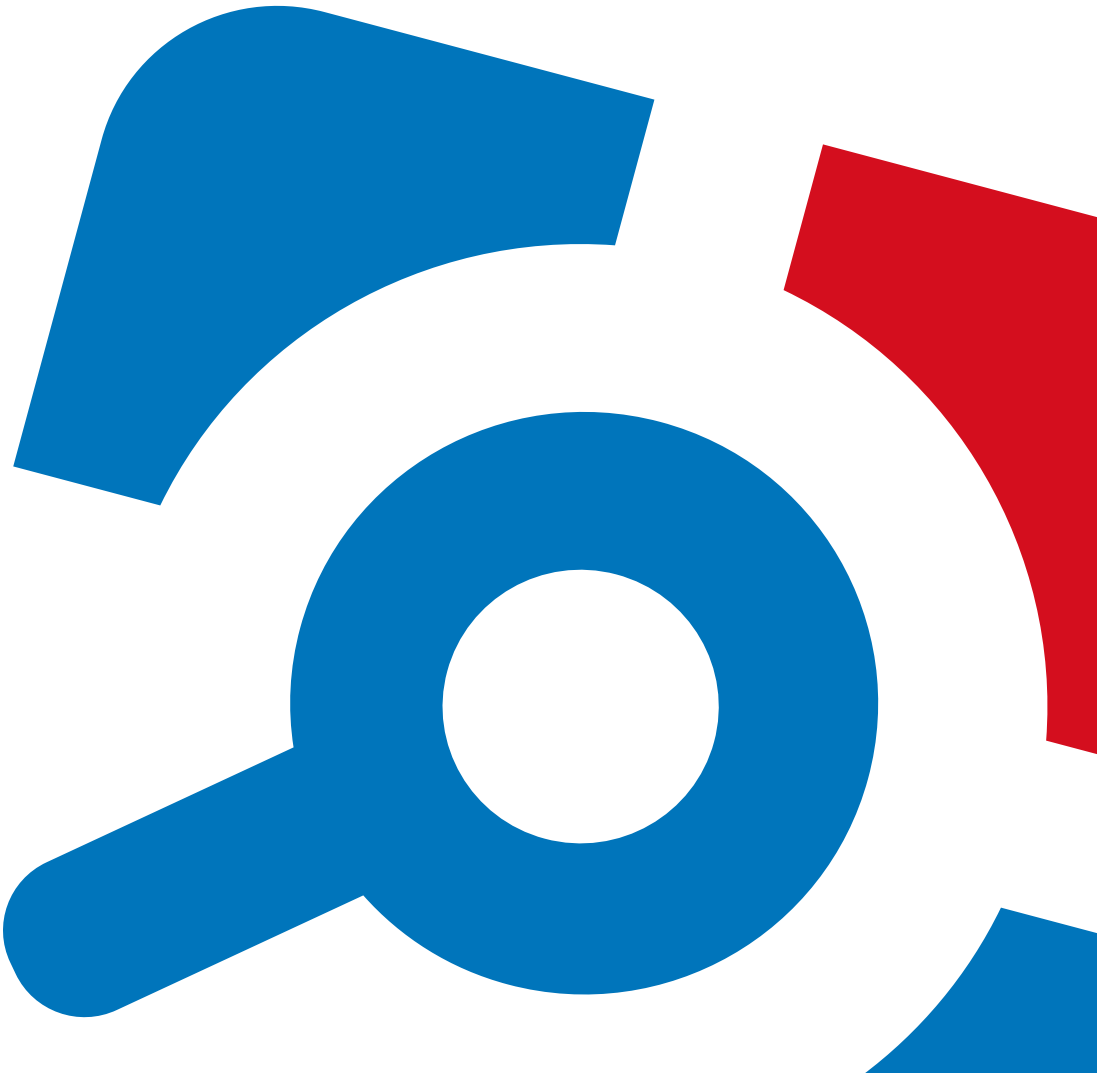
netwrix

Netwrix Auditor for Office 365

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.

Table of Contents

1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for Office 365. 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 Exchange Online and SharePoint Online within Office 365
- Launch data collection
- See how Netwrix Auditor enables complete visibility

NOTE: This guide only covers the basic configuration and usage options for auditing Exchange Online and SharePoint Online 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 Office 365 detects and reports on all changes made to Microsoft Exchange Online and SharePoint Online. For Exchange Online, the product provides auditing of configuration and permissions changes. In addition, it tracks mailbox access events in the managed Exchange Online organization, and

notifies the users whose mailboxes have been accessed by non–owners. For SharePoint Online, the product reports on read access and changes made to SharePoint Online sites, including modifications of content, security settings, and sharing permissions.

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 Office 365:

Audited System	Supported Versions
Exchange Online	Exchange Online version provided within Microsoft Office 365
SharePoint Online	SharePoint Online 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	• 500 MB physical disk space for the product installation • 30 GB for the file-based Long-Term Archive	

Hardware Component	Minimum	Recommended
	• 500 MB for the SQL Server-based Audit Database where audit data is going to be stored **NOTE:** These are rough estimations, calculated for evaluation of Netwrix Auditor for Office 365. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on the Netwrix Auditor disk space requirements.	
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	• 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	• .Net Framework 3.5 SP1
Installer	• 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
• SharePoint Online	• .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)	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. **NOTE:** Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor Administrator Console.

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 Processing Account Rights and Permissions 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 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

Exchange Online	***In the Cloud:***
	• To connect to Exchange Online, your personal Microsoft account must be assigned the following Exchange admin roles:
	  • **Audit logs**
	  • **Mail Recipients**
	  • **View-Only Configuration**

SharePoint Online	***In the Cloud:*** • The account must be assigned the **Global Administrator** role in Azure AD domain (**Company Administrator** in Azure AD PowerShell terms) — only required when first configuring a Managed Object. Later, any regular account can be used to collect audit data. **NOTE:** Accounts with multi-factor authentication are not supported.

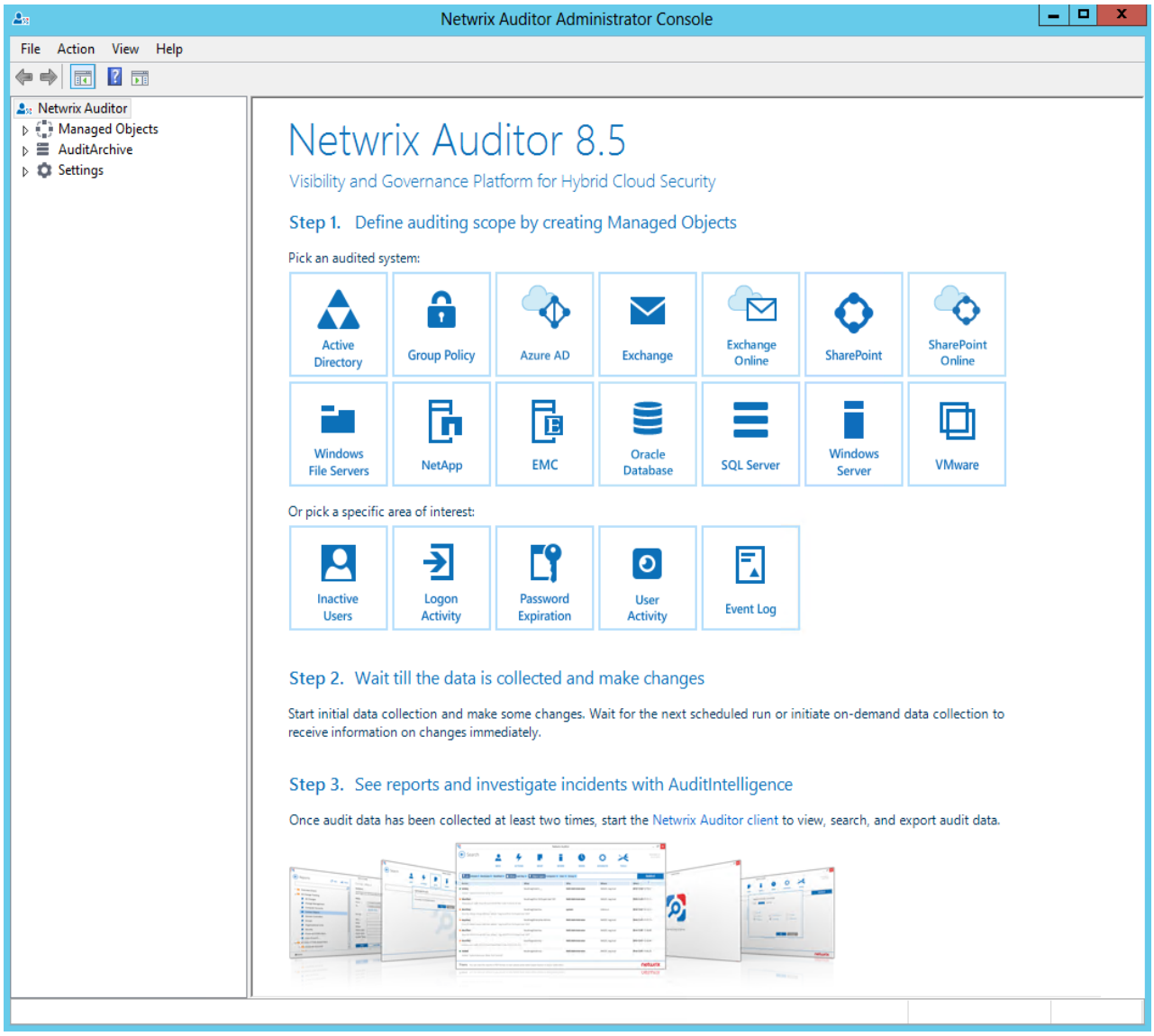
4. Install the Product

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.


Netwrix Auditor Administrator Console
File
Action
View
Help
Netwrix Auditor
Managed Objects
AuditArchive
Settings
Netwrix Auditor 8.5
Visibility and Governance Platform for Hybrid Cloud Security
Step 1. Define auditing scope by creating Managed Objects
Pick an audited system:
Active Directory
Group Policy
Azure AD
Exchange
Exchange Online
SharePoint
SharePoint Online
Windows File Servers
NetApp
EMC
Oracle Database
SQL Server
Windows Server
VMware
Or pick a specific area of interest:
Inactive Users
Logon Activity
Password Expiration
User Activity
Event Log
Step 2. Wait till the data is collected and make changes
Start initial data collection and make some changes. Wait for the next scheduled run or initiate on-demand data collection to receive information on changes immediately.
Step 3. See reports and investigate incidents with AuditIntelligence
Once audit data has been collected at least two times, start the Netwrix Auditor client to view, search, and export audit data.

5. Create Managed Object to Audit Exchange Online and SharePoint Online

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 Exchange Online and SharePoint Online

1. Select the **Managed Objects** node in the left pane and click **Create New Managed Object** in the right pane. Select **Office 365** as a Managed Object type in the **Create New Managed Object** wizard.
2. Select **Exchange Online** and **SharePoint Online** audited systems.
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.

Option	Description
User name	Enter a user name for the SMTP authentication.
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.

5. 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.
6. 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.
7. 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	
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:

Option	Description
	• 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 Netwrix Auditor Installation and Configuration Guide for more information.
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 Audit in Target Environment** step, select **Automatically for the selected audited systems** if you are going to audit Exchange Online. Your current audit settings will be checked on each data collection and adjusted if necessary. For SharePoint Online no special configuration required.
9. On the **Specify Exchange Online Change Summary Recipients** and **Specify SharePoint Online Change Summary Recipients** steps , 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 changes in your Exchange Online configuration within the last 2 days. After the first data collection has finished, an email notification is sent to your email listing changes, if any were detected. For SharePoint Online,

the product collects data on your SharePoint Online 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, it may take up to 12 hours since the Managed Object creation to start collecting SharePoint Online audit data. 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:

- For Exchange Online:
  - Edit User Mailbox details using Exchange Control Panel (ECP)
  - Add a user to a distribution group
  - Grant full access permissions to an existing mailbox to a non-owner user, and access this mailbox with a non-owner account
- For SharePoint Online:
  - Create a new group in your SharePoint site
  - Modify file contents

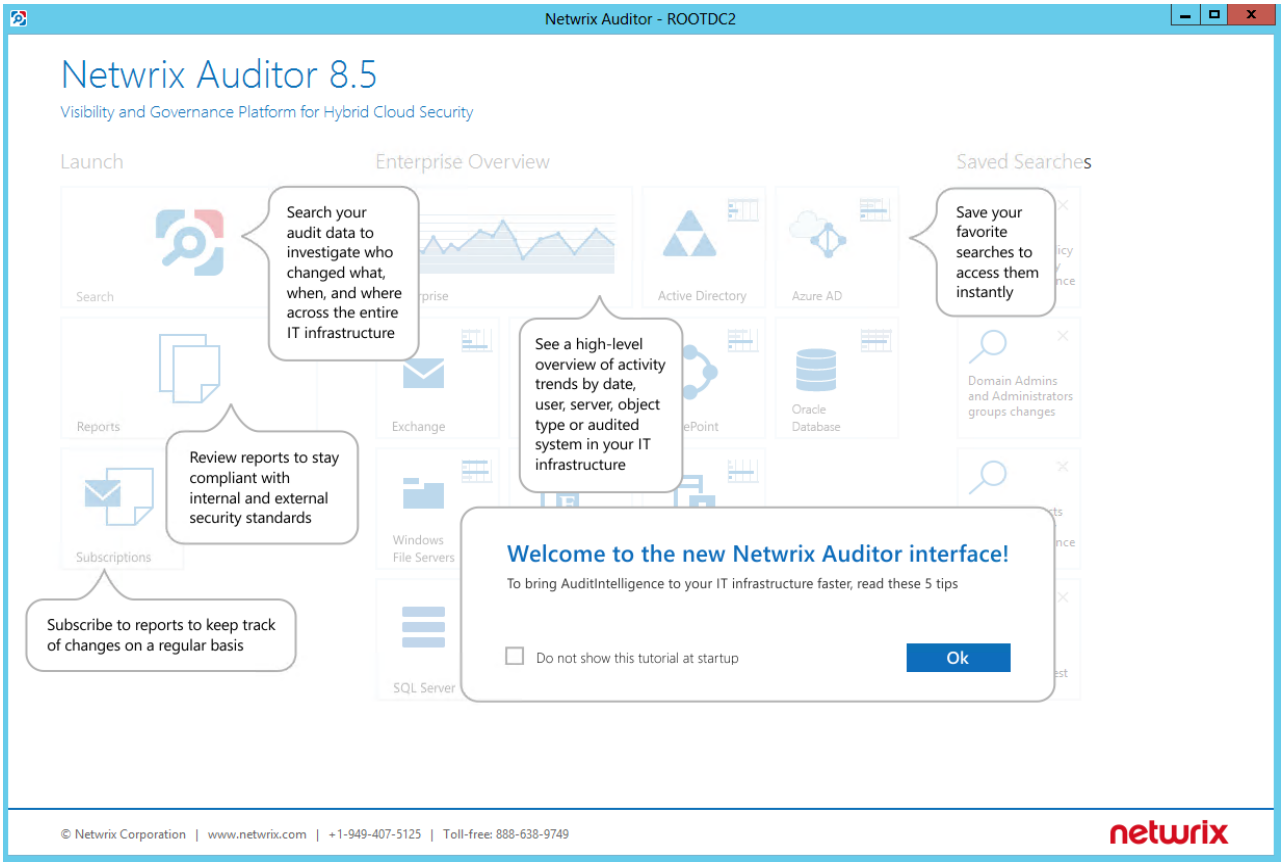
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

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 Office 365 Overview
- Review the All Exchange Online Changes and All SharePoint Online Activity by User Reports

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

To launch data collection manually

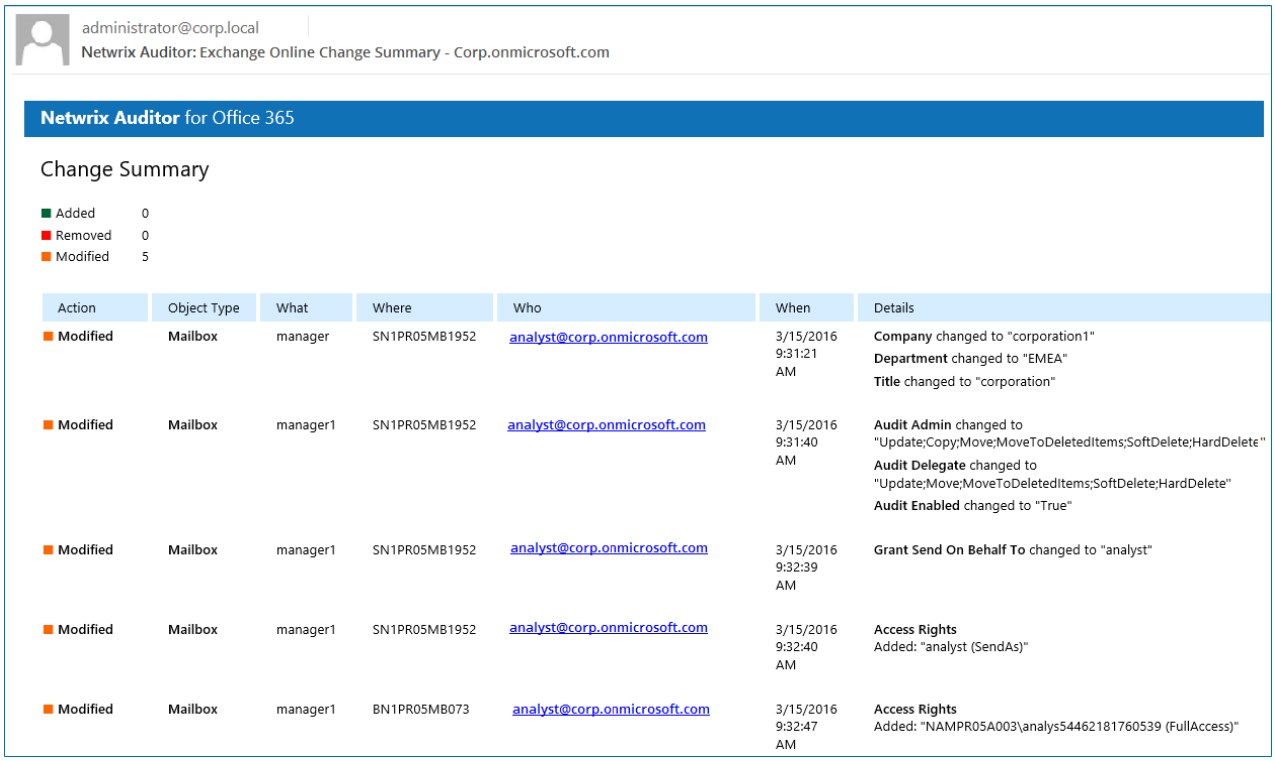
1. In the Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name**.
2. In the right pane, click **Run**.
3. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

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.

Netwrix Auditor Exchange Online Change Summary example:



administrator@corp.local
Netwrix Auditor: Exchange Online Change Summary - Corp.onmicrosoft.com

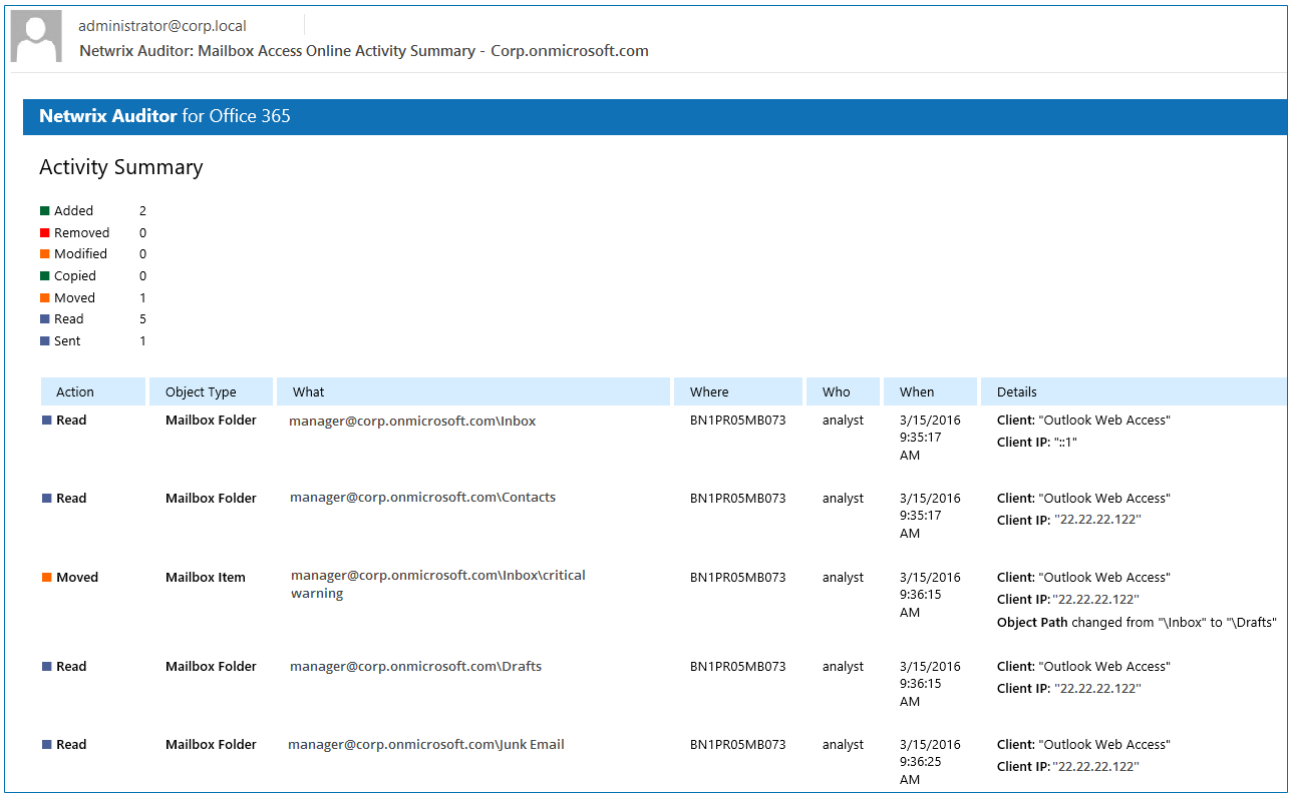
Netwrix Auditor for Office 365

Change Summary

Added 0
Removed 0
Modified 5

Action	Object Type	What	Where	Who	When	Details
Modified	Mailbox	manager	SN1PR05MB1952	analyst@corp.onmicrosoft.com	3/15/2016 9:31:21 AM	**Company** changed to "corporation1" **Department** changed to "EMEA" **Title** changed to "corporation"
Modified	Mailbox	manager1	SN1PR05MB1952	analyst@corp.onmicrosoft.com	3/15/2016 9:31:40 AM	**Audit Admin** changed to "Update;Copy;Move;MoveToDeletedItems;SoftDelete;HardDelete" **Audit Delegate** changed to "Update;Move;MoveToDeletedItems;SoftDelete;HardDelete" **Audit Enabled** changed to "True"
Modified	Mailbox	manager1	SN1PR05MB1952	analyst@corp.onmicrosoft.com	3/15/2016 9:32:39 AM	**Grant Send On Behalf To** changed to "analyst"
Modified	Mailbox	manager1	SN1PR05MB1952	analyst@corp.onmicrosoft.com	3/15/2016 9:32:40 AM	**Access Rights** Added: "analyst (SendAs)"
Modified	Mailbox	manager1	BN1PR05MB073	analyst@corp.onmicrosoft.com	3/15/2016 9:32:47 AM	**Access Rights** Added: "NAMPR05A003\analys54462181760539 (FullAccess)"

If you have configured Netwrix Auditor to track non-owner mailbox access within your Exchange Online, the special email listing all non-owner mailbox access online events will be sent along with the Exchange Online change summary. For example:



administrator@corp.local

Netwrix Auditor: Mailbox Access Online Activity Summary - Corp.onmicrosoft.com

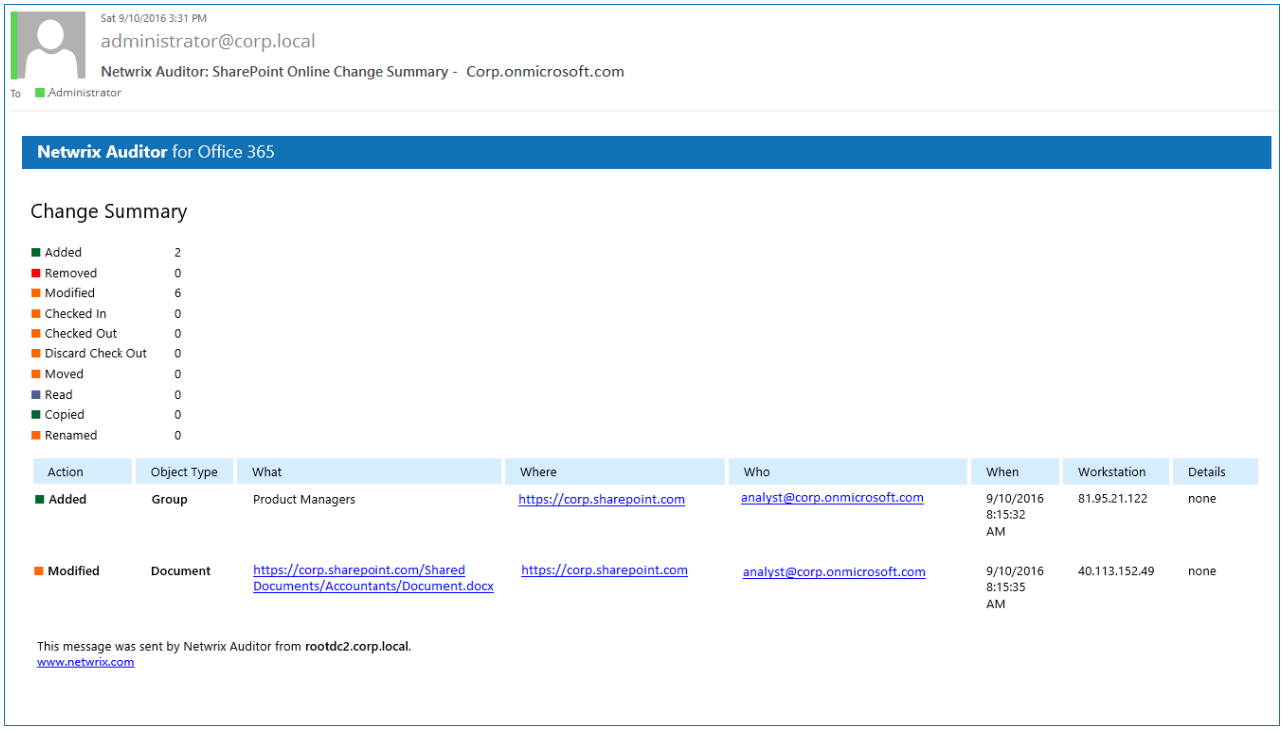
Netwrix Auditor for Office 365

Activity Summary

Added	2
Removed	0
Modified	0
Copied	0
Moved	1
Read	5
Sent	1

Action	Object Type	What	Where	Who	When	Details
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Inbox	BN1PR05MB073	analyst	3/15/2016 9:35:17 AM	**Client:** "Outlook Web Access" **Client IP:** "::1"
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Contacts	BN1PR05MB073	analyst	3/15/2016 9:35:17 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"
Moved	**Mailbox Item**	manager@corp.onmicrosoft.com\Inbox\critical warning	BN1PR05MB073	analyst	3/15/2016 9:36:15 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122" **Object Path** changed from "\Inbox" to "\Drafts"
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Drafts	BN1PR05MB073	analyst	3/15/2016 9:36:15 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"
Read	**Mailbox Folder**	manager@corp.onmicrosoft.com\Junk Email	BN1PR05MB073	analyst	3/15/2016 9:36:25 AM	**Client:** "Outlook Web Access" **Client IP:** "22.22.22.122"

Netwrix Auditor SharePoint Online Change Summary example:



Sat 9/10/2016 3:31 PM

administrator@corp.local

Netwrix Auditor: SharePoint Online Change Summary - Corp.onmicrosoft.com

To Administrator

Netwrix Auditor for Office 365

Change Summary

Added	2
Removed	0
Modified	6
Checked In	0
Checked Out	0
Discard Check Out	0
Moved	0
Read	0
Copied	0
Renamed	0

Action	Object Type	What	Where	Who	When	Workstation	Details
Added	**Group**	Product Managers	https://corp.sharepoint.com	analyst@corp.onmicrosoft.com	9/10/2016 8:15:32 AM	81.95.21.122	none
Modified	**Document**	https://corp.sharepoint.com/Shared Documents/Accountants/Document.docx	https://corp.sharepoint.com	analyst@corp.onmicrosoft.com	9/10/2016 8:15:35 AM	40.113.152.49	none

This message was sent by Netwrix Auditor from **rootdc2.corp.local**.
www.netwrix.com

The example Change Summaries provide the following information:

Column	Description
Action	Shows the type of action that was performed on the object.
Object Type	Shows the type of the object.
What	Shows the name of the changed object or its path (click on the link to navigate to this object).
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

NOTE: The example search applies to Exchange Online auditing.

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.

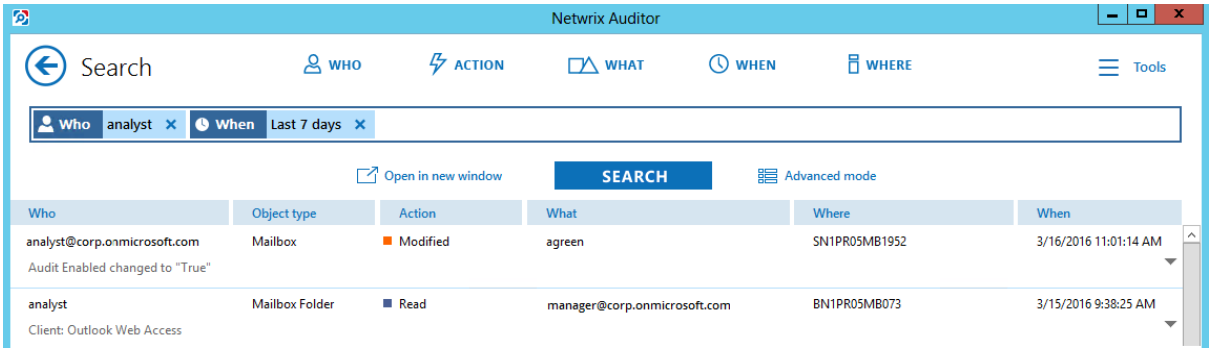
   For example, consider adding these filters:

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

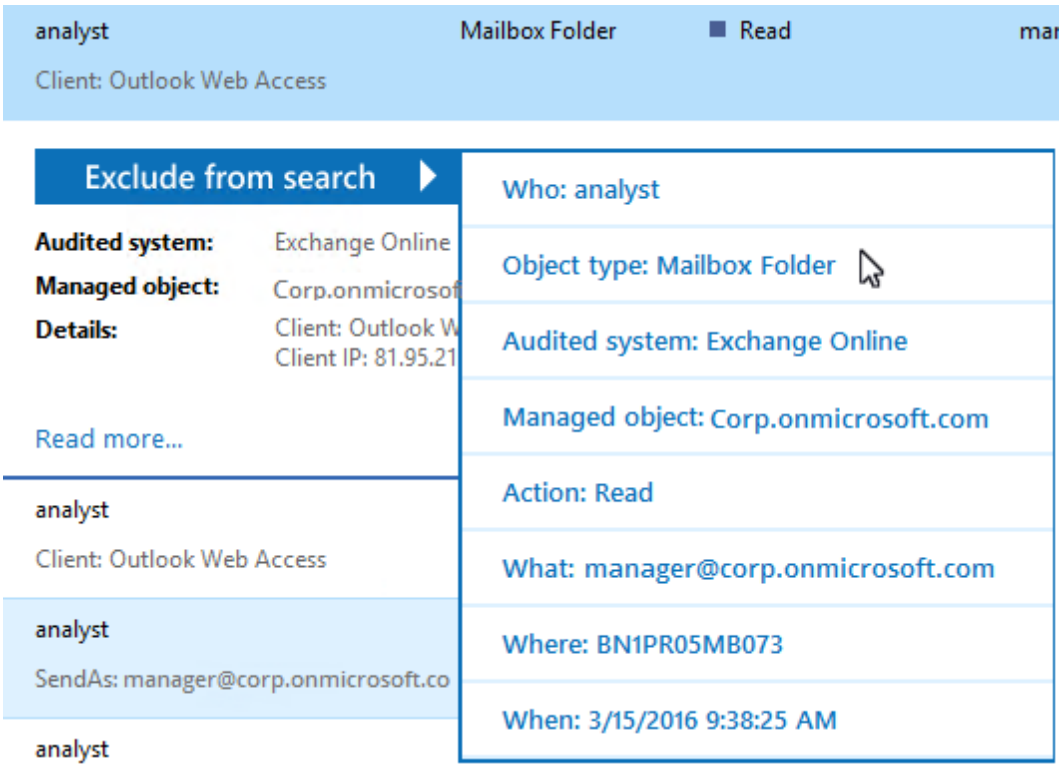
NOTE: Refer to Netwrix Auditor User Guide for detailed instructions on how to apply filters and change match types.

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

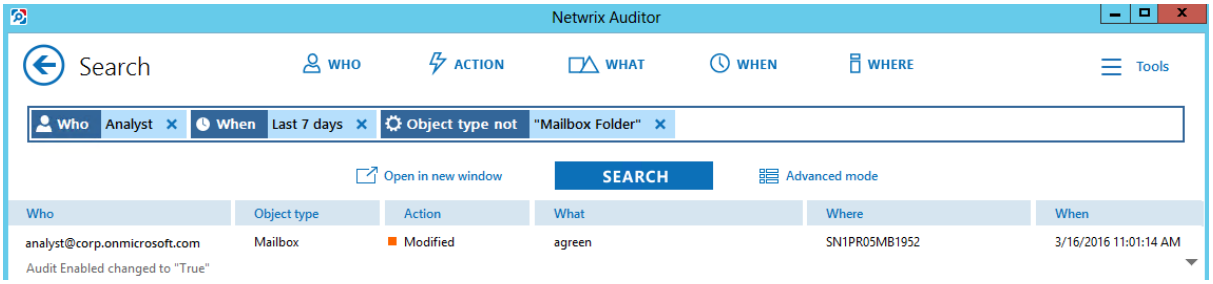
3. Click **Search**.



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., **Object type**: *Mailbox Folder* to leave the information on mailbox changes only.



Your **Search** field will be updated, the **Object type 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 **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 Netwrix Auditor page, so that you will be able to access it instantly. Refer to Netwrix Auditor User Guide for detailed instructions on how to create saved searches.

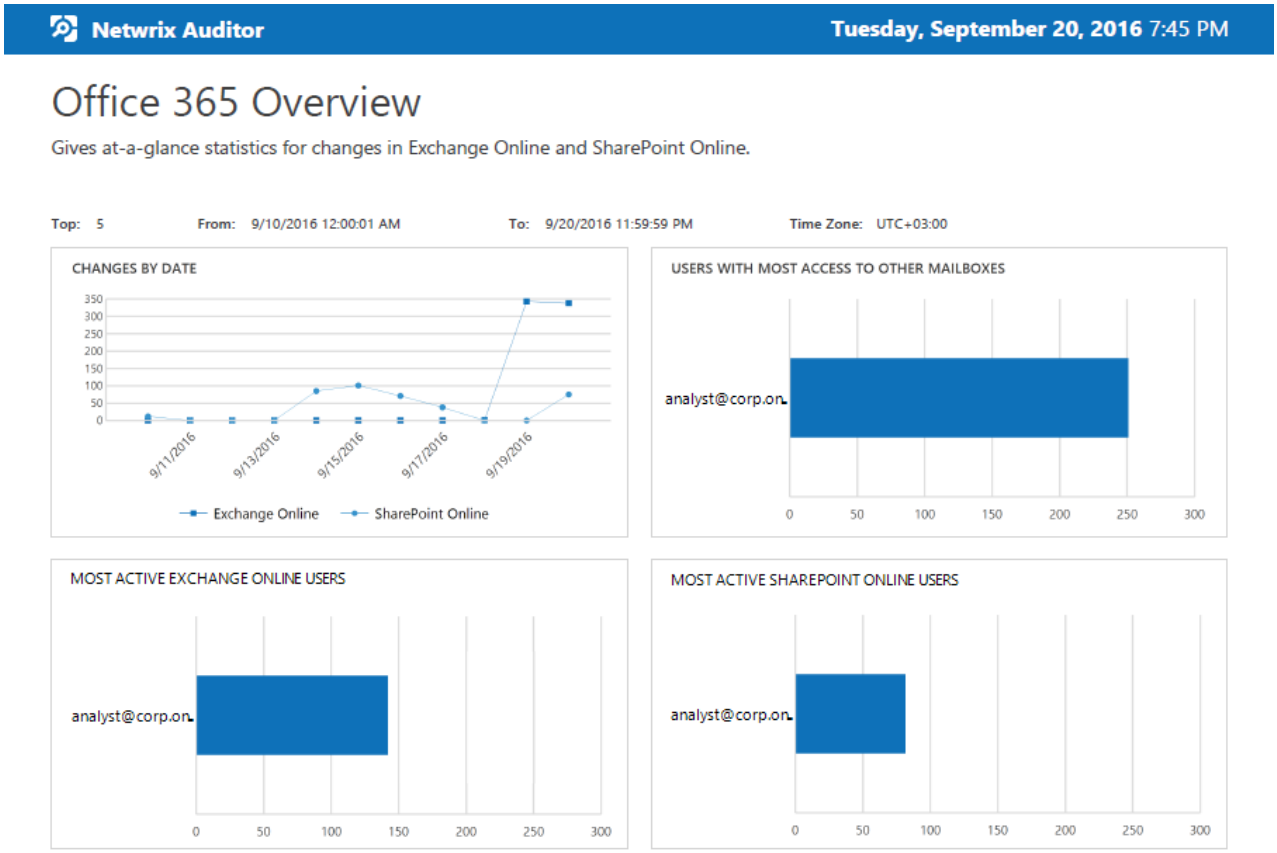
7.3. Review Office 365 Overview

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 **Office 365 Overview**.

To see how your changes are reported with Office 365 Overview

1. On the main Netwrix Auditor page, navigate to the **Enterprise Overview** section.
2. Click the **Office 365** 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 Exchange Online Changes and All SharePoint Online Activity by User Reports

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.

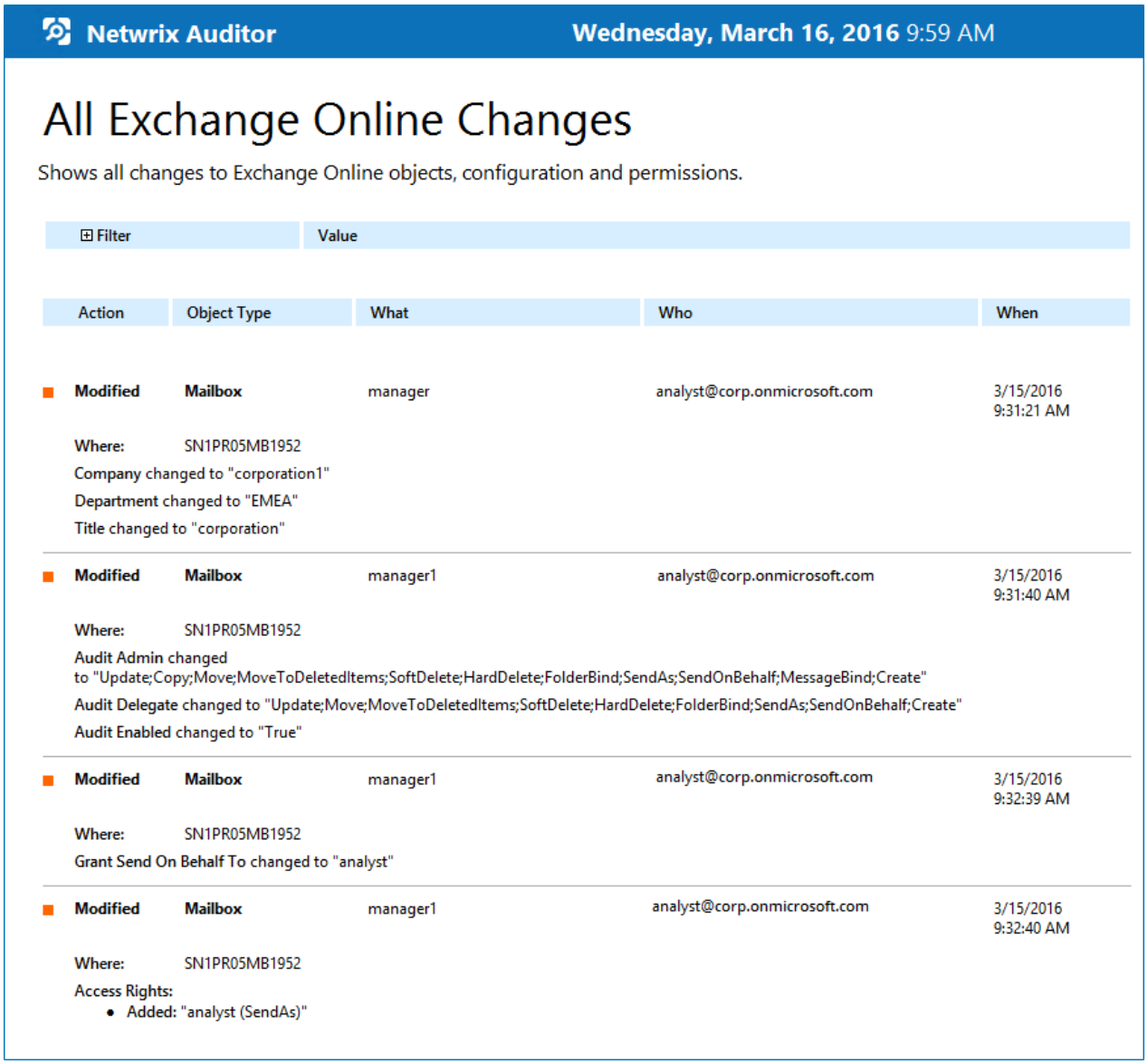
Change reports can be found under the **Reports** → **Exchange Online** and **SharePoint Online** and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

After collecting initial data, making test changes to your environment and running data collection again, you can take advantage of the reports functionality.

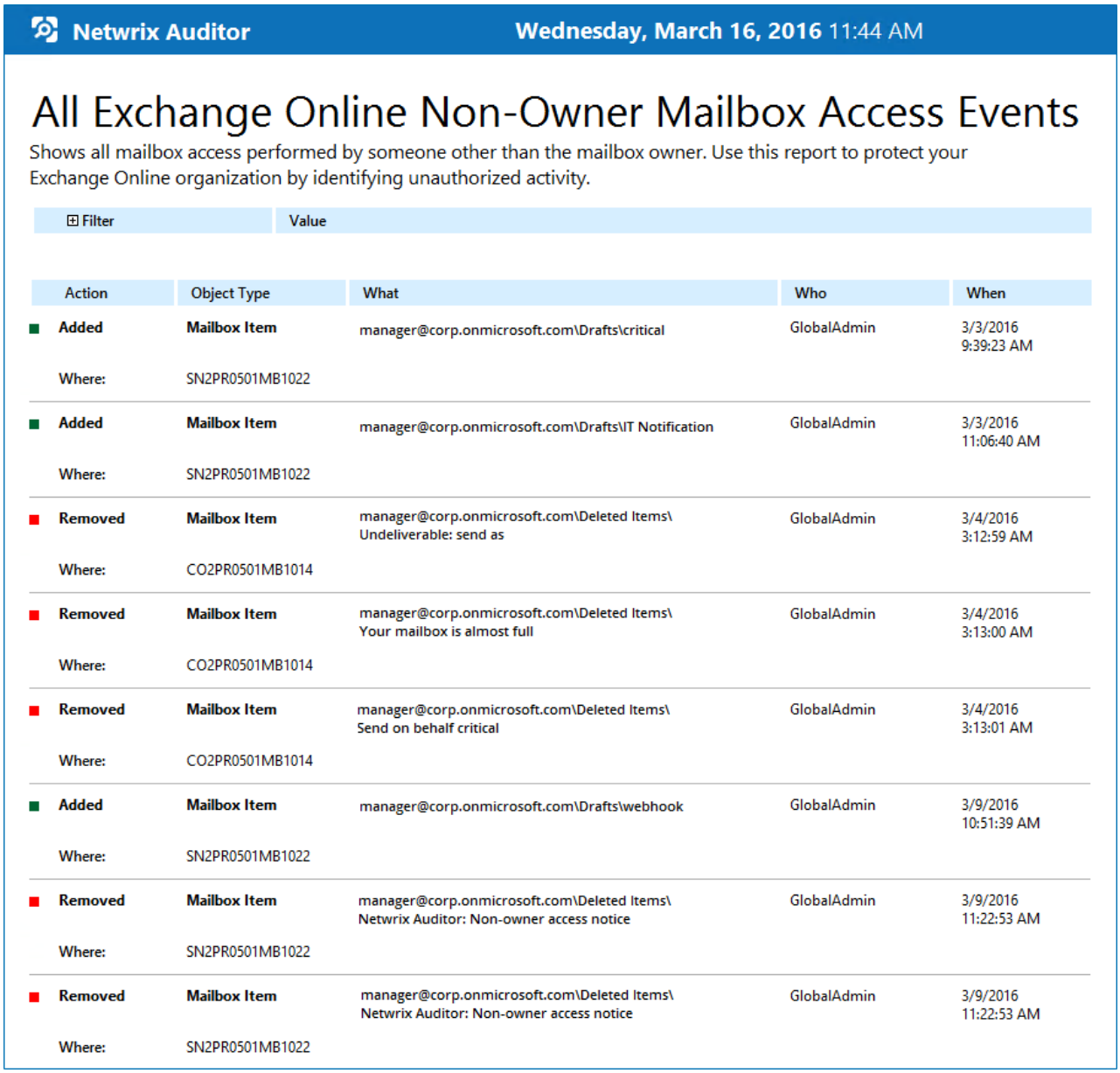
To see how your changes are listed in the report

1. In the Netwrix Auditor client, navigate to **Reports** → **Exchange Online** or **SharePoint Online**.
2. Select the **All Exchange Online Changes** or **All SharePoint Online Activity by User** report.
3. Click **View** to open the report.

The **All Exchange Online Changes** report:



If you have configured Netwrix Auditor to track non-owner mailbox access within your Exchange Online, navigate to **Reports** → **Exchange Online** and select the **All Exchange Online Non-Owner Mailbox Access Events** report. Click **View**.



Netwrix Auditor — Wednesday, March 16, 2016 11:44 AM

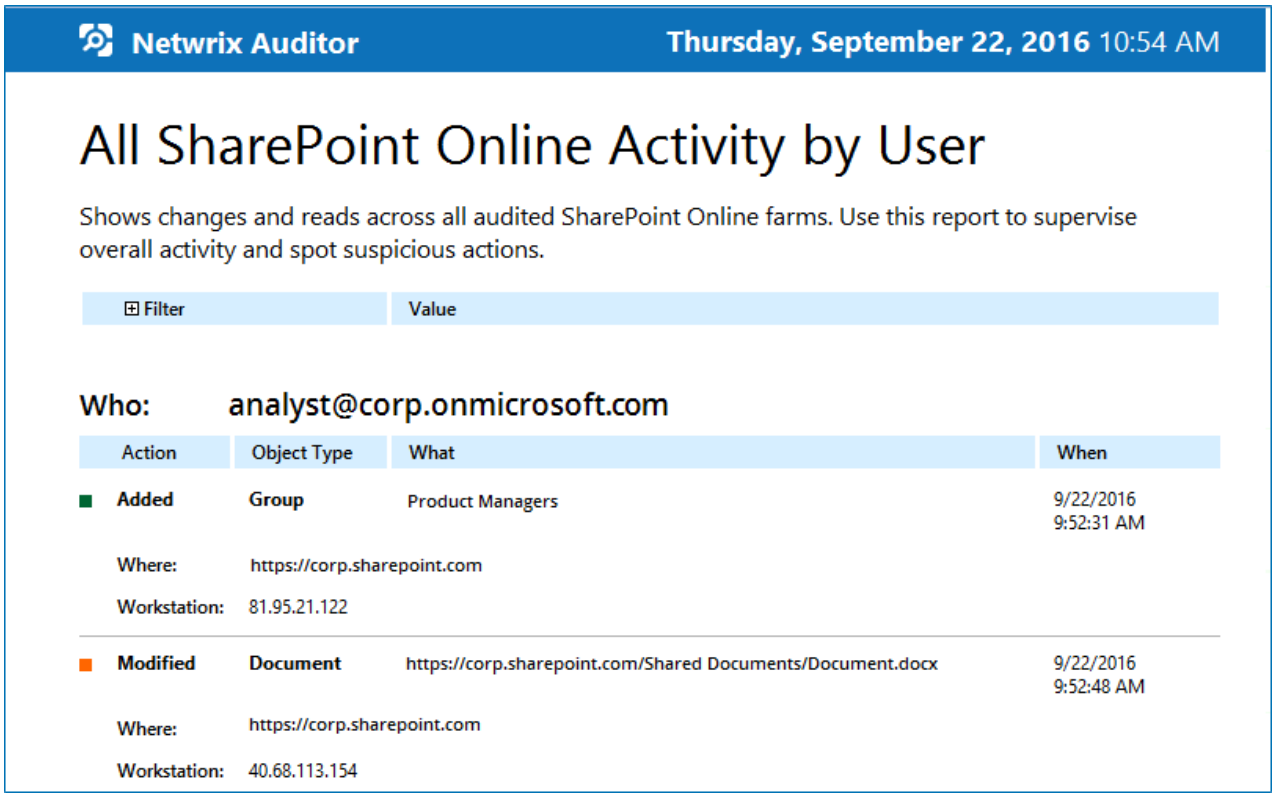
All Exchange Online Non-Owner Mailbox Access Events

Shows all mailbox access performed by someone other than the mailbox owner. Use this report to protect your Exchange Online organization by identifying unauthorized activity.

Filter	Value

Action	Object Type	What	Who	When
Added	**Mailbox Item**	manager@corp.onmicrosoft.com\Drafts\critical	GlobalAdmin	3/3/2016 9:39:23 AM
Where:	SN2PR0501MB1022			
Added	**Mailbox Item**	manager@corp.onmicrosoft.com\Drafts\IT Notification	GlobalAdmin	3/3/2016 11:06:40 AM
Where:	SN2PR0501MB1022			
Removed	**Mailbox Item**	manager@corp.onmicrosoft.com\Deleted Items\ Undeliverable: send as	GlobalAdmin	3/4/2016 3:12:59 AM
Where:	CO2PR0501MB1014			
Removed	**Mailbox Item**	manager@corp.onmicrosoft.com\Deleted Items\ Your mailbox is almost full	GlobalAdmin	3/4/2016 3:13:00 AM
Where:	CO2PR0501MB1014			
Removed	**Mailbox Item**	manager@corp.onmicrosoft.com\Deleted Items\ Send on behalf critical	GlobalAdmin	3/4/2016 3:13:01 AM
Where:	CO2PR0501MB1014			
Added	**Mailbox Item**	manager@corp.onmicrosoft.com\Drafts\webhook	GlobalAdmin	3/9/2016 10:51:39 AM
Where:	SN2PR0501MB1022			
Removed	**Mailbox Item**	manager@corp.onmicrosoft.com\Deleted Items\ Netwrix Auditor: Non-owner access notice	GlobalAdmin	3/9/2016 11:22:53 AM
Where:	SN2PR0501MB1022			
Removed	**Mailbox Item**	manager@corp.onmicrosoft.com\Deleted Items\ Netwrix Auditor: Non-owner access notice	GlobalAdmin	3/9/2016 11:22:53 AM
Where:	SN2PR0501MB1022			

The **All SharePoint Online Activity by User** report:



Netwrix Auditor Thursday, September 22, 2016 10:54 AM

All SharePoint Online Activity by User

Shows changes and reads across all audited SharePoint Online farms. Use this report to supervise overall activity and spot suspicious actions.

⊞ Filter	Value

Who: analyst@corp.onmicrosoft.com

Action	Object Type	What	When
Added	**Group**	Product Managers	9/22/2016 9:52:31 AM
Where:	https://corp.sharepoint.com		
Workstation:	81.95.21.122		
Modified	**Document**	https://corp.sharepoint.com/Shared Documents/Document.docx	9/22/2016 9:52:48 AM
Where:	https://corp.sharepoint.com		
Workstation:	40.68.113.154		

8. Related Documentation

The table below lists all documents available to support Netwrix Auditor for Office 365:

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.