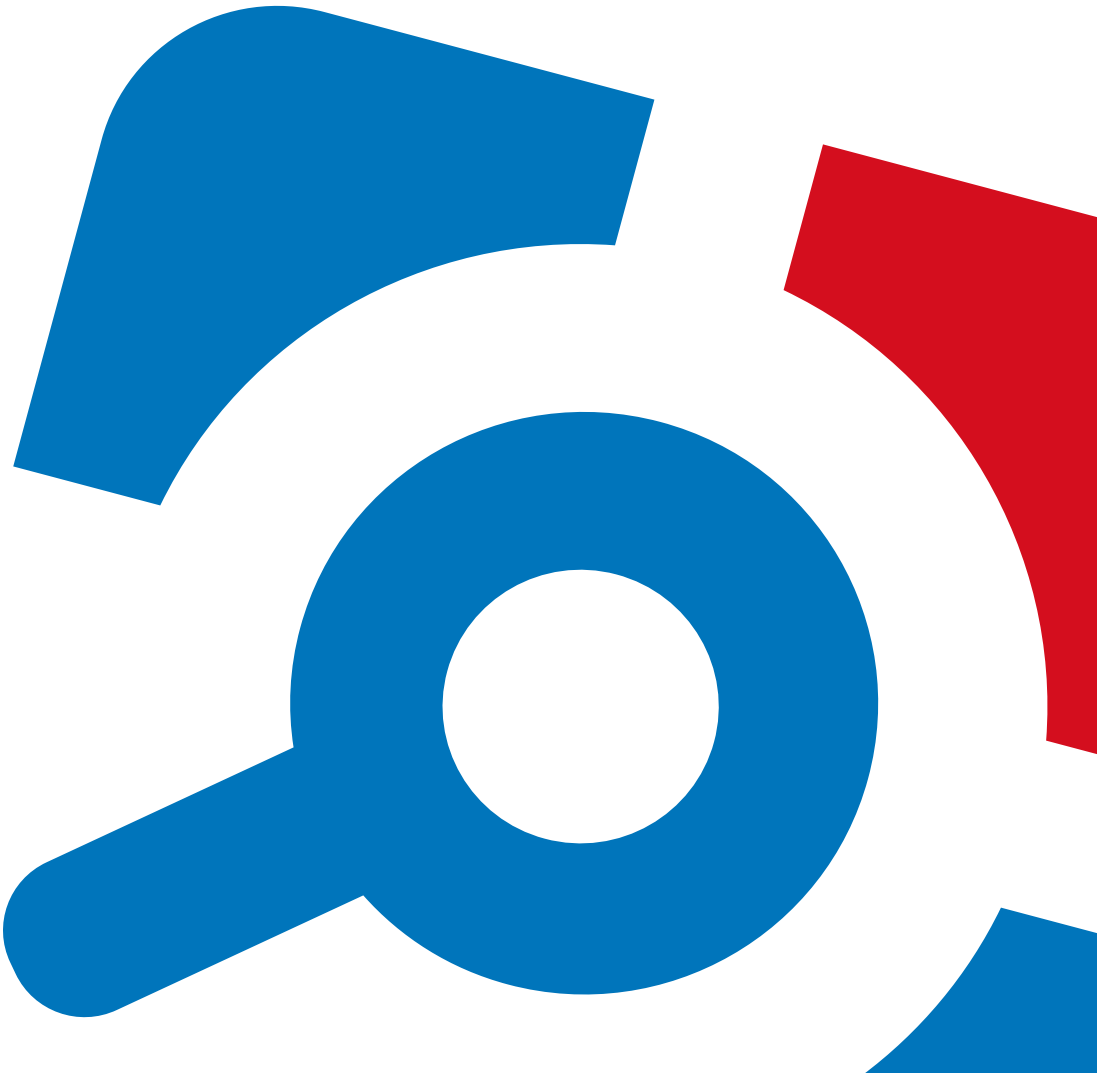
netwrix

Netwrix Auditor for User Activity

Quick-Start Guide

Version: 10
9/14/2021



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 User Activity. 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 User Activity
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing User Activity 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, Active Directory Federation Services, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, Nutanix Files, 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 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

This section lists platforms and systems that can be monitored with Netwrix Auditor for User Activity.

Active Directory domain

Supported Data Sources

Supported Data Sources

Supported Data Sources

Supported Data Sources

Exchange

Supported Data Sources

Office 365 and Azure AD

Supported Data Sources

Supported Data Sources

Supported Data Sources

SharePoint

Supported Data Sources

File storage systems

Supported Data Sources

Supported Data Sources

Supported Data Sources

Supported Data Sources

Network devices

Supported Data Sources

Databases

Supported Data Sources

Considerations for Oracle Database Auditing

Supported Data Sources

Windows server

Supported Data Sources

Supported Data Sources

Supported Data Sources

User Activity

VMware server

Supported Data Sources

Data source	Supported Versions

User Activity	• Windows Server OS:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012/2012 R2
	  • Windows Server 2008/2008 R2
	• Windows Desktop OS (32 and 64-bit):
	  • Windows 10
	  • Windows 8.1
	  • Windows 7
	User Activity data source can support around 300 targets with one user session per target without scalability issues:
	• Depending on how dense is the actual user activity, the number

Data source	Supported Versions
	can be more for servers but less for workstations. • 50-100 concurrent sessions per terminal server. We recommend using the User Activity auditing only for those infrastructure areas that require more attention due to their sensitivity/criticality. Applicable usage scenarios include, for example: • terminal servers where users can log in from external locations • areas accessible by contractor personnel • servers with sensitive information • sessions with elevated privileges, and so on.

2.1.1. Considerations for Oracle Database Auditing

Starting with version 9.95, Netwrix Auditor for Oracle Database is focused on versions 12c and above. It means that Oracle Database 11g users will not be able to benefit from latest features and improvements of the product. Oracle Database 11g users should also consider its support expiration dates set by the vendor. So, when planning your Netwrix Auditor deployment, consider the following:

- Several limitations apply to Oracle 11g support in Netwrix Auditor 9.96:
  - Oracle wallets are not supported
  - Lightweight drivers for Oracle Instant Client are not supported
  - Netwrix Auditor client UI does not display any warnings and / or errors regarding to trail audit mode operation
- If you are using Oracle Database 11g and Netwrix Auditor 9.9 (or earlier) and do not plan to upgrade your deployment, you will have all 9.9 capabilities unchanged.
- If you are using Oracle Database 11g and have performed seamless upgrade to Newrix Auditor 9.96, the audit data collection will operate properly. However, consider General Considerations and Known Issues and keep in mind Oracle Database 11g support expiration dates.

If you are using Oracle Database 12c or later, make sure you have **Unified auditing** mode enabled. Otherwise, Netwrix Auditor may not operate properly. Refer to Migrate to Unified Audit for more information.

Check out the following documentation sections:

- ◦ Software Requirements
  ◦ Configure Oracle Database for Monitoring

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 estimations of the resources required for Netwrix Auditor deployment.

IMPORTANT! 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. It is strongly recommended that you go through the Deployment Planning section before you start the installation.

Requirements provided in this section apply to a clean installation on a server without any additional roles or third-party applications installed.

Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for User Activity. Refer to Netwrix Online Help Center for more 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.

2.2.1.0.1. Scenario 1

Netwrix Auditor and SQL Server instance will be deployed on different servers.

Requirements below apply to Netwrix Auditor server.

Hardware component	Evaluation, PoC or starter environment

2.2.1.0.2. Scenario 2

Netwrix Auditor server and SQL Server instance will be deployed on the same machine.

IMPORTANT! In large and extra -large environments, installation of Netwrix Auditor and SQL Server on the same server is not recommended. Instead, deploy an SQL Server instance on a separate server or cluster that meets the requirement in Scenario 1. Refer to related Microsoft guidelines.

Hardware component	Evaluation, PoC or starter environment
Processor	2 cores
RAM	8 GB
Disk space	100 GB—System drive 100 GB—Data drive (Long-Term Archive and SQL Server)

2.2.2. Software Requirements

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

Component	Requirements
Operating system (English-only)	Windows Server OS: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 Windows Desktop OS (64-bit): • Windows 10 • Windows 8.1
.NET Framework	• .NET Framework 4.5 and above.
Installer	• Windows Installer 3.1 and above

2.2.2.1. Other Components

To monitor your data sources, you will need to install additional software components on Netwrix Auditor Server, in the monitored environment, or in both locations.

Data source	Components
• User Activity	*In the monitored environment:* • .NET Framework 4.5 or above depending on the target server

2.2.2.2. Using SSRS-based Reports

SQL Server Reporting Services are needed for this kind of reports (see SQL Server Reporting Services). If you plan to export or print such reports, check the requirements below.

Export

To export SSRS-based reports, **Internet Explorer** must be installed on the machine where Netwrix Auditor client runs.

Internet Options must be configured to allow file downloads for the **Local intranet** zone:

1. Select **Internet Options** and click **Security**.
2. Select **Local intranet** zone and click **Custom level**.
3. In the **Settings** list, locate **Downloads >File download** and make sure the **Enabled** option is selected.

Printing

To print SSRS-based reports, SSRS Report Viewer and Netwrix Auditor Client require ActiveX Control to be installed and enabled on the local machine. See this Knowledge Base article for details.

You can, for example, open any SSRS-based report using Internet Explorer and click **Print**. Internet Explorer will prompt for installation of the additional components it needs for printing. Having them installed, you will be able to print the reports from Netwrix Auditor UI as well.

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
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 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. Data Collecting Account

This is a service account that Netwrix Auditor uses to collect audit data from the monitored items (domains, OUs, servers, etc.). Netwrix recommends creating a dedicated service account for that purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements (see the table below).

NOTE: If you are going to enable integration with Netwrix Data Classification (NDC Provider), additional server roles must be assigned to the account. See For NDC Provider for more information.

For more information about NDC provider, refer to the

Starting with version 9.96, you can use group Managed Service Account (gMSA) as data collecting account. Currently, the following data sources are supported: Active Directory (also for Group Policy and Logon Activity), Windows Server, File Server (currently for Windows File Servers), SQL Server, SharePoint.

For more details about gMSA usage, see Using Group Managed Service Account (gMSA).

The gMSA should also meet the related requirements (see the table below).

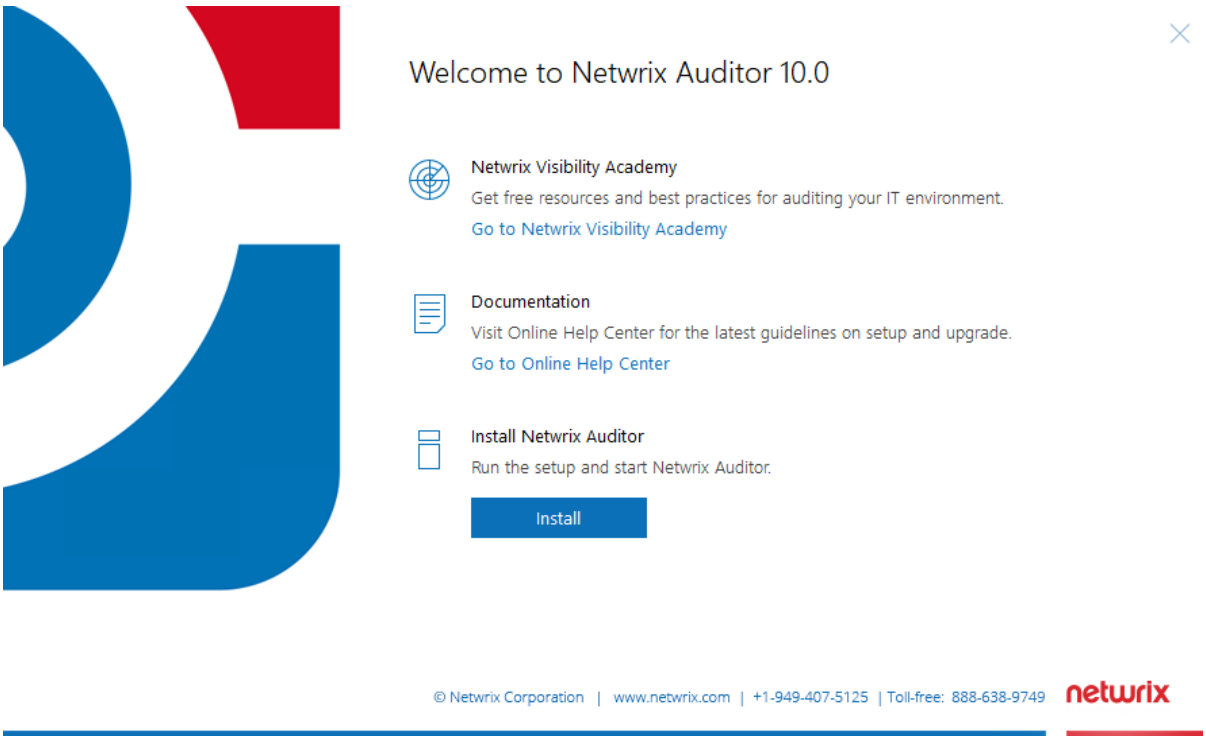
NOTE: The information in this section is outside the quick-start guide scope and is provided for reference only. For detailed instructions on how to configure the data collecting account to access your audited platform or application, see Netwrix Auditor Online Help Center .

Data source	Required rights and permissions:
User Activity	***On the target server*** • A member of the local **Administrators** group
NDC Provider	

4. Install the Product

To install Netwrix Auditor

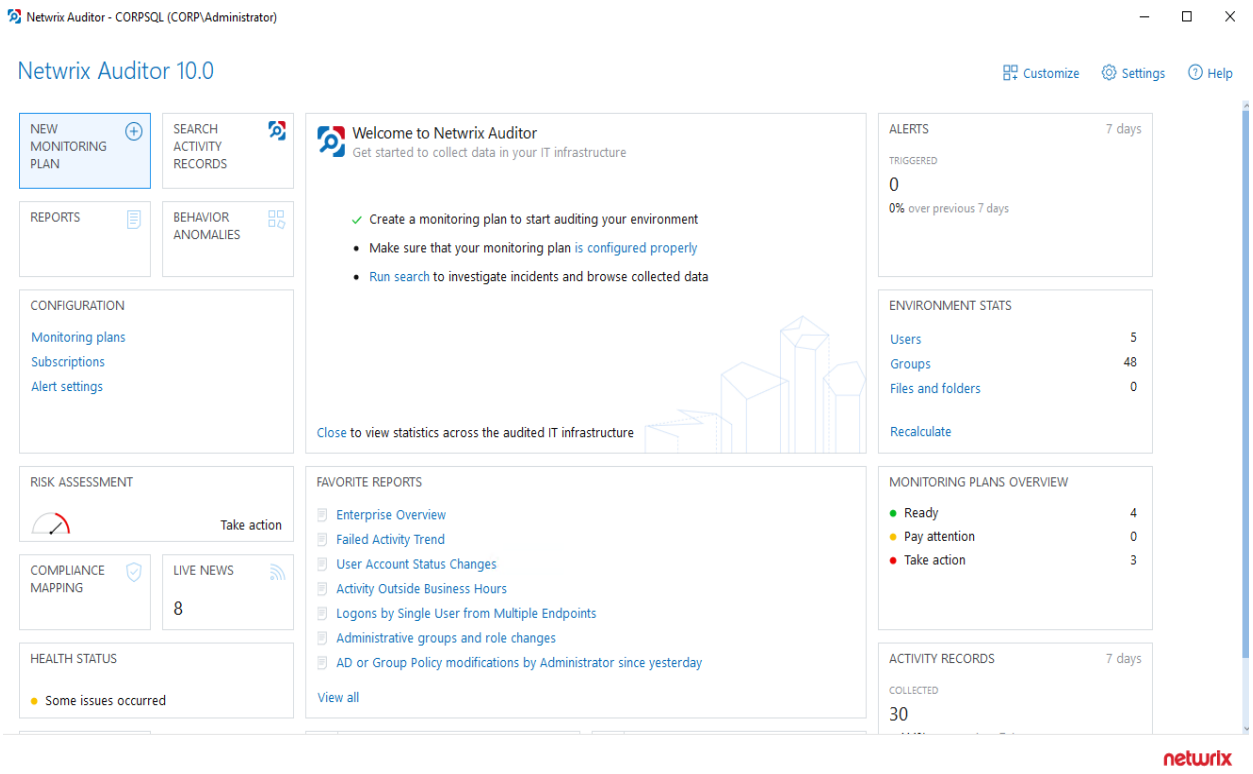
1. Download Netwrix Auditor 10 from Netwrix website.
2. Unpack the installation package. The following window will be displayed on successful operation completion:



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. Review the following for more information about the product navigation: First Launch.


Netwrix Auditor - CORPSQL (CORP\Administrator)
Netwrix Auditor 10.0
Customize
Settings
Help
NEW MONITORING PLAN
SEARCH ACTIVITY RECORDS
REPORTS
BEHAVIOR ANOMALIES
CONFIGURATION
Monitoring plans
Subscriptions
Alert settings
Welcome to Netwrix Auditor
Get started to collect data in your IT infrastructure
Create a monitoring plan to start auditing your environment
Make sure that your monitoring plan is configured properly
Run search to investigate incidents and browse collected data
Close to view statistics across the audited IT infrastructure
ALERTS
7 days
TRIGGERED
0
0% over previous 7 days
ENVIRONMENT STATS
Users 5
Groups 48
Files and folders 0
Recalculate
RISK ASSESSMENT
Take action
COMPLIANCE MAPPING
LIVE NEWS
8
FAVORITE REPORTS
Enterprise Overview
Failed Activity Trend
User Account Status Changes
Activity Outside Business Hours
Logons by Single User from Multiple Endpoints
Administrative groups and role changes
AD or Group Policy modifications by Administrator since yesterday
View all
MONITORING PLANS OVERVIEW
Ready 4
Pay attention 0
Take action 3
HEALTH STATUS
Some issues occurred
ACTIVITY RECORDS
7 days
COLLECTED
30
netwrix

5. Monitoring Plans

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan.

A monitoring plan defines data collection, notification, and storage settings.

To start collecting data, and add items to its scope.

So, to collect data from your environment, you need to do the following:

1. Specify a data source and create a monitoring plan with a wizard. See Create a New Plan for more information.
2. Add items to be monitored. An item is a specific object you want to audit. As soon as the item is added, to the monitoring plan, Netwrix Auditor starts collecting data from it. See Add Items for Monitoring for more information.

5.1. Using historical data

For many data sources, you can instruct Netwrix Auditor to collect state-in-time data along with event data. For that, Netwrix Auditor uses state-in-time snapshots of the relevant system (for example, see Data Collection from VMware Servers).

To keep users up-to-date on actual system state, Netwrix Auditor updates the latest snapshot on the regular basis. Thus, only the latest snapshot is available for ongoing reporting in Netwrix Auditor.

However, you may need to generate reports based on the historical data. For that, you must import the historical snapshots to the database.

NOTE: To import snapshots, you must be assigned the *Global administrator* or the *Global reviewer* role. See Assign Roles for more information.

To import historical snapshots:

1. Select the monitoring plan you need.
2. Select the required data source and click **Edit data source** on the right to open its properties.
3. Click **General** on the left.
4. In the **Manage historical snapshots** section, click **Manage**.
5. In the **Manage Snapshots** window, select the snapshots that you want to import — use the arrows to move the selected snapshots to the **Snapshots available for reporting** list. When finished, click **OK**.

5.2. Create a New Plan

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

Then follow the steps of the Monitoring Plan Wizard:

- 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

5.2.1. 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 Data Collecting Account. Netwrix recommends creating a special service account with extended permissions. **NOTE:** If you want to audit network devices or Azure AD/Office 365 infrastructure, you can use any account here.

5.2.2. 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 2016 SP2 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.
Password	Enter a password.

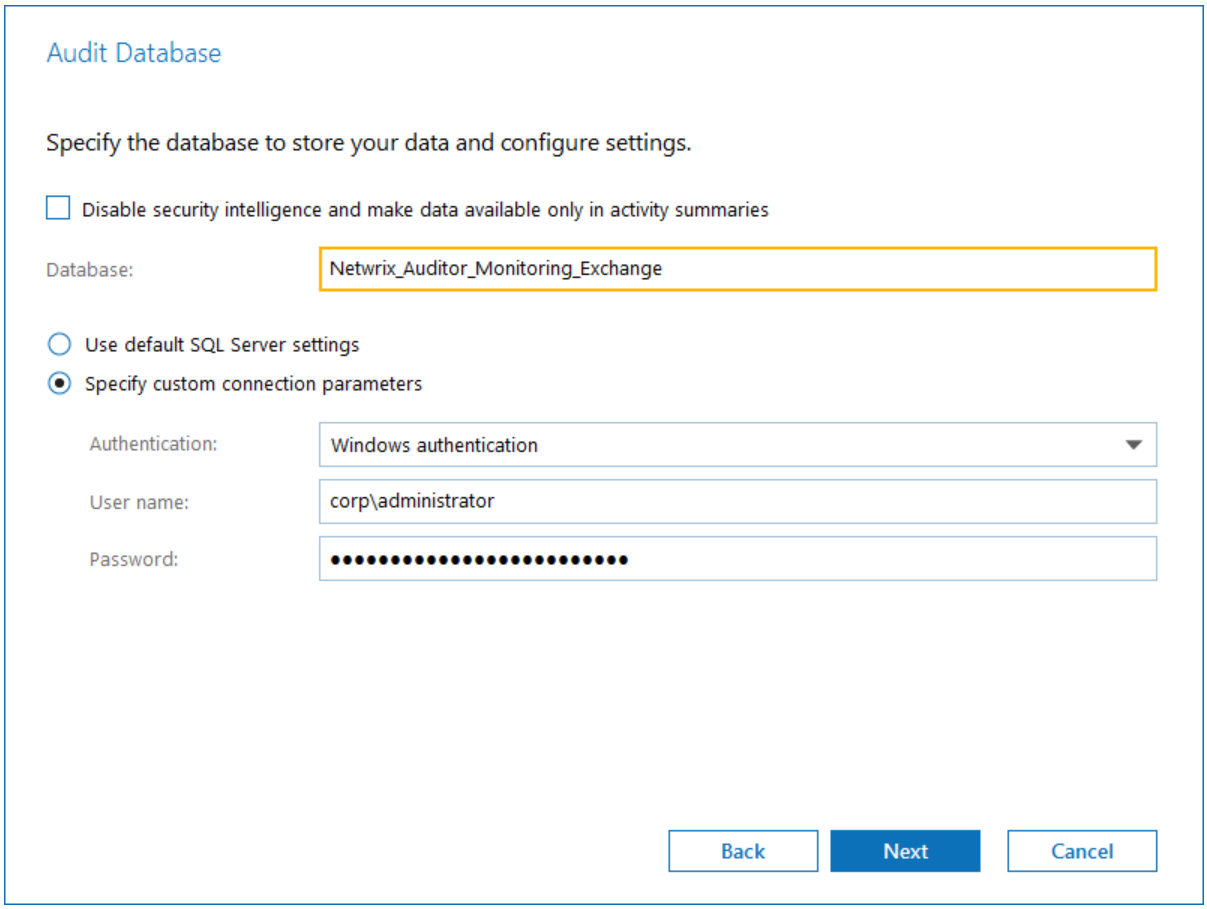
IMPORTANT! If you want to use Group Managed Service Account (gMSA) to access the SQL Server instance hosting the database, consider that in this case Netwrix Auditor will not be able to generate SSRS-based reports (due to Microsoft limitations).

5.2.3. 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.

5.2.4. 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.

5.2.5. 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.

5.2.6. 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.

5.3. 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.

5.3.1. AD Container

NOTE: For evaluation purposes, Netwrix recommends selecting **Computer** as an item for a monitoring plan. Once the product is configured to collect data from the specified items, audit settings (including Core and Compression services installation) will be applied to all computers within AD Container or IP Range.

Complete the following fields:

Option	Description
	General
Specify AD container	Specify a whole AD domain, OU or container. Click **Browse** to select from the list of containers in your network. You can also: • Select a particular computer type to be audited within the chosen AD container: **Domain controllers, Servers (excluding domain controllers)**, or **Workstations**. • Click **Exclude** to specify AD domains, OUs, and containers you do not want to audit. In the **Exclude Containers** dialog, click **Add** and specify an object. **NOTE:** The list of containers does not include child domains of trusted domains. Use other options **(Computer, IP range** to specify the target computers.
Specify the account for collecting data	Select the account that will be used to collect data for this item. Starting with version 9.96, you can use group Managed Service Accounts (gMSA) as data collecting accounts.

Option	Description
	Containers and Computers
Monitor hidden shares	By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. **IMPORTANT!** Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Depending on the type of the object you want to exclude, select one of the following: • **Add AD Container** – browse for a container to be excluded from being audited. You can select a whole AD domain, OU or container. • **Add Computer** – Provide the name of the computer you want to exclude as shown in the "*Where*" column of reports and Activity Summaries. For example, *backupsrv01.mydomain.local*. **NOTE:** Wildcards (*) are not supported. **TIP:** In addition to the restrictions for a monitoring plan, you can use the *.txt files to collect more granular audit data. Note that the new monitoring scope restrictions apply together with previous exclusion settings configured in the *.txt files. Review the following for more information: Exclude Objects from Monitoring Scope.

5.3.2. Computer

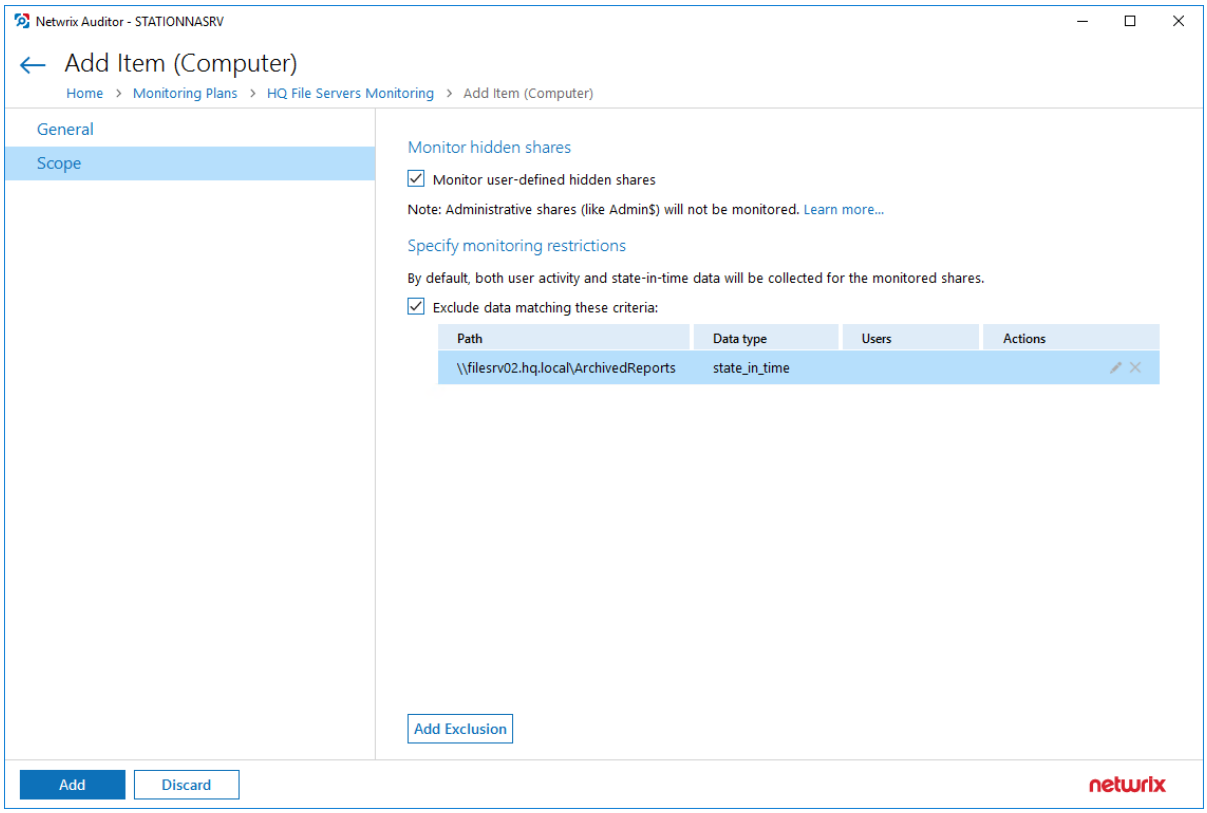
Complete the following fields:

Option	Description
	General

Option	Description
Specify a computer	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 hidden shares	By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. **IMPORTANT!** Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.
Specify monitoring restrictions	Specify restriction filters to narrow your monitoring scope (search results, reports and Activity Summaries). All filters are applied using AND logic. Refer to Configure Scope for detailed instructions on how to narrow your monitoring scope.

5.3.2.1. Configure Scope

By default, both user activity and state-in-time data will be collected for the monitored item. However, you can narrow your monitoring scope by specifying certain locations, user accounts or actions to exclude .



Click **Add Exclusion**, then in the **Specify Filters** dialog do the following:

1. Provide the path to the file share where you are going to exclude some audit data. Use the path format as it appears in the "*What*" column of reports and Activity Summaries — for example, *\\corpsrv\shared*.

   NOTE: You can use a wildcard (*) only if you need to exclude **user activity** on this file share. For other data types (*state-in-time* or *all data*) wildcards are not supported. This refers to the specified shared folder, its subfolders and files.

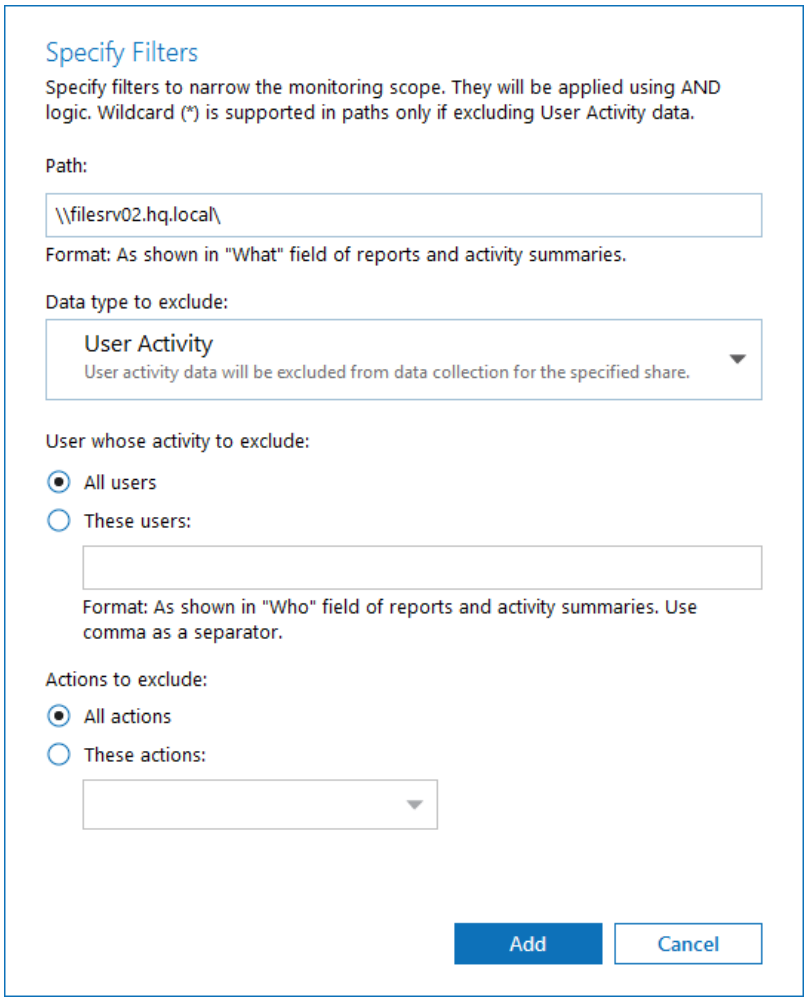
2. Select what type of data you want to exclude:

Option	Description	Example
All Data	Select if you want to completely exclude the specified file share from being audited. The product will not collect any user activity or state-in-time data. **NOTE:** In this case,Netwrix Auditor does not adjust audit settings automatically for the selected folders.	A Security Officer wants to monitor a file share but s/he does not have access to a certain folder on this share. Thus, s/he configures the product not to monitor this folder at all.

Option	Description	Example
State-in-Time	Select to configure Netwrix Auditor to exclude data for the state-in-time reports from the monitoring scope.	A Security Officer wants to monitor a file share, but it contains a folder with a huge amount of objects, so s/he does not want Netwrix Auditor to collect state-in-time data for this folder.
User Activity	Select to exclude actions performed by specific users on the selected file share. See the procedure below for details. **NOTE:** In this case, the product still collects stat-in-time data for this share.	A Security Officer wants to monitor a file share that contains a public folder for which s/he does not want to collect *Read* operations.

To exclude specific user activity:

1. Specify what user accounts should be excluded:
   - **All Users** — select to exclude the activity of any user on the file share you specified.
   - **These users** — select to exclude specific users' activity. Provide user names as shown in the "*Who*" column in reports and Activity Summaries, e.g., *MyDomain\user1*. To enter multiple accounts, use comma as a separator.
2. Specify what actions should be excluded:
   - **All actions** — exclude all actions of the selected users
   - **These actions:** — use the drop-down list to select the actions to exclude, e.g. *Added* and *Moved*.



After configuring all filters, click **Add** to save them and return to the item settings.

5.3.3. IP Range

NOTE: For evaluation purposes, Netwrix recommends selecting **Computer** as an item for a monitoring plan. Once the product is configured to collect data from the specified items, audit settings (including Core and Compression services installation) will be applied to all computers within AD Container or IP Range.

Complete the following fields:

Option	Description
	General
Specify IP range	Specify an IP range for the audited computers. To exclude computers from within the specified range, click **Exclude**. Enter the IP subrange you want to exclude, and click **Add**.

Option	Description
Specify the account for collecting data	Select the account that will be used to collect data for this item.
	Scope
Monitor hidden shares	By default, Netwrix Auditor will monitor all shares stored in the specified location, except for hidden shares (both default and user-defined). Select **Monitor user-defined hidden shares** if necessary. **IMPORTANT!** Even when this option is selected, the product will not collect data from administrative hidden shares such as: default system root or Windows directory (ADMIN$), default drive shares (D$, E$, etc.), shares used by printers to enable remote administration (PRINT$), etc.

5.4. Launch Data Collection Manually and Update Status

If you do not want to wait until a scheduled data collection, you can launch it manually.

NOTE: Not applicable to Netwrix Auditor for User Activity. For this data source, the product sends real-time data about sessions and activity.

Along with data collection, the following actions will be performed:

- An Activity Summary email will be generated and sent to the specified recipients. It will list all changes that occurred since the last scheduled or on-demand Activity Summary delivery.
- Changes that occurred between data collections will be written to the Long-Term Archive and the Audit Database, and become available in the Netwrix Auditor client.
- A state-in-time data will be updated.

To launch data collection manually

1. Navigate to **All monitoring plans** → your monitoring plan, select **Edit**.
2. In the right pane, click **Update**.

NOTE: Depending on the size of the monitored environment and the number of changes, data collection may take a while.

6. 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.

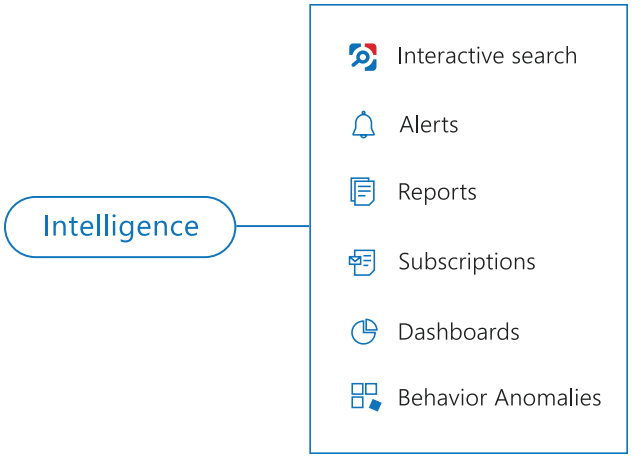
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

For example, make the following test changes:

- Lock your computer
- Start a program as another user

7. 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.



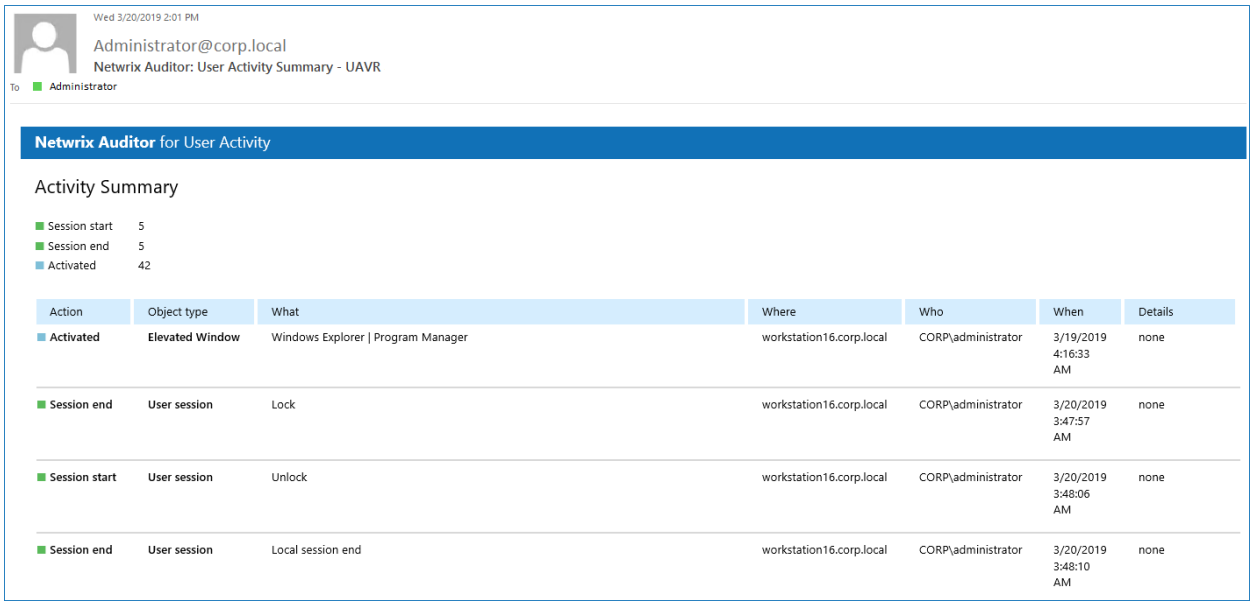
This chapter explains how to review your test changes with some of the Intelligence options and Activity Summary. Review the following for additional information:

- Review an Activity Summary
- Review the All Changes Report
- Browse Data with Intelligence Search

7.1. 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.

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



Wed 3/20/2019 2:01 PM

Administrator@corp.local

Netwrix Auditor: User Activity Summary - UAVR

To Administrator

Netwrix Auditor for User Activity

Activity Summary

- Session start 5
- Session end 5
- Activated 42

Action	Object type	What	Where	Who	When	Details
Activated	Elevated Window	Windows Explorer | Program Manager	workstation16.corp.local	CORP\administrator	3/19/2019 4:16:33 AM	none
Session end	User session	Lock	workstation16.corp.local	CORP\administrator	3/20/2019 3:47:57 AM	none
Session start	User session	Unlock	workstation16.corp.local	CORP\administrator	3/20/2019 3:48:06 AM	none
Session end	User session	Local session end	workstation16.corp.local	CORP\administrator	3/20/2019 3:48:10 AM	none

The example Activity Summar provide 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 title of activated window or session event.
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.
Details	Shows the before and after values of the modified object, object attributes, etc.

7.2. Review the All Changes Report

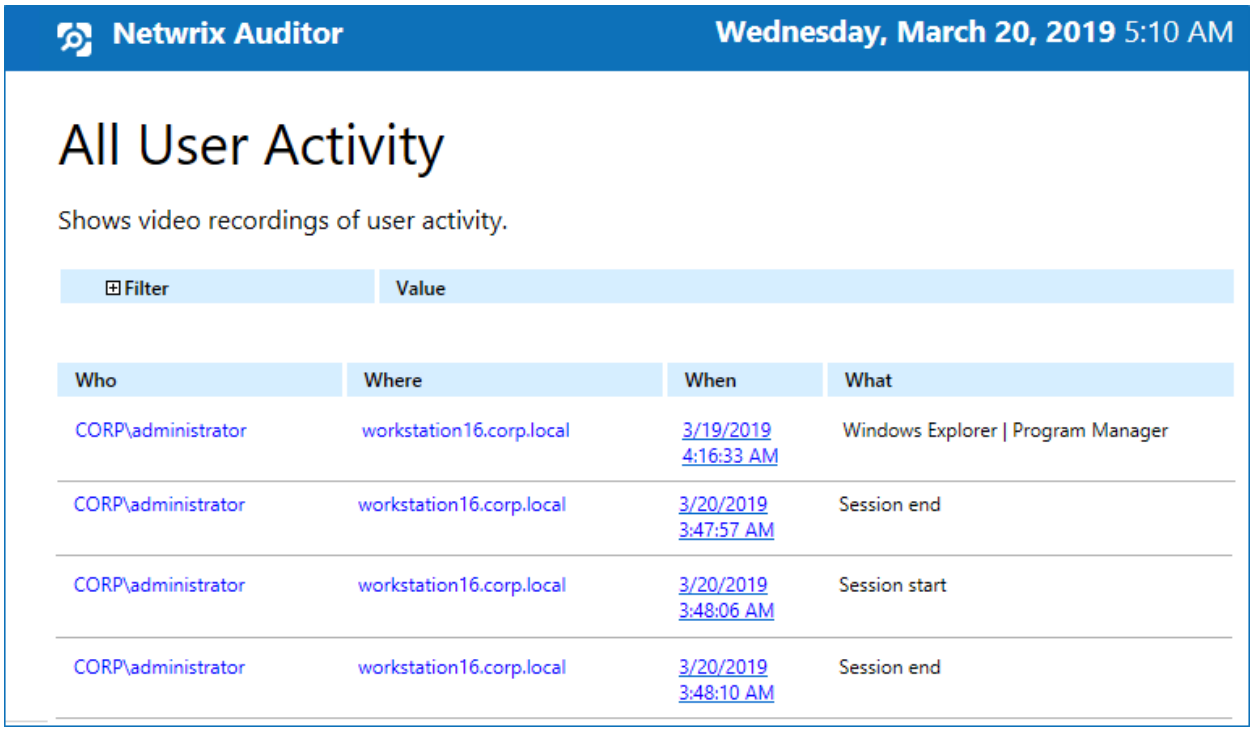
The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

Change and activity reports can be found under the **Reports → Predefined → your data source type** 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** → **your data source**.
2. Select the **All User Activity** report.
3. Click **View** to open the report.



7.3. 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.

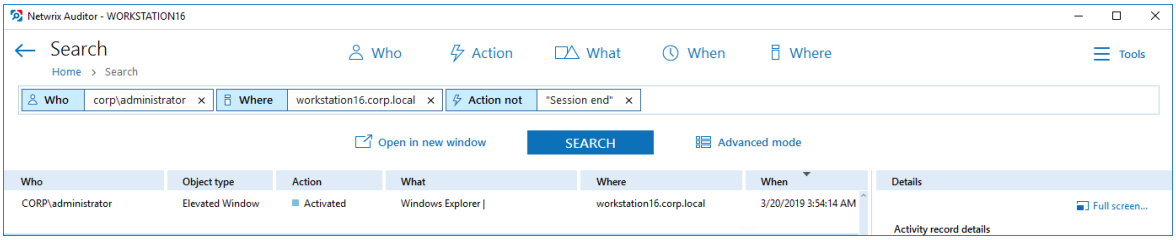
   Filters are used to narrow your search results. To create a unique set of filters, you can:

- 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.

NOTE: Refer to Netwrix Online Helpcenter for detailed instructions on how to apply filters and change match types

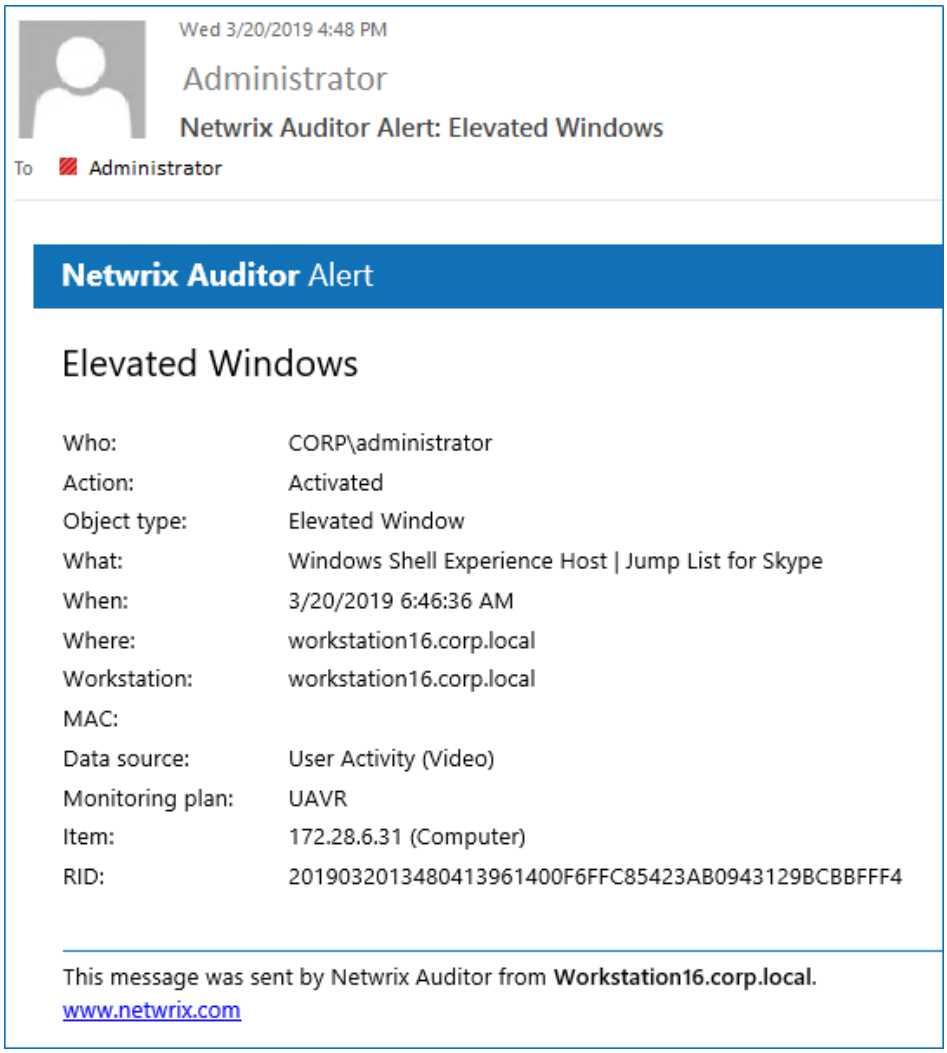
3. Click **Search**.
4. Now, you can narrow your search and modify it right from the search results pane. Click any entry that contains excess data, select **Exclude from search** in the **Details** section and specify a filter, e.g., **Action**: *Session end* to leave information on elevated windows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

   Your **Search** field will be updated, the **Action not equal to** 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

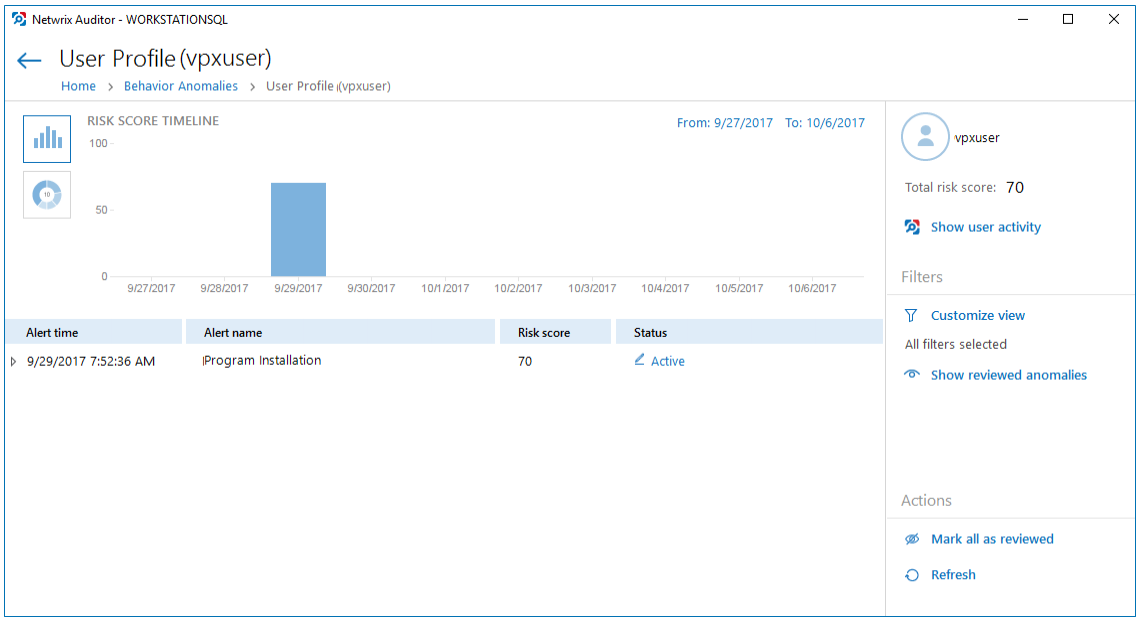
Netwrix Auditor Alert

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 (vpxuser)
Home › Behavior Anomalies › User Profile (vpxuser)
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
Program Installation
70
Active
vpxuser
Total risk score: 70
Show user activity
Filters
Customize view
All filters selected
Show reviewed anomalies
Actions
Mark all as reviewed
Refresh

8. Related Documentation

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

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 10, and suggests workarounds for these issues.

9. Glossary

M

My Term
: My definition

10. Index

N

O

R

S

U