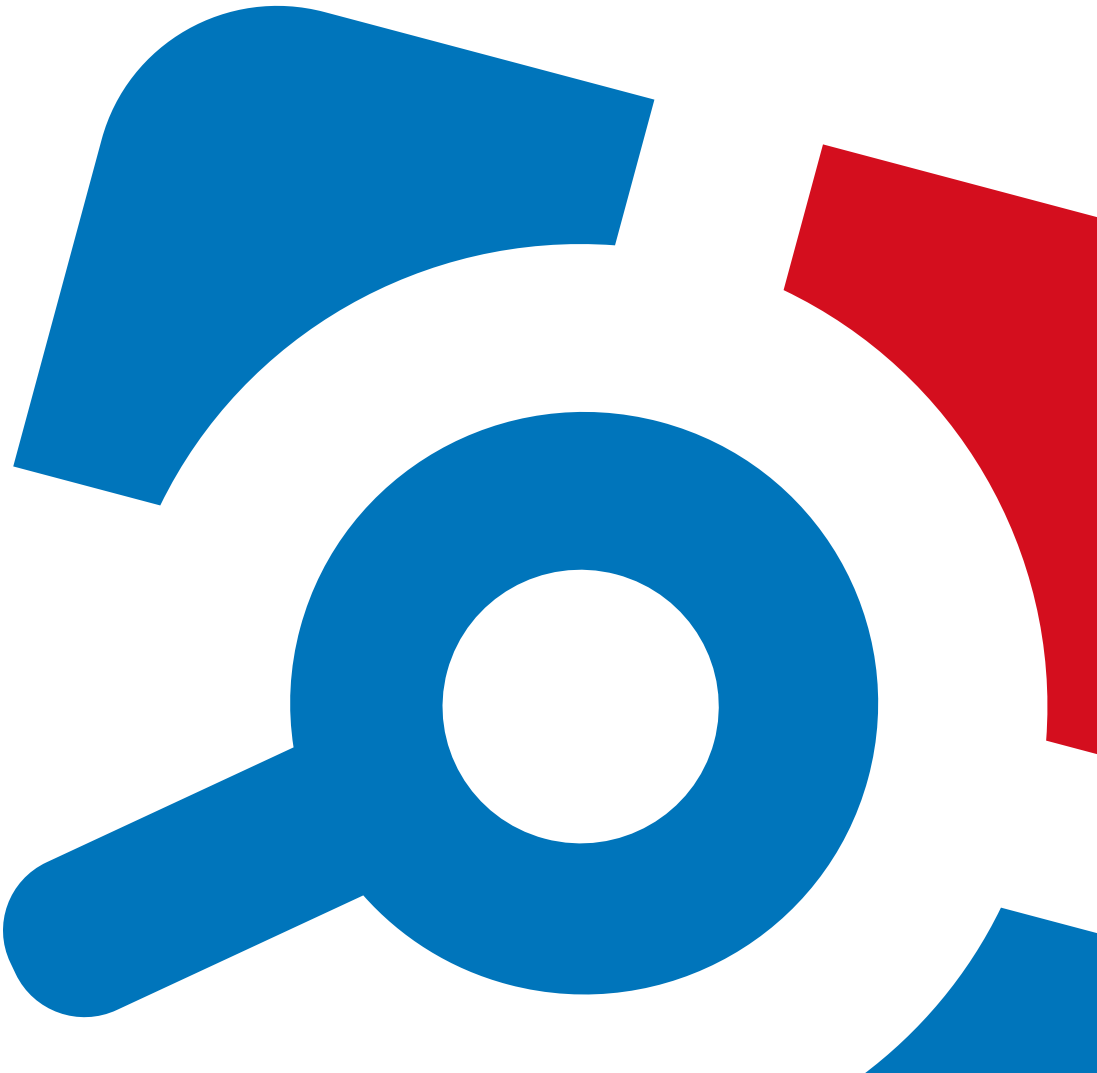
netwrix

Netwrix Auditor for Active Directory

Quick-Start Guide

Version: 9.8
7/15/2019



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.

Table of Contents

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for Active Directory. 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 an Active Directory domain
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing Active Directory 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 Overview

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

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, 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 Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain structure that can be used to assess its state at present or at any moment in the past. The product provides logon activity summary, reports on interactive and non-interactive logons including failed logon attempts. Also, Netwrix Auditor for Active Directory helps address specific tasks—detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a stand-alone Netwrix Auditor Object Restore for Active Directory tool that allows

reverting unwanted changes to AD objects down to their attribute level.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 Active Directory:

Data source	Supported Versions
Active Directory	Domain Controller OS versions: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012/2012 R2 • Windows Server 2008/2008 R2

2.2. Requirements to Install Netwrix Auditor

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

- Hardware Requirements
- Software Requirements

2.2.1. Hardware Requirements

Review the hardware requirements for Netwrix Auditor installation.

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

The hardware configuration depends on the size of your monitored environment and the number of activity records processed by the product per day. Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for Active Directory. 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

Component	Requirements
	• Windows Server 2008 R2 SP1 Windows Desktop OS (64-bit): • 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.

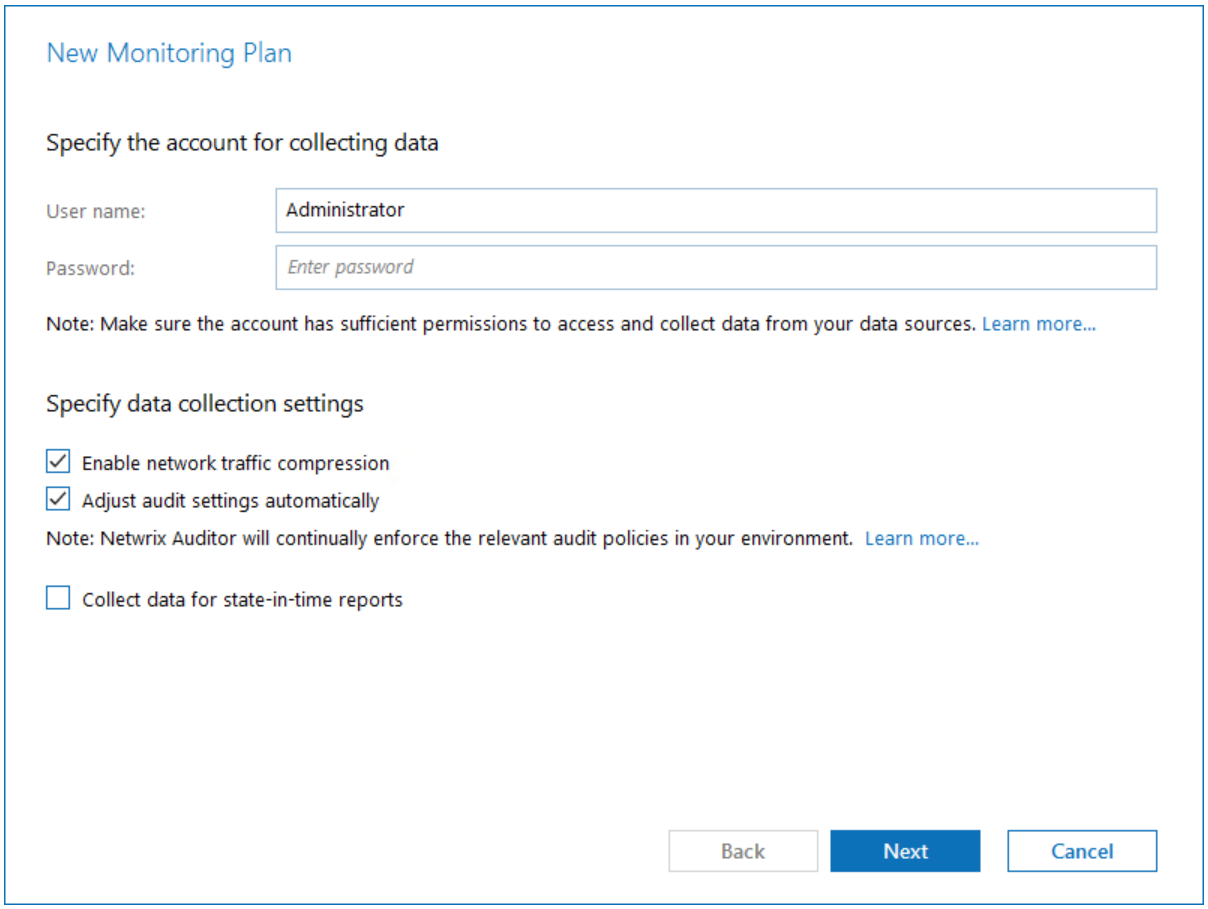
Service or component	Recommendations
Network and target systems or servers that work as your data sources	Test connectivity to your data source. Make sure you can access it by its NetBIOS and FQDN name from the computer where you intend to install Netwrix Auditor—use the nslookup command-line tool to 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.

NOTE: There is no need to perform any additional configuration steps to prepare your IT infrastructure for auditing. Netwrix Auditor provides an option that automatically configures audit settings in the target environment. For a full list of settings required for Netwrix Auditor to collect comprehensive audit data and instructions on how to configure them manually, refer to Netwrix Auditor Installation and Configuration Guide.

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:
Active Directory	***On the computer where Netwrix Auditor is installed:*** • Membership in the local **Administrators** group (for auditing local or trusted domain) ***In the target domain*** 1. Depending on the network traffic compression setting you need to use, one of the

Data source	Required rights and permissions:

following is required:

- If network traffic compression is ***enabled***, then the account must belong to the **Domain Admins** group

  NOTE: If you need granular rights to be assigned instead, please contact Netwrix Technical support.

- If network traffic compression is ***disabled***, and the account you plan to use for data collection is not a member of the Domain Admins group, then the **Manage auditing and security log** policy must be defined for this account. See Configuring 'Manage Auditing and Security Log' Policy for more information.

2. If you plan to process Active Directory **Deleted Objects** container, **Read** permission on this container is required. See Granting Permissions for 'Deleted Objects' Container for more information.

   NOTE: Grant this permission only if the account you plan to use for data collection is not a member of the Domain Admins group

3. If auto-backup is ***enabled*** for the domain controller event logs, then the following is required:

   a. Permissions to access the *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security* registry key on the domain controllers in the target domain. See Assigning Permission To Read the Registry Key for more information.

   b. Membership in one of the following groups: **Administrators**, **Print Operators**, **Server Operators**

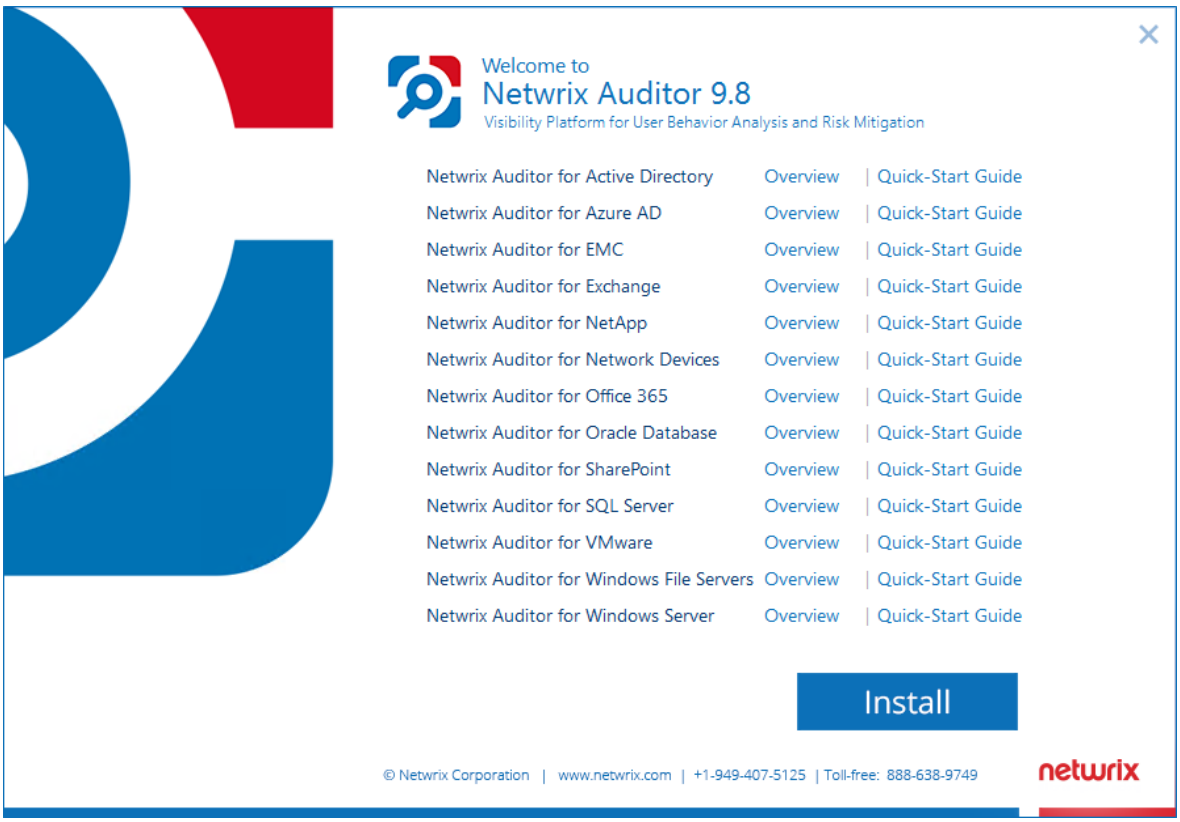
   c. **Read/Write** share permission and **Full control** security permission on the logs backup folder

NOTE: Grant these permissions only if the account you plan to use for data collection is not a member of the Domain Admins group.

4. Install the Product

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:

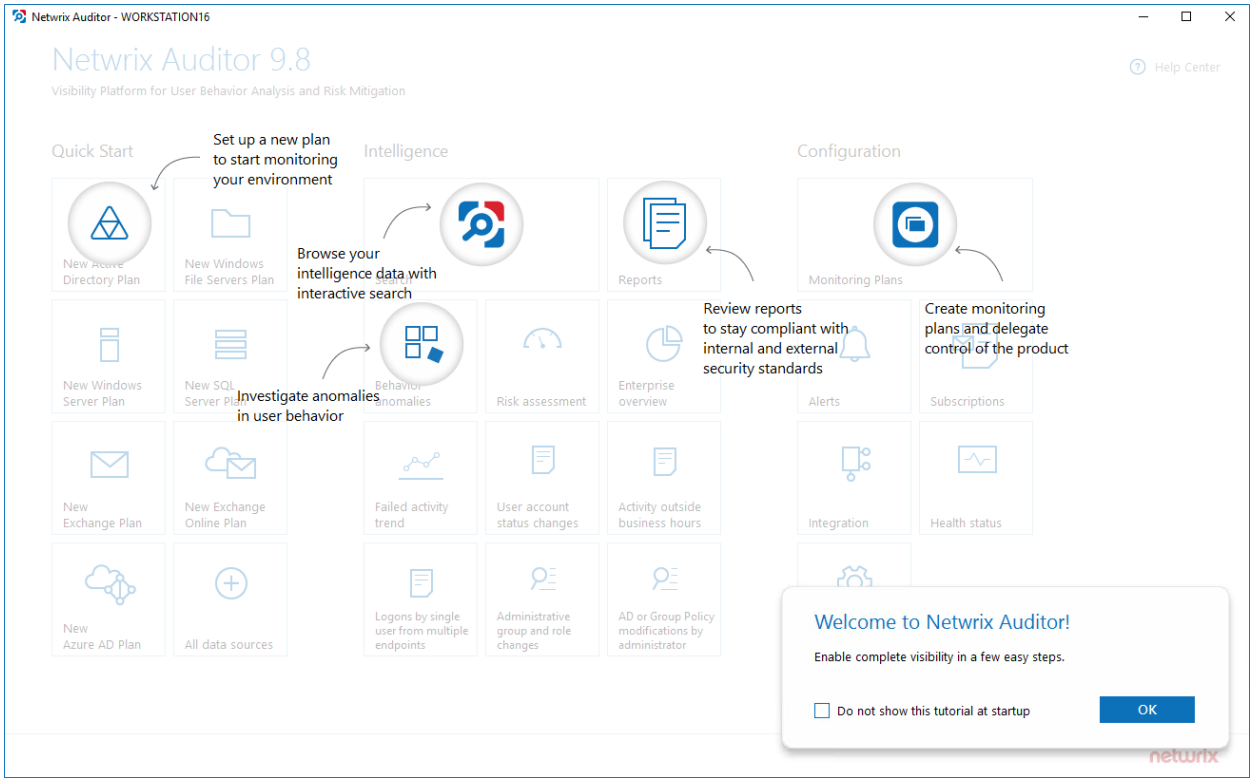


3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.
4. On the **Select Installation Type** step, select **Full installation**.
5. On the **Destination Folder** step, specify the installation folder.
6. On the **Netwrix Customer Experience Program** step, you are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



5. 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 Active Directory, 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.

5.1. Create a New Plan

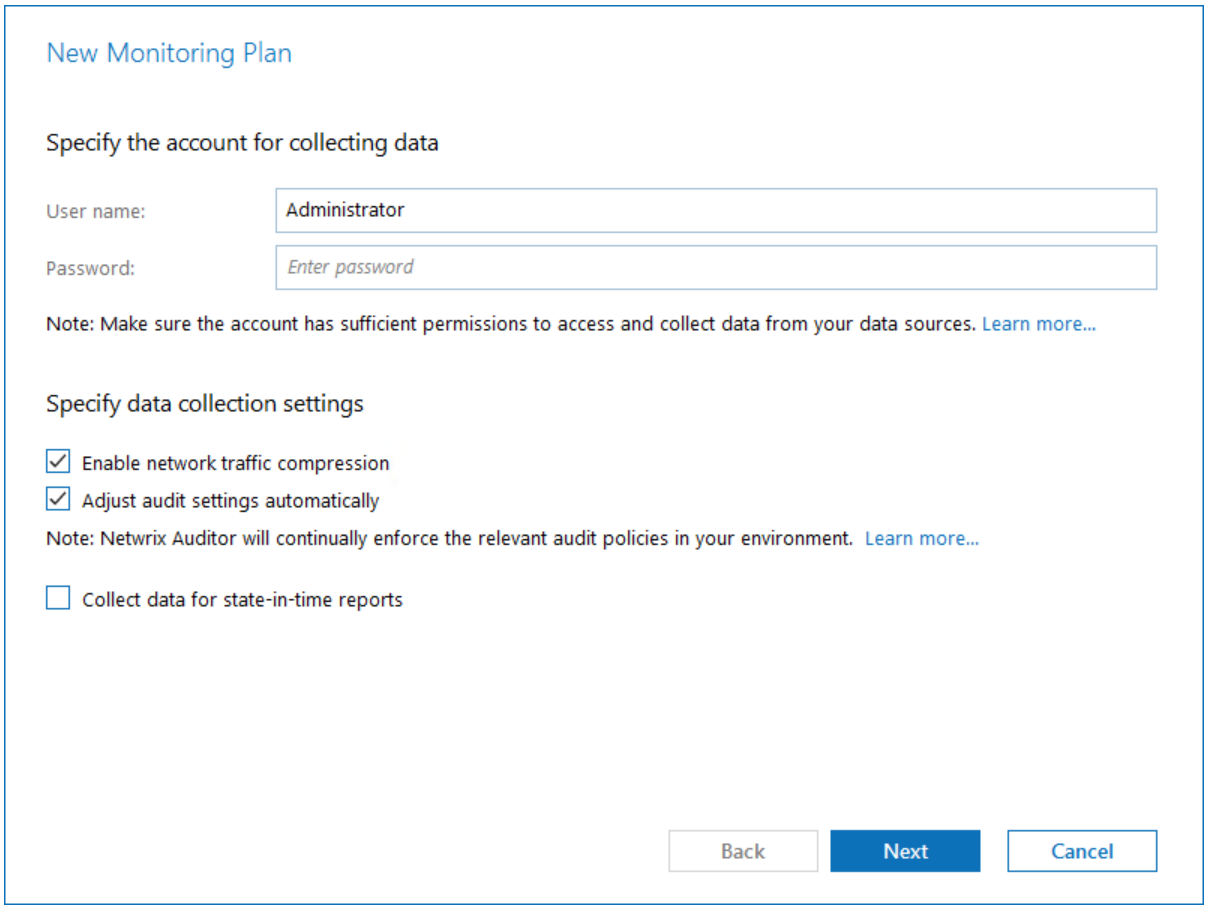
On the main Netwrix Auditor page, click the **New Active Directory Plan** tile in the **Quick Start** section.

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

5.1.1. 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:** If any conflicts are detected with your current settings, automatic audit configuration will not be performed. For a full list of audit settings and instructions on how to configure them manually, refer to Configure IT Infrastructure for Auditing and Monitoring.
Collect data for state-in-time reports	State-in-time reports are based on the daily configuration snapshots of your audited systems; they help you to analyze particular aspects of the environment. State-in-time configuration snapshots are also used for IT risks assessment metrics and reports. This data collection option is available if you are creating a monitoring plan for any of the following data sources: • Active Directory • File Servers • Windows Server • Group Policy • SharePoint To read more, refer to State-in-Time Reports and IT Risk Assessment Overview.

5.1.2. Default SQL Server Instance

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

Specify one of the following options:

- **Install a new instance of Microsoft SQL Server Express automatically**—Select if you want Netwrix Auditor to download and configure SQL Server 2014 Express with Advanced Services.

- **Use an existing SQL Server instance**—Select to continue using an installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and prepopulates the fields. Complete the following fields:

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

5.1.3. Audit Database

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

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

5.1.4. Notifications

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

Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.

Option	Description
Sender address	Enter the address that will appear in the **From** field. NOTE: It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.
Password	Enter a password for the SMTP authentication.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Use implicit SSL authentication	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.
Enforce certificate validation to ensure security	Select this checkbox if you want to verify security certificate on every email transmission.

5.1.5. Recipients

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

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

5.1.6. Monitoring Plan Summary

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

5.2. 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.

5.2.1. Domain

Complete the following fields:

Option	Description
Specify Active Directory domain	Specify the audited domain name in the FQDN format. For example, "*company.local*".
Specify the account for collecting data	Select the account that will be used to collect data for this item.

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.

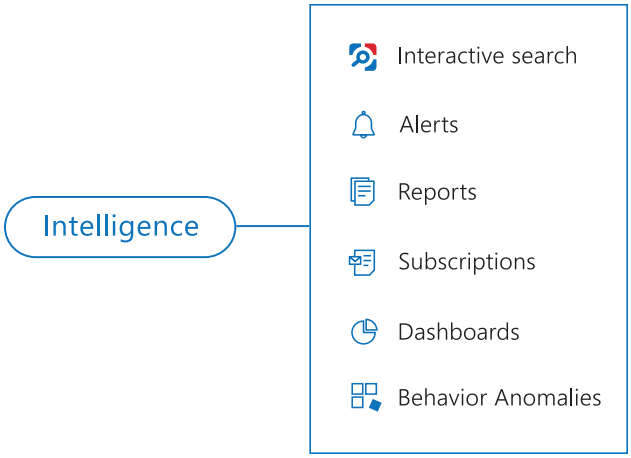
For example, make the following test changes:

- Create a user using **Active Directory Users and Computers**
- Add this user to the **Domain Admins** group

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.

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 Active Directory Overview
- Review the All Active Directory Changes Report
- Browse Data with Intelligence Search

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

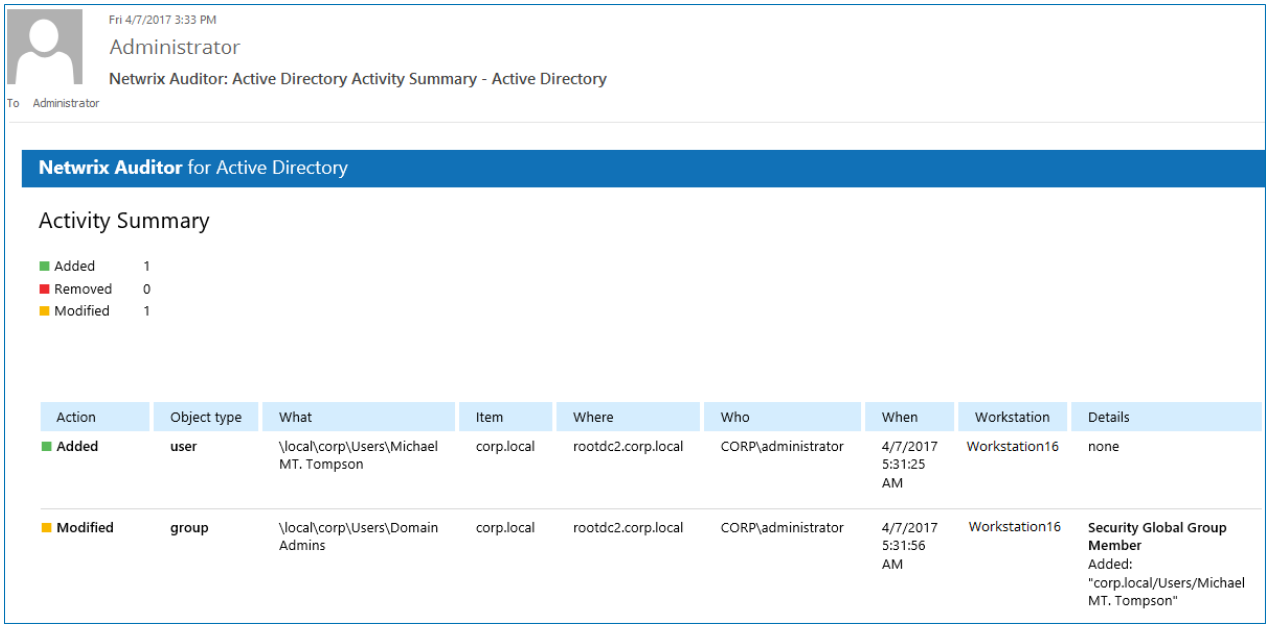
To launch data collection manually

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.

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. 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:



Fri 4/7/2017 3:33 PM
Administrator
Netwrix Auditor: Active Directory Activity Summary - Active Directory
To Administrator

Netwrix Auditor for Active Directory

Activity Summary

Added 1
Removed 0
Modified 1

Action	Object type	What	Item	Where	Who	When	Workstation	Details
Added	**user**	\local\corp\Users\Michael MT. Tompson	corp.local	rootdc2.corp.local	CORP\administrator	4/7/2017 5:31:25 AM	Workstation16	none
Modified	**group**	\local\corp\Users\Domain Admins	corp.local	rootdc2.corp.local	CORP\administrator	4/7/2017 5:31:56 AM	Workstation16	**Security Global Group Member** Added: "corp.local/Users/Michael MT. Tompson"

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 domain controller where the change was made.
Who	Shows the name of the account under which the change was made.
When	Shows the exact time when the change occurred.
Workstation	Shows the name of the computer where the user was logged on when the change was made.
Details	Shows the before and after values of the modified object, object attributes, etc.

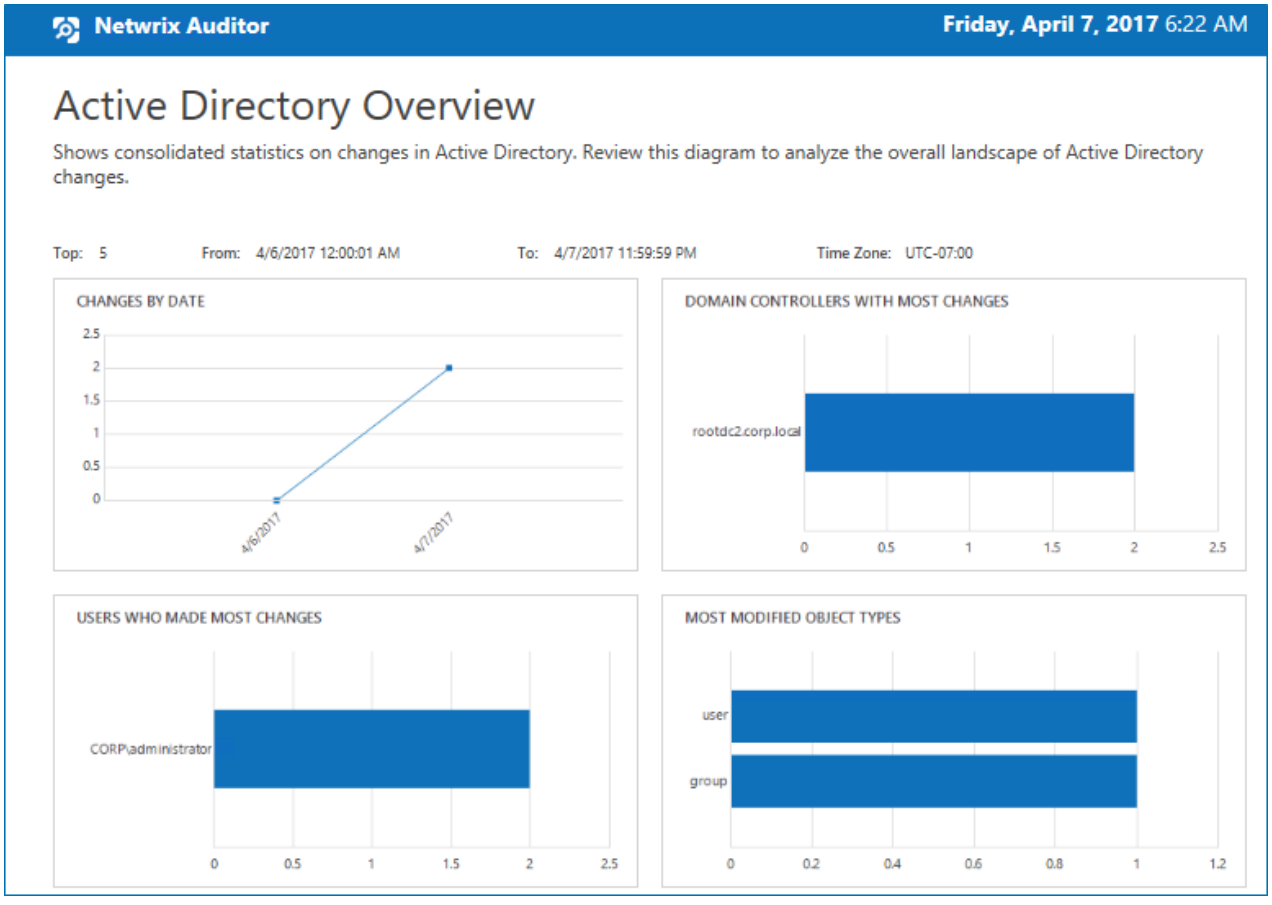
7.2. Review Active Directory Overview

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 **Active Directory Overview**.

To see how your changes are reported with Active Directory Overview

1. On the main Netwrix Auditor page, navigate to the **Intelligence** section and click the **Reports** tile.
2. Expand the **Predefined** → **Active Directory** → **Active Directory Changes** reports.
3. Select the **Active Directory 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.



7.3. Review the All Active Directory Changes Report

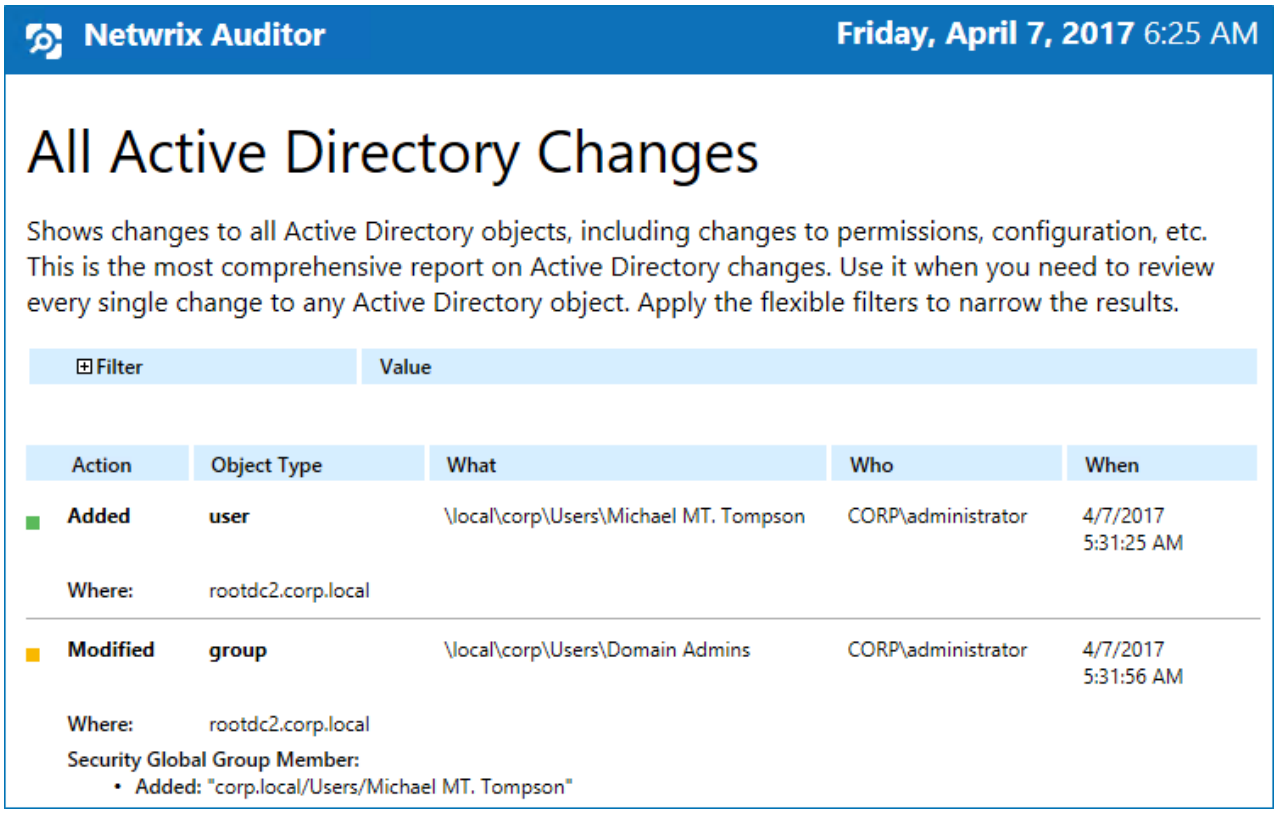
The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

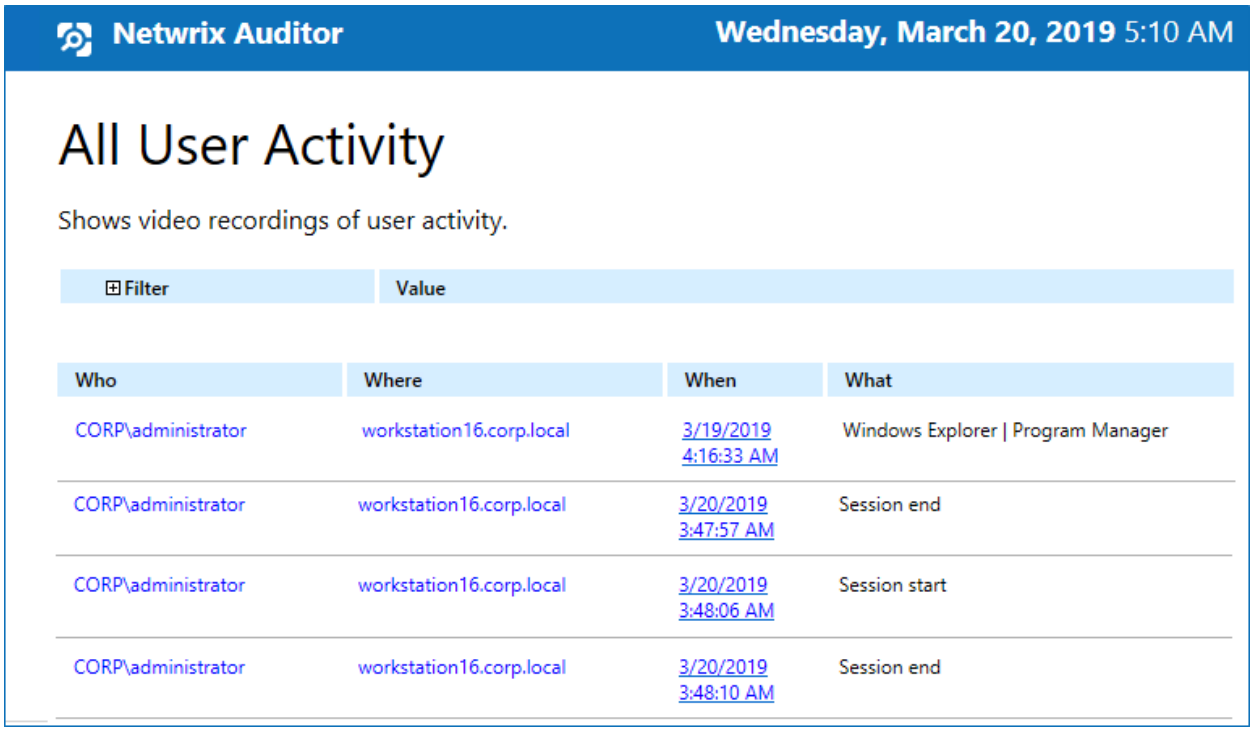
Change and activity reports can be found under the **Reports** → **Predefined** → **Active Directory** → **Active Directory Changes** and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, 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** → **Active Directory** → **Active Directory Changes**.
2. Select the **All Active Directory Changes** report.
3. Click **View** to open the report.





7.4. 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.

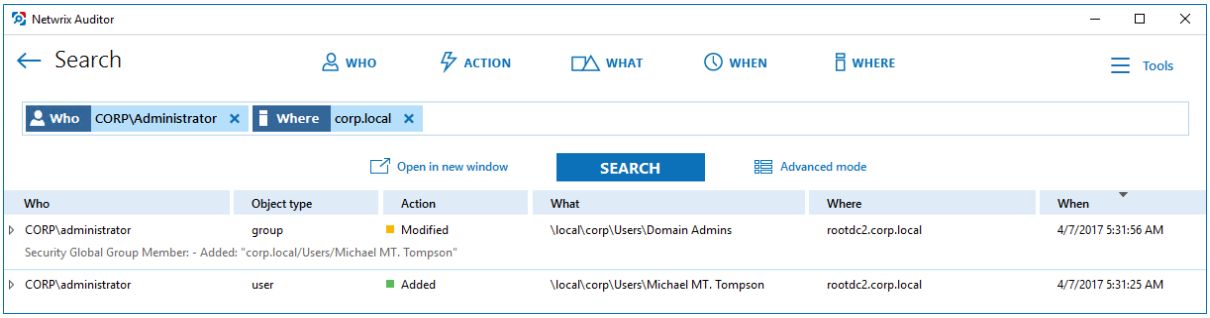
   For example, consider adding these filters:

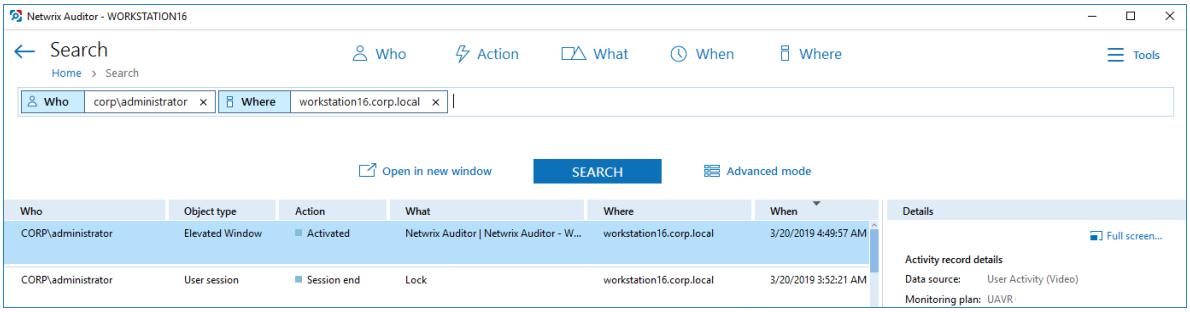
Filter	Value
WHO	Specify your account name, as you performed test changes.
WHERE	Specify your Active Directory domain name.

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:

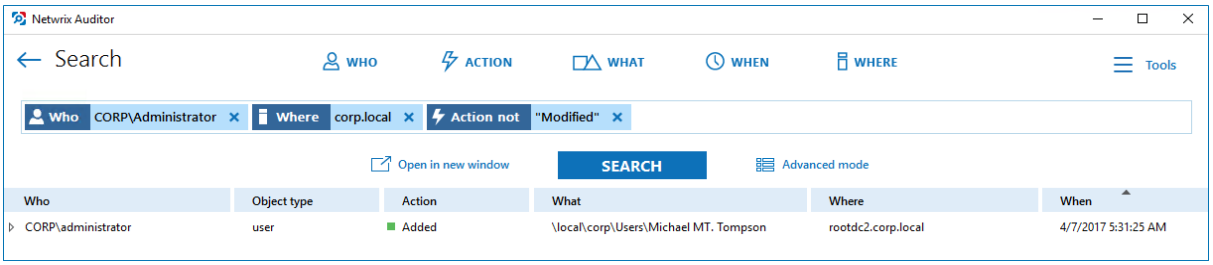
3. Click **Search**.

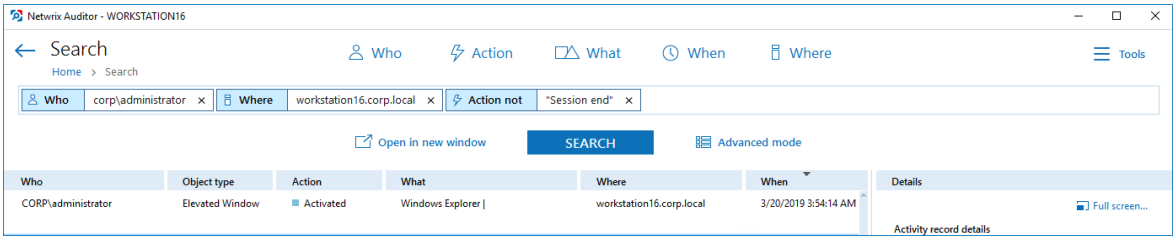




4. Now, you can narrow your search and modify it right from the search results pane. Click any entry that contains excess data, select **Exclude from search** in the **Details** section and specify a filter, e.g., **Action**: *Modified* to leave information on newly created users only.

   Your **Search** field will be updated, the **Action not** filter will be added. Make sure to click **Search** again to update your search results.

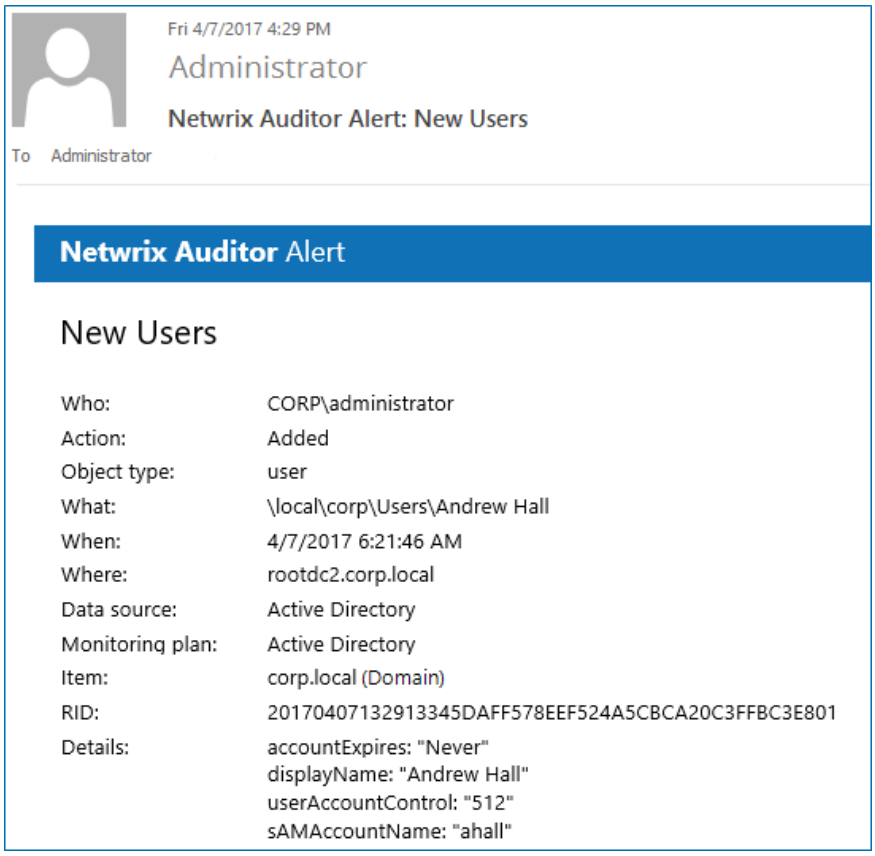




5. Having reviewed your search results, navigate to **Tools**.

   - 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:



Fri 4/7/2017 4:29 PM

Administrator

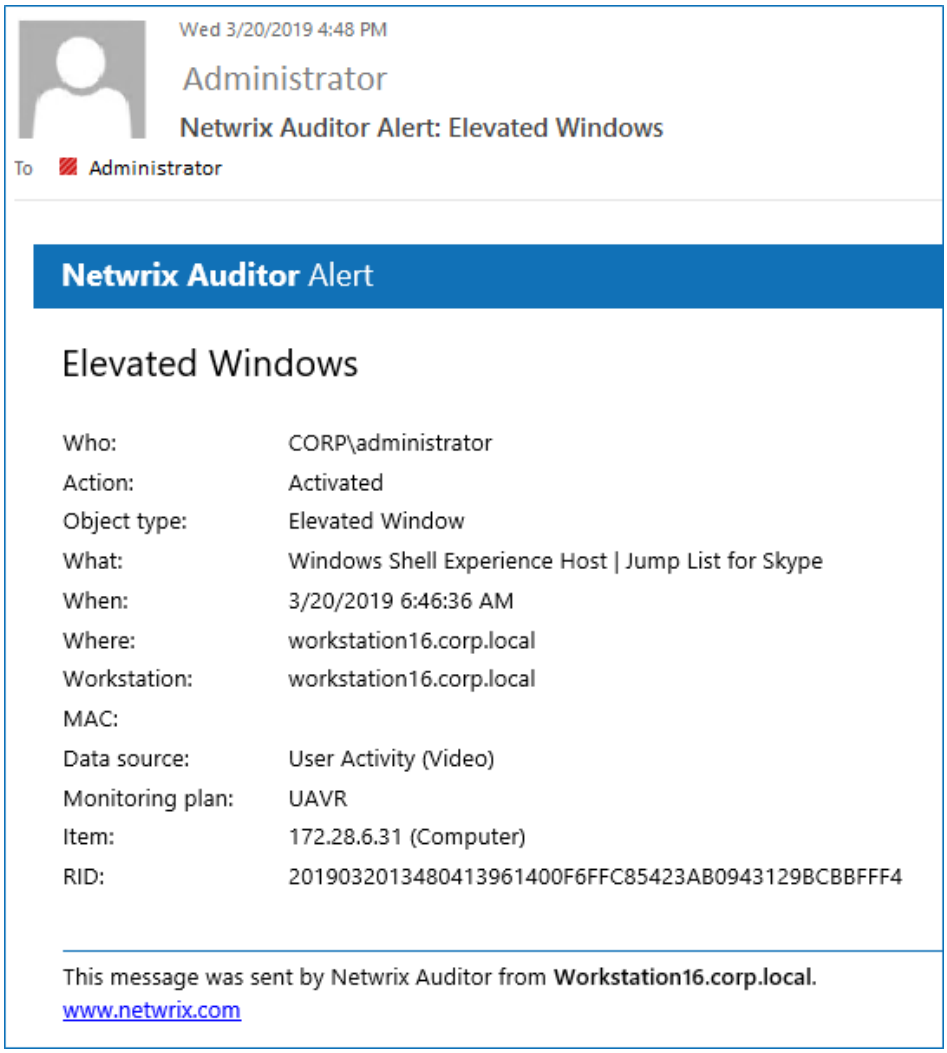
Netwrix Auditor Alert: New Users

To Administrator

Netwrix Auditor Alert

New Users

Who:	CORP\administrator
Action:	Added
Object type:	user
What:	\local\corp\Users\Andrew Hall
When:	4/7/2017 6:21:46 AM
Where:	rootdc2.corp.local
Data source:	Active Directory
Monitoring plan:	Active Directory
Item:	corp.local (Domain)
RID:	20170407132913345DAFF578EEF524A5CBCA20C3FFBC3E801
Details:	accountExpires: "Never" displayName: "Andrew Hall" userAccountControl: "512" sAMAccountName: "ahall"



Wed 3/20/2019 4:48 PM

Administrator

Netwrix Auditor Alert: Elevated Windows

To Administrator

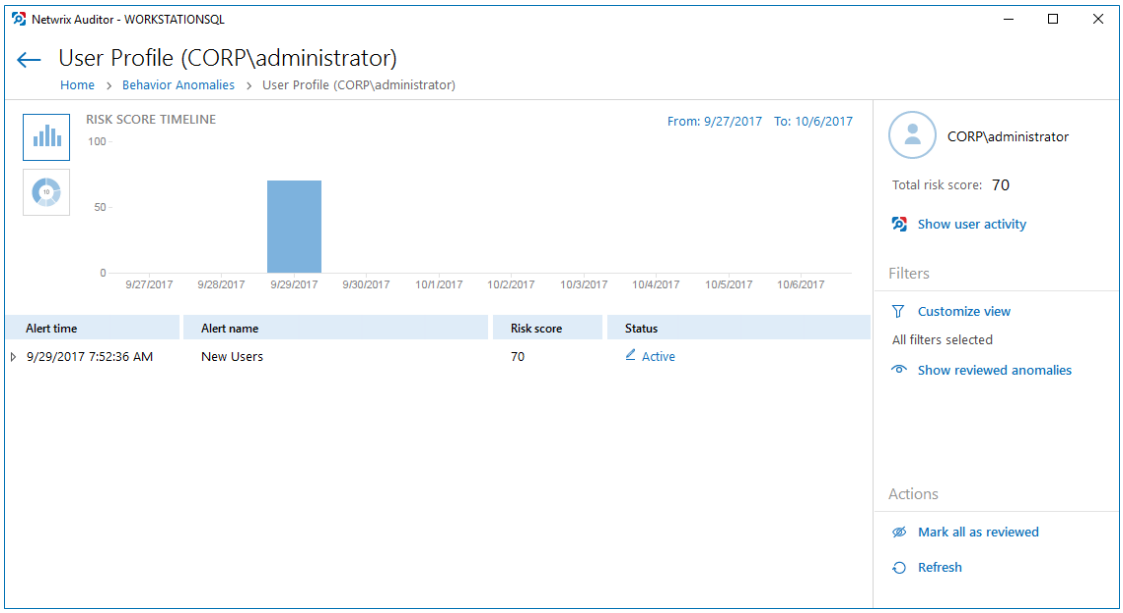
Netwrix Auditor Alert

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
New Users
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

8. Related Documentation

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

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.