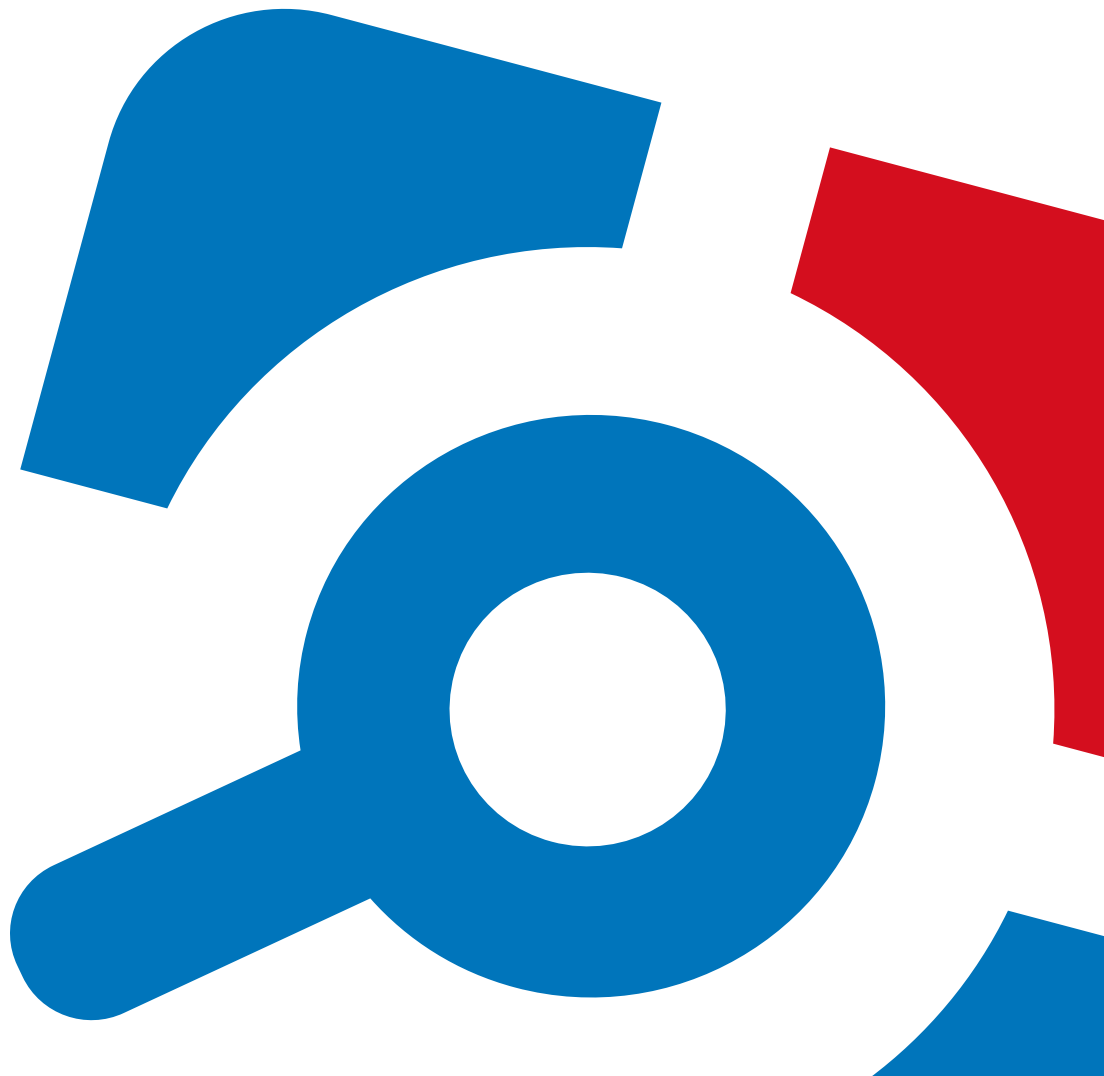


Netwrix Auditor for Azure AD Quick-Start Guide

Version: 8.5
10/17/2016



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.

© 2016 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 Audited Systems	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	7
3.1. Configure Data Processing Account Rights and Permissions	7
4. Install the Product	9
5. Create Managed Object to Audit Azure AD	11
6. Make Test Changes	15
7. See How Netwrix Auditor Enables Complete Visibility	16
7.1. Review a Change Summary	17
7.2. Browse Data with AuditIntelligence Search	18
7.3. Review Azure AD Overview	20
7.4. Review the All Azure AD Activity by User Report	21
8. Related Documentation	24

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 Managed Object 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 Administrator's Guide](#)
- [Netwrix Auditor User 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 Audited Systems

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

Audited System	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 32 bit, 2 GHz	Intel Core 2 Duo 2x 64 bit, 3 GHz Preferably a virtual machine
RAM	2 GB	8 GB
Disk space	<ul style="list-style-type: none">• 500 MB physical disk space for the product installation• 30 GB for the file-based Long-Term Archive• 500 MB for the SQL Server-based Audit Database where audit data is going	

Hardware Component	Minimum	Recommended
	to be stored	
	<p>NOTE: These are rough estimations, calculated for evaluation of Netwrix Auditor for Azure AD. Refer to Netwrix Auditor Installation and Configuration Guide 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 minimum software requirements for the Netwrix Auditor installation:

Component	Requirements
Operating system	<ul style="list-style-type: none"> Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8.1 Windows Server OS (64-bit): Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2
Framework	<ul style="list-style-type: none"> .Net Framework 3.5 SP1
Installer	<ul style="list-style-type: none"> Windows Installer 3.1 and above

2.2.2.1. Additional Components

Some audited systems may require you to install additional software components.

Audited system	Components
<ul style="list-style-type: none"> Azure AD 	<ul style="list-style-type: none"> .Net Framework 4.5 Microsoft Online Services Sign-In Assistant Windows Azure Active Directory Module for Windows PowerShell

These components may be required for auditing. If needed, Netwrix Auditor can install them automatically during the Managed Object creation.

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 Administrator Console, it is recommended to deploy SQL Server instance in advance. Test your SQL Server connectivity.</p> <p>NOTE: Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor Administrator Console.</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">• Collect audit data. See Configure Data Processing Account Rights and Permissions for more information.• Access data stored in the SQL Server instance:<ul style="list-style-type: none">• The account must be assigned the Database owner (db_owner) role and the dbcreator server role.• The account must be assigned the Content Manager role on the SSRS Home folder.• Make test changes in your environment.

3.1. Configure Data Processing Account Rights and Permissions

The Data Processing Account is used to collect audit data from the target systems. To ensure successful data collection, the Data Processing Account must comply with the following requirements depending on the audited system.

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.

Audited system	Rights and permissions
----------------	------------------------

Azure AD	
----------	--

In the Cloud:

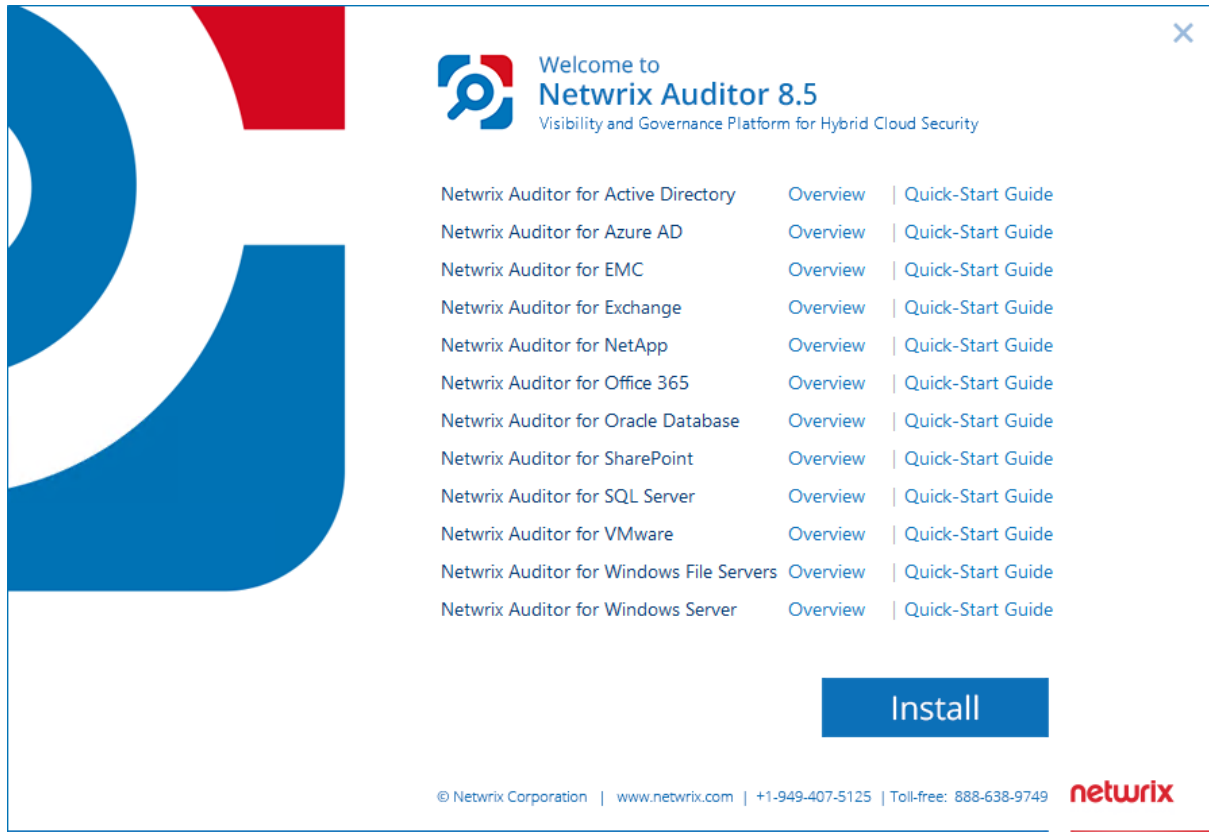
- The account must be assigned the **Global Administrator** role in Azure AD (**Company Administrator** in Azure AD PowerShell terms)—only required when first configuring a Managed Object for auditing Azure AD domain. Later, any regular account can be used to collect audit data.

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

4. Install the Product

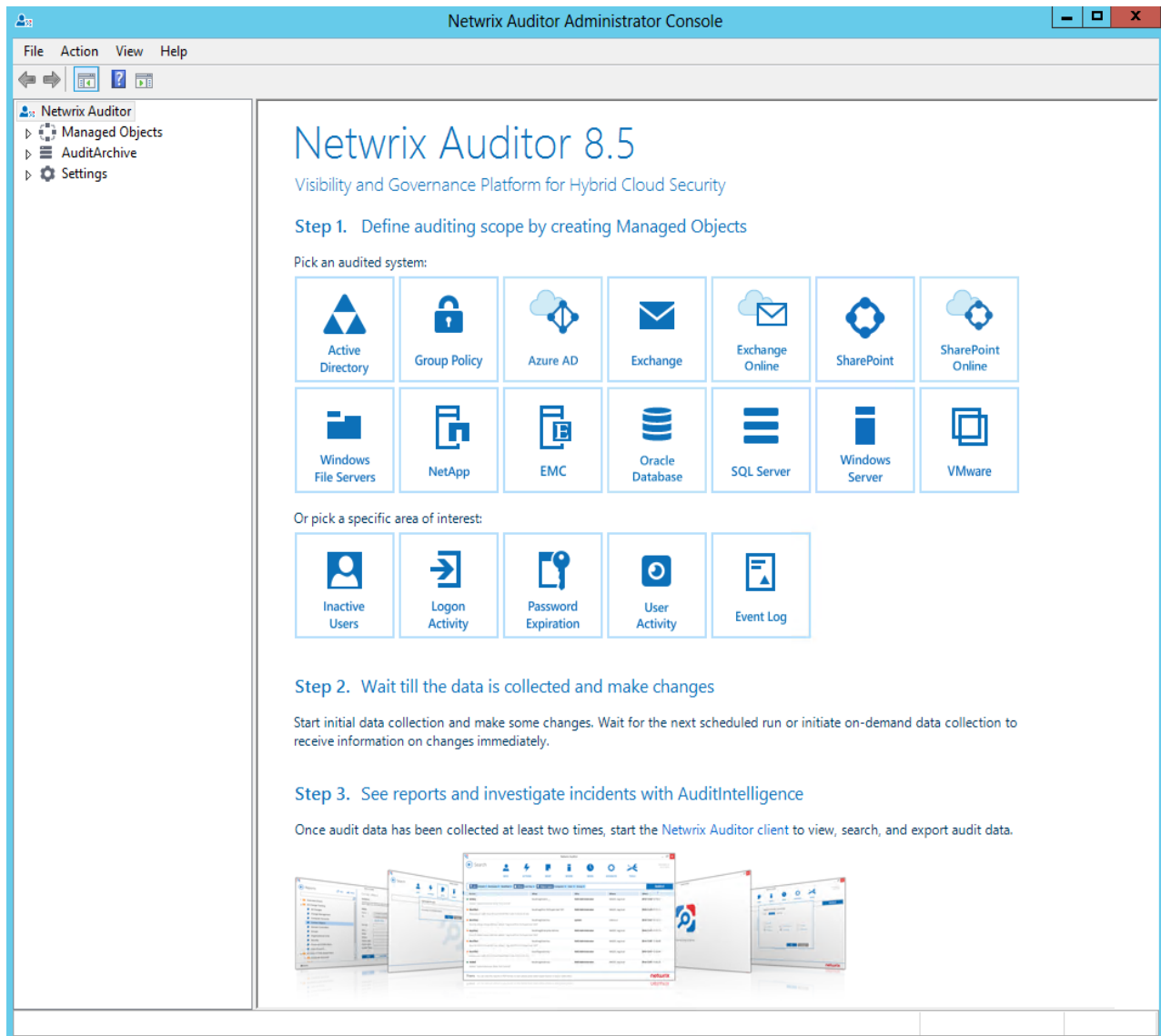
To install Netwrix Auditor

1. Download Netwrix Auditor 8.5 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 shortcuts will be added to the **Start** menu/screen and Netwrix Auditor Administrator Console will open.



5. Create Managed Object to Audit Azure AD

To start auditing your IT Infrastructure with Netwrix Auditor, you must create a Managed Object. A Managed Object is a container within Netwrix Auditor that stores information on the auditing scope, the Data Processing Account used for data collection, Audit Database settings, etc.

To create a Managed Object to audit Azure AD

1. On the main Netwrix Auditor Administrator Console page, click the **Azure AD** tile to launch the **New Managed Object** wizard.
2. On the **Select Managed Object Type** step, select **Office 365** as a Managed Object type.
3. On the **Specify Default Data Processing Account** step, click **Specify Account**.

Enter the default Data Processing Account that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to [Netwrix Auditor Installation and Configuration Guide](#).

4. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time 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 name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the From field. NOTE: It is recommended to click Verify . The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP Authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.

Option	Description
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

- On the **Specify Office 365 Account** step, specify email address and password of a Microsoft account that will be used to connect to Office 365.

NOTE: When first configuring a Managed Object, Netwrix Auditor creates an application in your Azure AD domain with the account you specified. Therefore, this account must be granted the **Global Administrator** role. Later on, you can use another—less powerful account—to collect audit data. See [Configure Data Processing Account Rights and Permissions](#) for more information.

- On the **Check Prerequisites** step, Netwrix Auditor will automatically look up additional system components and prompt you to install those that are missing. In case all required components have been already installed, this step will be omitted. See [Netwrix Auditor Installation and Configuration Guide](#) for more information on software requirements.
- On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

Select one of the following:

- **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.
- **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

Complete the following fields:

Option	Description
SQL Server Settings	

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"> Windows authentication SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. <p>NOTE: This account must be granted the database owner (db_owner) role and the dbcreator server role. See Netwrix Auditor Installation and Configuration Guide for more information.</p>
Password	Enter a password.
SQL Server Reporting Services Settings	
Report Server URL	Specify the Report Server URL. Make sure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Make sure that the resource is reachable.
User name	Specify the account to be used to connect to SSRS.
Password	Enter a password.

8. On the **Configure Azure AD Auditing Scope** step, define the auditing scope. Review the following for additional information:

Option	Description
Audit Azure AD changes	Always enabled. Includes changes to domain objects, permissions, users and groups, etc.
Audit Azure AD logons	Netwrix Auditor allows specifying what types of logon events you want to audit: successful logons, failed logons.

9. On the **Specify Azure AD Change Summary Recipients** step, enter your email.

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

10. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

When a new Managed Object is created, Netwrix Auditor starts collecting data from the audited IT infrastructure. The first data collection runs automatically and gathers information on the audited system's current configuration state. Netwrix Auditor uses this information as a benchmark to collect data on changes. After the first data collection has finished, an email notification is sent to your email stating that the analysis has completed.

NOTE: Due to Office 365 Management Activity API limitations, audit data collected during the first 12 hours since the Managed Object creation may contain "system" values. "System" values will be replaced with data once events appear in Office 365 blobs. For more information, refer to [Microsoft article](#).

6. Make Test Changes

Now that the product has collected a snapshot of the audited system'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

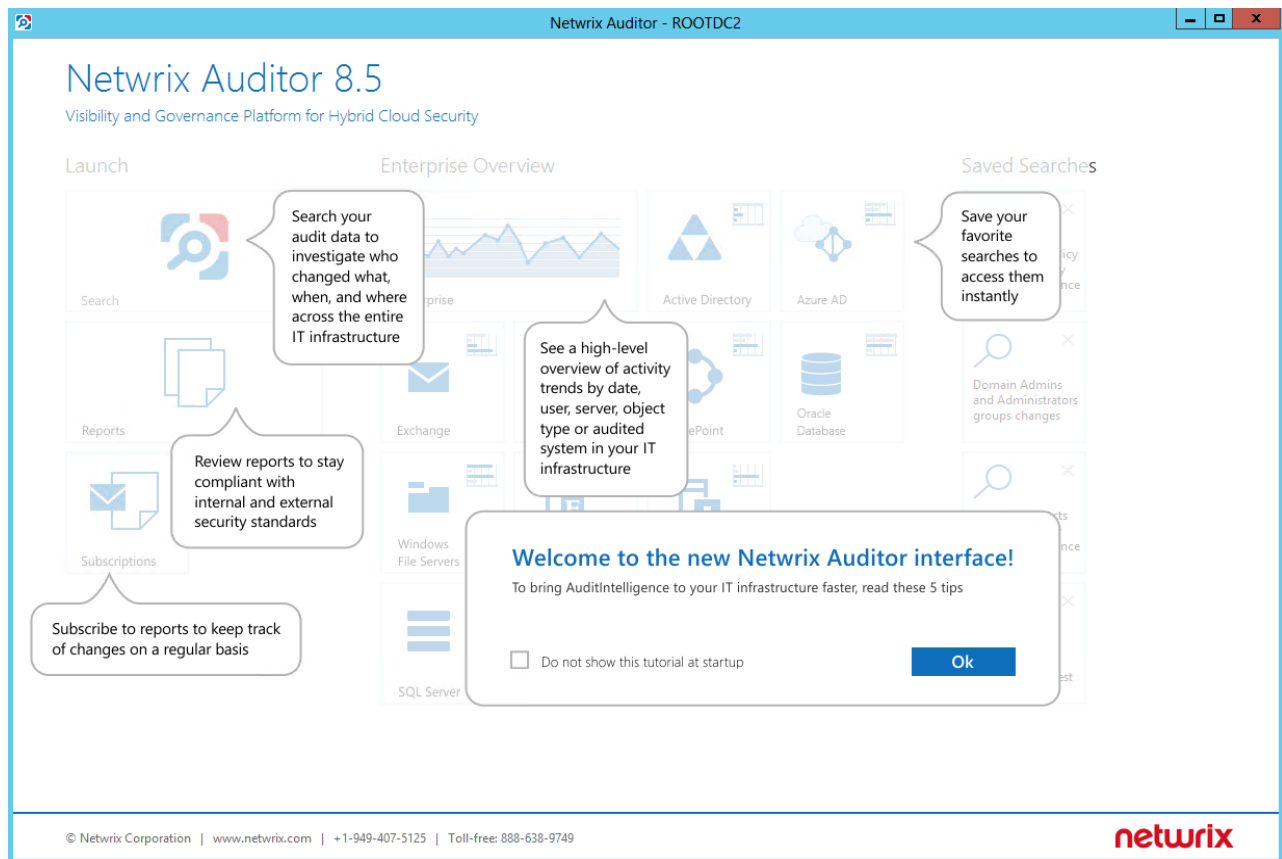
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

7. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to the audited environment, you can see how Netwrix Auditor brings AuditIntelligence into your IT infrastructure and enables its complete visibility. This section explains how to review your test changes in the Netwrix Auditor client and Change Summary.

To launch the Netwrix Auditor client

- Navigate to Start → Netwrix Auditor.



Review the following for additional information:

- [Review a Change Summary](#)
- [Browse Data with AuditIntelligence Search](#)
- [Review Azure AD Overview](#)
- [Review the All Azure AD Activity by User Report](#)

In order not to wait for a scheduled data collection and a Change Summary generation, launch data collection manually.

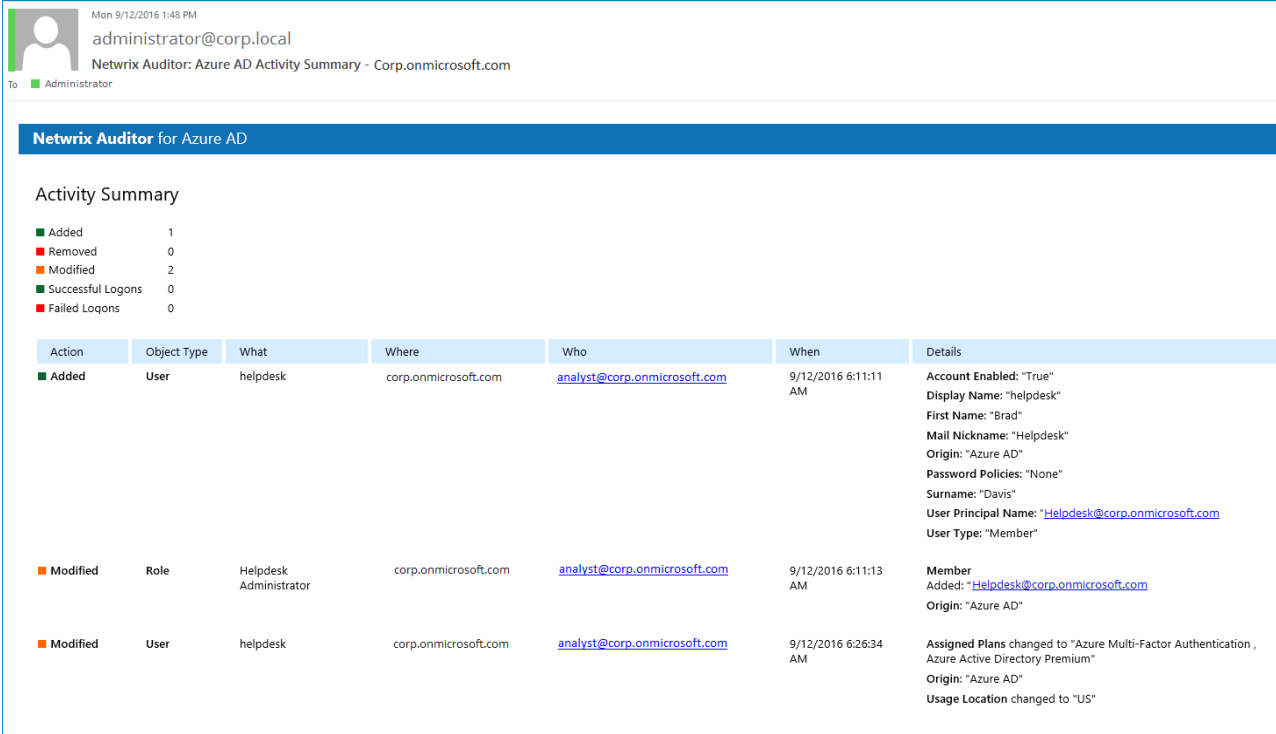
To launch data collection manually

1. In the Netrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name**.
2. In the right pane, click **Run**.
3. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

7.1. Review a Change Summary

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

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



The screenshot shows an email notification from Netrix Auditor for Azure AD. The email header includes the date and time (Mon 9/12/2016 1:48 PM), the sender (administrator@corp.local), and the subject (Netrix Auditor: Azure AD Activity Summary - Corp.onmicrosoft.com). The email body features a blue header bar with the text 'Netrix Auditor for Azure AD'. Below this, the title 'Activity Summary' is followed by a summary of changes: 1 Added, 0 Removed, 2 Modified, 0 Successful Logons, and 0 Failed Logons. A table lists the specific changes, with columns for Action, Object Type, What, Where, Who, When, and Details. The table contains three rows: an 'Added' user named 'helpdesk', a 'Modified' role named 'Helpdesk Administrator', and a 'Modified' user named 'helpdesk'.

Action	Object Type	What	Where	Who	When	Details
Added	User	helpdesk	corp.onmicrosoft.com	analyst@corp.onmicrosoft.com	9/12/2016 6:11:11 AM	Account Enabled: "True" Display Name: "helpdesk" First Name: "Brad" Mail Nickname: "Helpdesk" Origin: "Azure AD" Password Policies: "None" Surname: "Davis" User Principal Name: " Helpdesk@corp.onmicrosoft.com " User Type: "Member"
Modified	Role	Helpdesk Administrator	corp.onmicrosoft.com	analyst@corp.onmicrosoft.com	9/12/2016 6:11:13 AM	Member Added: " Helpdesk@corp.onmicrosoft.com " Origin: "Azure AD"
Modified	User	helpdesk	corp.onmicrosoft.com	analyst@corp.onmicrosoft.com	9/12/2016 6:26:34 AM	Assigned Plans changed to "Azure Multi-Factor Authentication , Azure Active Directory Premium" Origin: "Azure AD" Usage Location changed to "US"

The example Change 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.
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 AuditIntelligence Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient AuditIntelligence search interface enables you to investigate incidents and browse audit data collected across the entire IT infrastructure. When running a search in Netwrix Auditor, you are not limited to a certain audited system, 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 AuditIntelligence search.



To browse your audit data and see you test changes

1. On the main Netwrix Auditor page, navigate to **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:

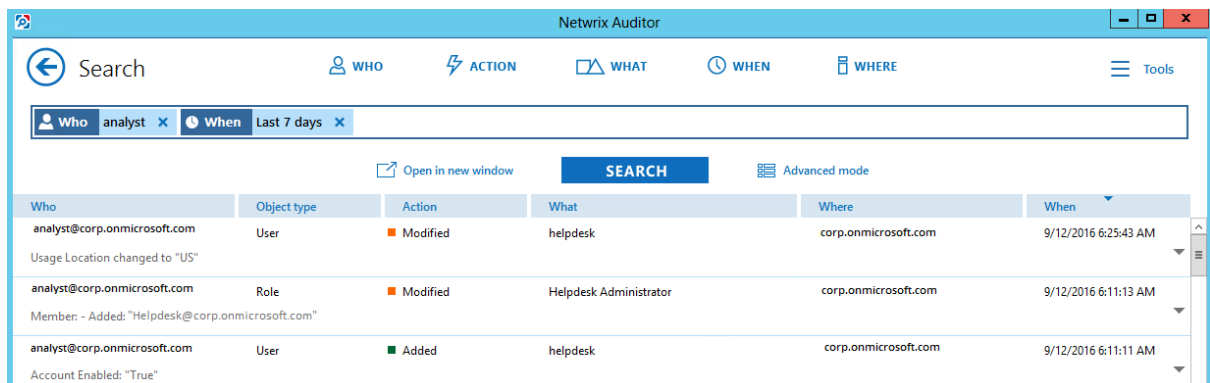
Filter	Value
 WHO	Specify your Office 365 account name, as you performed test changes.
 WHEN	Specify a timeframe.

NOTE: Refer to [Netrix Auditor User 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:

 **Who** analyst x
  **When** Last 7 days x

3. Click **Search**.



The screenshot shows the Netrix Auditor interface with the search results pane open. The search filters are 'Who: analyst' and 'When: Last 7 days'. The search results table is as follows:

Who	Object type	Action	What	Where	When
analyst@corp.onmicrosoft.com	User	Modified	helpdesk	corp.onmicrosoft.com	9/12/2016 6:25:43 AM
Usage Location changed to "US"					
analyst@corp.onmicrosoft.com	Role	Modified	Helpdesk Administrator	corp.onmicrosoft.com	9/12/2016 6:11:13 AM
Member: - Added: "Helpdesk@corp.onmicrosoft.com"					
analyst@corp.onmicrosoft.com	User	Added	helpdesk	corp.onmicrosoft.com	9/12/2016 6:11:11 AM
Account Enabled: "True"					

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.

Who	Object type	Action
analyst@corp.onmicrosoft.com	User	Modified
Usage Location changed to "US"		

Exclude from search

Audited system: Azure AD

Managed object: Corp.onmicroso

Details: Usage Location cl
Origin: Azure AD

[Read more...](#)

Who: analyst@corp.onmicrosoft.com

Object type: User

Audited system: Azure AD

Managed object: Corp.onmicrosoft.com

Action: Modified

What: helpdesk

Where: corp.onmicrosoft.com

When: 9/12/2016 6:25:43 AM

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

The screenshot shows the Netrix Auditor search interface. At the top, there are tabs for WHO, ACTION, WHAT, WHEN, and WHERE. Below these, there is a search bar with filters: Who (analyst), When (Last 7 days), Action not (Modified). A blue SEARCH button is visible. Below the search bar, there is a table with columns: Who, Object type, Action, What, Where, and When. The table contains one row with the following data: Who: Analyst@corp.onmicrosoft.com, Object type: User, Action: Added, What: helpdesk, Where: corp.onmicrosoft.com, When: 9/12/2016 6:11:11 AM. Below the table, there is a note: Account Enabled: "True".

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

- Click **Export data** to save your search results as a *.pdf or *.csv file.
- Click **Save search** to save the selected set of filters. This search will be added to the **Saved Searches** section on the main Netrix Auditor page, so that you will be able to access it instantly. Refer to [Netrix Auditor User Guide](#) for detailed instructions on how to create saved searches.

7.3. Review Azure AD Overview

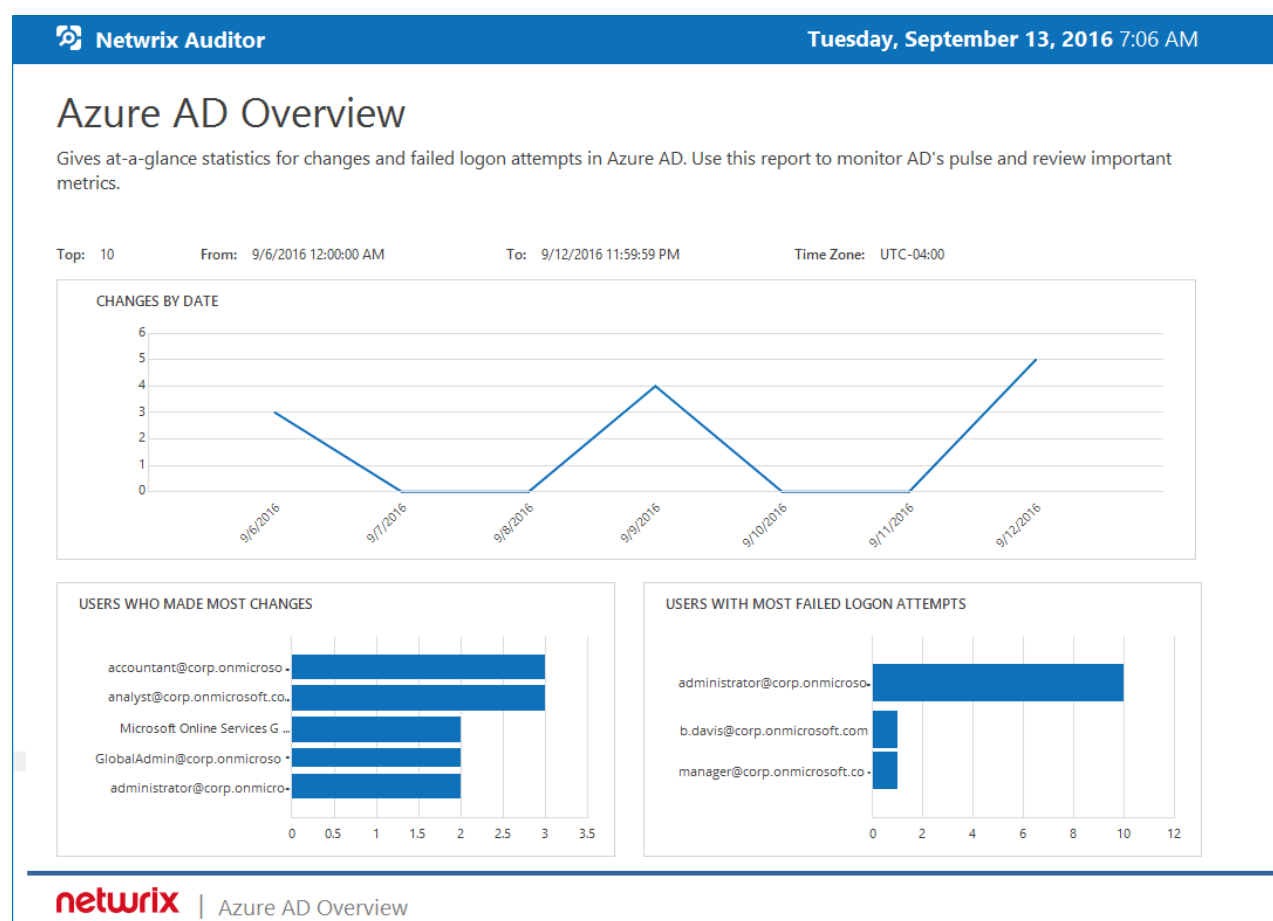
Enterprise Overview provides a high-level overview of activity trends by date, user, server, object type or audited system in your IT infrastructure. The **Enterprise** diagram aggregates data on all Managed Objects

and all audited systems, while system-specific diagrams provide quick access to important statistics within one audited system.

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 **Enterprise Overview** section.
2. Click the **Azure AD** tile to open it.
3. Review your changes.
4. 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

Netwrix Auditor allows generating audit reports based on Microsoft SQL Server Reporting Services (SSRS). The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure, an individual system, or a Managed Object.

Change 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. In the Netwrix Auditor client, 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	helpdesk	9/12/2016 6:11:11 AM
Where: Corp.onmicrosoft.com Account Enabled: "True" DisplayName: "helpdesk" First Name: "Brad" Mail Nickname: "Helpdesk" Password Policies: "None" Surname: "Davis" User Principal Name: "Helpdesk@corp.onmicrosoft.com" User Type: "Member" Origin: Azure AD			
■ Modified	Role	Helpdesk Administrator	9/12/2016 6:11:13 AM
Where: Corp.onmicrosoft.com Member: <ul style="list-style-type: none"> Added: "Helpdesk@corp.onmicrosoft.com" Origin: Azure AD			
■ Modified	User	helpdesk	9/12/2016 6:25:43 AM
Where: Corp.onmicrosoft.com Usage Location changed to "US" Origin: Azure AD			

8. Related Documentation

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

Document	Description
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 Administrator's Guide	Provides step-by-step instructions on how to configure and use the product.
Netwrix Auditor User Guide	Provides detailed instructions on how to enable complete visibility with AuditIntelligence.
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 8.5, and suggests workarounds for these issues.