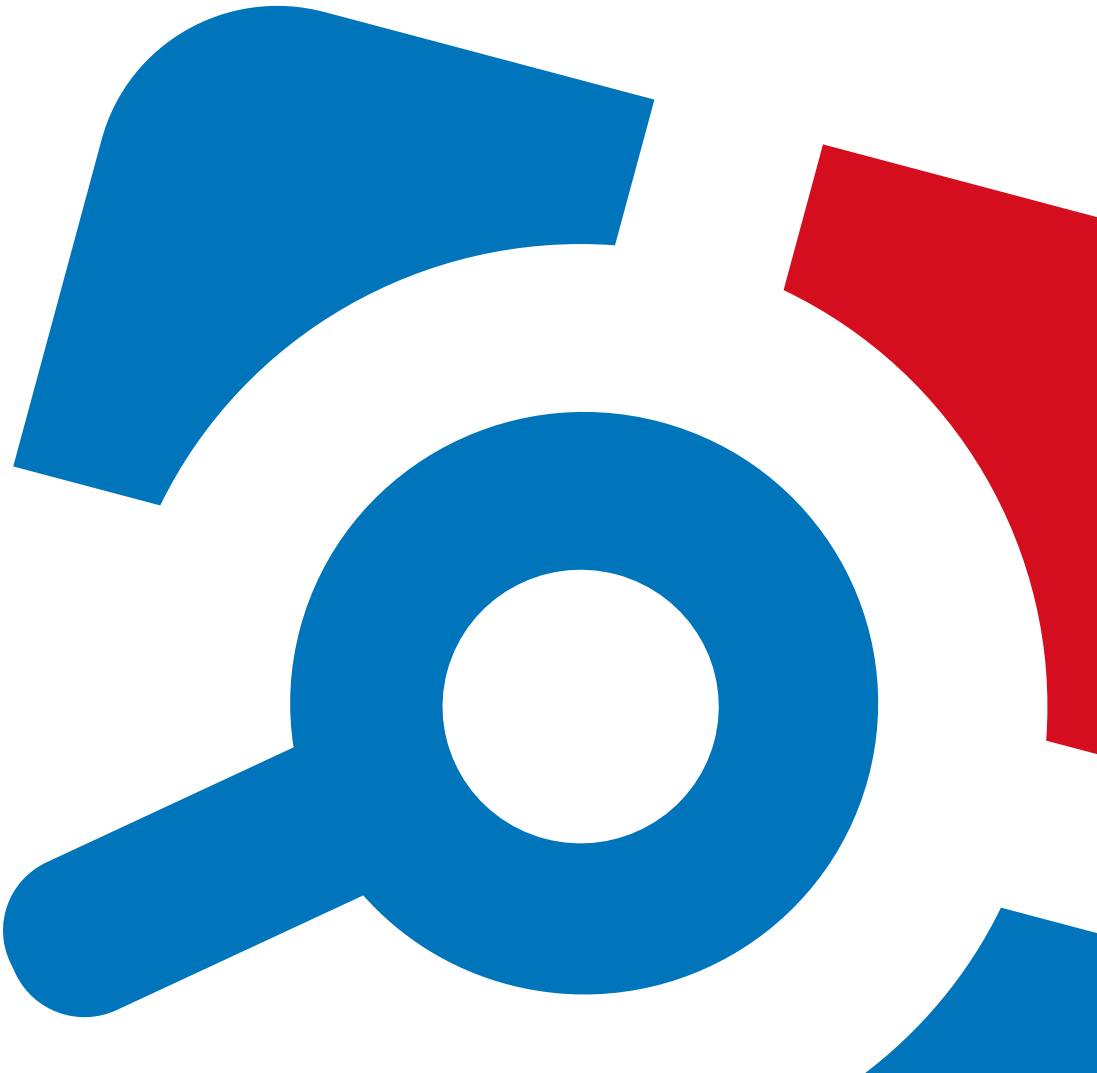
netwrix

Netwrix Auditor for NetApp

Quick-Start Guide

Version: 9.8
10/8/2019



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.

© 2019 Netwrix Corporation.

All rights reserved.

Table of Contents

1. Introduction 5
   1.1. Netwrix Auditor Features and Benefits 5
2. Prerequisites and System Requirements 6
   2.1. Supported Data Sources 6
   2.2. Requirements to Install Netwrix Auditor 6
      2.2.1. Hardware Requirements 6
      2.2.2. Software Requirements 7
3. Review Components Checklist 9
   3.1. Configure Data Collecting Account 9
4. Configure NetApp Filer for Monitoring 12
   4.1. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring 12
      4.1.1. Prerequisites 12
      4.1.2. Configure ONTAPI Web Access 13
      4.1.3. Configure Firewall Policy 14
      4.1.4. Configure Event Categories and Log 15
5. Installing Netwrix Auditor 19
6. Monitoring Plans 21
   6.1. Create a New Plan 21
      6.1.1. Settings for Data Collection 21
      6.1.2. Default SQL Server Instance 23
      6.1.3. Database Settings 24
      6.1.4. SMTP Server Settings 26
      6.1.5. Email Notification Recipients 26
      6.1.6. Monitoring Plan Summary 26
   6.2. Add Items for Monitoring 27
      6.2.1. NetApp 27
7. Make Test Changes 29
8. See How Netwrix Auditor Enables Complete Visibility 30

8.1. Review an Activity Summary 31
8.2. Review File Servers Overview 32
8.3. Review the All File Server Activity Report 33
8.4. Browse Data with Intelligence Search 34
9. Related Documentation 40

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for NetApp. 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 NetApp appliances
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing NetApp 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 Online Help Center.

1.1. Netwrix Auditor Features and Benefits

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, network devices, SharePoint, Oracle Database, SQL Server, VMware, Windows Server, and User Activity. Empowered with a RESTful API, 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 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 User Activity collects and reports on user actions performed within a session and can be configured to capture a video of users' activity on the audited computers.

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.

To learn about ports and protocols required for product operation, refer to Protocols and Ports Required for Netwrix Auditor.

To learn about security roles and permissions required for product operation, refer to Configure Netwrix Auditor Service Accounts.

2.1. Supported Data Sources

The table below lists systems that can be monitored with Netwrix Auditor for NetApp:

Data source	Supported Versions
NetApp	• NetApp ONTAP 9.0 – 9.6 (CIFS configuration only) • NetApp Clustered Data ONTAP 8.2.1 – 8.2.3, 8.3, 8.3.1, 8.3.2 (CIFS configuration only) • NetApp Data ONTAP 8 in 7-mode (CIFS configuration only) • NetApp Data ONTAP 7 (CIFS configuration only)

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

This section provides rough estimations of the resources required for Netwrix Auditor PoC or evaluation deployment. Consider that actual hardware requirements will depend on your monitored infrastructure, the number of users in your environment, and activities that occur in the infrastructure per day.

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.

Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for NetApp. Refer to Netwrix Online Help Center for complete information on the Netwrix Auditor hardware requirements.

You can deploy Netwrix Auditor on a virtual machine running Microsoft Windows guest OS on the corresponding virtualization platform, in particular:

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV

Note that Netwrix Auditor supports only Windows OS versions listed in the Software Requirements section.

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 Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 SP1 Windows Desktop OS (64-bit):

Component	Requirements
	• Windows 10 • Windows 8.1 • Windows 7 SP1
.NET Framework	• .NET Framework 3.5 SP1. **NOTE:** To audit VMware vSphere 6.7 or 6.5, .NET Framework 4.5 or 4.6 is required.
Installer	• Windows Installer 3.1 and above

3. Review Components Checklist

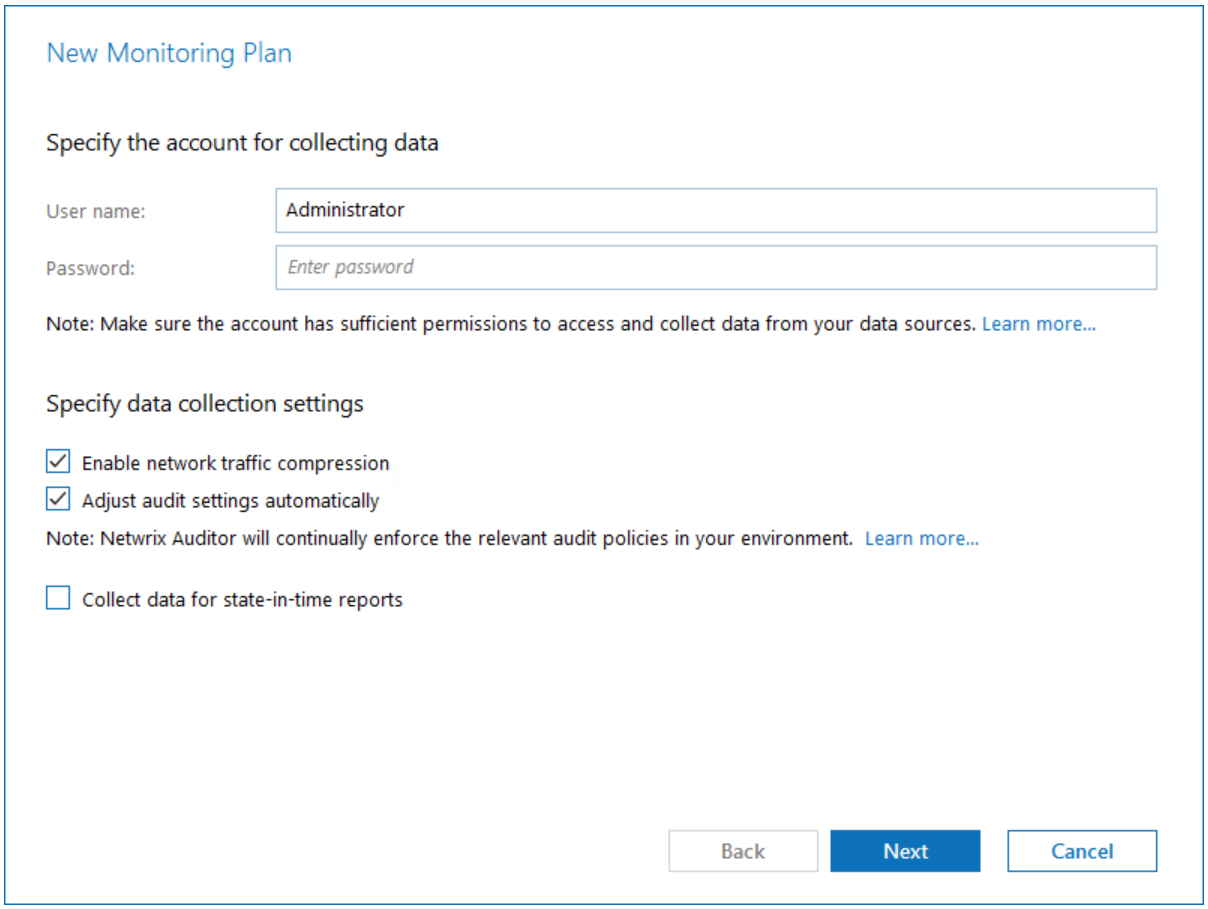
To speed up the evaluation process, Netwrix recommends you to ensure that the following services and components are up and running prior to the Netwrix Auditor installation.

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 with Reporting Services (or Advanced Services) 2008 or higher.	Supported SQL Server versions are listed here. Consider maximum database size in different versions. Make your choice based on the size of the environment you are going to monitor, the number of users, and other factors. Remember that maximum database size in Express editions may be insufficient. **NOTE:** Although Netwrix Auditor provides a convenient way to download SQL Server 2014 Express edition right from the product, it is recommended to deploy SQL Server instance in advance. If installed separately, remember to test SQL Server connectivity.

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 used to collect audit data from the data source items; it is specified during the monitoring plan creation:



Netwrix recommends creating a special service account for that purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements.

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

Data source	Required rights and permissions:

NetApp	***On the target server:***
	• A member of the local **Administrators** group
	• The **Read** permissions (resultant set) on the audited shared folders
	• The **Read** permissions (resultant set) on the audit logs folder and its contents and **Delete** permissions (resultant set) on the contents of this folder
	• To connect to **NetApp Data ONTAP 7** or **Data ONTAP 8 in 7-mode**, an account must have the following capabilities:
	  ◦ login-http-admin
	  ◦ api-vfiler-list-info

Data source	Required rights and permissions:

- api-volume-get-root-name
- api-system-cli
- api-options-get
- cli-cifs

- To connect to **NetApp Clustered Data ONTAP 8** or **ONTAP 9**, an account must be assigned a custom role (e.g., fsa_role) on SVM that has the following capabilities with access query levels:

  - version readonly
  - volume readonly
  - vserver audit all
  - vserver audit rotate-log all
  - vserver cifs readonly

  NOTE: You can also assign the builtin **vsadmin** role.

  If you want to authenticate with AD user account, you must enable it to access SVM through ONTAPI. The credentials are case sensitive.

Review the following for additional information:

4. Configure NetApp Filer for Monitoring

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

- Automatically when creating a monitoring plan

  NOTE: For NetApp Data ONTAP 7 and 8 in 7-mode, configure audit automatically. For NetApp Clustered Data ONTAP 8 or ONTAP 9 only file share audit settings can be configured automatically. See Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring for more information.

- Manually. See Netwrix Auditor Installation and Configuration Guide for more information.

4.1. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring

To configure Clustered Data ONTAP 8 and ONTAP 9 for monitoring, perform the following procedures:

- Prerequisites
- Configure ONTAPI Web Access
- Configure Firewall Policy
- Configure Event Categories and Log

4.1.1. Prerequisites

Perform the steps below before proceeding with audit configuration:

1. Configure CIFS server and make sure it functions properly.

   NOTE: NFS file shares are not supported.

2. Configure System Access Control List (SACL) on your file share.
3. Set the **Security Style** for **Volume** or **Qtree** where the audited file shares are located to the *"ntfs"* or *"mixed"*.
4. Configure audit manually. For 8.3, review the **Auditing NAS events on SVMs with FlexVol volumes** section in Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS.

   NOTE: The current version of Netwrix Auditor does not support auditing of Infinite Volumes.

4.1.2. Configure ONTAPI Web Access

Netwrix Auditor uses ONTAPI to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an MS Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current web access settings. Make sure that External Web Services are allowed. For example:

```
cluster1::> system services web show
       External Web Services: true
                      Status: online
          HTTP Protocol Port: 80
         HTTPs Protocol Port: 443
               TLSv1 Enabled: true
               SSLv3 Enabled: true
               SSLv2 Enabled: false
```

3. Enable ONTAPI access on the SVM where CIFS server is set up and configured. The example command output shows correct web access settings where `vs1` is your SVM name.

```
cluster1::>  vserver  services web show -vserver vs1
Vserver      Type     Service     Description                Enabled
                      Name
----------   -------  --------    -----------------------    ------
vs1             data  ontapi      Remote Administrative API  true
                                  Support
```

4. Enable **HTTP/HTTPS** access. For example:

```
cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled
true
```

5. Enable only **SSL** access (HTTPS in Netwrix Auditor). For example:

```
cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled
true -ssl-only true
```

6. Make sure that the builtin **vsadmin** role or a custom role (e.g., fsa_role) assigned to your account specified for data collection can access ONTAPI. For example:

```
cluster2::> vserver services web access show -vserver vs2
Vserver           Type      Service Name    Role
--------------    -------   ------------    ---------------
vs2               data      ontapi          fsa_role
vs2               data      ontapi          vsadmin
vs2               data      ontapi          vsadmin-protocol
vs2               data      ontapi          vsadmin-readonly
```

```
cluster2::> vserver services web access show -vserver vs2
vs2                data      ontapi          vsadmin-volume
5 entries were displayed.
```

4.1.3. Configure Firewall Policy

Configure firewall to make file shares and Clustered Data ONTAP HTTP/HTTPS ports accessible from the computer where Netwrix Auditor Server is installed. Your firewall configuration depends on network settings and security policies in your organization. Below is an example of configuration:

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current firewall configuration. For example:

```
cluster1::> system services firewall show
Node           Enabled       Logging
------------   ------------  -------
cluster1-01    true          false
```

3. Create firewall policy or edit existing policy to allow HTTP/HTTPS (note that modifying a policy you may overwrite some settings). For example:

To...	Execute...
	NetApp Clustered Data ONTAP 8.2
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
	NetApp Clustered Data ONTAP 8.3, ONTAP 9.0 - 9.5
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`

To...	Execute...
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`

where `pol1` is your Firewall policy name and `192.168.1.0/24` is your subnet where Netwrix Auditor Server resides.

4. Apply the firewall policy to a LIF.

   ```
   cluster1::>network interface modify -vserver vs1 -lif vs1-cifs-lif1 -firewall-policy pol1
   ```

   To verify the policy was applied correctly, execute the following:

   ```
   cluster1::>network interface show -fields -firewall-policy
   ```

4.1.4. Configure Event Categories and Log

Perform the following procedures to configure audit:

- To configure auditing state, event categories and log
- To configure logs retention period

To configure auditing state, event categories and log

Configure audit settings in the context of Cluster or Storage Virtual Machine. All examples in the procedure below apply to SVM, to execute commands in the context of Cluster, add `-vserver name`, where `name` is your server name.

1. Navigate to command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and switch to the context of SVM from the cluster. For example to switch to the SVM called `vs1`:

   ```
   cluster1::> vserver context -vserver vs1
   ```

   After a switch, you will be in the context of SVM:

   ```
   vs1::>
   ```

3. Create and enable audit. For more information on audit configuration, refer to NetApp documentation. For example:

To...	Execute...
Create audit	`vs1::> vserver audit create -destination <path to the volume>` In the example above, the `vserver audit create -destination /audit` command executed on the `vs1` SVM creates and enables audit on the volume `/audit`. **NOTE:** Netwrix Auditor accesses audit logs via file shares. Make sure the volume you specified is mounted on SVM and shared (e.g., `audit$` is a share name and its path is `/audit`).
Enable audit	`vs1::> vserver audit enable`

4. Review your audit settings. For example, on ONTAPI 8.3 the default audit is configured as follows:

```
vs1::> vserver audit show -instance

                         Auditing State: true
                   Log Destination Path: /audit
        Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                   Log File Size Limit: 100MB
          Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
             Log Files Rotation Limit: 0
```

For ONTAPI 9.0 or later the default audit is configured as follows:

```
vs1::> vserver audit show -instance

                         Auditing State: true
                   Log Destination Path: /audit
        Categories of Events to Audit: file-ops, file-share, audit-policy-
                                       change, cifs-logon-logoff
                          Log Format: evtx
                   Log File Size Limit: 100MB
          Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
             Log Files Rotation Limit: 0
```

5. Check the following options:

Option	Setting
`Auditing State`	`true`
`Categories of Events to Audit`	`file-ops` **NOTE:** Only required if you use Clustered Data ONTAP 8.3, ONTAP 9.0, ONTAP 9.1 or later. You cannot select event categories if you use Clustered Data ONTAP 8.2. For ONTAP 9.0 and later, also check the following options: `file-ops, file-share, audit-policychange`. For ONTAP 8.3, just check `file-ops`.
`Log Format`	*"XML"* or *"EVTX"*

6. Modify the log file size limit—set to 300 MB. Execute:

```
vs1::> vserver audit modify -rotate-size 300MB
```

300MB is the recommended maximum log size proceeding from performance evaluations.

7. After configuration, double-check your settings.

```
vs1::> vserver audit show -instance
```

```
                    Auditing State: true
              Log Destination Path: /audit
     Categories of Events to Audit: file-ops, cifs-logon-logoff
                        Log Format: evtx
                Log File Size Limit: 300MB
       Log Rotation Schedule: Month: -
 Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
           Log Files Rotation Limit: 0
```

NOTE: For ONTAP 9.0 and later, also check the following settings: `file-ops, file-share, audit-policychange`.

For ONTAP 8.3, just check `file-ops`.

To configure logs retention period

1. On the computer where Netwrix Auditor Server resides, open **Registry Editor**: navigate to **Start** →

Run and type *"regedit"*.

2. Navigate to **HKEY_LOCAL_MACHINE → SOFTWARE → Wow6432Node → Netwrix Auditor → File Server Change Reporter**.
3. In the right-pane, right-click and select **New → DWORD (32-bit Value)**.

   NOTE: For the backup logs retention functionality to work properly, you need to specify the **CleanAutoBackupLogs** name for the newly created registry value.

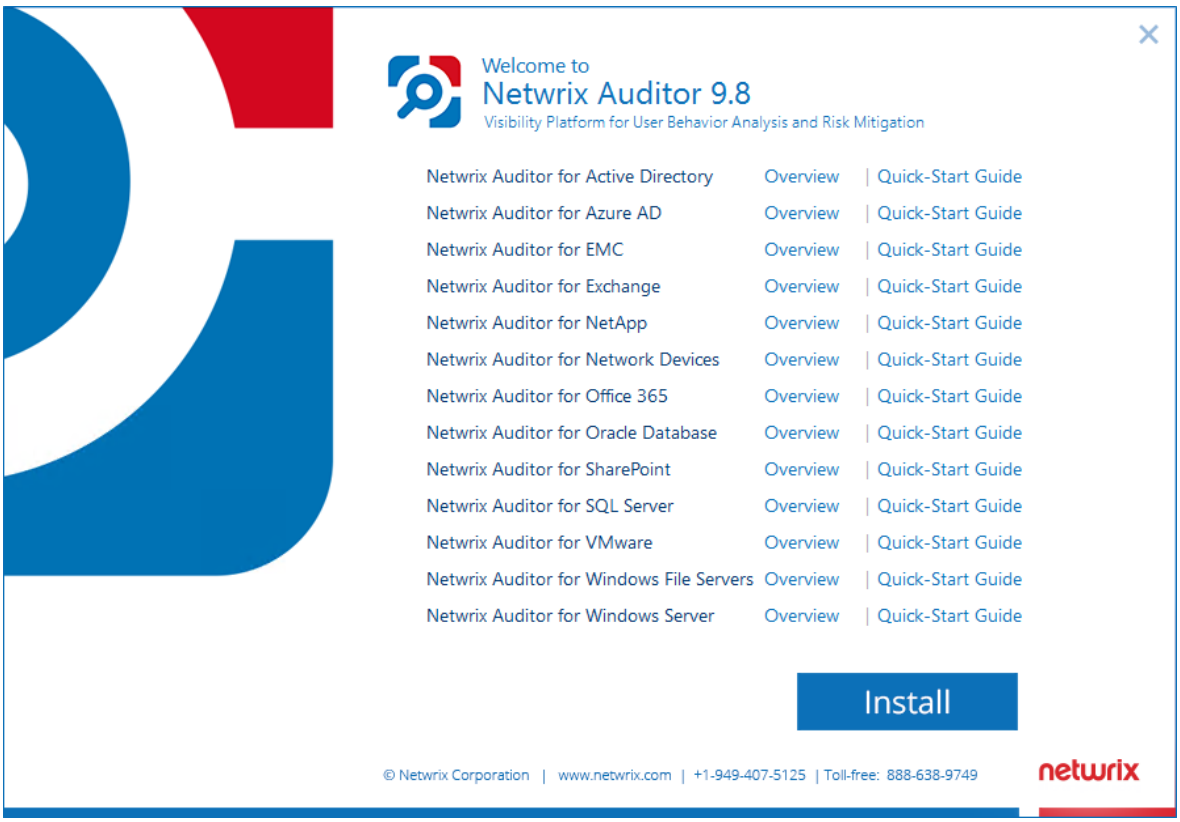
4. Double-click **CleanAutoBackupLogs**. The **Edit DWORD Value** dialog will open.
5. This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to *"0"* (decimal). Modify this value, if necessary, and click **OK** to save the changes.

6. **NOTE:** If the **CleanAutoBackupLogs** registry value is set to *"0"*, you will have to remove the old logs manually, or you may run out of space on your hard drive.

5. Installing Netwrix Auditor

To install Netwrix Auditor

1. Download Netwrix Auditor 9.8 from Netwrix website.
2. Unpack the installation package. The following window will be displayed on successful operation completion:

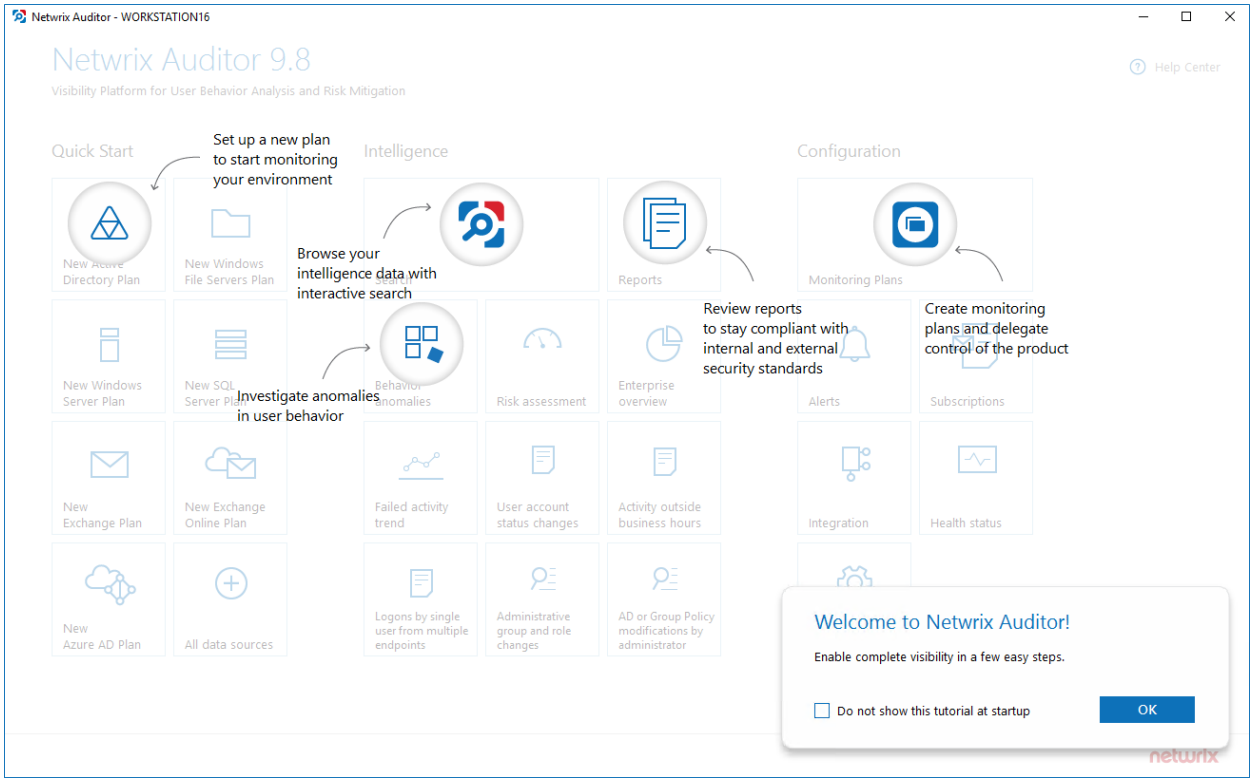


3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are 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 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 NetApp, 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

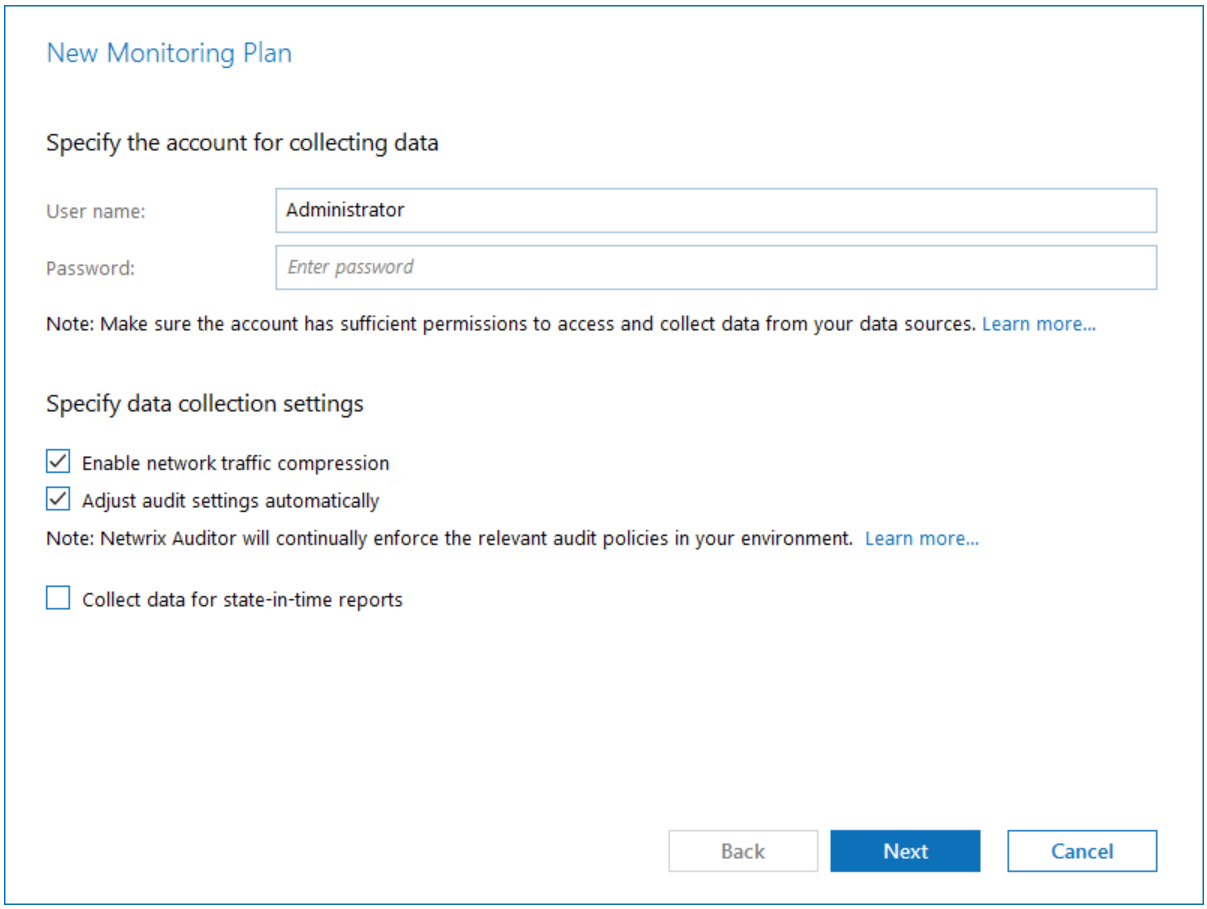
On the main Netwrix Auditor page, click the **All data sources** tile in the **Quick Start** section.

Then follow the steps of the Monitoring Plan Wizard:

- 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. Settings for Data Collection

At this step of the wizard, specify the account that Netwrix Auditor will use to access the data source, and general settings for data collection.



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 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 Configure Data Collecting Account. Netwrix recommends creating a special service account with extended permissions.
Enable network traffic compression	If selected, this option instructs Netwrix Auditor to deploy a special utility that will run on the audited computers and do the following: • collect and pre-filter audit data • compress data and forward it to Netwrix Auditor Server This approach helps to optimize load balance and reduce network traffic. So, using this option can be recommended especially for distributed networks with remote locations that have limited bandwidth. See Network Traffic Compression for more information.

Option	Description
Adjust audit settings automatically	Netwrix Auditor can configure audit settings in your environment automatically. Select **Adjust audit settings automatically**. In this case, Netwrix Auditor will continually check and enforce the relevant audit policies. Consider, however, that for some data sources this approach is mostly recommended for evaluation purposes in test environments; in the production environment, manual cofniguration is used more often (for example, for Windows File Servers). You may also want to apply audit settings via GPO (for example, for Windows Servers). **NOTE:** Select this option if you want to audit file shares on NetApp Data ONTAP 7 and 8 in 7-mode. For NetApp Clustered Data ONTAP 8 and ONTAP 9, only audit settings for file shares can be configured automatically, other settings must be applied manually. For a full list of audit settings and instructions on how to configure them manually, refer to Configure IT Infrastructure for Auditing and Monitoring.

6.1.2. Default SQL Server Instance

To provide searching, alerting and reporting capabilities, Netwrix Auditor needs an SQL Server where audit data will be stored in the databases. To store data from the data sources included in the monitoring plan, the wizard creates an Audit Database for each plan. At this step, you should specify the default SQL Server instance that will host Netwrix Auditor databases. To read more, refer to SQL Server and Audit Database.

NOTE: Alternatively, you can instruct Netwrix Auditor not to store data to the databases but only to the repository (Long-Term Archive) – in this scenario, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided.

NOTE: Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared.

Select one of the following options:

- **Install a new instance of Microsoft SQL Server Express automatically** — this option is available at the first run of the wizard. It allows you to deploy SQL Server 2014 Express with Advanced Services on the local machine. This SQL Server will be used as default host for Netwrix Auditor databases.
- **Use an existing SQL Server instance** — select this option to use an existing SQL Server instance.

  NOTE: Local SQL Server instance is detected automatically, and input fields are pre-populated with its settings.

  Complete the following fields:

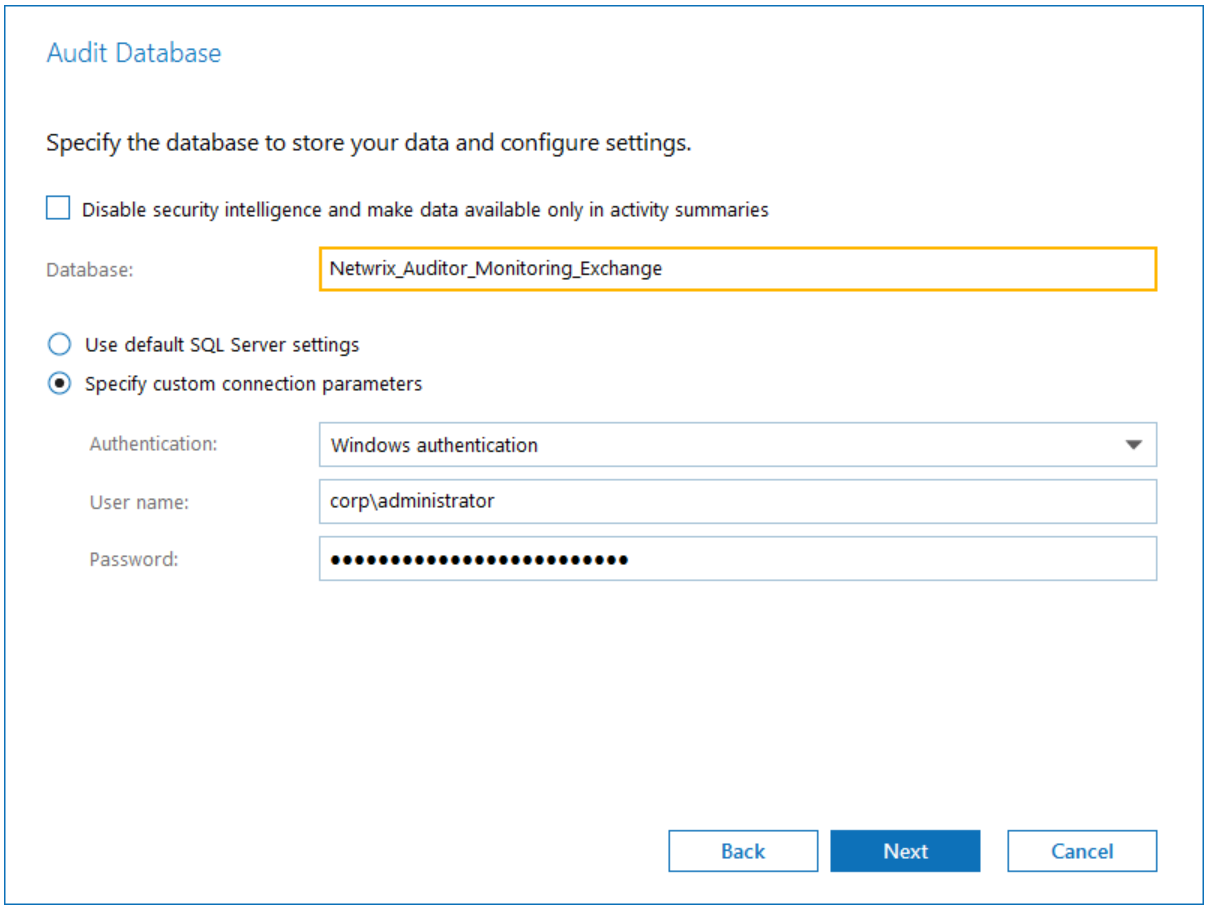
Option	Description
SQL Server instance	Specify the name of the SQL Server instance to store audit data.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to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

6.1.3. Database Settings

At this step, you need to specify a database where Netwrix Auditor will store data collected from the data sources included in this monitoring plan.

NOTE: It is strongly recommended to target each monitoring plan at a separate database.

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.



Configure the following:

Setting	Description
Disable security intelligence ...	Only select this option if you do not want your data to be stored in the database. In this case, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided. To store data to the database, leave this check box cleared.
Database	Default database name is *Netwrix_Auditor_<monitoring_plan_name>*. It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g. *Exchange_Audit_Data* or *OracleSrv02_Audit_Data*), or so. If you decided to use the existing SQL Server instance instead of dedicated, you may want to use *Netwrix_Auditor* prefix to distinguish Netwrix Auditor databases

Setting	Description
	from others.
Use default SQL Server settings	Select this option if you want Netwrix Auditor to connect to the SQL Server instance using the default settings you specified Default SQL Server Instance .
Specify custom connection parameters	Select this option to use custom credentials when connecting to SQL Server. Specify authentication method and the account that Netwrix Auditor will use. Make sure this account has sufficient rights to connect to SQL Server and work with the databases. See Configure Audit Database Account for details.

Netwrix Auditor will connect to the default SQL Server instance and create a database with the specified name on it.

NOTE: Global settings that apply to all databases with audit data (including retention period and SSRS server used for reporting) are available on the **Audit Database** page of Netwrix Auditor settings. See Audit Database for details.

6.1.4. SMTP Server Settings

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 detect SMTP settings; however, for your first plan you should provide them manually. See this section for details.

6.1.5. Email Notification Recipients

Specify who will receive daily emails: Activity Summary Email on changes in the monitored infrastructure, and Health Summary Email on Netwrix Auditor operations and health.

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.

6.1.6. Monitoring Plan Summary

At this step of the wizard, to provide a meaningful name and optional description for your monitoring plan.

To start collecting data, you should specify the objects (items) that belong to the target data source and should be processed according to the settings of this monitoring plan. For example, for Exchange data source the item will be your Exchange server, for Windows Server data source - computer, IP range or AD container, and so on. To add items right after finishing the monitoring plan wizard, select the **Add item now** checkbox. See Add Items for Monitoring for details.

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. Select the **NetApp** item.

6.2.1. NetApp

Complete the following fields:

Option	Description
	General
Specify NetApp file server	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.
File share UNC path to audit logs	Select one of the following: • **Detect automatically**—If selected, a shared resource will be detected automatically. • **Use this path**—UNC path to the file share located on a NetApp Filer with event log files (e.g., *CORP**ETC$**log*\).
Specify the account for collecting data	Select the account that will be used to collect data for this item.
	ONTAPI
Specify protocol for accessing ONTAPI	Select one of the following: • **Detect automatically**—If selected, a connection protocol will be detected automatically. • **HTTP** • **HTTPS**

Option	Description
	NOTE: Refer to Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to enable HTTP or HTTPS admin access.
Specify management interface	Select management interface to connect to ONTAPI. If you want to use custom management interface for ONTAPI, select **Custom** and provide a server name by entering its FQDN, NETBIOS or IP address.
Specify account for connecting to ONTAPI	Select an account to connect to NetApp and collect data through ONTAPI. If you want to use a specific account (other than the one you specified on the **General** tab), select **Custom** and enter credentials. The credentials are case sensitive. Take into consideration that even if a custom account is specified, the account selected on the **General** tab must be a member of the **Builtin\Administrators** group and have sufficient permissions to access audit logs shared folder and audited shares. **NOTE:** See Netwrix Auditor Installation and Configuration Guide for more information on required rights and permissions.
	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.

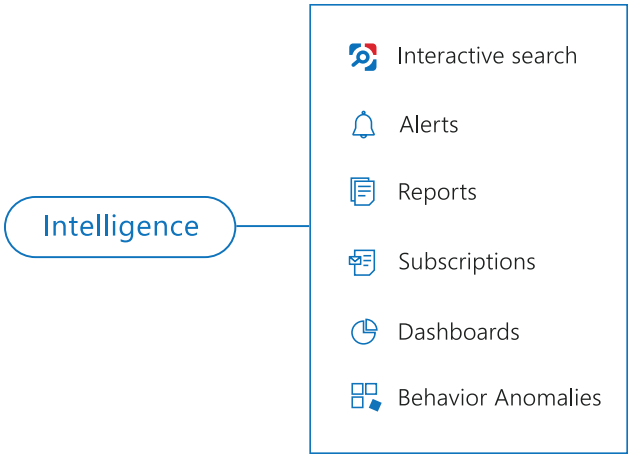
For example, make the following test changes:

- 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.

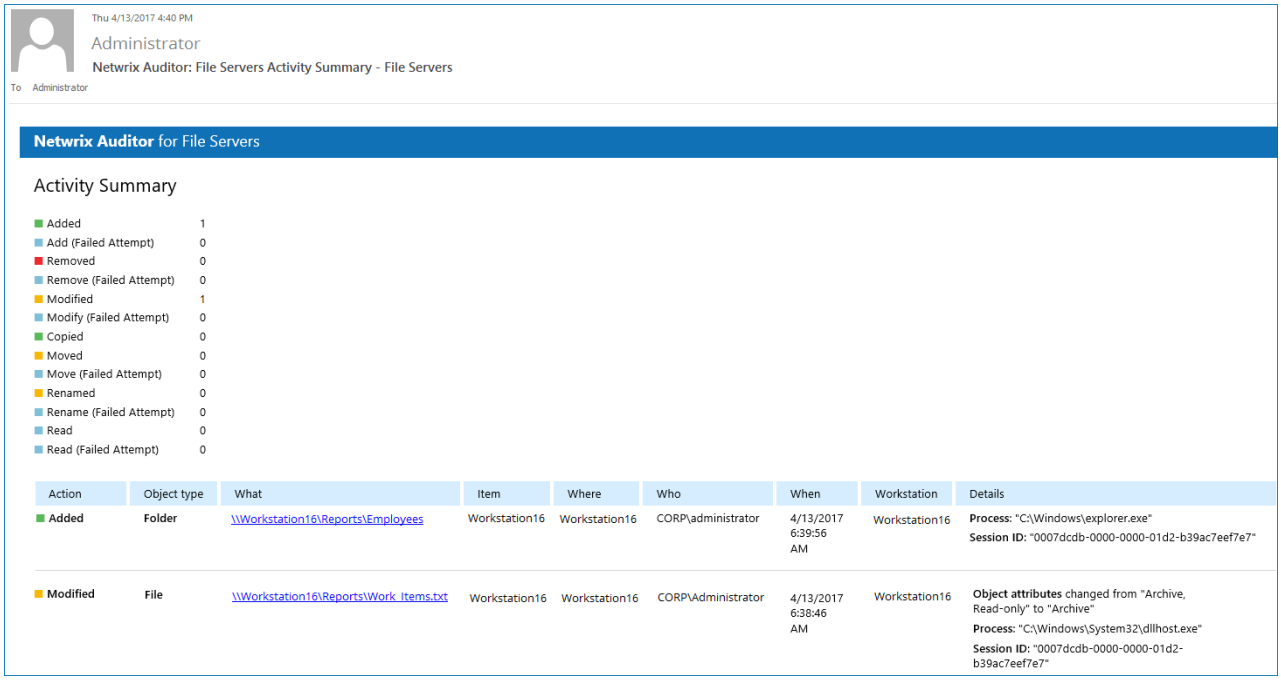
To launch data collection manually

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.

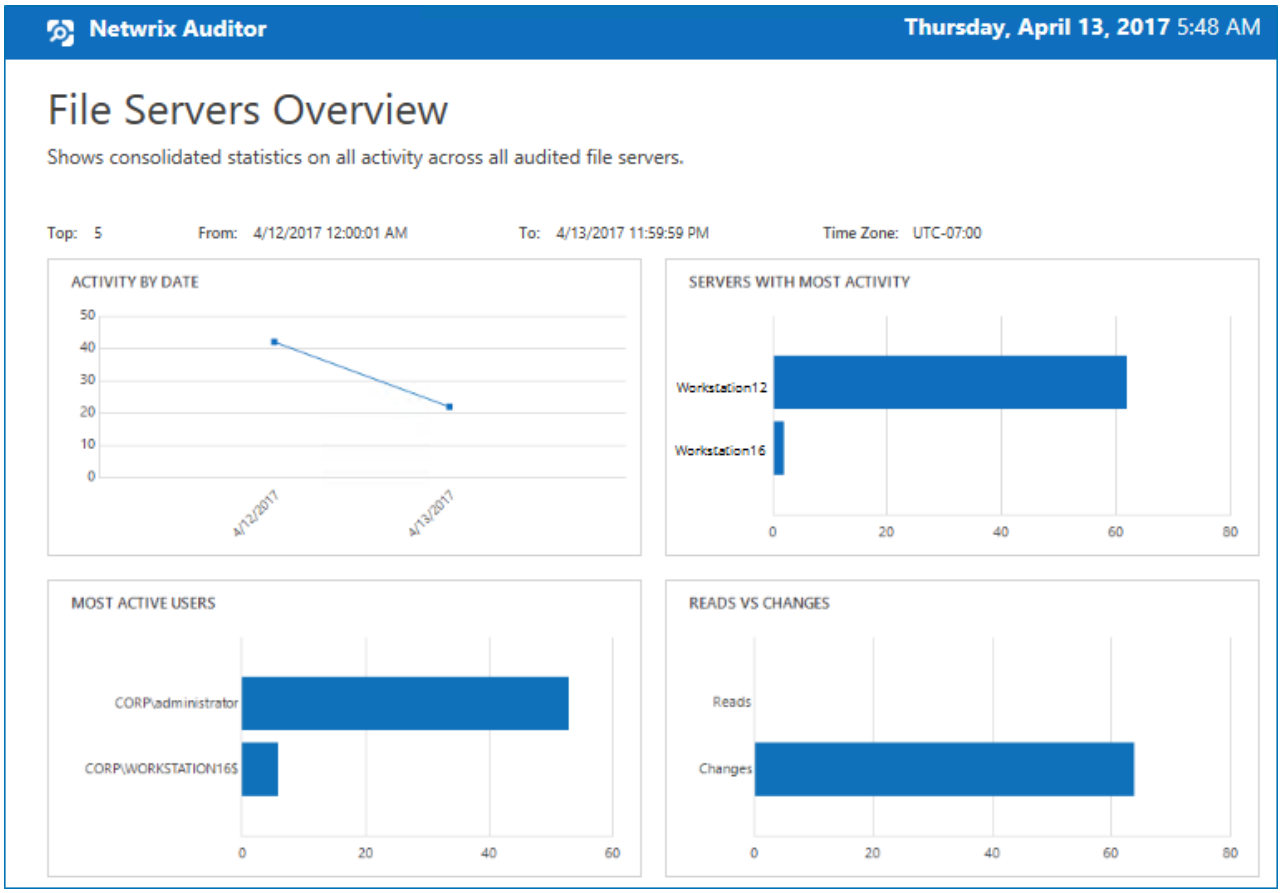
8.2. Review File Servers Overview

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

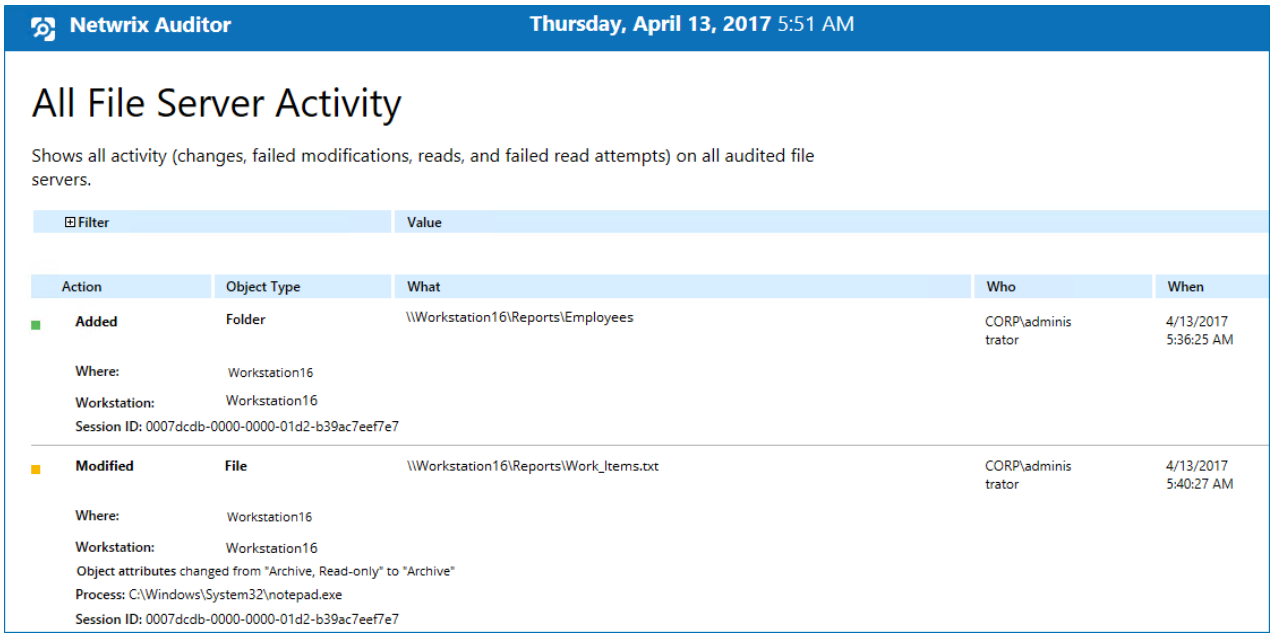
The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

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.



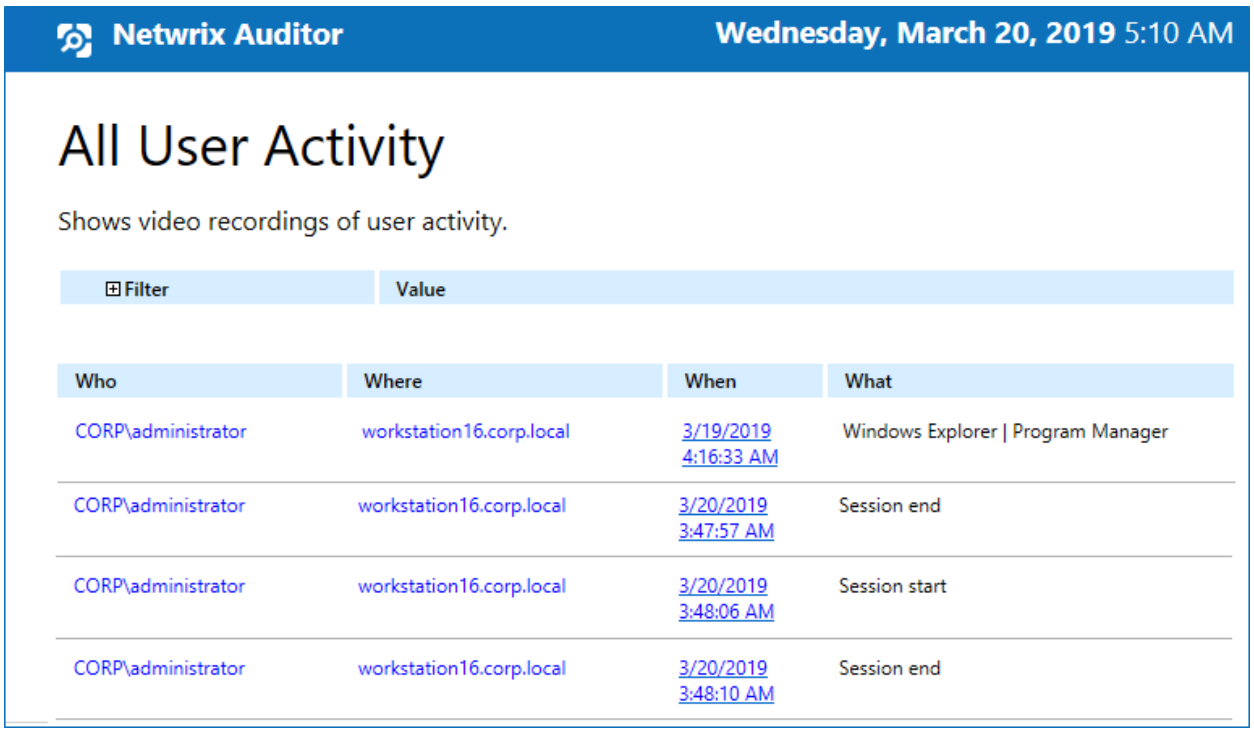
Netwrix Auditor Thursday, April 13, 2017 5:51 AM

All File Server Activity

Shows all activity (changes, failed modifications, reads, and failed read attempts) on all audited file servers.

Filter | Value

Action	Object Type	What	Who	When
Added	Folder	\\Workstation16\Reports\Employees	CORP\administrator	4/13/2017 5:36:25 AM
Where: Workstation16				
Workstation: Workstation16				
Session ID: 0007dcdb-0000-0000-01d2-b39ac7eef7e7				
Modified	File	\\Workstation16\Reports\Work_Items.txt	CORP\administrator	4/13/2017 5:40:27 AM
Where: Workstation16				
Workstation: Workstation16				
Object attributes changed from "Archive, Read-only" to "Archive"				
Process: C:\Windows\System32\notepad.exe				
Session ID: 0007dcdb-0000-0000-01d2-b39ac7eef7e7				



Netwrix Auditor Wednesday, March 20, 2019 5:10 AM

All User Activity

Shows video recordings of user activity.

Filter | Value

Who	Where	When	What
CORP\administrator	workstation16.corp.local	3/19/2019 4:16:33 AM	Windows Explorer | Program Manager
CORP\administrator	workstation16.corp.local	3/20/2019 3:47:57 AM	Session end
CORP\administrator	workstation16.corp.local	3/20/2019 3:48:06 AM	Session start
CORP\administrator	workstation16.corp.local	3/20/2019 3:48:10 AM	Session end

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.

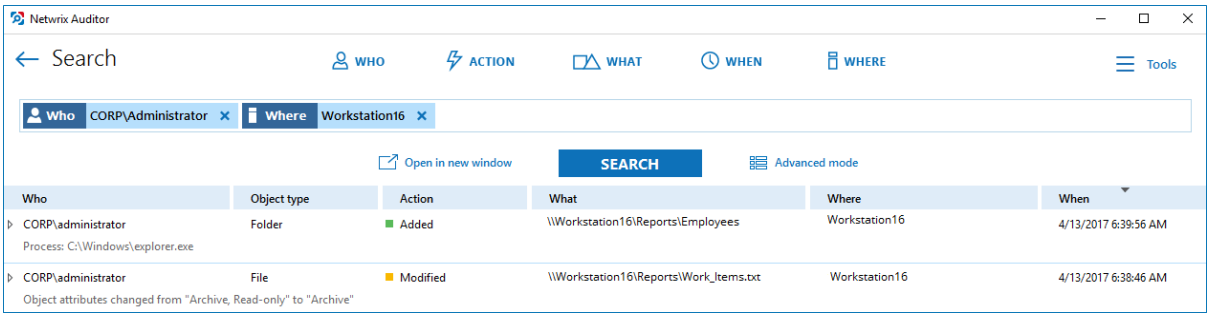
   For example, consider adding these filters:

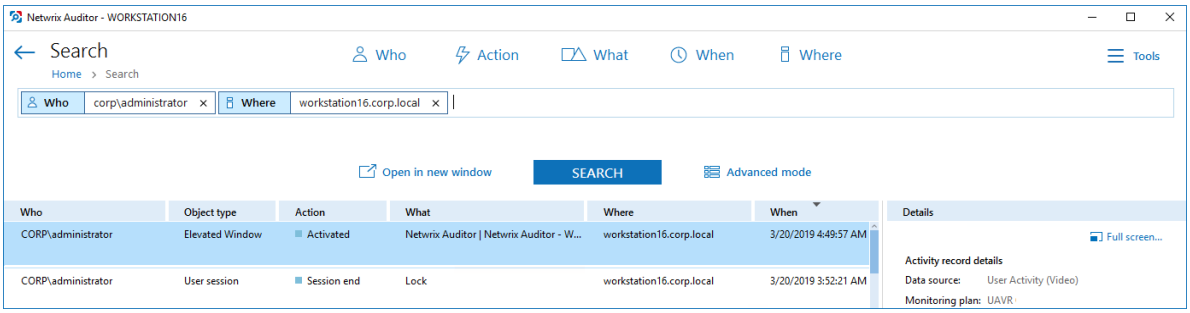
Filter	Value
 WHO	Specify your account name, as you performed test changes.
 WHERE	Specify your file server name.

   NOTE: Refer to Netwrix Online Helpcenter 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:

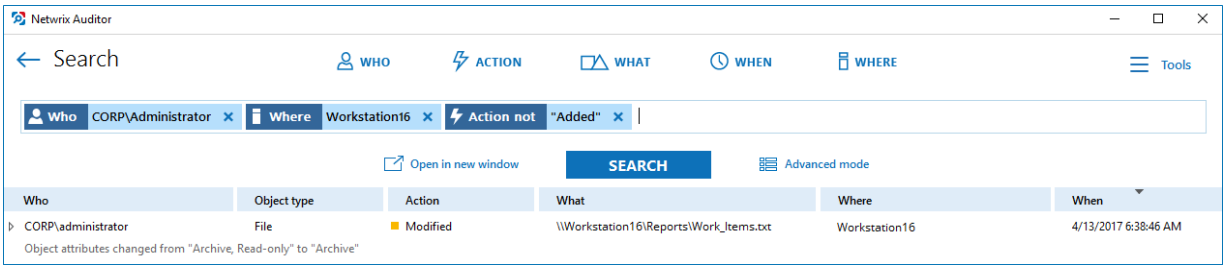
3. Click **Search**.

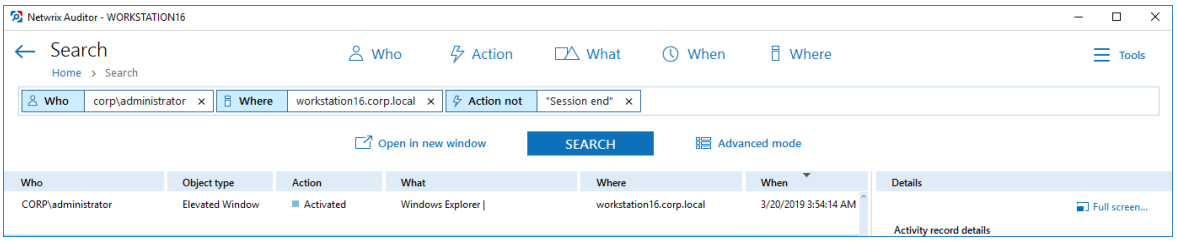




4. Now, you can narrow your search and modify it right from the search results pane. Click any entry that contains excess data, select **Exclude from search** in the **Details** section and specify a filter, e.g., **Action**: *Added* to leave information on modifications only.

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



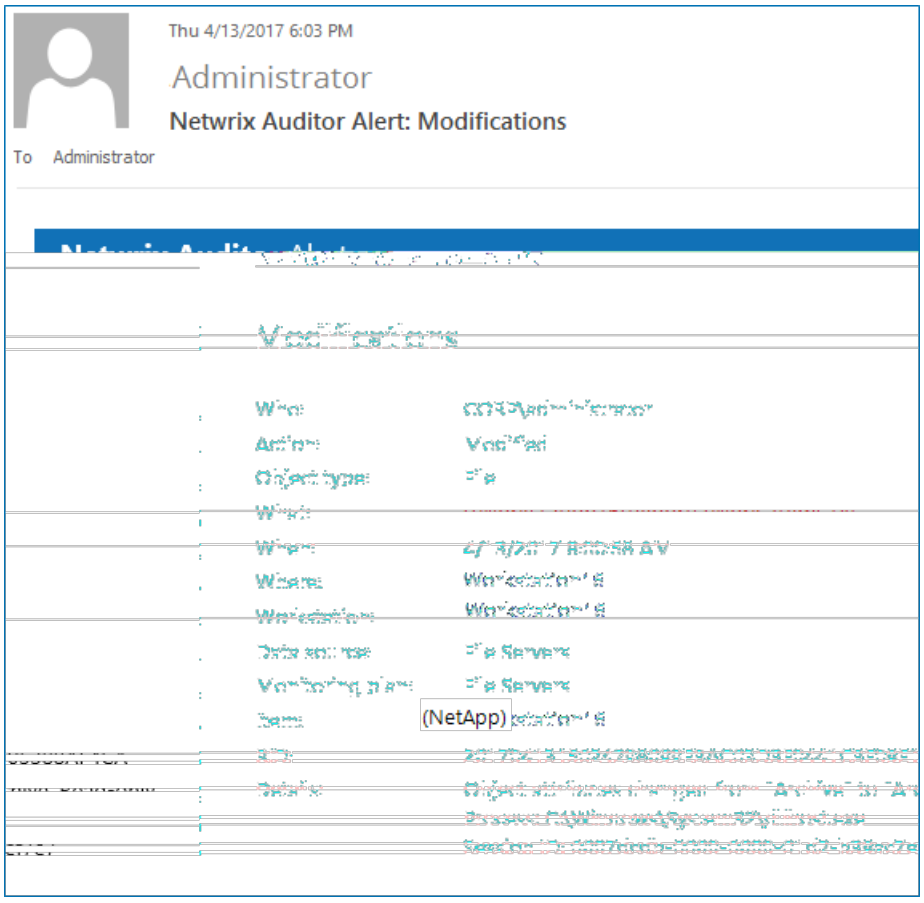


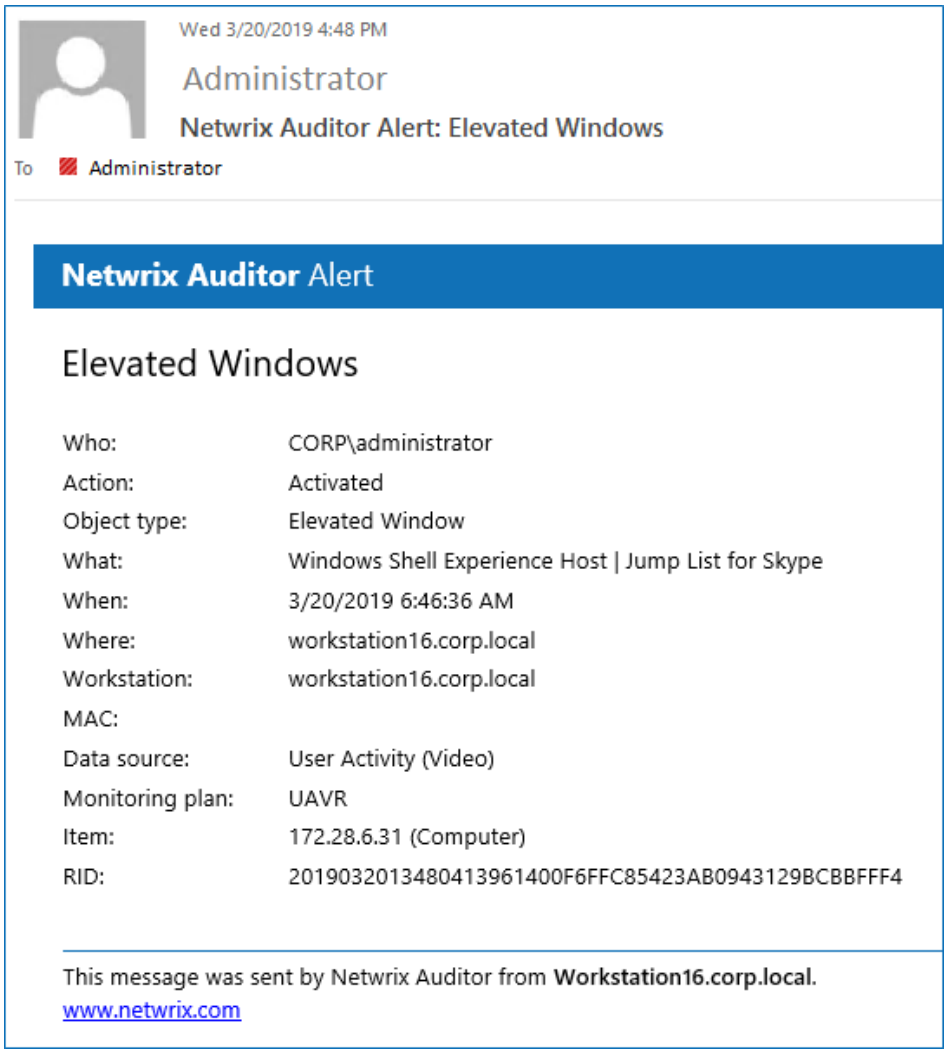
5. Having reviewed your search results, navigate to **Tools**.

   - 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 Custom Search-Based Reports 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 Alerts for detailed instructions on how to create and configure alerts.

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





Wed 3/20/2019 4:48 PM

Administrator

Netwrix Auditor Alert: Elevated Windows

To Administrator

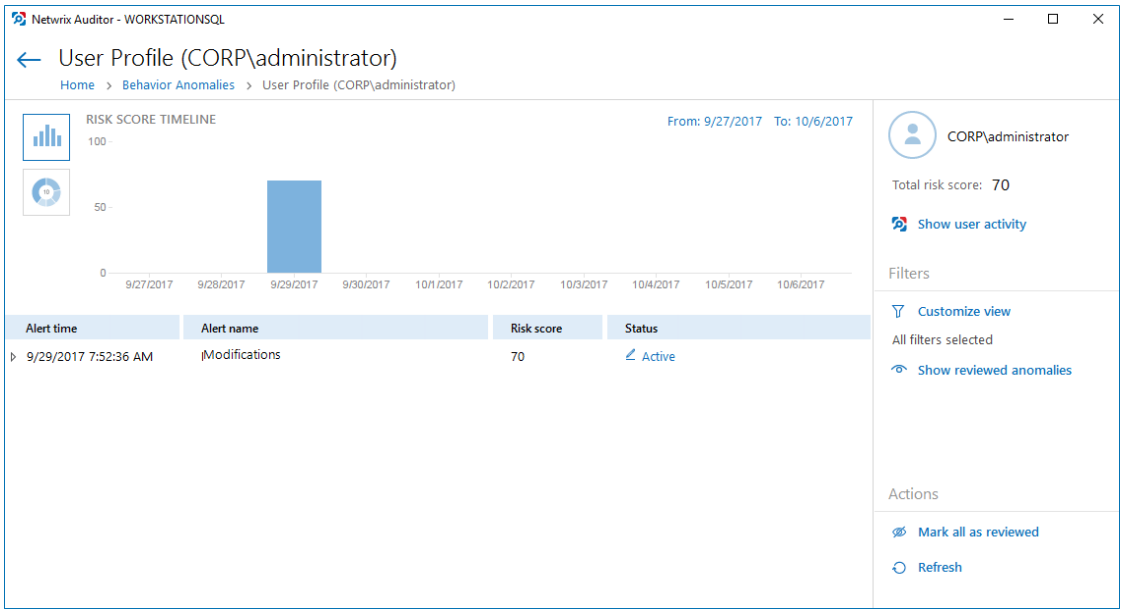
Netwrix Auditor Alert

Elevated Windows

Who:	CORP\administrator
Action:	Activated
Object type:	Elevated Window
What:	Windows Shell Experience Host | Jump List for Skype
When:	3/20/2019 6:46:36 AM
Where:	workstation16.corp.local
Workstation:	workstation16.corp.local
MAC:	
Data source:	User Activity (Video)
Monitoring plan:	UAVR
Item:	172.28.6.31 (Computer)
RID:	20190320134804139614 00F6FFC85423AB0943129BCBBFFF4

This message was sent by Netwrix Auditor from **Workstation16.corp.local**.
www.netwrix.com

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 Online Helpcenter for more information on behavior anomalies and risk scores.


Netwrix Auditor - WORKSTATIONSQL
User Profile (CORP\administrator)
Home › Behavior Anomalies › User Profile (CORP\administrator)
RISK SCORE TIMELINE
From: 9/27/2017 To: 10/6/2017
100
50
0
9/27/2017
9/28/2017
9/29/2017
9/30/2017
10/1/2017
10/2/2017
10/3/2017
10/4/2017
10/5/2017
10/6/2017
Alert time
Alert name
Risk score
Status
9/29/2017 7:52:36 AM
Modifications
70
Active
CORP\administrator
Total risk score: 70
Show user activity
Filters
Customize view
All filters selected
Show reviewed anomalies
Actions
Mark all as reviewed
Refresh

9. Related Documentation

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

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 9.8, and suggests workarounds for these issues.