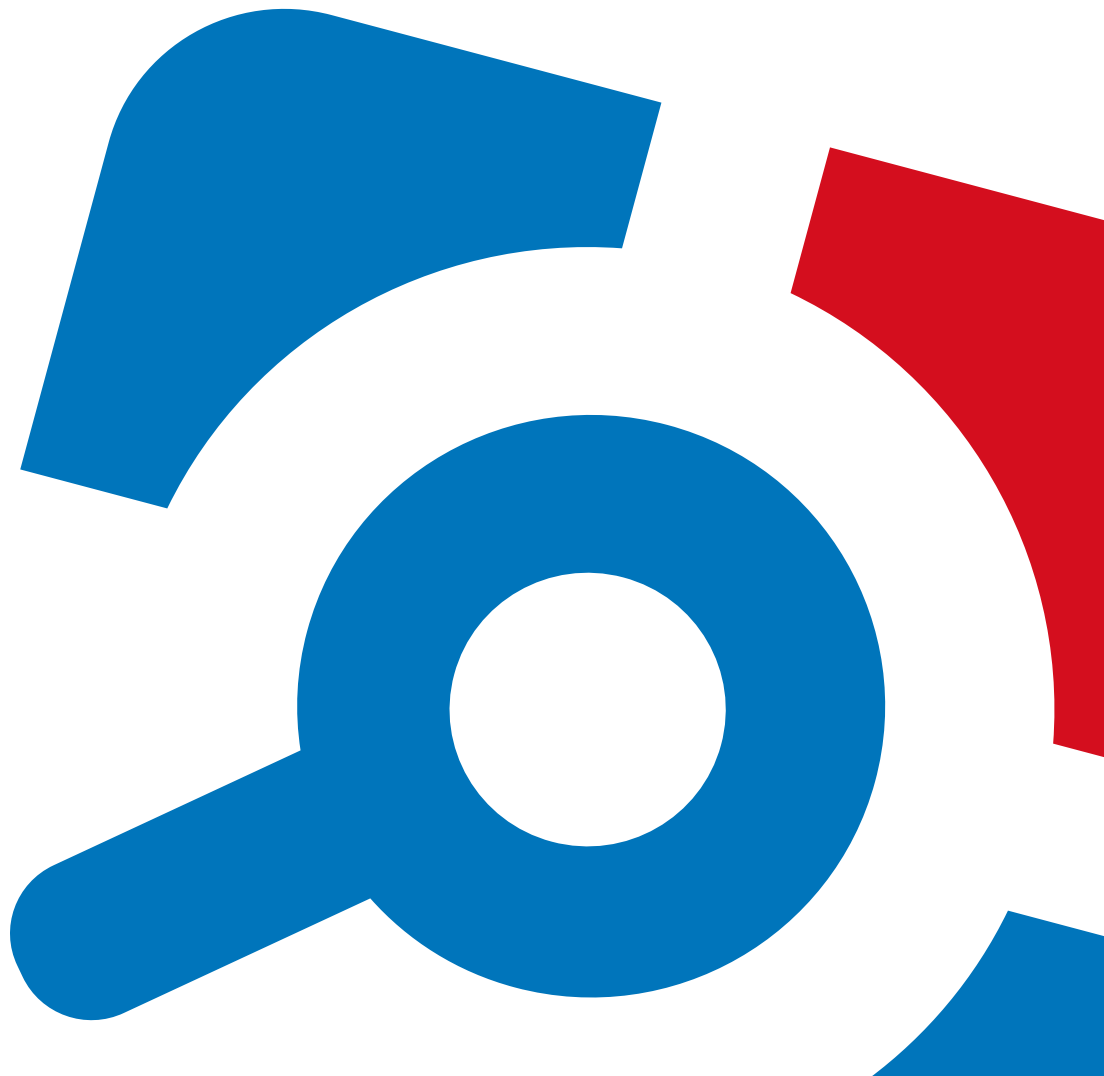


# Netwrix Auditor for Azure AD Quick-Start Guide

Version: 9.0  
4/28/2017



## **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.

© 2017 Netwrix Corporation.

All rights reserved.

# Table of Contents

1. Introduction .....	4
1.1. Netwrix Auditor Overview .....	4
2. Netwrix Auditor System Requirements .....	5
2.1. Supported Data Sources .....	5
2.2. Requirements to Install Netwrix Auditor .....	5
2.2.1. Hardware Requirements .....	5
2.2.2. Software Requirements .....	6
2.2.2.1. Additional Components .....	6
3. Review Components Checklist .....	8
3.1. Configure Data Collecting Account .....	8
4. Install the Product .....	10
5. Monitoring Plans .....	12
5.1. Create a New Plan .....	12
5.1.1. New Monitoring Plan .....	12
5.1.2. Default SQL Server Instance .....	13
5.1.3. Audit Database .....	13
5.1.4. Notifications .....	14
5.1.5. Recipients .....	14
5.1.6. Monitoring Plan Summary .....	15
5.2. Add Items for Monitoring .....	15
5.2.1. Office 365 Tenant .....	15
6. Make Test Changes .....	16
7. See How Netwrix Auditor Enables Complete Visibility .....	17
7.1. Review an Activity Summary .....	18
7.2. Browse Data with Intelligence Search .....	19
7.3. Review Azure AD Overview .....	22
7.4. Review the All Azure AD Activity by User Report .....	23
8. Related Documentation .....	25

# 1. Introduction

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

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

- [Netwrix Auditor Installation and Configuration Guide](#)
- [Netwrix Auditor Administration Guide](#)
- [Netwrix Auditor Intelligence Guide](#)

## 1.1. Netwrix Auditor Overview

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

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

Major benefits:

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

Netwrix Auditor for Azure AD detects and reports on all changes made to Azure AD configuration and permissions, including Azure AD objects, user accounts and passwords, group membership. The products also reports on successful and failed logon attempts.

## 2. Netwrix Auditor 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.

### 2.1. Supported Data Sources

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

Data source	Supported Versions
Azure AD	Azure Active Directory version provided within Microsoft Office 365

### 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

Before installing Netwrix Auditor, make sure that your hardware meets the following requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 64 bit, 2 GHz or any similar	Intel Core 2 Duo 2x or 4x 64 bit, 3 GHz or any similar, preferably a virtual machine
RAM	2 GB	8 GB  Required size highly depends on the number of changes per day and may be up to 32 GB (approximately 3 million changes per day).

Hardware Component	Minimum	Recommended
Disk space	<ul style="list-style-type: none"> <li>500 MB physical disk space for the product installation</li> <li>30 GB for the local file-based Long-Term Archive</li> <li>500 MB for the local SQL Server-based Audit Database</li> </ul> <p><b>NOTE:</b> These are rough estimations, calculated for evaluation of Netwrix Auditor for Azure AD. Refer to <a href="#">Netwrix Auditor Installation and Configuration Guide</a> for complete information on the Netwrix Auditor disk space requirements.</p>	
Screen resolution	1280 x 1024	1920 x 1080 and higher

## 2.2.2. Software Requirements

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

Component	Requirements
Operating system	<ul style="list-style-type: none"> <li>Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8.1, and Windows 10</li> <li>Windows Server OS: Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2, and Windows Server 2016</li> </ul>
.NET Framework	<ul style="list-style-type: none"> <li><a href="#">3.5 SP1</a>, <a href="#">4.0</a>, <a href="#">4.5</a>, or <a href="#">4.6</a> depending on your OS</li> </ul>
Installer	<ul style="list-style-type: none"> <li><a href="#">Windows Installer 3.1</a> and above</li> </ul>

### 2.2.2.1. Additional Components

In order to monitor some data sources, you may be required to install additional software components.

Data source	Components
<ul style="list-style-type: none"> <li>Azure AD</li> </ul>	<p>In rare cases, these components may be required for data source monitoring. Netwrix Auditor will display a data collection error with details.</p> <p><b>On the computer where Netwrix Auditor Server is installed:</b></p> <ul style="list-style-type: none"> <li>.NET Framework <a href="#">4.5</a> or <a href="#">4.6</a></li> <li><a href="#">Microsoft Online Services Sign-In Assistant</a></li> </ul>

## Data source

## Components

- [Windows Azure Active Directory Module for Windows PowerShell](#)

## 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 2014 with SSRS (optional step)	<p>Although Netwrix Auditor provides a convenient interface for downloading SQL Server 2014 Express right from Netwrix Auditor, it is recommended to deploy SQL Server instance in advance. Test your SQL Server connectivity.</p> <p><b>NOTE:</b> Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor.</p>
Test account	<p>Netwrix recommends you to create a special account with extensive privileges. This account should have sufficient permissions to:</p> <ul style="list-style-type: none"><li>• Collect audit data. See <a href="#">Configure Data Collecting Account</a> for more information.</li><li>• Access data stored in the SQL Server instance:<ul style="list-style-type: none"><li>• The account must be assigned the <b>Database owner (db_owner)</b> role and the <b>dbcreator</b> server role.</li><li>• The account must be assigned the <b>Content Manager</b> role on the SSRS Home folder.</li></ul></li><li>• Make test changes in your environment.</li></ul>

### 3.1. Configure Data Collecting Account

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

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



## Data source

## Rights and permissions

Azure AD

*In the Cloud:*

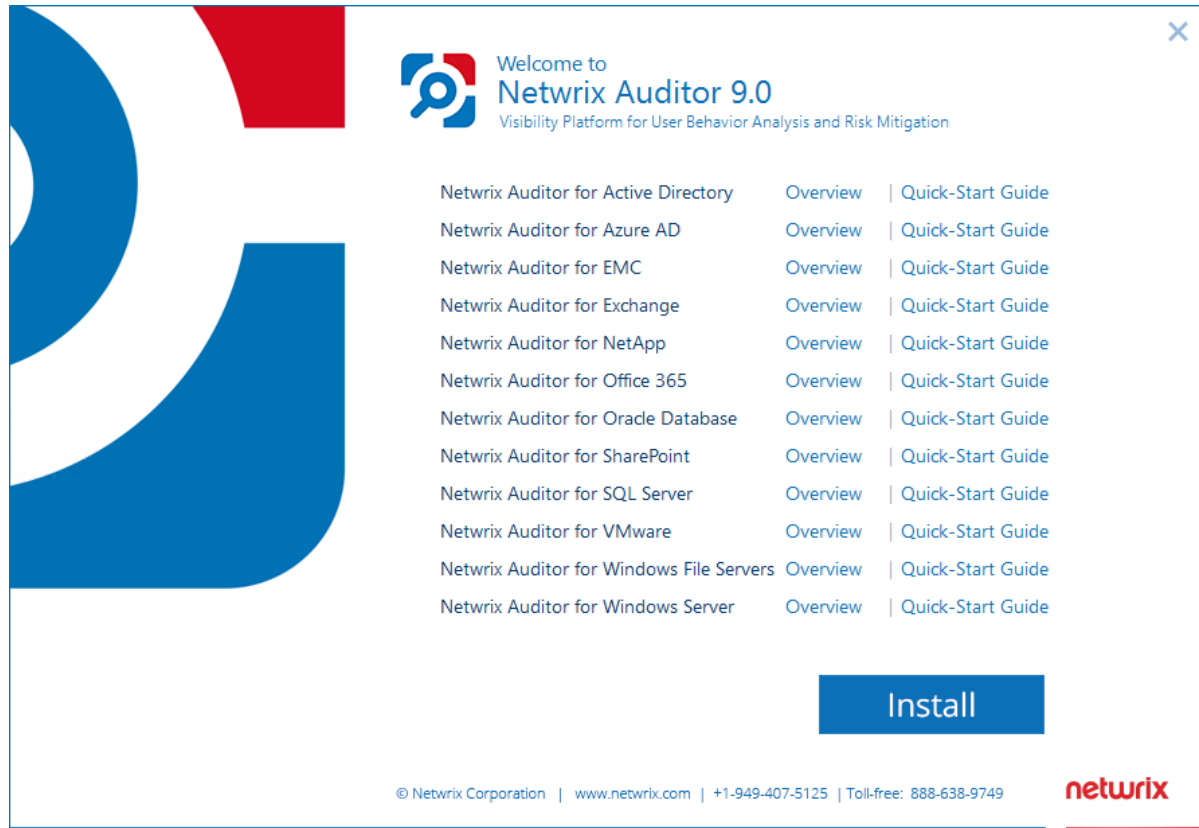
- The account must be assigned the **Global Administrator** role in Azure AD (**Company Administrator** in Azure AD PowerShell terms)—only required when first configuring a monitoring plan for auditing Azure AD domain. Later, any regular account can be used to collect audit data.

**NOTE:** Accounts with multi-factor authentication are not supported.

## 4. Install the Product

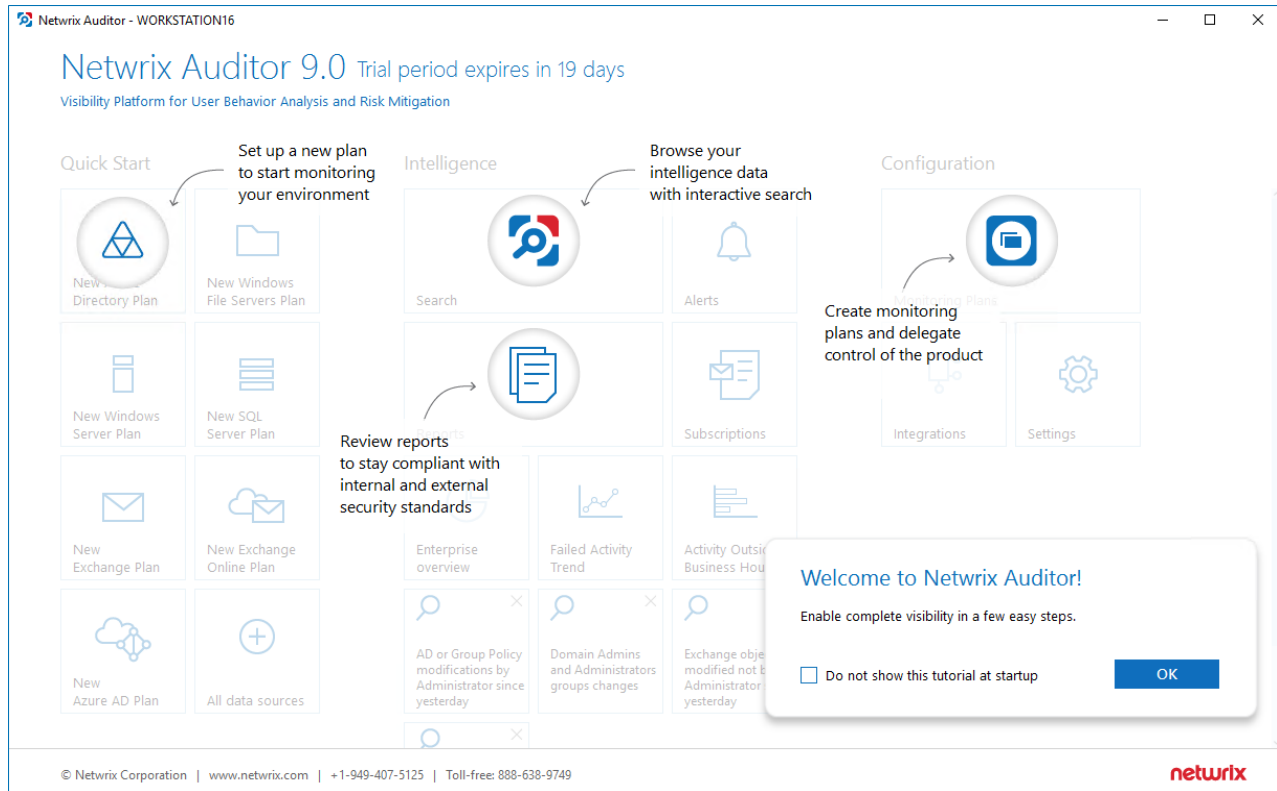
### To install Netwrix Auditor

1. Download Netwrix Auditor 9.0 on [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. 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 Azure AD, 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 Azure AD Plan** tile in the **Quick Start** section.

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

- 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. New Monitoring Plan

Option	Description
Specify the account for collecting data	<p>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.</p> <p>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 <a href="#">Netwrix Auditor Installation and Configuration Guide</a>. Netwrix recommends creating a special service account with extended permissions.</p>

## 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: <ul style="list-style-type: none"><li>• Windows authentication</li><li>• SQL Server authentication</li></ul>
User name	Specify the account to be used to connect to the SQL Server instance.  <b>NOTE:</b> This account must be granted the <b>database owner (db_owner)</b> role and the <b>dbcreator</b> server role. See <a href="#">Netwrix Auditor Installation and Configuration Guide</a> 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

Specify the email settings that will be used for activity summaries, reports and alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Option	Description
SMTP server	Enter your SMTP server address. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port number	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the <b>From</b> field.  <b>NOTE:</b> It is recommended to click <b>Send Test Email</b> . 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 the users 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. Office 365 Tenant

Complete the following fields:

Option	Description
Specify Office 365 Account	Specify email address and password of your Microsoft account that will be used to connect to Office 365.

Now your Office 365 monitoring plan is almost ready. You only need to add the **SharePoint Online** data source with the same Office 365 tenant item. Do the following:

1. On your **Office 365 monitoring plan** page, navigate to **Data source** → **Add data source** in the right pane and select the **SharePoint Online** tile.
2. For evaluation purposes, leave the data source settings unchanged. Click **Add** to add the data source.
3. Now you are again on the main page of your monitoring plan. Click **Add item** under **SharePoint Online**.
4. You will be prompted to select the **Office 365 tenant** item. Specify the same Microsoft account credentials as you provided for Exchange Online.

## 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:

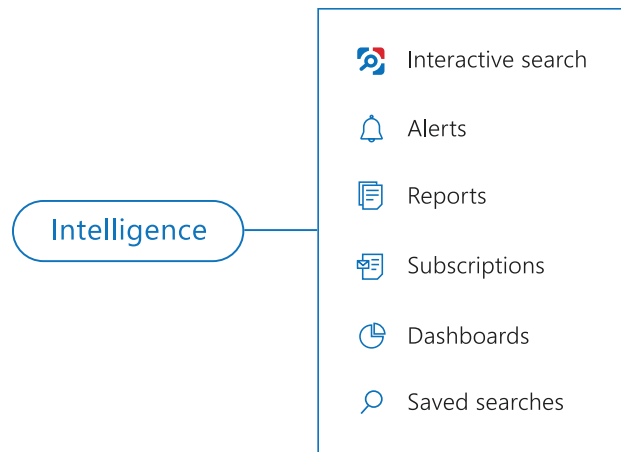
- Create a new user using **Azure AD**
- Assign the Azure Active Directory Premium license plan to this user account

**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](#)
- [Browse Data with Intelligence Search](#)
- [Review Azure AD Overview](#)
- [Review the All Azure AD Activity by User Report](#)

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

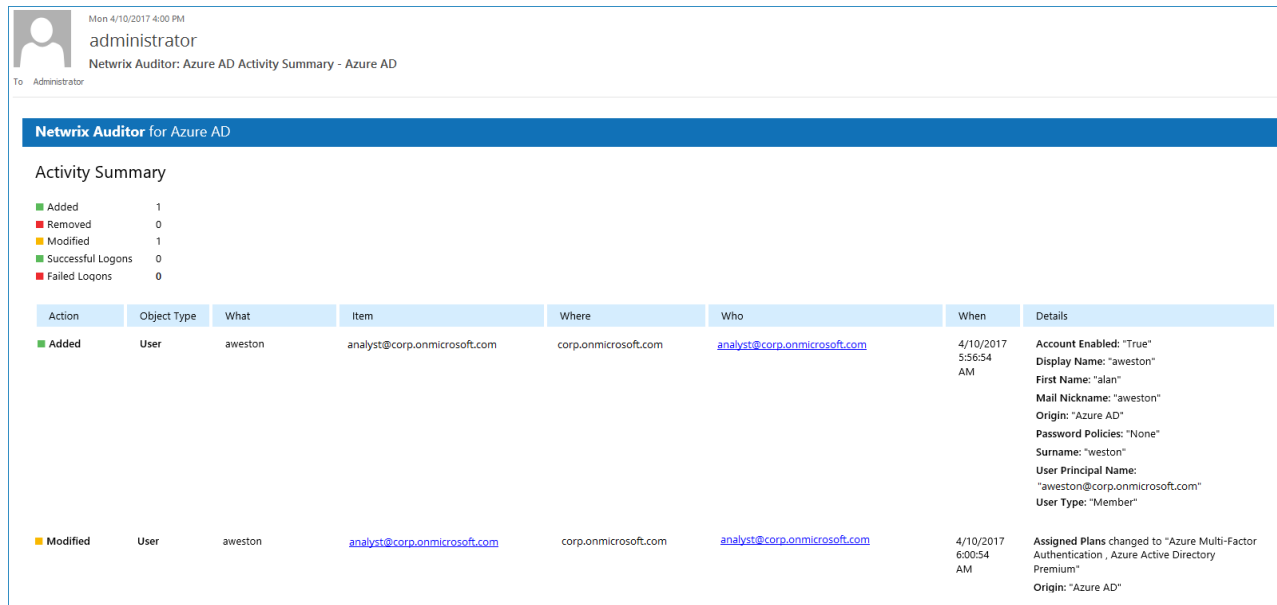
### *To launch data collection manually*

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

An Activity Summary is email that 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 an 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:



Action	Object Type	What	Item	Where	Who	When	Details
Added	User	aweston	analyst@corp.onmicrosoft.com	corp.onmicrosoft.com	analyst@corp.onmicrosoft.com	4/10/2017 5:56:54 AM	Account Enabled: "True" Display Name: "aweston" First Name: "alan" Mail Nickname: "aweston" Origin: "Azure AD" Password Policies: "None" Surname: "weston" User Principal Name: "aweston@corp.onmicrosoft.com" User Type: "Member"
Modified	User	aweston	analyst@corp.onmicrosoft.com	corp.onmicrosoft.com	analyst@corp.onmicrosoft.com	4/10/2017 6:00:54 AM	Assigned Plans changed to "Azure Multi-Factor Authentication , Azure Active Directory Premium" Origin: "Azure AD"

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 Microsoft cloud 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. 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:

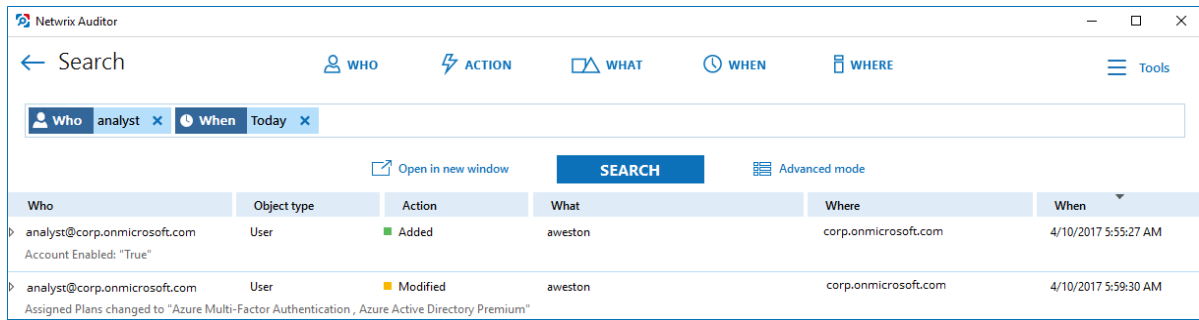
Filter	Value
 <b>WHO</b>	Specify your Office 365 account name, as you performed test changes.
 <b>WHEN</b>	Specify a timeframe.

**NOTE:** Refer to [Netwrix Auditor Intelligence Guide](#) for detailed instructions on how to apply filters and change match types.

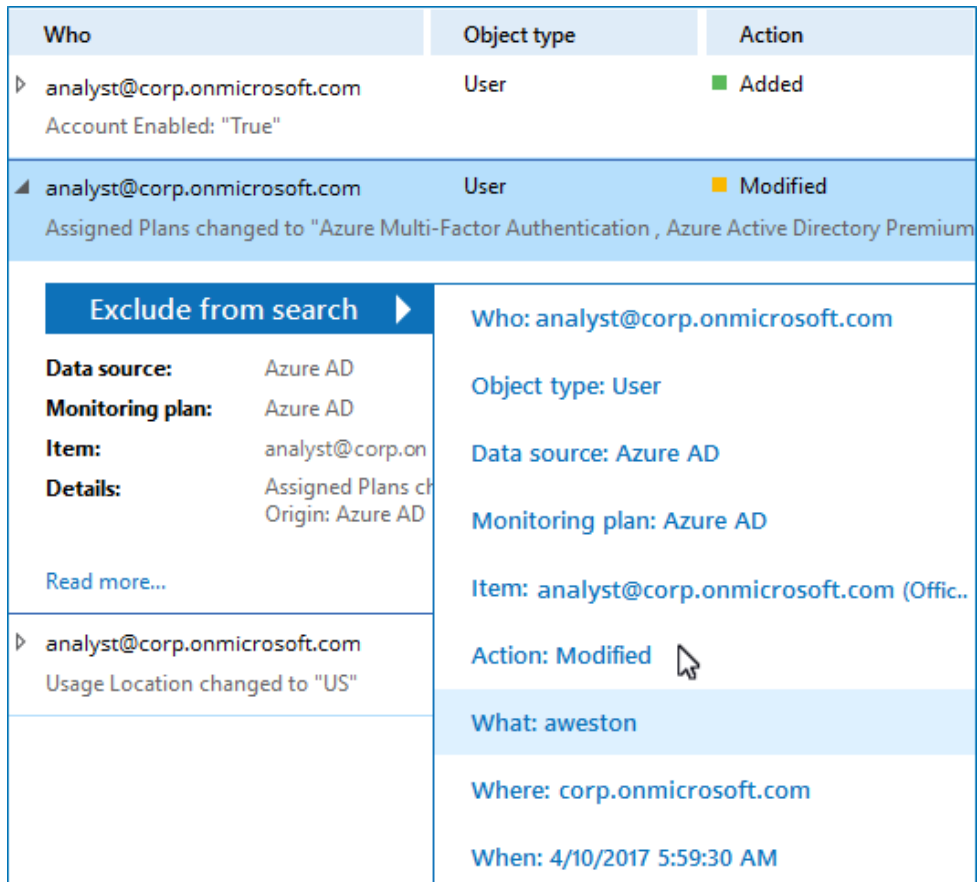
As a result, you will see the following filters in the **Search** field:



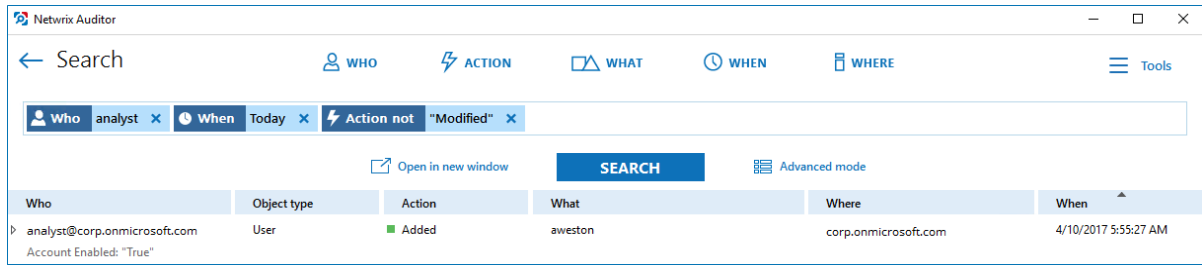
### 3. Click Search.



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

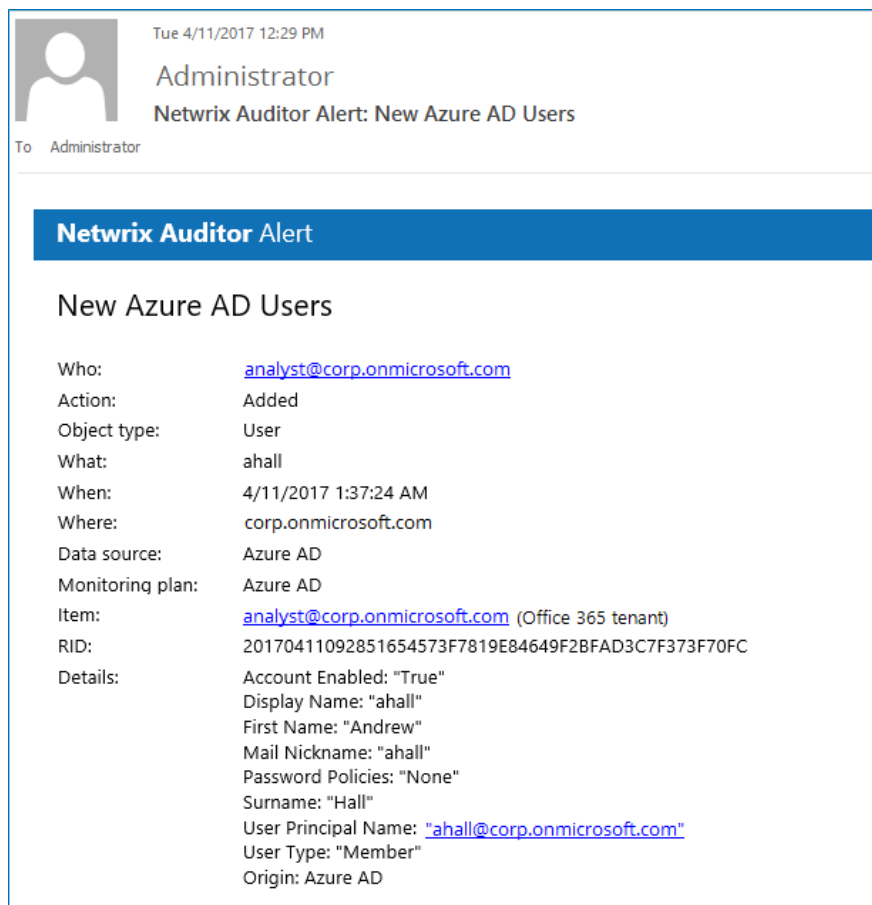


Your **Search** field will be updated, the **Action not** filter will be added. Make sure to click **Search** again to update your search results.



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

- Click **Copy Search** to copy the search filters that are currently applied to your search.
- Click **Paste Search** to paste the search filters you copied before. These can be filters copied from a previous search.
- Click **Save search** to save the selected set of filters. This search will be added to the **Intelligence** section on the main Netwrix Auditor page, so that you will be able to access it instantly. Refer to [Netwrix Auditor Intelligence Guide](#) for detailed instructions on how to create saved searches.
- Click **Create alert** to get instant email or SMS notifications on suspicious activity that matches your current search criteria. You only need to specify a name for a new alert, add recipient and enable threshold where applicable. The selected set of search criteria will be associated with the new alert automatically. Refer to [Netwrix Auditor Administration Guide](#) for detailed instructions on how to create and configure alerts.



- Click **Export data** to save your search results as a \*.pdf or \*.csv file.

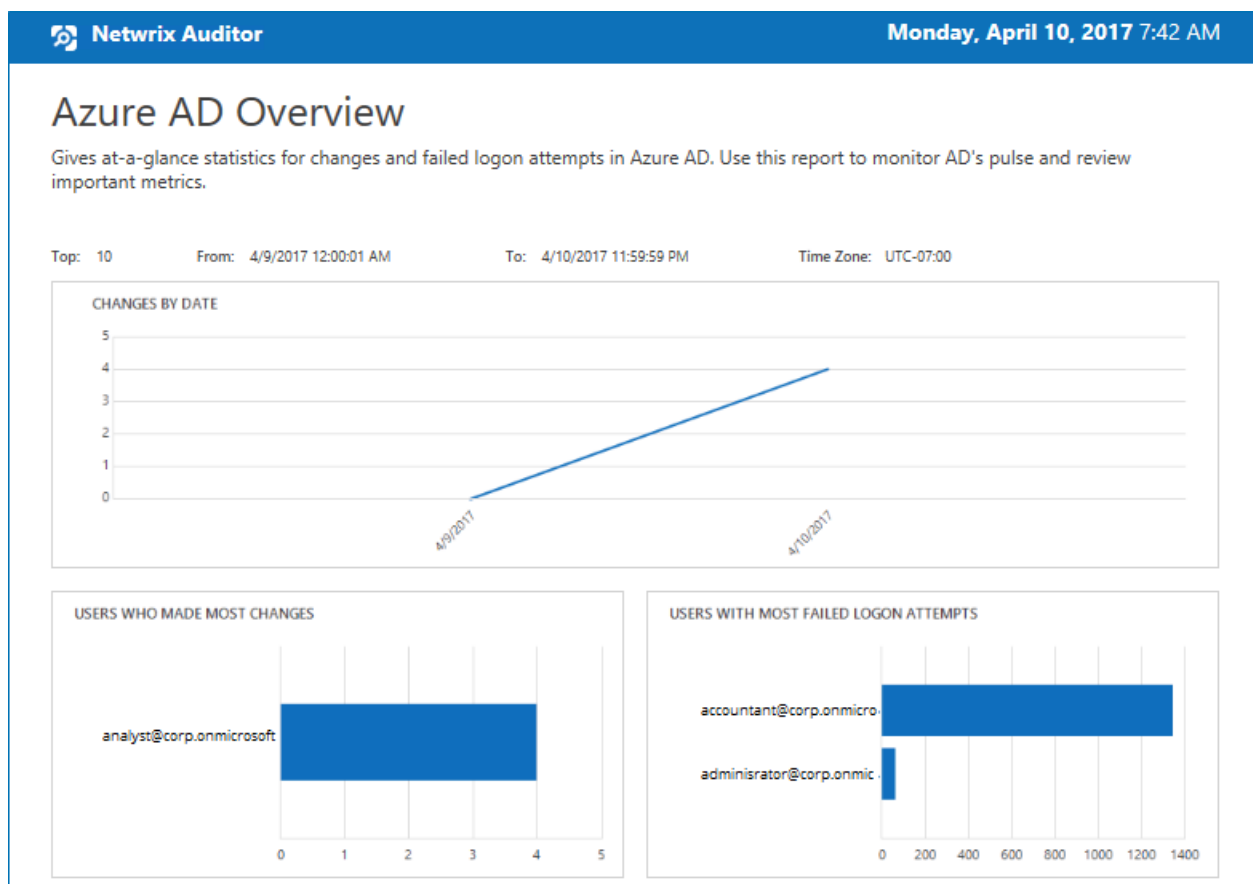
## 7.3. Review Azure AD Overview

**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 **Azure AD Overview**.

### *To see how your changes are reported with Azure AD Overview*

1. On the main Netwrix Auditor page, navigate to the **Intelligence** section and click the **Reports** tile.
2. Expand the **Azure AD** reports.
3. Select the **Azure AD 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.



## 7.4. Review the All Azure AD Activity by User 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** → **Azure AD** 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** → **Azure AD**.
2. Select the **All Azure AD Activity by User** report.
3. Click **View** to open the report.

## All Azure AD Activity by User

Shows all changes made to Azure AD objects (creation, modification, and deletion), as well as successful and failed logon attempts, grouped by user. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

Filter

Value

**Who: analyst@corp.onmicrosoft.com**

Action	Object Type	What	When
■ Added	User	aweston	4/10/2017 5:55:27 AM
Where: corp.onmicrosoft.com			
Origin: Azure AD			
Account Enabled: "True"			
Display Name: "aweston"			
First Name: "alan"			
Mail Nickname: "aweston"			
Password Policies: "None"			
Surname: "weston"			
User Principal Name: "aweston@corp.onmicrosoft.com"			
User Type: "Member"			
Origin: Azure AD			
■ Modified	User	aweston	4/10/2017 5:59:30 AM
Where: corp.onmicrosoft.com			
Origin: Azure AD			
Assigned Plans changed to "Azure Multi-Factor Authentication , Azure Active Directory Premium"			
Origin: Azure AD			



## 8. Related Documentation

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

Document	Description
<a href="#">Netwrix Auditor Installation and Configuration Guide</a>	Provides detailed instructions on how to install Netwrix Auditor, and explains how to configure your environment for auditing.
<a href="#">Netwrix Auditor Administration Guide</a>	Provides step-by-step instructions on how to configure and use the product.
<a href="#">Netwrix Auditor Intelligence Guide</a>	Provides detailed instructions on how to enable complete visibility with Netwrix Auditor interactive search, report, and alert functionality.
<a href="#">Netwrix Auditor Integration API Guide</a>	Provides step-by-step instructions on how to leverage Netwrix Auditor audit data with on-premises and cloud auditing solutions using RESTful API.
<a href="#">Netwrix Auditor Release Notes</a>	Lists the known issues that customers may experience with Netwrix Auditor 9.0, and suggests workarounds for these issues.