Using the **configure_ifs.sh** shell script that comes with Netwrix Auditor. See To configure EMC Isilon cluster in Normal and Enterprise mode via shell script for more information.
- Manually. See Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to configure EMC Isilon for auditing manually.

To configure EMC Isilon cluster in Normal and Enterprise mode via shell script

1. On the computer where Netwrix Auditor Server resides, navigate to *C:\Program Files (x86)\Netwrix Auditor\File Server Auditing* and copy the **configure_ifs.sh** shell script to */ifs/data* catalog on your cluster.
2. Navigate to your cluster command prompt through the **SSH** connection.
3. Log in to your cluster as a root user.

4. Run the shell script by executing the following command:

   ```
   sh /ifs/data/configure_ifs.sh -z zone1 -a 15
   ```

   where

   `zone1` is the name of the audited access zone on your file server.

   `15` is a combination of the bitwise flags. The table below shows the example combination of 4 flags:

   ```
   Successful changes        1
   Failed change attempts    2
   Successful reads          4
   Failed read attempts      8
   Total:                    15
   ```

5. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 9.6 from Netwrix website.
2. Unpack the installation package. The following window will be displayed on successful operation completion:

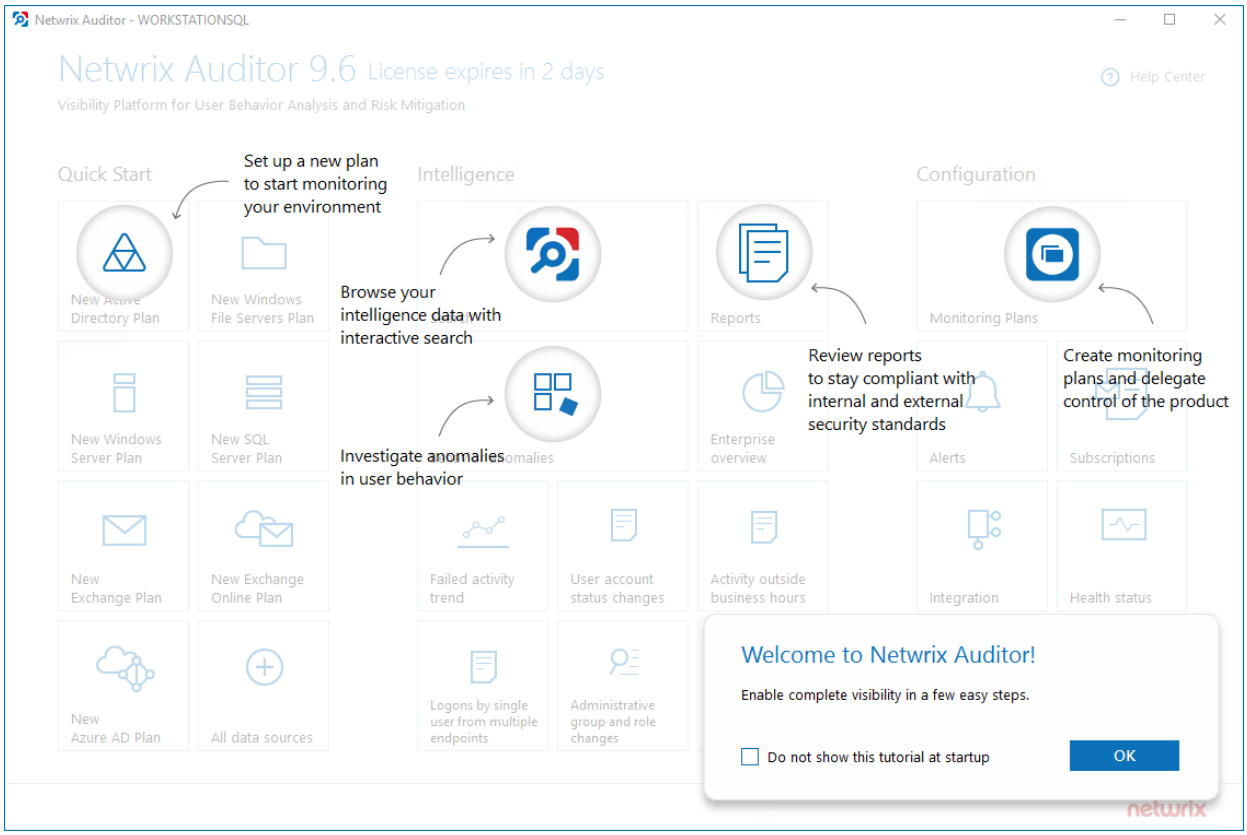
3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.

   NOTE: See Netwrix AuditorServer and Client for details.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are invited to take part in the Netwrix Customer Experience Program. It is optional on your part to help Netwrix improve the quality, reliability, and performance of Netwrix products and services. If you accept, Netwrix collects statistical information on how the Licensee uses the product in accordance with applicable law. Select **Skip** if you do not want to participate in the program.

NOTE: You can always opt-out of the Netwrix Customer Experience Program later. See Netwrix Auditor Online Helpcenter for instructions on how to cancel participation in the program.

7. Click **Install**.

After a successful installation, Netwrix Auditor shortcut will be added to the **Start** menu/screen and the product will start.



6. Monitoring Plans

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan. All your monitoring plans are listed in the **Monitoring Plans** section.

A monitoring plan defines your data sources and general data collection, notification, and storage settings. To start collecting data, choose a data source, such as EMC, and add items to its scope. Item is a specific object you want to audit. All data sources and items in your plan share common settings so that you can supervise and manage several data collections as one.

On a high level, you should perform the following steps to start monitoring your environment:

1. Specify a data source and create a monitoring plan with a wizard. See Create a New Plan for more information.
2. Add items for monitoring. Netwrix Auditor does not collect data until you specify an item. See Add Items for Monitoring for more information.

6.1. Create a New Plan

On the main Netwrix Auditor page, click the **All data sources** tile in the **Quick Start** section.

The wizard that appears will help you set up a new plan in a few easy steps:

- Choose a data source for monitoring
- Specify an account for collecting data
- Specify default SQL Server instance and configure the Audit Database to store your data
- Configure notification settings
- Specify the recipients who will receive daily activity summaries
- Specify a plan name

6.1.1. New Monitoring Plan (Data Source)

Specify the **EMC** tile.

6.1.2. New Monitoring Plan

Option	Description
Specify the account for collecting data	Provide a user name and a password for the account that Netwrix Auditor will use to collect data. By default, the user name is prepopulated with your

Option	Description
	account name. Make sure the account has sufficient permissions to collect data. For a full list of the rights and permissions, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide. Netwrix recommends creating a special service account with extended permissions.
Configure audit settings	Select **Adjust audit settings automatically**. In this case, Netwrix Auditor will continually check and enforce the relevant audit policies. **NOTE:** If you plan to monitor EMC Isilon, clear the checkbox. Currently, Netwrix Auditor cannot configure audit on EMC Isilon appliances automatically. If you want to audit EMC VNX/VNXe, select **Adjust audit settings automatically**, but only audit settings for file shares will configured, the rest of settings must be configured manually. For a full list of audit settings and instructions on how to configure them manually, refer to Netwrix Auditor Installation and Configuration Guide.

6.1.3. Default SQL Server Instance

To provide search, alerting, and report capabilities, Netwrix Auditor has to store security intelligence data in the Audit Database hosted on a SQL Server instance. Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared.

Specify one of the following options:

- **Install a new instance of Microsoft SQL Server Express automatically**—Select if you want Netwrix Auditor to download and configure SQL Server 2014 Express with Advanced Services.
- **Use an existing SQL Server instance**—Select to continue using an installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and prepopulates the fields. Complete the following fields:

Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication

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

6.1.4. Audit Database

Specify a database name to store security intelligence data for your monitoring plan, or disable this functionality. Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared and **Use default SQL Server settings** is checked.

Netwrix Auditor will create a database on the SQL Server instance you specify.

6.1.5. Notifications

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

Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the **From** field. NOTE: It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.

Option	Description
Password	Enter a password for the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL authentication	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission.

6.1.6. Recipients

Specify who will receive daily activity summaries that list changes that occurred for a given time period. Click **Add Recipient** and enter your email.

NOTE: It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

6.1.7. Monitoring Plan Summary

Your plan is almost complete. Provide a name and description for your monitoring plan. Make sure the **Add item now** checkbox is selected. In this case, on the next step, you will be prompted to add an item for monitoring.

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

6.2. Add Items for Monitoring

Once you completed monitoring plan wizard and specified data sources, add items for monitoring.

Each data source has a dedicated item type. Netwrix Auditor automatically suggests item types associated with your data source. For example, select the **EMC VNX/VNXe** item.

6.2.1. EMC VNX/VNXe

Complete the following fields:

Option	Description
	General
Specify EMC VNX or VNXe storage array	Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click **Browse** to select a computer from the list of computers in your network.
Specify the account for collecting data	Select the account that will be used to collect data for this item.
	Scope
Monitor the following shares	If you want to limit your auditing scope by several shares, click **Add** under the **Specific file shares** and select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.

7. Make Test Changes

Now that the product has collected a snapshot of the data source's current configuration state, you can make test changes to see how they will be reported by Netwrix Auditor.

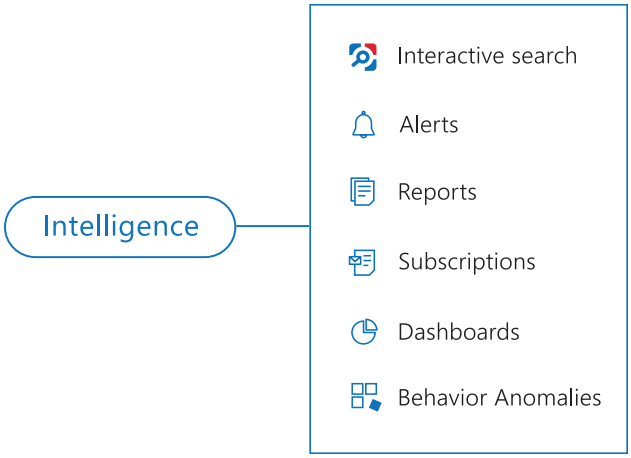
For example, make the following test changes:

- Create a new file/folder in your file share
- Modify a file attribute in your file share

NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

8. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to your environment, you can see how Netwrix Auditor brings security intelligence into your IT infrastructure and enables complete visibility. Take a closer look at the **Intelligence** section. It contains everything you need to enable complete visibility in your environment.



This chapter explains how to review your test changes with some of the Intelligence options and Activity Summary. Review the following for additional information:

- Review an Activity Summary
- Review File Servers Overview
- Review the All File Server Activity Report
- Browse Data with Intelligence Search

In order not to wait for a scheduled Activity Summary generation, force data collection and email delivery.

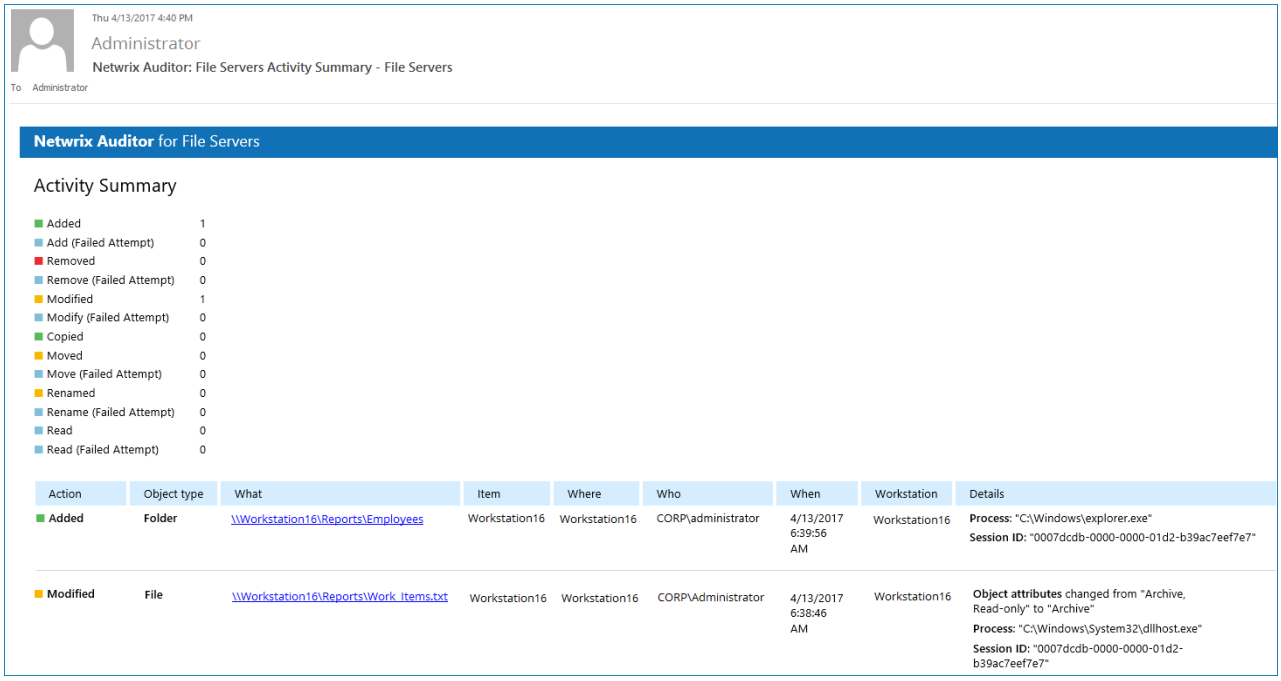
To launch data collection manually

1. Navigate to **Monitoring Plans** and select your plan in the list.
2. Click **Edit**.
3. In the your monitoring plan settings, click **Update** in the right pane.
4. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

8.1. Review an Activity Summary

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

After the data collection has completed, check your mailbox for an Activity Summary and see how your test changes are reported:



Thu 4/13/2017 4:40 PM

Administrator

Netwrix Auditor: File Servers Activity Summary - File Servers

To Administrator

Netwrix Auditor for File Servers

Activity Summary

Added	1
Add (Failed Attempt)	0
Removed	0
Remove (Failed Attempt)	0
Modified	1
Modify (Failed Attempt)	0
Copied	0
Moved	0
Move (Failed Attempt)	0
Renamed	0
Rename (Failed Attempt)	0
Read	0
Read (Failed Attempt)	0

Action	Object type	What	Item	Where	Who	When	Workstation	Details
Added	Folder	\\Workstation16\Reports\Employees	Workstation16	Workstation16	CORP\administrator	4/13/2017 6:39:56 AM	Workstation16	**Process:** "C:\Windows\explorer.exe" **Session ID:** "0007dcdb-0000-0000-01d2-b39ac7eef7e7"
Modified	File	\\Workstation16\Reports\Work Items.txt	Workstation16	Workstation16	CORP\Administrator	4/13/2017 6:38:46 AM	Workstation16	**Object attributes** changed from "Archive, Read-only" to "Archive" **Process:** "C:\Windows\System32\dllhost.exe" **Session ID:** "0007dcdb-0000-0000-01d2-b39ac7eef7e7"

The example Activity 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 object.
What	Shows the name of the changed object or its path.
Item	Shows the item associated with the selected monitoring plan.
Where	Shows the name of the server where the change occurred.
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 of the computer where the user was logged on when the change was

Column	Description
	made.
Details	Shows the before and after values of the modified object, object attributes, etc.

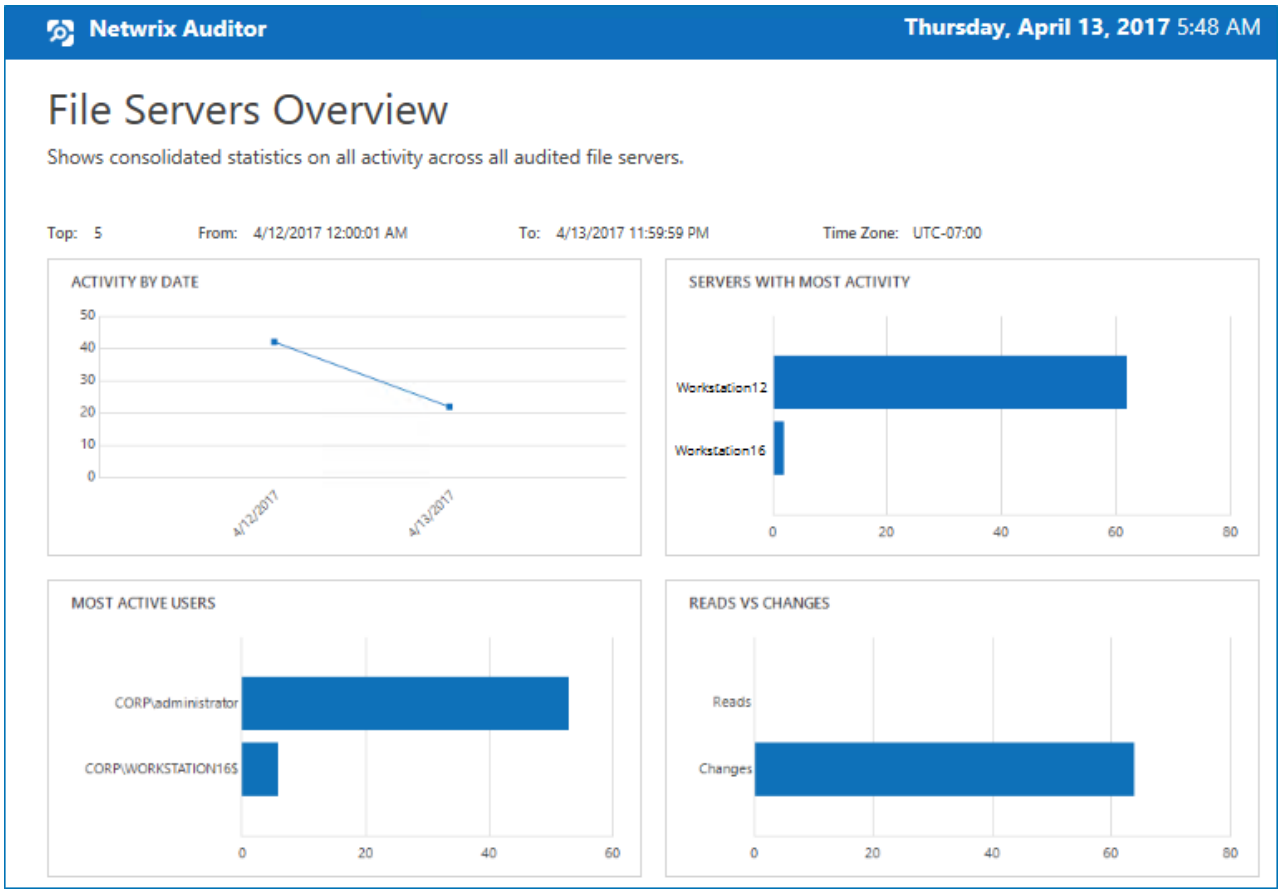
8.2. Review File Servers Overview

Enterprise diagram provides a high-level overview of activity trends by date, user, server, object type or data source in your IT infrastructure. The **Enterprise** diagram aggregates data on all monitoring plans and all data sources, while system-specific diagrams provide quick access to important statistics within one data source.

After collecting initial data, making test changes to your environment and running data collection again, you can get at-a-glance statistics for changes with the **File Servers Overview**.

To see how your changes are reported with File Servers Overview

1. On the main Netwrix Auditor page, navigate to the **Intelligence** section and click the **Reports** tile.
2. Expand the **Predefined** → **File Servers** → **File Servers Activity** reports.
3. Select the **File Servers Overview** report and click **View**.
4. Review your changes.
5. Click on any chart to jump to a table report with the corresponding grouping and filtering of data.



8.3. Review the All File Server Activity Report

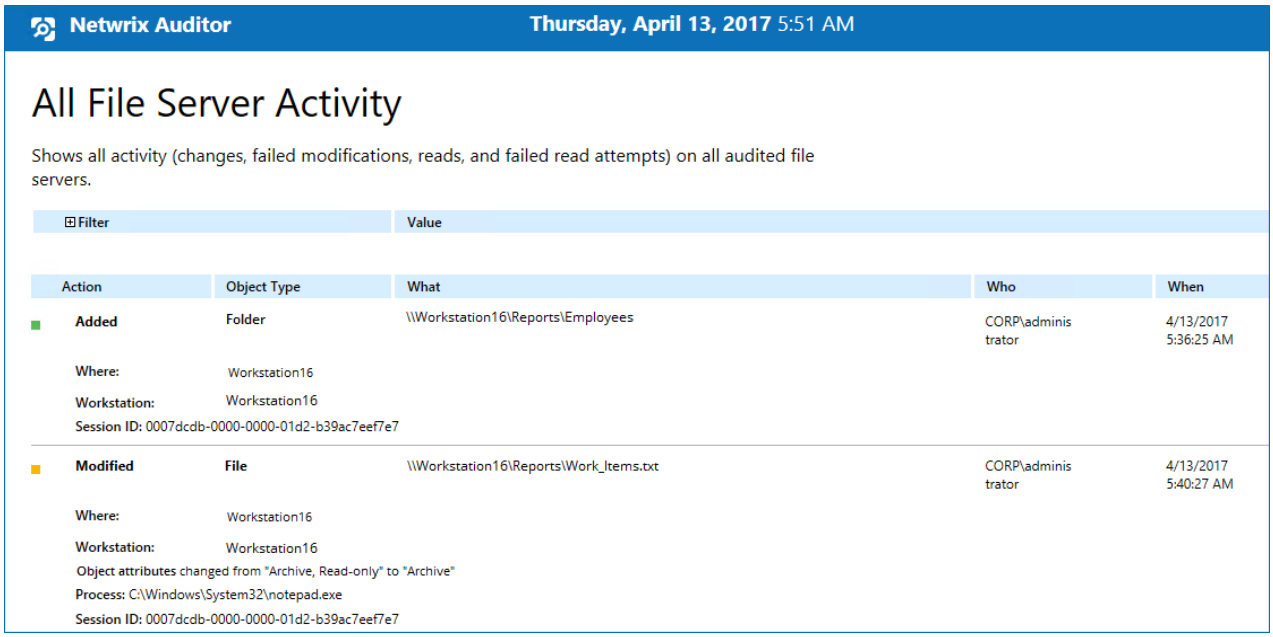
The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

Change and activity reports can be found under the **Reports → Predefined → File Servers → File Servers Activity** and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

After collecting initial data, making test changes to your environment and running data collection again, you can take advantage of the reports functionality.

To see how your changes are listed in the report

1. On the main Netwrix Auditor page, navigate to **Reports → Predefined → File Servers → File Servers Activity**.
2. Select the **All File Server Activity** report.
3. Click **View** to open the report.



8.4. Browse Data with Intelligence Search

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

After collecting initial data, making test changes to your environment and running data collection again, you can review changes in details with Intelligence search.

To browse your audit data and see you test changes

1. On the main Netwrix Auditor page, navigate to **Intelligence → Search**.
2. Add search filters to your search by clicking on a corresponding icon and providing a value. By default, all entries that contain this filter value are shown. For an exact match, use quotation marks.

   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.

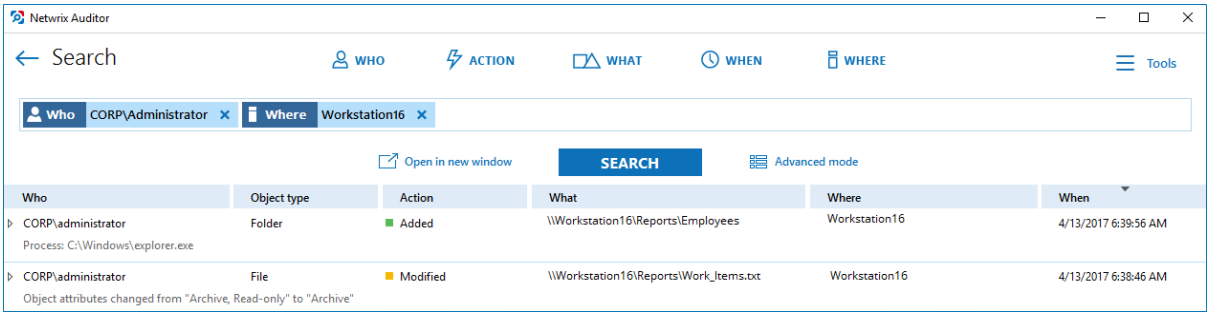
   For example, consider adding these filters:

Filter	Value
WHO	Specify your account name, as you performed test changes.
WHERE	Specify your file server name.

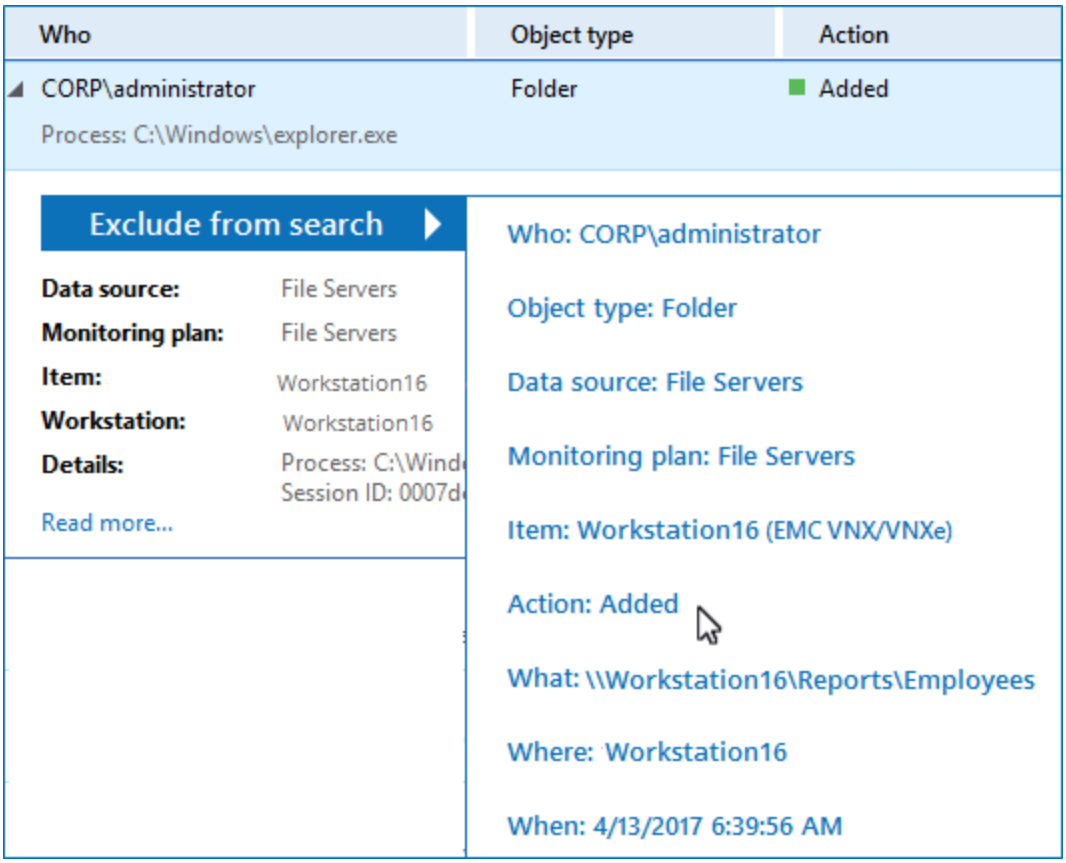
NOTE: Refer to Netwrix Auditor Intelligence Guide for detailed instructions on how to apply filters and change match types.

As a result, you will see the following filters in the **Search** field:

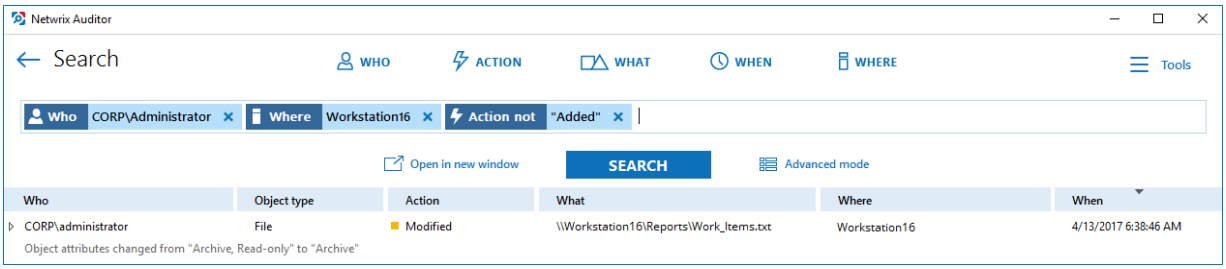
3. Click **Search**.



4. Now, you can narrow your search and modify it right from the search results pane. Double-click any entry that contains excess data, select **Exclude from search** and specify a filter, e.g., **Action**: *Added* to leave information on modifications only.



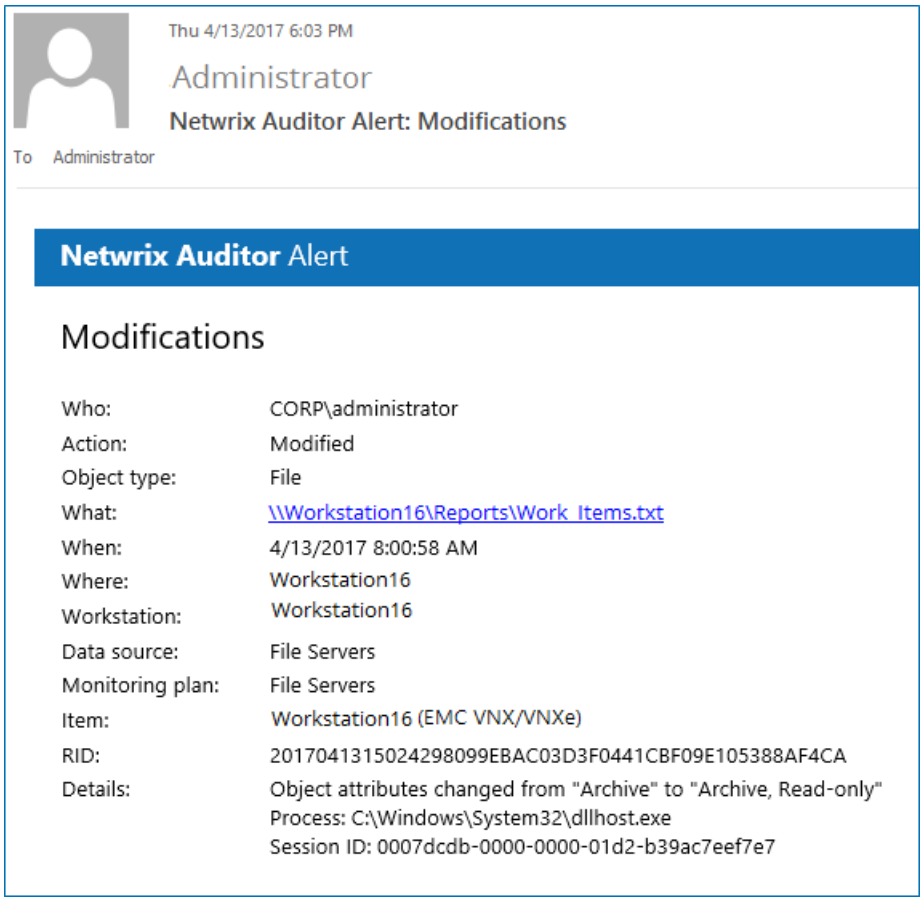
Your **Search** field will be updated, the filter will be added. Make sure to click **Search** again to update your search results.



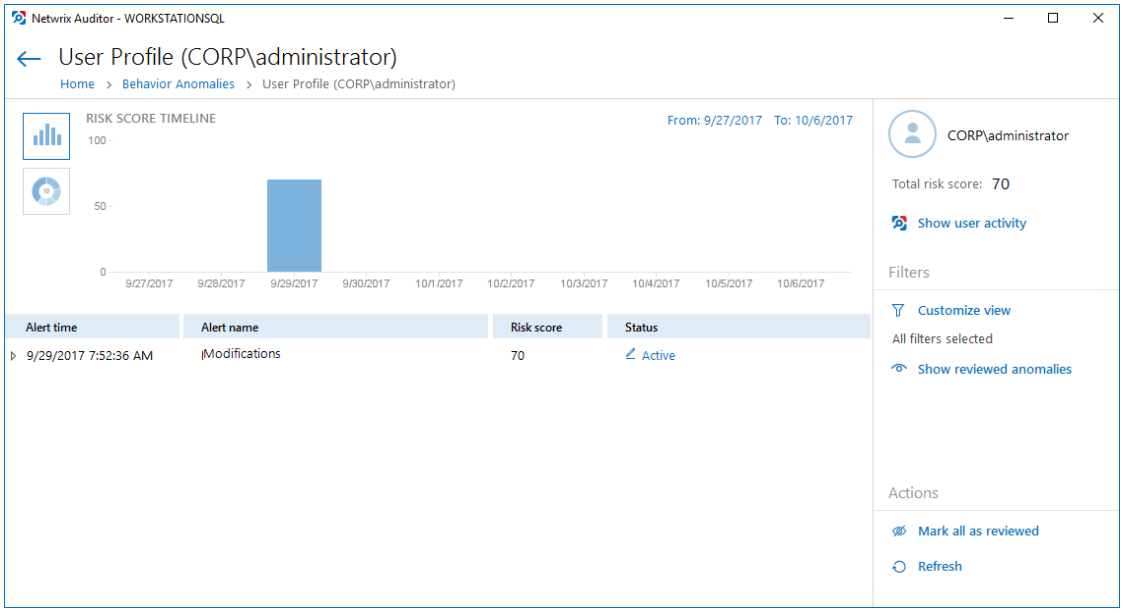
5. Having reviewed your search results, navigate to **Tools**.

   - Click **Save as report** to save the selected set of filters. This search will be added to the **Custom** section inside **Reports**, so that you will be able to access it instantly. Refer to Netwrix Auditor Intelligence Guide for detailed instructions on how to create saved searches.
   - Click **Create alert** to get instant email or SMS notifications on suspicious activity that matches your current search criteria. You only need to specify a name for a new alert, add recipient and assign a risk score. The selected set of search criteria will be associated with the new alert automatically. Refer to Netwrix Auditor Administration Guide for detailed instructions on how to create and configure alerts.

     Try making more similar test changes to provoke an alert. For example:



Once you have received the alert, click the **Behavior Anomalies** tile on the main Netwrix Auditor page to see how the product identifies potentially harmful users and displays their risk scores. Drill-down to user profile to review anomalies and mitigate risks. Refer to Netwrix Auditor Intelligence Guide for more information on behavior anomalies and risk scores.



9. Related Documentation

The table below lists all documents available to support Netwrix Auditor for EMC:

Document	Description
Netwrix Auditor Online Help Center	Gathers information about Netwrix Auditor from multiple sources and stores it in one place, so you can easily search and access any data you need for your business. Read on for details about the product configuration and administration, its security intelligence features, such as interactive search and alerts, and Integration API capabilities.
Netwrix Auditor Installation and Configuration Guide	Provides detailed instructions on how to install Netwrix Auditor, and explains how to configure your environment for auditing.
Netwrix Auditor Administration Guide	Provides step-by-step instructions on how to configure and use the product.
Netwrix Auditor Intelligence Guide	Provides detailed instructions on how to enable complete visibility with Netwrix Auditor interactive search, report, and alert functionality.
Netwrix Auditor Integration API Guide	Provides step-by-step instructions on how to leverage Netwrix Auditor audit data with on-premises and cloud auditing solutions using RESTful API.
Netwrix Auditor Release Notes	Lists the known issues that customers may experience with Netwrix Auditor 9.6, and suggests workarounds for these issues.