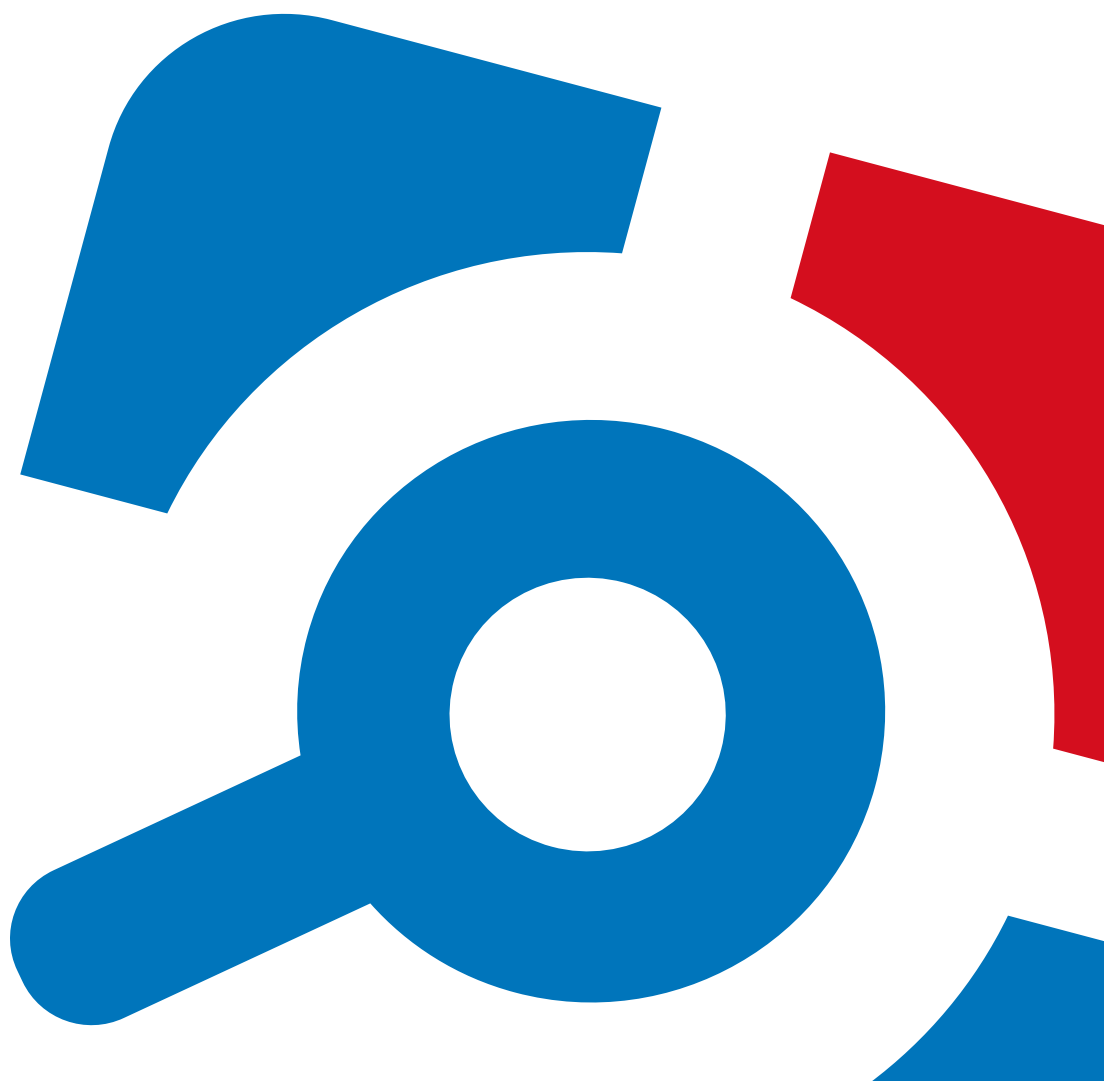


Netwrix Auditor

User Guide

Version: 9.96
12/9/2020



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.

© 2020 Netwrix Corporation.

All rights reserved.

Table of Contents

1. Introduction	7
1.1. Netwrix Auditor Features and Benefits	7
1.2. How It Works	11
1.2.1. Workflow Stages	12
1.3. Product Editions	12
2. First Launch	17
3. View and Search Collected Data	20
3.1. Browsing Your Audit Data	21
3.1.1. Examining Activity Record in Detail	22
3.1.2. Troubleshooting Tips	22
3.2. Use Filters (Simple Mode)	22
3.2.1. Filter Types	23
3.2.2. Modifying and Removing Filters	24
3.2.3. Exporting and Importing Filters	25
3.3. Customize View	25
3.4. Advanced Mode	26
3.4.1. Apply Additional Filters	26
3.4.2. Search Conditions	29
3.5. Include and Exclude Data	32
3.6. Save Search Query Results	33
4. Reports and Report Packs	35
4.1. Viewing Reports	35
4.1.1. Troubleshooting	36
4.1.2. Using Report Filters	37
4.2. Predefined Reports	38
4.2.1. Overview Dashboards	39
4.2.2. Organization Level Reports	42
4.2.3. Change and Activity Reports	43

4.2.4. State-in-Time Reports	45
4.2.4.1. Baseline Reports	47
4.2.5. User Behavior and Blind Spot Analysis Reports	48
4.2.6. Interactive Reports for Change Management Workflow	50
4.2.7. Reports with Video	52
4.3. Compliance Reports	53
4.4. Custom Search-Based Reports	54
5. Alerts	56
5.1. Create Alerts	56
5.2. Manage Alerts	60
5.3. Configure a Response Action for Alert	60
5.3.1. Writing data to CSV file	63
6. IT Risk Assessment Overview	65
6.1. Providing Data for Risk Assessment	65
6.2. Required Monitoring Plan Settings	66
6.3. IT Risk Assessment Dashboard	69
6.3.1. Customizing Metrics for Your Organization	70
6.3.2. Delivering Assessment Results as a File	72
6.4. How Risk Levels Are Estimated	72
7. Behavior Anomalies	76
7.1. Review Behavior Anomalies Dashboard	76
7.2. Review User Profiles and Process Anomalies	77
7.2.1. Process Anomalies and Reduce Risk Score	79
7.2.2. Customize Anomalies List	80
7.3. Behavior Anomalies Assessment Tips and Tricks	80
8. Subscriptions	81
8.1. Subscription to Reports	81
8.2. Subscription to Search Results	81
8.3. Subscription to Risk Assessment Overview	81
8.4. Subscription to Behavior Anomalies	82
8.5. Create Subscriptions	82

8.6. Review and Manage Subscriptions	85
Index	86

1. Introduction

Looking for online version? Check out [Netwrix Auditor help center](#).

This guide describes Intelligence features that help enable complete visibility in your environment. The guide is intended for Netwrix Auditor users (both Reviewers and Global administrators) who want to take advantage of searching and filtering of audit data in the easy-to-use searching interface, generating system-specific and overview reports, etc.

After reading this guide you will be able to:

- Investigate incidents and browse your audit data with Google-like interactive search
- Generate reports and add filters
- Subscribe to important reports you want to receive on a regular basis
- Create alerts to stay notified on actions critical to your organization security

This guide is intended for developers and Managed Service Providers. It provides instructions on how to use Netwrix Auditor Configuration API for managing Netwrix Auditor configuration objects.

NOTE: It assumed that document readers have prior experience with RESTful architecture and solid understanding of HTTP protocol. Technology and tools overview is outside the scope of the current guide.

The product functionality described in this guide applies to Netwrix Auditor Standard Edition. Note that Free Community Edition provides limited functionality. See [Product Editions](#) for more information.

1.1. Netwrix Auditor Features and Benefits

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

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

Major benefits:

- Detect insider threats—on premises and in the cloud
- Pass compliance audits with less effort and expense

- Increase productivity of IT security and operations teams

To learn how Netwrix Auditor can help you achieve your specific business objectives, refer to [Netwrix Auditor Best Practices Guide](#).

The table below provides an overview of each Netwrix Auditor application:

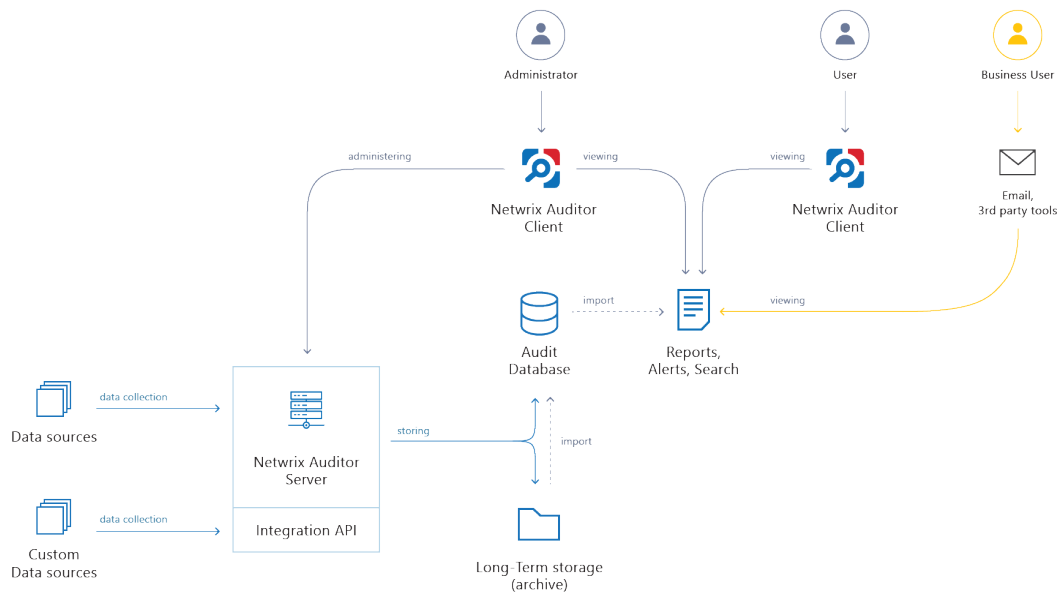
Application	Features
Netwrix Auditor for Active Directory	<p>Netwrix Auditor for Active Directory detects and reports on all changes made to the managed Active Directory domain, including AD objects, Group Policy configuration, directory partitions, and more. It makes daily snapshots of the managed domain structure that can be used to assess its state at present or at any moment in the past. The product provides logon activity summary, reports on interactive and non-interactive logons including failed logon attempts.</p> <p>Also, Netwrix Auditor for Active Directory helps address specific tasks—detect and manage inactive users and expiring passwords. In addition, Netwrix Auditor for Active Directory provides a stand-alone Active Directory Object Restore tool that allows reverting unwanted changes to AD objects down to their attribute level.</p>
Netwrix Auditor for Azure AD	<p>Netwrix Auditor for Azure AD detects and reports on all changes made to Azure AD configuration and permissions, including Azure AD objects, user accounts, passwords, group membership, and more. The products also reports on successful and failed logon attempts.</p>
Netwrix Auditor for Exchange	<p>Netwrix Auditor for Exchange detects and reports on all changes made to Microsoft Exchange configuration and permissions. In addition, it tracks mailbox access events in the managed Exchange organization, and notifies the users whose mailboxes have been accessed by non-owners.</p>
Netwrix Auditor for Exchange Online	<p>Netwrix Auditor for Exchange Online detects and reports on all changes made to Microsoft Exchange Online.</p> <p>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.</p>
Netwrix Auditor for SharePoint Online	<p>Netwrix Auditor for SharePoint Online detects and reports on all changes made to SharePoint Online.</p> <p>The product reports on read access and changes made to SharePoint Online sites, including modifications of content, security settings, and sharing permissions. In addition to SharePoint Online, OneDrive for Business changes are reported too.</p>

Application	Features
Netwrix Auditor for Windows File Servers	Netwrix Auditor for Windows File Servers detects and reports on all changes made to Windows-based file servers, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for EMC	Netwrix Auditor for EMC detects and reports on all changes made to EMC VNX/VNXe and Isilon storages, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for NetApp	Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
Netwrix Auditor for Nutanix Files	Netwrix Auditor for Nutanix Files detects and reports on changes made to SMB shared folders, subfolders and files stored on the Nutanix File Server, including failed and successful attempts.
Netwrix Auditor for Oracle Database	Netwrix Auditor for Oracle Database detects and reports on all changes made to your Oracle Database instance configuration, privileges and security settings, including database objects and directories, user accounts, audit policies, sensitive data, and triggers. The product also reports on failed and successful access attempts.
Netwrix Auditor for SharePoint	Netwrix Auditor for SharePoint detects and reports on read access and changes made to SharePoint farms, servers and sites, including modifications of content, security settings and permissions.
Netwrix Auditor for SQL Server	Netwrix Auditor for SQL Server detects and reports on all changes to SQL Server configuration, database content, and logon activity.
Netwrix Auditor for VMware	Netwrix Auditor for VMware detects and reports on all changes made to ESX servers, folders, clusters, resource pools, virtual machines and their virtual hardware configuration.
Netwrix Auditor for Windows Server	Netwrix Auditor for Windows Server detects and reports on all changes made to Windows-based server configuration, including hardware devices, drivers, software, services, applications, networking settings, registry settings, DNS, and more. It also provides automatic consolidation and archiving of event logs data. With a stand-alone Event Log Manager tool, Netwrix Auditor collects Windows event logs from multiple computers across the network, stores them centrally in a compressed format, and enables convenient analysis of event log

Application		Features
		data.
Netwrix Auditor Activity	for User	Netwrix Auditor for User Sessions detects and reports on all user actions during a session with the ability to monitor specific users, applications and computers. The product can be configured to capture a video of users' activity on the audited computers.

1.2. How It Works

Netwrix Auditor provides comprehensive auditing of applications, platforms and storage systems. Netwrix Auditor architecture and components interactions are shown in the figure below.



- **Netwrix Auditor Server** — the central component that handles the collection, transfer and processing of audit data from the various data sources (audited systems). Data from the sources not yet supported out of the box is collected using RESTful Integration API.
- **Netwrix Auditor Client** — a component that provides a friendly interface to authorized personnel who can use this console UI to manage Netwrix Auditor settings, examine alerts, reports and search results. Other users can obtain audit data by email or with 3rd party tools — for example, reports can be provided to the management team via the intranet portal.
- **Data sources** — entities that represent the types of audited systems supported by Netwrix Auditor (for example, Active Directory, Exchange Online, NetApp storage system, and so on), or the areas you are interested in (Group Policy, User Activity, and others).
- **Long-Term Archive** — a file-based repository storage keeps the audit data collected from all your data sources or imported using Integration API in a compressed format for a long period of time. Default retention period is 120 months.
- **Audit databases** — these are Microsoft SQL Server databases used as operational storage. This type of data storage allows you to browse recent data, run search queries, generate reports and alerts. Typically, data collected from the certain data source (for example, Exchange Server) is stored to the dedicated Audit database and the long-term archive. So, you can configure as many databases as the data sources you want to process. Default retention period for data stored in the Audit database is 180 days.

1.2.1. Workflow Stages

General workflow stages are as follows:

1. Authorized administrators prepare IT infrastructure and data sources they are going to audit, as recommended in Netwrix Auditor documentation and industry best practices; they use Netwrix Auditor client (management UI) to set up automated data processing.
2. Netwrix Auditor collects audit data from the specified data source (application, server, storage system, and so on).

To provide a coherent picture of changes that occurred in the audited systems, Netwrix Auditor can consolidate data from multiple independent sources (event logs, configuration snapshots, change history records, etc.). This capability is implemented with Netwrix Auditor Server and Integration API.

NOTE: For details on custom data source processing workflow, refer to the [Integration API](#) documentation.

3. Audit data is stored to the Audit databases and the repository (Long-Term Archive) and preserved there according to the corresponding retention settings.
4. Netwrix Auditor analyzes the incoming audit data and alerts appropriate staff about critical changes, according to the built-in alerts you choose to use and any custom alerts you have created. Authorized users use the Netwrix Auditor Client to view pre-built dashboards, run predefined reports, conduct investigations, and create custom reports based on their searches. Other users obtain the data they need via email or third-party tools.
5. To enable historical data analysis, Netwrix Auditor can extract data from the repository and import it to the Audit database, where it becomes available for search queries and report generation.

1.3. Product Editions

Netwrix Auditor is available in three editions: full-featured Enterprise Advanced and limited Business Essentials (that are activated with a license key), and the most limited Free Community Edition that is distributed free of charge.

Netwrix Auditor Enterprise Advanced can be evaluated for 20 days. During this period you have free, unlimited access to all features and functions. After the evaluation license expires, the product will prompt you to supply a commercial license where you can choose if you want to stay on advanced version or have limited set of functions available in Business Essentials. Alternatively, you can switch to Free Community Edition.

Free Community Edition helps you maintain visibility into your environment by delivering daily reports that summarize changes that took place in the last 24 hours. However, you will no longer be able to use interactive search, predefined reports, alerts and dashboards, or store your security intelligence. After switching to free mode, you may need to re-arrange your audit configuration due to the limitations.

When running Free Community Edition, at any time you can upgrade to Enterprise Advanced or Business Essentials, simply by supplying a commercial license in **Settings → Licenses**.

Refer to a table below to compare product editions.

Feature	Free Community Edition	Business Essentials	Enterprise Advanced
Deployment options	One Netwrix Auditor client instance per one Netwrix Auditor Server	Multiple Netwrix Auditor clients for Netwrix Auditor Server	Multiple Netwrix Auditor clients for Netwrix Auditor Server
Role-based access and delegation	–	–	+
Support plan	Forum support only	Full	Full
Automatic audit configuration	+	+	+
Data sources			
Active Directory (including Group Policy and Logon Activity)	One domain	Unlimited domains Up to 250 AD users	Unlimited
Azure AD	One Office 365 tenant	–	Unlimited
Exchange	One domain	–	Unlimited
EMC	One server or one file share, or one IP range, or one OU	–	Unlimited
NetApp	One server or one file share, or one IP range, or one OU	–	Unlimited
Windows File Servers	One server or one file share, or one	Up to 10 TB of data	Unlimited

Feature	Free Community Edition	Business Essentials	Enterprise Advanced
	IP range, or one OU		
Office 365 (including Exchange Online, SharePoint Online, and OneDrive for Business)	One Office 365 tenant	–	Unlimited
Network Devices	One network device or one IP range	–	Unlimited
Oracle Database	One Oracle Database instance	–	Unlimited
SharePoint	One SharePoint farm	–	Unlimited
SQL Server	One SQL Server instance	–	Unlimited
VMware	One VMware Virtual Center	–	Unlimited
Windows Server	One server or IP range or one Active Directory container	Up to 10 Windows Servers	Unlimited
Netwrix Auditor tools			
Netwrix Auditor Object Restore for Active Directory	–	+	+
Netwrix Auditor Event Log Manager	–	+	+
Netwrix Auditor Inactive User Tracker	–	+	+
Netwrix Auditor Password Expiration	–	+	+

Feature	Free Community Edition	Business Essentials	Enterprise Advanced
Notifier			
Data collection details			
Who	–	+	+
What	+	+	+
When	+	+	+
Where	+	+	+
Workstation	+	+	+
User Activity video recording	–	+	+
Intelligence			
Activity Summary	1 recipient	2 recipients	Multiple recipients
AuditArchive	–	Both Long-Term Archive and Audit Database	Both Long-Term Archive and Audit Database
Search	–	No user profile details in Search	+
Reports (including organization-level reports, overview diagrams, change and activity reports, reports with video and review status) and special report packs	–	+	+
State-in-time reports	–	No Risk Assessment reports	+
Ability to save search as a custom report	–	+	+
Subscriptions	–	Up to 2	+

Feature			Free Community Edition	Business Essentials	Enterprise Advanced
				recipients	
Alerts			-	Up to 2 recipients of alerts; No tags in alerts	+
Behavior dashboard	Anomaly	Discovery	-	-	+
IT Risk Assessment dashboard			-	-	+
Netwrix Auditor Integration API					
Data in			-	-	+
Data out			-	-	+

2. First Launch

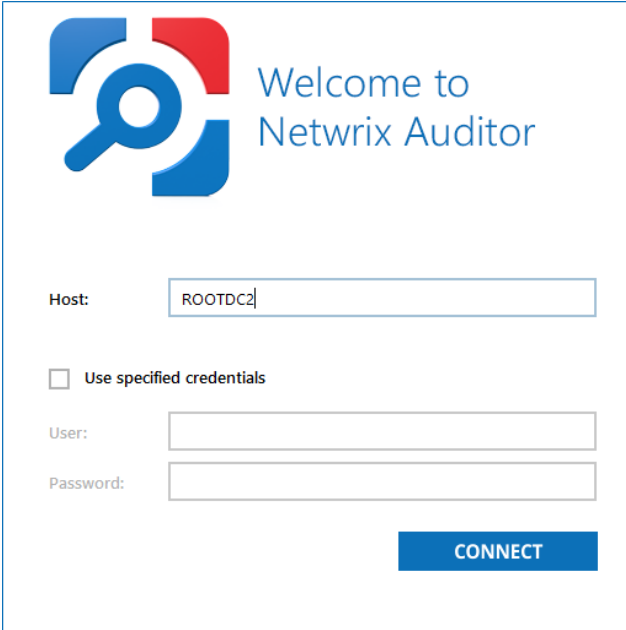
To start using Netwrix Auditor

1. Navigate to **Start** → **Netwrix Auditor**.
2. Log into the product.

NOTE: This step is required if Netwrix Auditor is installed remotely (not on computer that hosts Netwrix Auditor Server).

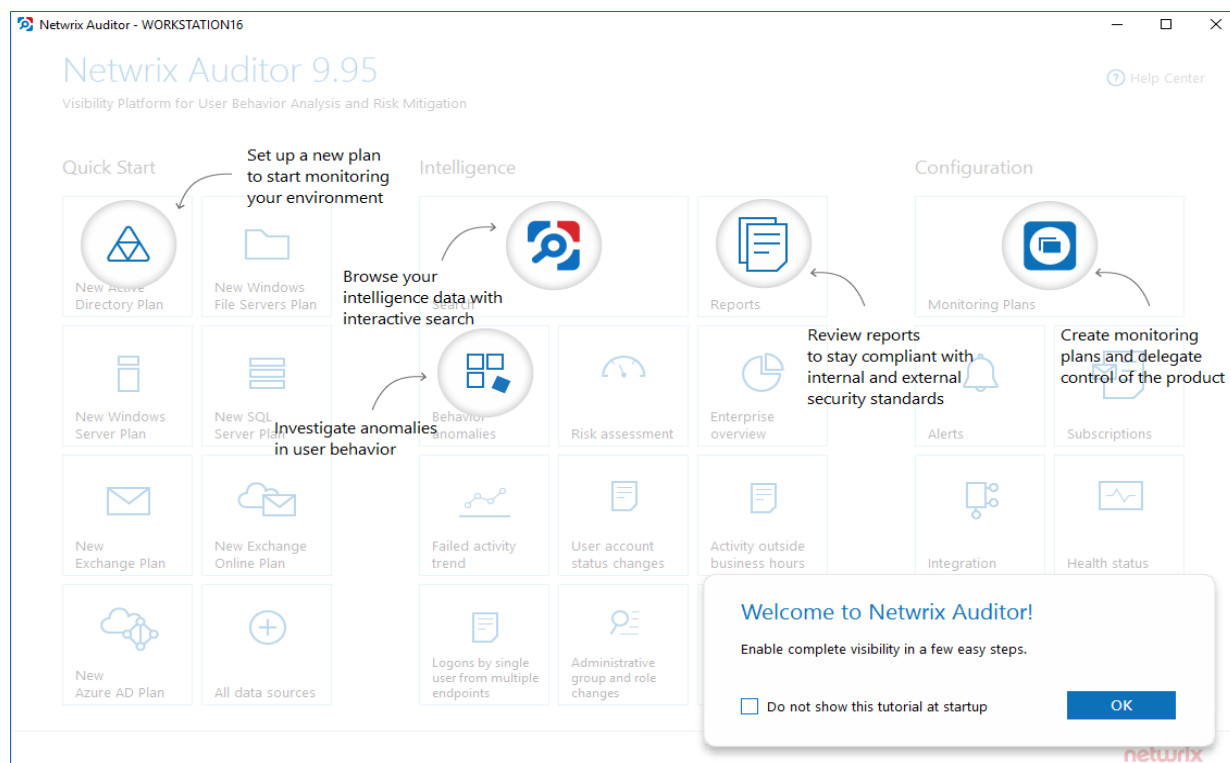
You can configure a single Netwrix Auditor client to work with several Netwrix Auditor Servers. To switch to another server, reopen the Netwrix Auditor client and provide another host name (e.g., *rootdc2*, *WKSWin12r2.enterprise.local*).

For your convenience, the **Host** field is prepopulated with your computer name. By default, you can log in with your Windows credentials by simply clicking **Connect**. Select **Use specified credentials** if you want to log in as another user.

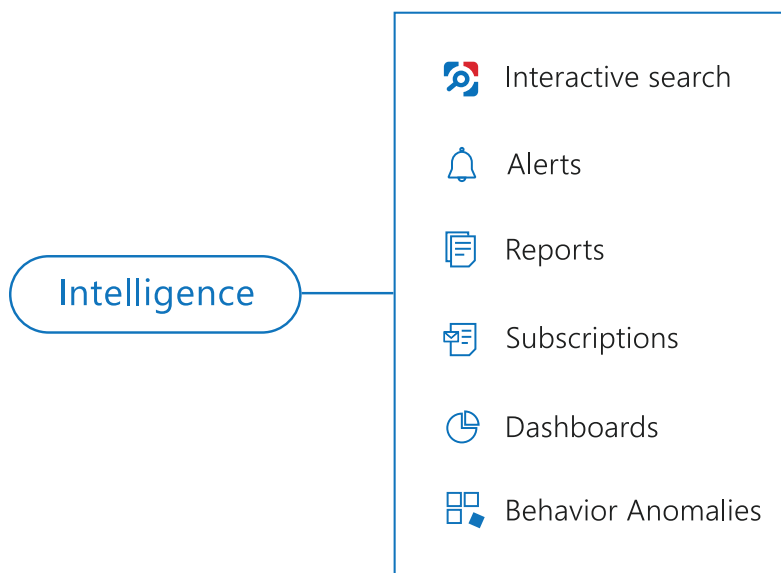
The image shows the 'Welcome to Netwrix Auditor' login window. It features the Netwrix Auditor logo (a stylized magnifying glass with blue and red segments) on the left. To the right of the logo, the text 'Welcome to Netwrix Auditor' is displayed. Below the logo and text, there is a 'Host:' label followed by a text input field containing 'ROOTDC2'. Underneath the host field is a checkbox labeled 'Use specified credentials'. Below the checkbox are two more text input fields, one for 'User:' and one for 'Password:'. At the bottom right of the window is a blue button labeled 'CONNECT'.

NOTE: Make sure you have sufficient permissions to access the product. If you cannot log into Netwrix Auditor with your Windows credentials, contact your Netwrix Auditor administrator.

After logging into Netwrix Auditor, you will see the following window:



Take a closer look at the Home page. It contains everything you need to enable complete visibility in your environment.



Review the following for additional information:

- [View and Search Collected Data](#)
- [Alerts](#)
- [Reports and Report Packs](#)
- [Subscriptions](#)

- [Overview Dashboards](#)
- [Behavior Anomalies](#)

3. View and Search Collected Data

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.

NOTE: To review collected data, you must be assigned the **Global administrator** or **Global reviewer** Netwrix Auditor role. Users with the **Reviewer** role on a certain plan or folder have limited access to data—only within their delegated scope. See [Netwrix Auditor Administration Guide](#) for more information.

This functionality is currently available for the following data sources:

- Active Directory
- Azure AD
- Exchange
- Exchange Online
- File Servers (Windows File Servers, EMC, and NetApp)
- Network Devices
- Oracle Database
- SharePoint
- SharePoint Online
- SQL Server
- VMware
- Windows Server
- Group Policy
- Logon Activity
- User Activity (Video)
- Netwrix API—data imported to the Audit Database from other sources using Netwrix Auditor Integration API
- Netwrix Auditor Self-Audit

Netwrix Auditor executes interactive search queries against data stored in the audit databases, that is, on data collected in the last 180 days (default retention period). If you want to investigate incidents that occurred more than 180 days ago, then you should import that data from the Long-Term Archive. See [Investigations](#).

3.1. Browsing Your Audit Data

On the main Netwrix Auditor page, navigate to **Search**. There you can use the UI controls to run the variety of search queries that will fetch you exactly the data you need.

- To view all audit data stored in all Audit Databases by all monitoring plans, click **Search** button in the center.

NOTE: Be aware that this type of search query may take time due to a large amount of data. Thus, it is recommended that instead of retrieving a massive data set, you pre-configure your search query using filters.

By default, Netwrix Auditor shows only the top 2,000 entries in the search results.

- To pre-configure your search query before you click **Search**, you can add filters. Then the search query will return only data matching your filtering criteria. See [Use Filters \(Simple Mode\)](#)

You can also use advanced filtering capabilities based on regular expressions (they involve filter fields and conditions). See [Advanced Mode](#) for details.



- By default, search results are open in the same window, so the subsequent search results will overwrite the previous search results. To view them in different windows, click **Open in new window**.
- In addition, you can customize your view by selecting columns to display. See [Customize View](#)

Use search results for your own needs: save, share, create search-based alerts, subscribe to periodic delivery of search query results, etc. See [Save Search Query Results](#) for more information.

Who	Object type	Action	What	Where	When
ENTERPRISE\admini...	group	Modified	\\local\\enterprise\\Users\\E...	enterprisedc.enterpri...	9/26/2018 3:44:...
Security Universal Group Member - Removed: "enterprise.local/Users/Mark Brown"					
ENTERPRISE\admini...	user	Modified	\\local\\enterprise\\Users\\B...	enterprisedc.enterpri...	9/26/2018 3:43:...
User Account Disabled					
ENTERPRISE\admini...	computer	Modified	\\local\\enterprise\\Compu...	enterprisedc.enterpri...	9/26/2018 3:42:...
Computer Account Enabled					
ENTERPRISE\admini...	computer	Modified	\\local\\enterprise\\Compu...	enterprisedc.enterpri...	9/13/2018 8:39:...
Computer Account Disabled					
ENTERPRISE\admini...	group	Modified	\\local\\enterprise\\Users\\E...	enterprisedc.enterpri...	9/11/2018 8:45:...
Security Universal Group Member - Added: "enterprise.local/Users/Mark Brown"					
ENTERPRISE\admini...	group	Modified	\\local\\enterprise\\Compu...	enterprisedc.enterpri...	8/28/2018 2:56:...
Security Global Group Member - Added: "enterprise.local/Computers/STATIONSQ12016"					

Details

Activity record details

Data source: Active Directory

Monitoring plan: AD Monitoring

Item: enterprise.local (Domain)

Workstation: enterprisedc.enterprise.local

Details: Security Universal Group Member - Removed: "enterprise.local/Users/Mark Brown"

User account details

Account: ENTERPRISE\\administrator

Full name: Administrator

Display name: Administrator

ADStatus: Enabled

Last logon: 10/6/2018 6:26:44 PM

Member of: [10 groups](#)

Exclude from search | Include in search

You can also use the **Search** window to examine details for the selected activity record, or watch a video recording (for User Activity data).

3.1.1. Examining Activity Record in Detail

To work with a certain activity record:

1. Select the activity record which details you want to review. Its key fields and user (initiator) account details will be displayed in the right pane.

2. To display all fields and copy them if necessary, click the **Full screen...** link on the right.

If you are examining User Activity entries, click the **Show video...** link below the entry. Review details and play a video by clicking the **Show video** on the right.

3. You can instruct Netwrix Auditor to include or exclude this activity record from the search query results, as described in the [Include and Exclude Data](#)

3.1.2. Troubleshooting Tips

If you do not see the expected information in search results, try the following:

- Verify the Audit Database retention and SQL Server settings.
- Make sure that data collection is configured properly in the monitoring plan settings.
- Check the required audit settings in your monitored infrastructure.
- Verify the data collecting account.

See next:

- [Use Filters \(Simple Mode\)](#)
- [Advanced Mode](#)
- [Customize View](#)
- [Include and Exclude Data](#)
- [Save Search Query Results](#)

3.2. Use Filters (Simple Mode)






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

- Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., **Who: Administrator** AND **Action: Added**).
- Specify several values in the same filter to search for any of them (e.g., **Action: Modified** OR **Action:**

Removed). To do this, select a filter again and specify a new value.

NOTE: Spaces do not separate values, so the whole expression will be included in your search as a single value. For example, if you want to search for any of three names, do not enter *Anna Mark Bill* but instead create a separate filter entry for each name.

3.2.1. Filter Types

Filter	Description
 WHO	<p>Filter data by user (initiator) account.</p> <p>Specify an account name (e.g., <i>John</i>) to find all entries containing it (e.g., <i>Domain1\John</i>, <i>Domain1\Johnson</i>, <i>Domain2\Johnny</i>, <i>John@domain.com</i>).</p> <p>For exact match, use quotation marks and provide a user name in Domain\User or UPN format (e.g., "<i>Domain1\John</i>" or "<i>John@domain.com</i>").</p>
 ACTION	<p>Filter data by action type (Added, Removed, etc.)</p> <p>Select an action type from the list (Added, Removed, Modified, Read).</p> <p>For additional actions, navigate to Advanced mode. See Advanced Mode for more information.</p>
 WHAT	<p>Specify an object name (e.g., <i>Policy</i>) to find all entries containing it (e.g., <i>HiSecPolicy</i>, <i>\\FileServer\Share\NewFolder\NewPolicy.docx</i>, <i>http://sharepoint/sites/collection1/Lists/Policy</i>).</p> <p>NOTE: Netwrix Auditor searches across all data sources.</p> <p>For an exact match, use quotation marks and provide an object name in the format that is typical for your data source (e.g., "<i>HiSecPolicy</i>").</p>
 WHEN	<p>Filter data by the time interval when the change occurred.</p> <p>Specify a timeframe or provide a custom date range. Netwrix Auditor allows you to see changes that occurred today, yesterday, in the last 7 or 30 days, or within the specified date range.</p>
 WHERE	<p>Specify a resource name (e.g., <i>Enterprise</i>) to find all entries containing it (e.g., <i>Enterprise-SQL</i>, <i>FileStorage.enterprise.local</i>). The resource name can be a FQDN or NETBIOS server name, Active Directory domain or container, SQL Server instance, SharePoint farm, VMware host, etc.</p> <p>NOTE: Netwrix Auditor searches across all data sources.</p> <p>For an exact match, use quotation marks and provide a resource name in the</p>

Filter	Description
--------	-------------

format that is typical for your data source (e.g., "Enterprise-SQL").

To add a filter to your search

1. Click a filter type icon. Enter a value you want to search for.

Alternatively, you can type a value directly into the **Search** field.

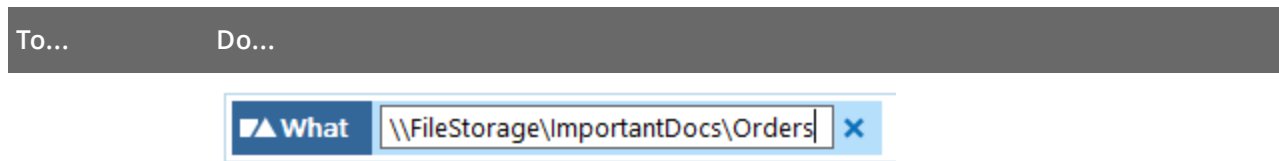
- For exact match, use quotation marks.
- To further restrict your search, right-click the value and select a filter from the pop-up menu. To search across all columns in the results view (everywhere—**Who**, **What**, **Where**, **Action**, etc.), leave it as is.

2. Click **Search** to apply your filters. By default, all entries that contain the filter value are shown.

3.2.2. Modifying and Removing Filters

To...	Do...
-------	-------

Modify filter	Double-click the filter and type a new value.
---------------	---



NOTE: If you need to modify the **When** filter, delete it and add a new value, or navigate to the **Advanced** mode (Simple mode does not support its modification).

Remove filter Click the **Close** icon next to it.



3.2.3. Exporting and Importing Filters

To export or import filters as regular expressions, use the **Tools** menu commands:

To...	Use...
Export	Copy search — copies the search filters that are currently applied to your search. This can be helpful if you want to share your search with a colleague (e.g., by pasting it in an email) or to modify a saved search query with your current filters.
Import	Paste search — pastes the search filters you copied before. These can be filters copied from a previous search or those someone shared with you.

3.3. Customize View

Having reviewed the search results, you can modify the way the data is presented, for example, hide a column or change its position, or hide the Details pane on the right.

To modify view:

1. Navigate to **Tools**
2. Click **Select columns**. The dialog that opens shows the search columns currently selected for display.
3. Check the columns you want to include and clear unwanted ones.
4. Set the order of displayed columns using arrows on the right.
5. Click **Hide details** if you want to hide the Details pane with the activity record and user (initiator) account details.
6. To restore the original view configuration, click **Restore Default**.

3.4. Advanced Mode

Netwrix Auditor provides an advanced set of filters and match type operators that enable you to customize your searches even more precisely.

Switch to **Advanced mode** to review your current search in details and modify it if necessary. Click **Add** to add a new filter to your search.

Review the following for additional information:

- [Apply Additional Filters](#)
- [Search Conditions](#)

3.4.1. Apply Additional Filters

Expand the **Filter** list to find additional filters or filter values. The most commonly used filters are described in [Use Filters \(Simple Mode\)](#). Review the following for additional information:

Filter	Description	Example
Action	<p>Limits your search to the selected actions only.</p> <p>Specify an action from the Value list or type it yourself. The Action filter in the Advanced mode contains actions besides those available in basic mode (added, modified, removed, and read). Reported actions vary depending on the data source and object type. See Netwrix Auditor Administration Guide for more information.</p> <ul style="list-style-type: none"> • Added • Removed • Modified • Read • Moved • Renamed • Add (Failed Attempt) • Remove (Failed Attempt) • Modify (Failed Attempt) • Read (Failed Attempt) • Move (Failed Attempt) • Rename (Failed Attempt) 	<p>You are investigating suspicious user activity. You have already identified the intruder and now you want to see if any files were deleted or moved, and emails sent.</p> <p>Since you are interested in specific actions only, set the Action filter to Removed, Moved, and Sent.</p>

Filter	Description	Example
	<ul style="list-style-type: none"> • Checked in • Discard check out • Failed Logon • Copied • Activated 	<ul style="list-style-type: none"> • Checked out • Successful Logon • Logoff • Sent
Object type	<p>Limits your search to objects of a specific type only.</p> <p>Specify an object type from the Value list or type it yourself. This filter modifies the What filter.</p> <p>The value list is prepopulated with the most frequent object types.</p>	<p>You noticed that some domain policies were changed and you want to investigate this issue.</p> <p>Your What filter is set to <i>Policy</i>, and so you keep receiving search results such as <i>HiSecPolicy</i>, <i>\\FS\\Share\\NewPolicy.docx</i>, <i>http://corp/sites/col1/Lists/Policy</i>. These entries correspond to different object types and data sources.</p> <p>Since you are looking for GPOs only, select GroupPolicy from the Value list.</p>
Data source	<p>Limits your search to the selected data source only.</p> <p>Specify a data source from the Value list or type it yourself.</p>	<p>You are investigating suspicious user activity. A user specified in the Who filter made a lot of changes across your IT infrastructure, so the search results became difficult to review.</p> <p>Since you are only interested in the way this user's activity could affect your Active Directory domain and Exchange organization, set the Data source filter to Active Directory and Exchange to limit the search results.</p>
Monitoring plan	<p>Limits your search to the selected plan only.</p> <p>Specify the name from the Value list or type it yourself.</p>	<p>You are investigating suspicious user activity. A user specified in the Who filter made a lot of changes across your IT infrastructure, so the search results became difficult to review.</p> <p>Since you are only interested in the way this user's activity could affect file shares audited within a single plan, set the</p>

Filter	Description	Example
		Monitoring plan filter to <i>"My servers"</i> to limit the search results.
Item	<p>Limits your search to the selected item only.</p> <p>This filter can be helpful if have several items of the same type in your monitoring plan (e.g., two Active Directory domains).</p> <p>Specify the name from the Value list or type it yourself.</p>	<p>Your monitoring plan is configured to track domains and includes your secured corporate domain and a domain for temporary employees. You are investigating who logged in your secured corporate domain outside business hours.</p> <p>You can set the Item filter to this domain name to limit the search results and exclude logons to computers from a less important domain.</p>
Working hours	<p>Limits your search results to entries that occurred within the specified hours.</p> <p>You can use this filter together with When if you need, for example, to search for activity in the non-business hours during the last week.</p>	<p>You are investigating an incident and want to know who accessed sensitive data outside business hours.</p> <p>You can set this filter as <i>Not equal to</i> and specify the time interval from <i>8:00 AM</i> to <i>6:00 PM</i>. Filtered data will include only operations that occurred outside this interval, that is, during non-business hours.</p>
Details	<p>Limits your search results to entries that contain the specified information in the Details column.</p> <p>The Details column normally contains data specific to your target, e.g., assigned permissions, before and after values, start and end dates.</p> <p>This filter can be helpful when you are looking for a unique entry.</p>	<p>You discovered that a registry key was updated to <i>"242464"</i>. Now you want to investigate who made the change and what the value was before.</p> <p>You can set the Details filter to <i>242464</i> to find this change faster.</p>
Before*	Limits your search results to entries that contain the specified before value in the Details column.	<p>You are investigating an incident in which the SAM- account- name attribute was changed for an account in your Active Directory domain.</p> <p>You can set the Before filter to the previous name (e.g., <i>John2000</i>) to find the new name faster.</p>

Filter	Description	Example
After*	Limits your search results to entries that contain the specified after value in the Details column.	<p>You are investigating a security incident and want to know who enabled a local Administrator account on your Windows Server.</p> <p>You can set the After filter to this account's current state (e.g., <i>Enabled</i>) to find this change faster.</p>
Everywhere	Limits your search results to entries that contain the specified value in any column.	<p>You are investigating a security incident. You have already identified the intruder (e.g., <i>BadActor</i>) and now you want to see all actions made by intruder's account or with it.</p> <p>Since the intruder can be the actor (Who), the object (What), or can even show up in details, set the Everywhere filter to intruder's name.</p>

* – If you plan to audit an SQL Server for data changes and browse the results using 'Before' and 'After' filter values, make sure that the audited SQL database tables have a primary key (or a unique column). Otherwise, 'Before' and 'After' values will not be reported.

3.4.2. Search Conditions

When you apply filters at search, you can specify operators that should be used as conditions for data you want to retrieve and compare with the certain filter value. A condition can be, for example, **Contains**, **Starts with**, and so on.

The following operators can be used to specify search conditions:

30/87

Operator	Description	Example
	operator appears as not , e.g., Who not for the Who filter.	specified and find all changes performed by other users, e.g., <i>Domain1\Johnson</i> , <i>Domain2\John</i> .
Starts with	This operator shows all entries that start with the specified value.	If you set the Who filter to starts with <i>Domain1\John</i> , you will find all changes performed by <i>Domain1\John</i> , <i>Domain1\Johnson</i> , and <i>Domain1\Johnny</i> .
Ends with	This operator shows all entries that end with the exact specified value.	If you set the Who filter to ends with <i>John</i> , you will find all changes performed by <i>Domain1\John</i> , <i>Domain2\Dr.John</i> , <i>Domain3\John</i> .
Does not contain	<p>This operator shows all entries except those that contain the specified value.</p> <p>NOTE: In the Search field in the Simple mode, this operator appears as not, e.g., Who not for the Who filter.</p>	If you set the Who filter to does not contain <i>John</i> , you will exclude the following users: <i>Domain1\John</i> , <i>Domain2\Johnson</i> , and <i>Johnny@domain.com</i> .
In group	This operator relates to the Who filter. It instructs Netwrix Auditor to show only data for the accounts included in the specified group.	If you set the In group condition for Who filter to <i>Domain\Administrators</i> , only the data for the accounts included in that group will be displayed.
Not in group	This operator relates to the Who filter. It instructs Netwrix Auditor to show only data for the accounts not included in the specified group.	If you set the Not in group condition for Who filter to <i>Domain\Administrators</i> , only the data for the accounts not included in

Operator	Description	Example
		that group will be displayed.

NOTE: When you add a new search filter, the **Contains** operator is used by default.

To modify conditions for the selected filters, make sure you have switched to the Advanced search mode.

Filter	Operator	Value
Who	Not equal to	Enterprise\Administrator
Action	Equals	Modified
What	Ends with	SecPolicy
Data source	Equals	Active Directory
Before	Equals	Success

Open in new window SEARCH Simple mode

The image below represents the same search filters as they are shown in the **Search** field in the **Simple** mode.

Action "Modified" What SecPolicy Data source "Active Directory" Before "Success" Who not "Enterprise\Administrator"

3.5. Include and Exclude Data

Having reviewed the search results, you can proceed with your investigation by excluding or including data. Excluding a filter value is helpful if you want to skip it in your search results (e.g., a service account or trusted user account). On the other hand, including a filter value ensures that only the entries containing it will be shown (e.g., a suspicious user or potentially violated folder).

To include or exclude data

1. Review your search results and locate an entry with data you want to exclude or include.
2. Select this entry and review details.
3. Click **Exclude from search** or **Include to search** and specify a filter value from the list.
4. Click **Search** to update the search results.

Your exclusions and inclusions will automatically be added to the search filters, limiting the amount of data shown in the results pane.

Details

Full screen...

Activity record details

Data source: Active Directory
Monitoring plan: AD Monitoring
Item: enterprise.local (Domain)

Who: ENTERPRISE\administrator

Object type: group

Data source: Active Directory

Monitoring plan: AD Monitoring

Item: enterprise.local (Domain)

Action: Modified

What: \local\enterprise\Users\Enterprise Ad...

Where: enterprisedc.enterprise.local

When: 9/26/2018 3:44:09 AM

Exclude from search

Include in search

3.6. Save Search Query Results

You can export your search query results, save them as a custom report, subscribe to periodic delivery of this search results, create a search-based alert.

Navigate to **Tools** in the top right corner of the Search window and select the required action.

Use...	To...
Save as report	Save your search results as custom reports. See Custom Search-Based Reports .
Create alert	Create an alert with the same set of filters you have just specified for your search. Create Alerts
Subscribe	Create subscription for periodic delivery of the search query results. See Subscriptions
	NOTE: Subscription to the search results is not the same as creation of a custom report using this search.
Export data	Save your search results as a <i>.pdf</i> or <i>.csv</i> file. All audit data from your search query results will be exported (unlike the interactive view which is limited to the top 2,000

Use...	To...
--------	-------

entries).

NOTE: When exporting large amount of data (e.g., changes made by a newly retired employee during the last 8 months), it is recommended to use .csv format.

4. Reports and Report Packs

Netwrix Auditor provides a variety of reports for each data source. This helps you keep track of all changes in your IT infrastructure and validate compliance with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.). You can also create your custom reports based on the **Interactive Search** technology.

NOTE: To review intelligence data, you must be assigned the Global administrator or Global reviewer role in the product. The users assigned the Reviewer role on a certain plan or folder have a limited access to data—only within a delegated scope. See [Netwrix Auditor Administration Guide](#) for more information.

Review general report types available in Netwrix Auditor to meet your specific business needs:

Report type	Description
Predefined reports	Predefined reports pack contains over a hundred SSRS-based reports grouped by business categories and data sources. Predefined reports are helpful if you are looking for a ready-to-use template for your business needs. See Predefined Reports for more information.
Compliance reports	For your convenience, specific reports are grouped into folders by corresponding international standards and regulations such as security controls, information security, etc. See Compliance Reports for more information.
Custom reports	For your convenience, the Reports section has been enhanced with Custom reports. Initially, the product provides templates for the best common workflows within Netwrix Auditor. Later, you can always create custom report from interactive search and find them here. See Custom Search-Based Reports for more information.

4.1. Viewing Reports

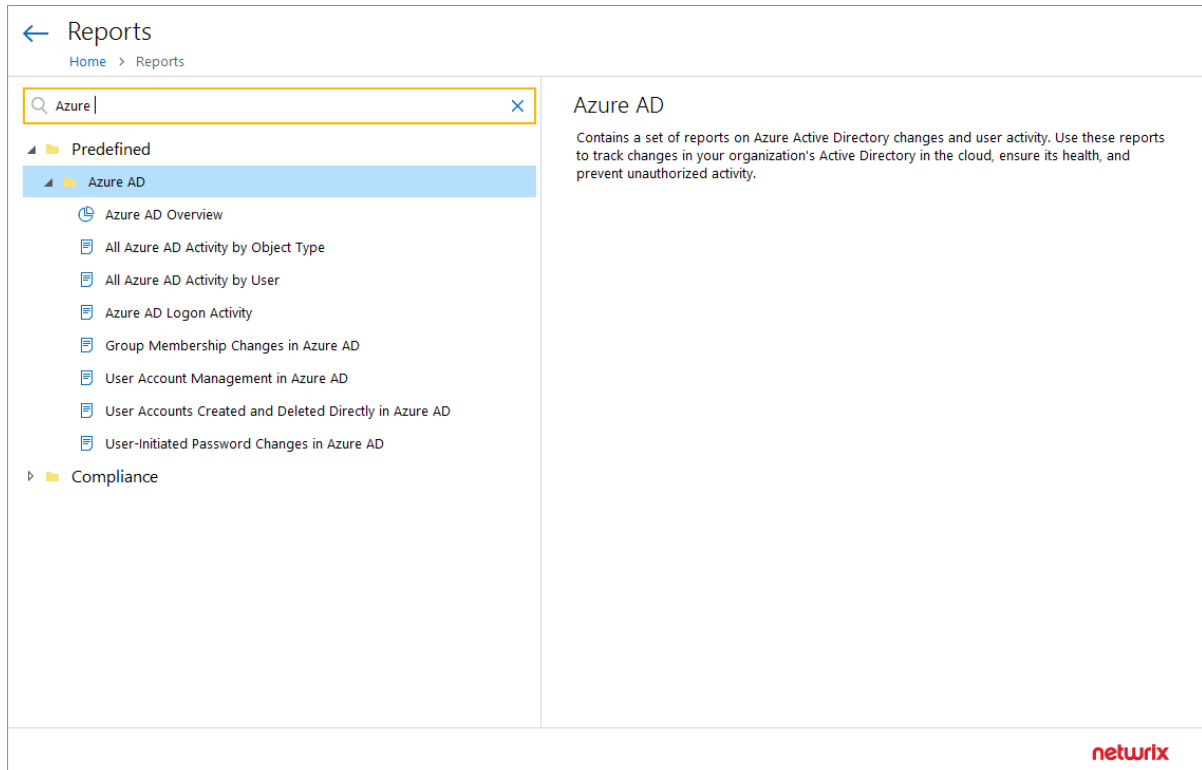
To view reports, users need the following:

1. Sufficient access rights in Netwrix Auditor, which are provided through role assignment:
 - Users with *Reviewer* role can generate the reports for their delegated scope only, and view them in any Netwrix Auditor client or in a web browser.
 - Users with *Global administrator* or *Global reviewer* role can also create subscriptions to reports.
2. The **Browser** role on the SSRS Report Server. See [Netwrix Auditor Installation and Configuration Guide](#) for more information.

To view a report

1. In Netwrix Auditor main screen, navigate to the **Reports** tile, and in the tree on the left select the report you need.

TIP: To speed up the process, you can use the **Search** field, entering the keyword to search by.



2. Click **View** button in the right pane.

To learn how to subscribe to a report, see [Create Subscriptions](#).

4.1.1. Troubleshooting

If no data is displayed in the report, you may need to do the following:

1. Make sure that the Audit Database settings are configured properly in the monitoring plan, and that data is written to databases that reside on the default SQL Server instance. See [Audit Database](#) and [Database Settings](#) for details.
2. For SSRS-based reports - verify that SSRS (SQL Server Reporting Services) settings are configured properly. See [Audit Database](#) for details.
3. For state-in-time reports - verify that the monitoring plan that provides data for the report has the corresponding option selected. See [Settings for Data Collection](#) for details.

4.1.2. Using Report Filters

Report filters allow you to display changes matching certain criteria. For example, you can filter changes by audited domain or object type. Filtering does not delete changes, but modifies the report view, allowing you to see changes you are interested in.

For example, you can update report timeframe, select specific values for *Who* and *Where*, apply sorting, etc.

Filters can be found in the upper part of the **Preview Report** page:

Filter	Value
Data Source:	%
Time Zone:	UTC-07:00
From:	9/29/2019 12:00:01 AM
To:	9/30/2019 11:59:59 PM
Who (Domain\User):	%
What:	%
Where:	%
Object Type:	%

To apply filters

1. Navigate to **Reports**, select the report you need and click **View**.
2. Specify filters to apply to the report, and click **View Report**.

When applying filters, mind the following:

- Wildcards are supported.
For example, if you want to view changes made by users with the name containing "administrator" (e.g., *enterprise\administrator*, *corp\administrator*, *sqladmin*), type *%admin%* in the **Who (domain\user)** filter field.
- *escape_characters* are not supported.
- Do not use % in the exclusive filters (e.g., *Who (Exclude domain\user)*). Otherwise, you will receive an empty report.

4.2. Predefined Reports

Netwrix Auditor is shipped with 250+ ready-to-use reports designed by Netwrix industry experts. To find a report that is right for you, check out the predefined report types available in the product.

- **Enterprise Overview**—A dashboard with a set of widgets that provide quick access to important statistics across the audited IT infrastructure. They allow you to see the activity trends by date, user, data source, server or audited IT system, and drill through to detailed reports for further analysis. The **Enterprise Overview** dashboard aggregates the information on changes from all data sources and provides a centralized overview. System-specific dashboards reflect all changes across all monitoring plans where audit of this target system is enabled. See [Overview Dashboards](#) for more information.
- **Organization level reports**—High-level reports that aggregate data from all data sources and monitoring plans. They list all activity that occurred across the audited IT infrastructure. **Enterprise Overview** provides bird's eye view of changes and activity from all data sources and provides a centralized overview. See [Organization Level Reports](#) for more information.
- **Overview diagrams**—System-specific diagram reports that aggregate audit data for an auditing system. They provide a high-level overview of changes within a selected time period. Overviews consist of four charts, showing the activity trends by date, user, object type or server, and drill through to detailed reports for further analysis. See [Overview Dashboards](#) for more information.
- **Change and activity reports**—System-specific reports that aggregate audit data for a specific data source within specified monitoring plans. These reports show detailed data on changes and activity and provide grouping, sorting and filtering capabilities. Each report has a different set of filters allowing you to manage collected data in the most convenient way. See [Change and Activity Reports](#) for more information.
- **State-in-time reports**—System-specific reports that aggregate data for a specific data source within a specified individual monitoring plan and allow reviewing the point-in-time state of the data source. These reports are based on daily snapshots and help you paint a picture of your system configuration at a specific moment in time. See [State-in-Time Reports](#) for more information. Currently, the Windows Server State-in-Time report set provides baselining functionality that help identify aberrant servers. See [Baseline Reports](#) for more information.
- **Changes with video reports**—Windows server-based reports that provide video recordings of user activity on audited computers. See [Reports with Video](#) for more information.
- **Changes with review status reports**—Both system-specific and overview reports that can be used in the basic change management process. These reports allow setting a review status for each change and providing comments. See [Interactive Reports for Change Management Workflow](#) for more information.

Review the following for additional information:

- Refer to [Viewing Reports](#) for detailed instructions on how to find the report you need and view reports in a web browser.
- Refer to [Using Report Filters](#) for detailed instructions on how to apply filters to reports.

4.2.1. Overview Dashboards

Overview dashboards offer a bird's eye view of your IT infrastructure. They allow you to see activity trends by date, user, object type, server or data source, and drill down to detailed reports for further analysis.

The **Enterprise Overview** dashboard includes diagrams that aggregate data on all monitoring plans and all data sources, while system-specific dashboards provide quick access to important statistics within one data source. All dashboards support the drill-down functionality: by clicking on a widget with diagram, you will be redirected to a report (with the corresponding filtering and grouping of data) that renders the next level of detail.

Currently, Netwrix Auditor offers the following dashboard reports:

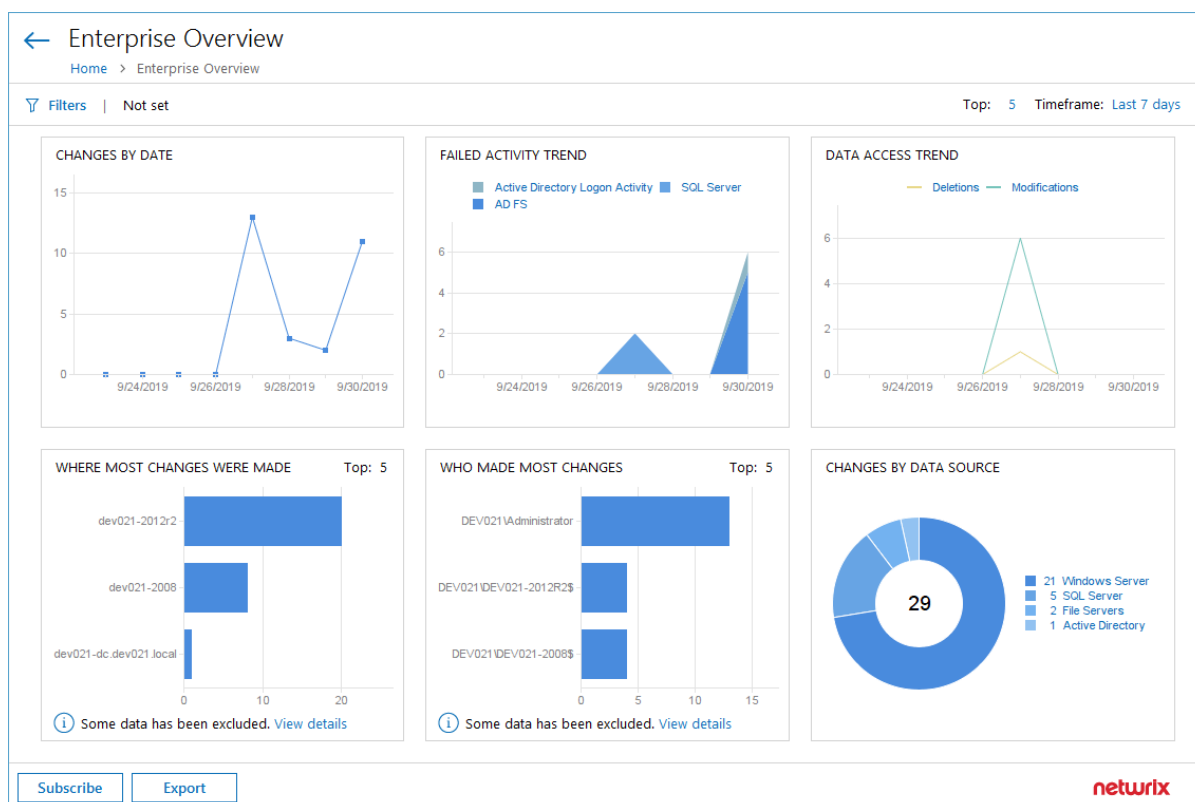
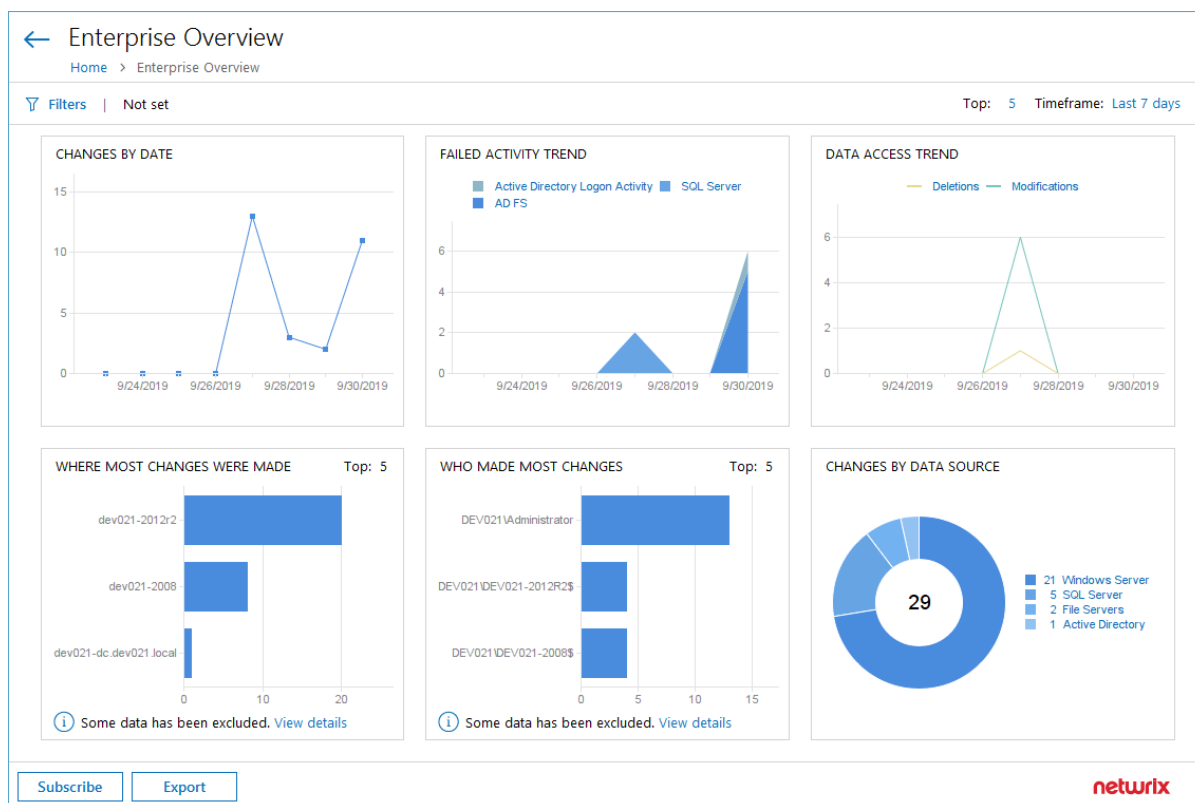
- Enterprise Overview
- Active Directory
- Active Directory Federation Services (AD FS)
- Azure AD
- Exchange
- File Servers (includes Windows File Servers, EMC, and NetApp)
- Office 365 (includes Exchange Online and SharePoint Online)
- Oracle Database
- SharePoint
- SQL Server
- VMware
- Windows Server

To open a dashboard

1. In the **Reports** window, search for *overview* keyword, using the search field. Click the search result you need - for example, Active Directory Overview or File Servers Overview.

TIP: To open the **Enterprise Overview** dashboard, just click the **Enterprise Overview** tile in the main Netwrix Auditor page.

2. To fine-tune the dashboard, you can apply **Filters** or use the **Top** and **Timeframe** parameters in the upper-right corner of the dashboard window.
3. Click the widget to drill down to the detailed report on your area of interest.

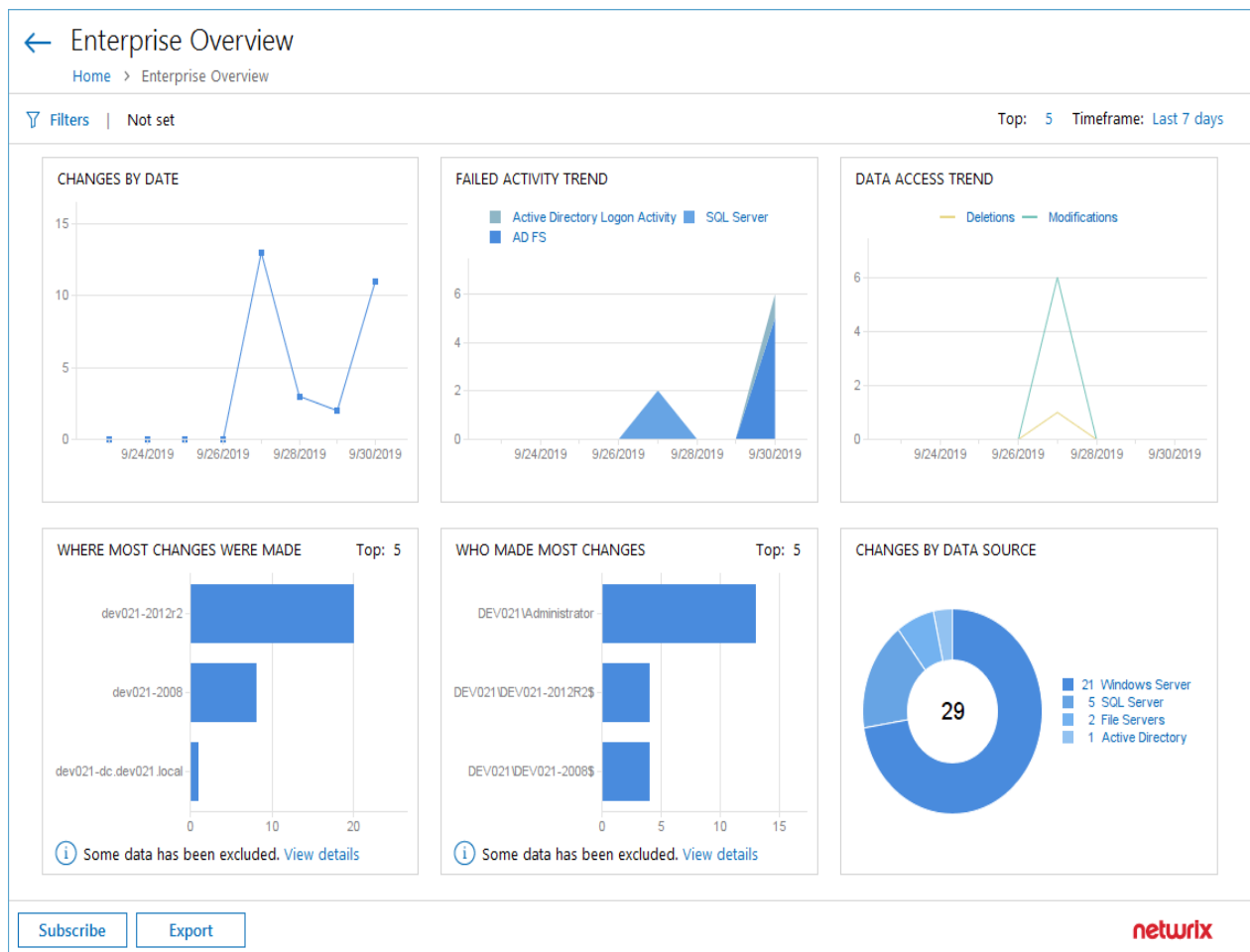


To review the data source-specific diagrams

- Navigate to **Reports** and select one of the following locations:

Title	Location
Enterprise Overview	Organization Level Reports
Active Directory Overview	Active Directory → Active Directory Changes
Azure AD Overview	Azure AD
Exchange Overview	Exchange
Office 365 Overview	Exchange Online SharePoint Online
File Servers Overview	File Servers → File Servers Activity
Oracle Database Overview	Oracle Database
SharePoint Overview	SharePoint
SQL Server Overview	SQL Server
VMware Overview	VMware
Windows Server Overview	Windows Server → Windows Server Changes

NOTE: The example below applies to **Enterprise Overview**.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.

4.2.2. Organization Level Reports

Organization Level reports aggregate data on all monitoring plans and list changes and activity that occurred across all data sources. Also, this folder includes a report on Netwrix Auditor self-audit - it provides detailed information on changes to monitoring plans, data sources and audited items.

Organization Level reports can be found in the **Organization Level Reports** folder under the **Reports** node.

This folder includes:

Report	Details
Enterprise Overview	Dashboard report with diagrams showing all activities and changes across the monitored data sources.

Report	Details
	See also Overview Dashboards
All Activity with Review Status	Shows all activity across the entire IT infrastructure, including changes, read access and logons. Features interactive review status to supplement your change management workflow. See also Interactive Reports for Change Management Workflow .
All Changes by Data Source	Shows all changes across your IT infrastructure, grouped by data source.
All Changes by Server	Shows all changes across the entire IT infrastructure, grouped by the server where the change was made.
All Changes by User	Shows all changes across your IT infrastructure, grouped by the user who made the change.
All Integration API Activity	Shows all activity records imported with Netwrix Auditor Integration API.
Netwrix Auditor Self-Audit	Help to ensure that the scope of data to be audited is complete and all changes are in line with the workflows adopted by your organization.

NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.


4.2.3. Change and Activity Reports

Change and activity reports provide information on changes to different aspects of the audited environment. Depending on the data source, navigate to one of the following locations, or use the search field to look for the keywords you need:

Data source	Report location
Active Directory	Active Directory → Active Directory Changes
Active Directory Federation Services	Active Directory Federation Services (AD FS)

Data source	Report location
Azure AD	Azure AD
Group Policy	Active Directory → Group Policy Changes
Exchange	Exchange
Exchange Online	Exchange Online
File Servers	File Servers → File Servers Activity
Oracle Database	Oracle Database
SharePoint	SharePoint
SharePoint Online	SharePoint Online
SQL Server	SQL Server
VMware	VMware
Windows Server	Windows Server → Windows Server Changes
Event Log	Windows Server → Event Log
IIS	Windows Server → Event Log
Logon Activity	Active Directory → Logon Activity
Integration API	Organization Level Reports
Netwrix Auditor self-audit	Organization Level Reports

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.




Netwrix Auditor

Monday, April 24, 2017 3:27 AM

All Active Directory Changes

Shows changes to all Active Directory objects, including changes to permissions, configuration, etc. This is the most comprehensive report on Active Directory changes. Use it when you need to review every single change to any Active Directory object. Apply the flexible filters to narrow the results.

Filter	Value

Action	Object Type	What	Who	When
 Added	user	\\local\corp\Users\Michael MT. Tompson	CORP\administrator	4/7/2017 5:31:25 AM
Where:		rootdc2.corp.local		
 Modified	group	\\local\corp\Users\Domain Admins	CORP\administrator	4/7/2017 5:31:56 AM
Where:		rootdc2.corp.local		
Security Global Group Member:		<ul style="list-style-type: none"> Added: "corp.local/Users/Michael MT. Tompson" 		

NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.

4.2.4. State-in-Time Reports

The state-in-time reports functionality allows generating reports on the system's state at a specific moment of time in addition to change and activity reports. State-in-time reports are based on the daily configuration snapshots, and reflect a particular aspect of the audited environment.

This functionality is currently available for the following data sources:

- Active Directory
- File Servers
- Exchange Online
- Windows Server
- SharePoint
- SharePoint Online
- Group Policy
- SharePoint
- SQL Server


- Office 365
- VMware

IMPORTANT! To provide data for state-in-time reports, remember to select the **Collect data for state-in-time reports** option when you configure a monitoring plan for the selected data source. See [Settings for Data Collection](#) for more information.

The state-in-time reports are available under the **Reports** node. Depending on the data source, navigate to the corresponding subfolder, for example, **Predefined → Active Directory → Active Directory — State-in-Time**.

Data source	Report location
Active Directory	Predefined → Active Directory → Active Directory State-in-Time
Group Policy	Predefined → Active Directory → Group Policy—State-in-Time
Exchange Online	Predefined → Exchange Online → Exchange Online—State-in-Time
File Servers	Predefined → File Servers → File Servers—State-in-Time
SharePoint	Predefined → SharePoint → SharePoint—State-in-Time
	<p>NOTE: The Account Permissions in SharePoint and SharePoint Object Permissions state-in-time reports list detailed permissions and permission levels by user account. See Means Granted for more information.</p>
SharePoint Online	Predefined → SharePoint Online → SharePoint Online—State-in-Time
SQL Server	Predefined → SQL Server → SQL Server—State-in-Time
Windows Server	Predefined → Windows Server → Windows Server—State-in-Time
	<p>Most reports in this set provide baselining capabilities. See Baseline Reports for more information.</p>
VMware	Predefined → VMware → VMware —State-in-Time

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.


Netwrix Auditor
Tuesday, March 05, 2019 8:49 AM

File Shares on Windows Servers


Lists file shares on your Windows servers, grouped by server. For each file share, the following is reported: the share name, its path, and the share type. Use this report to detect non-default shares and exercise security control over your data.

Server: [srv01](#)

Share Name	Share Path	Share Type
Netwrix_Auditor_Subscriptions\$	C:\ProgramData\Netwrix Auditor\Data\Subscriptions	Shared Folder
Netwrix_UAVR\$	C:\ProgramData\Netwrix Auditor\Data\User Activity Video Reporter	Shared Folder
SharedReports	C:\Share	Shared Folder

Server: [srv2012r2](#)

Share Name	Share Path	Share Type
Shared	D:\Shared	Shared Folder



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.

By default, state-in-time reports reflect the current state of the data source. If you want to generate a report to assess your system at a particular moment in the past, you can select the corresponding snapshot from the **Snapshot Date** filter.

NOTE: To be able to generate reports based on different snapshots, ask your Netwrix Auditor Global administrator to import historical snapshots to the Audit Database, otherwise only the **Current Session** option is available in the drop-down list.

When auditing file servers, changes to both access and audit permissions are tracked. To exclude information on access permissions, contact your Netwrix Auditor Global administrator or Configurator of this plan.

4.2.4.1. Baseline Reports

Most reports in **Windows Server—State-in-Time** folder allow you to specify baselines. A *baseline* defines a certain safe level or state. If a server parameter falls below it, it is considered a threat or at least merits your special attention. With baselines specified right in report filters, you can easily identify servers that are different from your corporate policies or best practices. Risks are marked with red color and are easy to spot in the report.

Filter		Value	
Server	OS Name	OS Version	Antivirus Status
EnterpriseDC.enterprise.local	Microsoft Windows Server 2008 R2 Enterprise	6.1.7601	Issues Detected
ENTERPRISEDC1.enterprise.local	Microsoft Windows Server 2012 Standard	6.2.9200	Issues Detected
stationwin16.enterprise.local	Microsoft Windows Server 2016 Standard	10.0.14393	Issues Detected

You can specify baseline values specific to your organization in one of the following ways:

- As a baseline filter value in the report filters. Baselines in the field should be separated by commas.

While inputting text inline is easy, your baseline values will not be preserved for the next report generation. You will have to input them every time you generate a report. This method is recommended you plan to subscribe to this report.

- In a special file stored on the computer where your Audit Database resides.

To secure your baseline values for the next report runs, create a text file with baselines; baselines in this file should on a separate line. In the report, provide a link to this file inside the baseline filter. You should create a separate file for each baseline. In this case, the baselines will be reused every time you run the report.

NOTE: Make sure the account running your SQL Server instance service with Audit Database has permissions to access the baseline file. Otherwise, Netwrix Auditor will not be able to process them.

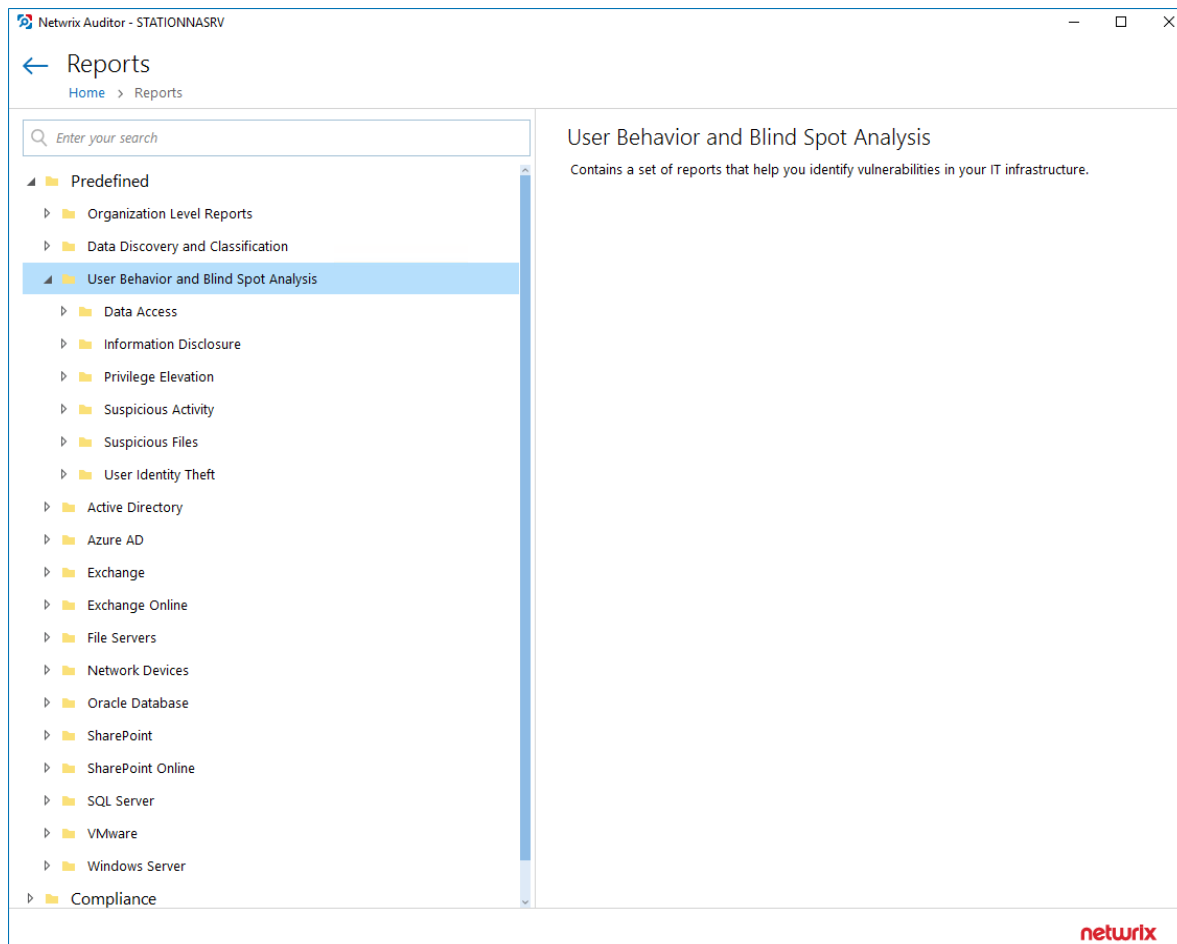
To learn more about state-in-time reports, refer to [State-in-Time Reports](#).

4.2.5. User Behavior and Blind Spot Analysis Reports

The **User Behavior and Blind Spot Analysis** report pack contains a set of smart reports that help you identify vulnerabilities and easily answer questions such as:

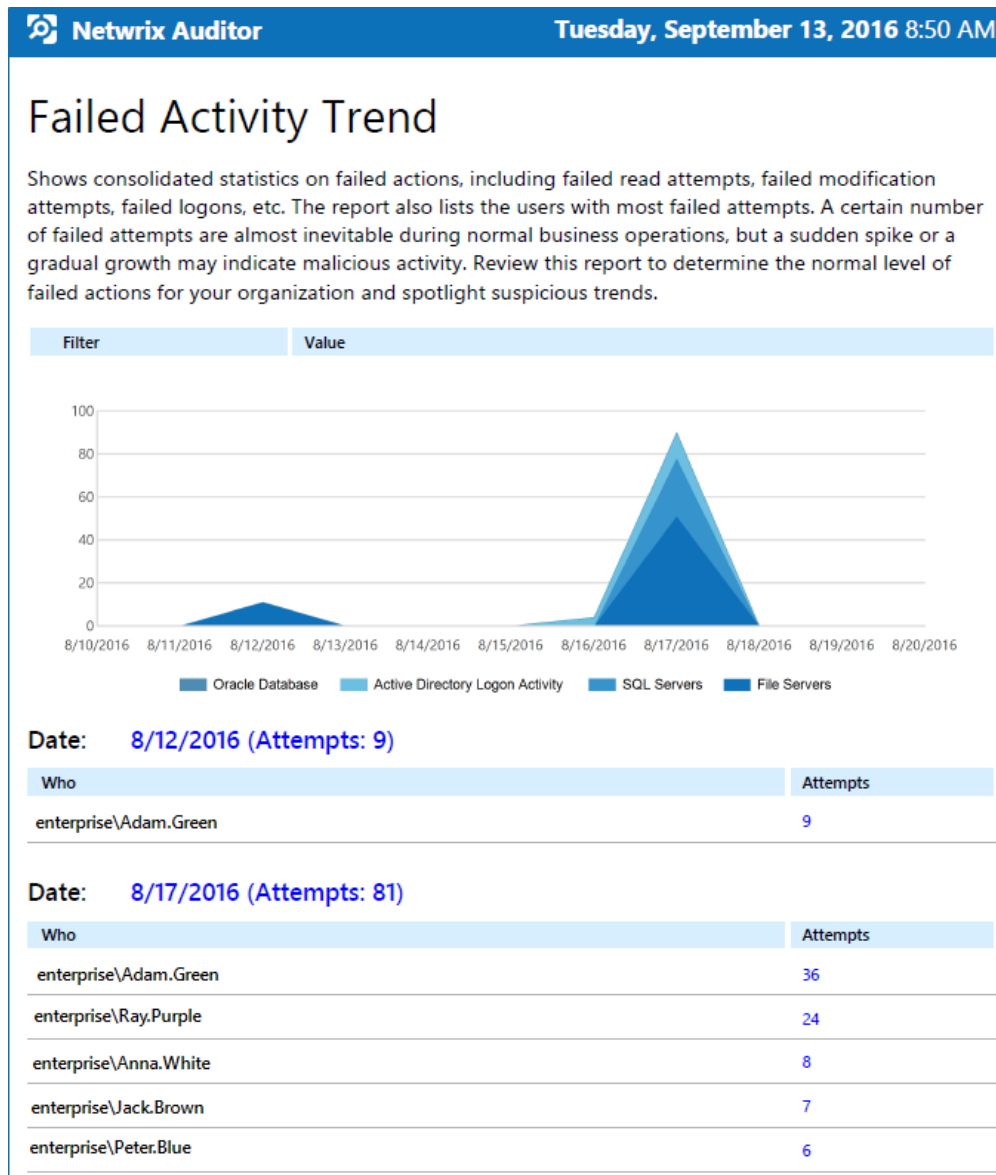
- Has there been any abnormal access to sensitive data?
- Is anyone accessing stale data?
- Have there been any unusual spikes in failed activity?
- Who is active outside of business hours and what are they doing?
- Has anyone put harmful files on corporate data storage?
- Are there any files likely to contain credentials, Social Security numbers, PHI or other sensitive data?

Analytics reports can be found in the **User Behavior and Blind Spot Analysis** folder under the **Predefined** node.



NOTE: If you are sure that some audit data is missing (e.g., you do not see information on your file servers in reports and search results), verify that the Audit Database settings are configured and that data is written to databases that reside on the default SQL Server instance.

By default, Netwrix Auditor allows generating reports and running interactive searches on data collected in the last 180 days. If you want to investigate incidents that occurred more than 180 days ago, ask your Netwrix Auditor Global administrator to import that data from the Long-Term Archive.



NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.

4.2.6. Interactive Reports for Change Management Workflow

Change management is one of the critical processes for many companies referring to such areas as requesting, planning, implementing, and evaluating changes to various systems. For your change management workflow, Netwrix Auditor offers several reports with interactive capabilities – not only they list changes in your infrastructure but also allow you to track, analyze, assign appropriate status and comment on these changes.

This capability can supplement your organization's workflow of monitoring and resolving potential issues through the following automated course of action:

1. The reported changes to the monitored environment are assigned the **New** status by default.
2. If a change seems unauthorized, or requires further analysis, you can click the **Click to update status** link next to the change detailed data:

Netwrix Auditor - All Windows Server Changes with Review Status

← Preview Report

Netwrix Auditor

All Windows Server Changes with Review Status

Shows all Windows Server changes with their review status. You can review changes to your IT infrastructure and track team workflows by making changes.

Action	Object Type	What
Added	Add or Remove Programs	Add or Remove Programs
Where: stationwin16.enterprise.local		
Installed For: "All users"		
Version: "44.0.2510.1218"		
Review status: New		
Removed	Add or Remove Programs	Add or Remove Programs
Where: stationwin16.enterprise.local		
Installed For: "All users"		
Version: "44.0.2510.1218"		
Review status: New		
Modified	Local Group	System Information\Local Groups\Remote Desktop Users
Where: stationwin16.enterprise.local		
Members: Added: "ENTERPRISE\it-operations"		
Review status: New		
Modified	Local Group	System Information\Local Groups\Remote Desktop Users
Where: stationwin16.enterprise.local		
Members: Removed: "ENTERPRISE\it-operations"		
Review status: New		
Modified	Local Group	System Information\Local Groups\Power Users
Where: stationwin16.enterprise.local		
Members: Added: "ENTERPRISE\it-operations"		
Review status: New		

[Click to update status](#)

[Click to update status](#)

[Click to update status](#)

Refresh Subscribe

Review status

Select a review status and specify your reason.

☐ New
A new change that has not been reviewed yet.

☒ In Review
This change has to be reviewed.

☐ Resolved
This change has been reviewed and the issue is closed.

Reason:

I'll be out of office for 2 weeks, so I granted additional permissions to my colleagues who will supervise this server.

OK Cancel

3. In the **Review status** dialog for selected change, set its status to **In Review** and provide a reason.
4. Once the change has been approved of, or rolled back, you can set its status to **Resolved**.

This capability is supported for the following reports:

Data source	Report location
Entire IT infrastructure	Organization Level Reports
Active Directory	Active Directory → Active Directory Changes → All Active Directory Changes with Review Status
Exchange	Exchange → All Exchange Server Changes with Review Status
SharePoint	SharePoint → All SharePoint Changes with Review Status
Windows Server	Windows Server → Windows Server Changes → All Windows Server Changes with Review Status
Group Policy	Active Directory → Group Policy Changes → All Group Policy Changes with Review Status

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.

They list

NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.

4.2.7. Reports with Video

Netwrix Auditor can be configured to capture video of user activity on the monitored computers that helps analyze and control changes made there. When you click a link, a video player opens and playback of the recorded user activity starts, showing launched applications, actions, etc.

To view reports with video, navigate to **Reports → User Activity**.

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.

Netwrix Auditor

Monday, April 24, 2017 4:49 AM

All User Activity

Shows video recordings of user activity.

Filter

Value

Who	Where	When	What
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:44:50 AM	Netwrix Auditor User Activity component
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:44:50 AM	Netwrix Auditor
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:44:59 AM	Netwrix Auditor WORKSTATIONS
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:45:01 AM	Netwrix Auditor Activity Trend
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:46:04 AM	Netwrix Auditor WORKSTATIONS
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:46:09 AM	Netwrix Auditor
CORP\Administrator	workstationsql.corp.local	4/24/2017 4:46:17 AM	Netwrix Auditor Activity

All User Activity

114450_58_2

NOTE: Each report has a set of filters which help organize audit data in the most convenient way. See [Using Report Filters](#) for more information. You can also create a subscription to any report you want to receive on a regular basis. See [Subscriptions](#) for more information.

To play a video

1. Navigate to **Reports** → **User Activity**. Select any report and click **View**.
2. Click a link in the When column.

NOTE: To open User Activity report for the selected user or server, you can also click the link in the **Who** and **Where** columns of the **All Users Activity** report.

4.3. Compliance Reports

For your convenience, besides grouping by data source the reports are grouped by compliance standards. Netwrix Auditor provides out-of-box reports that allow validating compliance with different standards and regulations, including but not limited to:

- FERPA
- FISMA/NIST SP800-53 rev4
- GDPR
- GLBA

- HIPAA
- ISO/IEC 27001
- NERC
- PCI DSS v3.2
- SOX
- CJIS

You can find **Compliance** folders under the **Reports** node in the **Compliance** folder. Each compliance folder provides overview on a selected standard, to read it, click on the folder name. Click **Read More** to learn more about mapping between these standards and Netwrix Auditor reports.

NOTE: In the report filters, select a monitoring plan you want to generate a report for. To review data sources and items included in each plan, navigate to the **Monitoring Plans** section.

Review the following for additional information:

- Refer to [Viewing Reports](#) for detailed instructions on how to find the report you need and view reports in a web browser.
- Refer to [Using Report Filters](#) for detailed instructions on how to apply filters to reports.

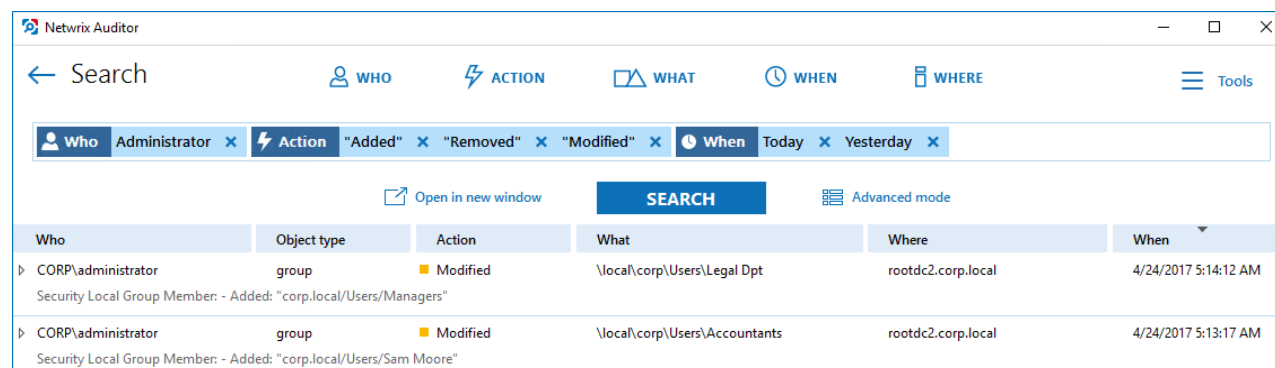
4.4. Custom Search-Based Reports

Netwrix Auditor allows you to save your favorite searches as reports to access them instantly. For your convenience, the product provides predefined templates for some popular usage scenarios. You can save your custom report or use one of the templates provided by Netwrix. Navigate to **Reports** → **Custom** to review these reports. Click **View** to generate the selected report.

Moreover, custom reports are shared between all Netwrix Auditor clients that have access to the same Netwrix Auditor Server (the main component responsible for collecting and processing audit data).

For your convenience, you can create additional folders for your custom reports. Select **Add Folder** under the **Custom** section and specify the name for a new folder. Then, select a custom report and move it to the new folder.

NOTE: The example custom report results apply to **AD or Group Policy modifications by administrator**.



The screenshot shows the Netwrix Auditor web interface. At the top, there's a search bar with filters for WHO, ACTION, WHAT, WHEN, and WHERE. The filters are set to: WHO: Administrator, ACTION: Added, Removed, Modified, WHEN: Today, Yesterday. Below the filters, there's a table with columns: Who, Object type, Action, What, Where, and When. The table contains two rows of results, both showing a group being modified by the administrator on 4/24/2017.

Who	Object type	Action	What	Where	When
CORP\administrator Security Local Group Member - Added: "corp.local/Users/Managers"	group	Modified	\\local\corp\Users\Legal Dpt	rootdc2.corp.local	4/24/2017 5:14:12 AM
CORP\administrator Security Local Group Member - Added: "corp.local/Users/Sam Moore"	group	Modified	\\local\corp\Users\Accountants	rootdc2.corp.local	4/24/2017 5:13:17 AM

Review the following for additional information:

- [To save a search as a custom report](#)
- [To modify a custom report](#)
- [To subscribe to a custom report](#)
- [To delete a custom report](#)

To save a search as a custom report

1. On the main Netwrix Auditor page, navigate to **Search**.
2. Apply filters and click **Search**.

NOTE: Refer to [View and Search Collected Data](#) for detailed instructions on how to apply filters when searching audit data.

3. Navigate to **Tools** and select **Save as report**.
4. In the **Specify a name for your custom report** dialog, specify a name. Make sure to specify a unique name.

To modify a custom report

1. On the main Netwrix Auditor page, navigate to **Reports** → **Custom**.
2. Select one of the custom reports in the list and review filters.
3. Click **View** to open search.
4. Modify filters and click **Search**.

NOTE: Refer to [View and Search Collected Data](#) for detailed instructions on how to apply filters when searching audit data.

5. Navigate to **Tools** and select **Save as report**.
6. In the **Specify a name for your custom report** dialog, specify a name. Netwrix Auditor automatically offers a previously used name so that this custom report will be overwritten. If you want to save both searches, specify a unique name for a modified search.

To subscribe to a custom report

1. Navigate to **Reports** → **Custom** and select the report you want to subscribe to.
2. Click **Subscribe** and complete the **Add Subscription to Search** wizard.


To delete a custom report

- Navigate to **Reports** → **Custom**, select a report and click **Delete**.

5. Alerts

If you want to be notified about suspicious activity, you can configure alerts that will be triggered by specific events. Alerts are sent after the specified action has been detected. Alerts are helpful if you want to be notified about actions critical to your organization security and have to mitigate risks once the suspicious action occurs.

The example alert is triggered when a new user is created in the monitored domain.



Fri 4/7/2017 4:29 PM

Administrator

Netwrix Auditor Alert: New Users

To Administrator

Netwrix Auditor Alert

New Users

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

5.1. Create Alerts

To create new alerts and modify existing alerts, the account used to connect to Netwrix Auditor Server via Netwrix Auditor client must be assigned the *Global administrator* or *Global reviewer* role in the product.

To set up a response action, this account must also be a member of the local *Administrators* group on Netwrix Auditor Server.

See [Role-Based Access and Delegation](#) for more information.

To create a custom alert

1. On the main Netwrix Auditor page, navigate to the **Configuration** section and click the **Alerts** tile.

NOTE: You can also create new alert directly from the interactive search results. Navigate to **Tools** and select **Create alert** to add a new alert with the same set of filters as your search.

2. In the **All Alerts** window, click **Add**. Configure the following:

Option	Description
General	<ul style="list-style-type: none"> Specify a name and enter the description for the new alert. <p>NOTE: Make sure that the Send alert when the action occurs option is enabled. Otherwise, the new alert will be disabled.</p> <ul style="list-style-type: none"> Apply tags—Create a set of tags to more efficiently identify and sort your alerts. Select Edit under Apply tags to associate tags with your alert. Later, you can quickly find an alert of interest using Filter by tags in the upper part of the All Alerts window. <p>NOTE: To see a full list of alerts ever created in the product, navigate to Settings → Tags.</p>
Recipients	<p>Select alert recipients. Click Add Recipient and select alert delivery type:</p> <ul style="list-style-type: none"> Email—Specify the email address where notifications will be delivered. You can add as many recipients as necessary. <p>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.</p> <ul style="list-style-type: none"> SMS-enabled email—Netwrix uses the sms gateway technology to deliver notifications to a phone number assigned to a dedicated email address. Specify email address to receive SMS notifications. <p>NOTE: Make sure that your carrier supports sms to email gateway technology.</p>
Filters	<p>Apply a set of filters to narrow events that trigger a new alert. Alerts use the same interface and logic as search.</p> <ul style="list-style-type: none"> Filter—Select general type of filter (e.g., <i>"Who"</i>, <i>"Data Source"</i>, <i>"Monitoring plan"</i>, etc.)

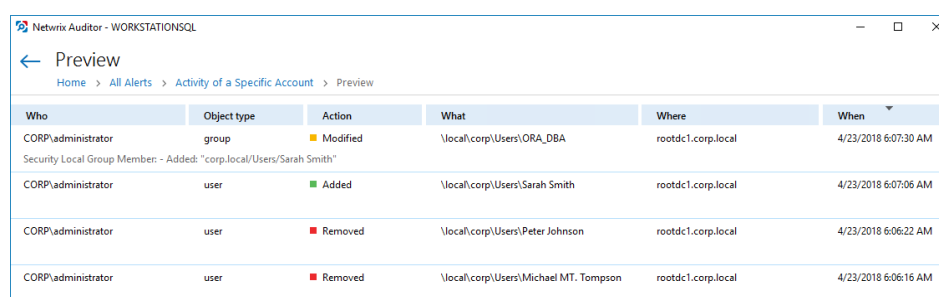
Option	Description
--------	-------------

- **Operator**—Configure match types for selected filter (e.g., "*Equals*", "*Does not contain*", etc.)
- **Value**—Specify filter value.

Refer to [View and Search Collected Data](#) for detailed instructions on how to create and modify filters.

NOTE: The Filters section contains required fields highlighted with red.

Once you completed all filters, click **Preview** on the right pane to see search-based list of events that will trigger your alert.



Who	Object type	Action	What	Where	When
CORP\Administrator	group	Modified	\\local\corp\Users\ORA_DBA	rootdc1.corp.local	4/23/2018 6:07:30 AM
Security Local Group Member: - Added: "corp.local\Users\Sarah Smith"					
CORP\Administrator	user	Added	\\local\corp\Users\Sarah Smith	rootdc1.corp.local	4/23/2018 6:07:06 AM
CORP\Administrator	user	Removed	\\local\corp\Users\Peter Johnson	rootdc1.corp.local	4/23/2018 6:06:22 AM
CORP\Administrator	user	Removed	\\local\corp\Users\Michael MT. Tompson	rootdc1.corp.local	4/23/2018 6:06:16 AM

Thresholds

If necessary, enable threshold to trigger the new alert. In this case, a single alert will be sent instead of many alerts. This can be helpful when Netwrix Auditor detects many activity records matching the filters you specified.

Slide the switch under the **Send alert when the threshold is exceeded** option and configure the following:

- **Limit alerting to activity records with the same...**—Select a filter in the drop-down list (e.g., who). Note that, Netwrix Auditor will search for activity records with the same value in the filter you selected.

NOTE: Only alerts grouped by the **Who** parameter can be included in the **Behavior Anomalies** list. Mind that in this case, the product does not summarize risk scores and shows the value you associated with this alert. This may significantly reduce risk score accuracy.


- **Send alert for <...> activity records within <...> seconds**—Select a number of changes that occurred in a given period (in seconds).

For example, you want to receive an alert on suspicious activity. You select "*Action*" in the **Limit alerting to activity records with the same** list and specify a number of actions to be considered an unexpected behavior: *1000* changes in *60* seconds. When the selected threshold exceeded, an alert will be delivered to the specified recipients: one for every 1000 removals in 60 seconds,

Option	Description
	<p>one for every 1000 failed removals in 60 seconds. So you can easily discover what is going on in your IT infrastructure.</p>
Risk Score	<ul style="list-style-type: none"> Slide the switch to On under Include this alert in Behavior Anomalies assessment. See Behavior Anomalies for more information. Associate a risk score with the alert—Assign a risk score based on the type of anomaly and the severity of the deviation from the normal behavior. An action's risk score is a numerical value from 1 (Low) to 100 (High) that designates the level of risk with 100 being the riskiest and 1 the least risky. <p>These are general guidelines you can adopt when setting a risk score:</p> <ul style="list-style-type: none"> High score—Assign to an action that requires your immediate response (e.g., adding account to a privileged group). Configure a non-threshold alert with email recipients. Above medium score—Assign to a repetitive action occurring during a short period of time. While a standalone action is not suspicious, multiple actions merit your attention (e.g., mass deletions from a SharePoint site). Configure a threshold-based alert with email recipients. Low score—Assign to an infrequent action. While a single action is safe, multiple occurrences aggregated over a long period of time may indicate a potential in-house bad actor (e.g., creation of potentially harmful files on a file share). Configure a non-threshold alert, email recipients are optional but make sure to regularly review the Behavior Anomalies dashboard. Low score—Assign to a repetitive action that does not occur too often (e.g., rapid logons). Multiple occurrences of action sets may indicate a potential in-house bad actor or account compromise. Configure a threshold-based alert, email recipients are optional but make sure to regularly review the Behavior Anomalies dashboard.
Response Action	<p>You can instruct Netwrix Auditor to perform a response action when the alert occurs — for example, start an executable file (command, batch file, or other) that will remediate the issue, or open a ticket with the help desk, and so on. For that, you will need an executable file stored locally on the Netwrix Auditor server. Slide the switch to turn the feature ON, then follow the steps described in Configure a Response Action for Alert section.</p>

5.2. Manage Alerts

For your convenience, Netwrix provides you with a set of predefined alerts that are commonly used for IT infrastructure monitoring. The out-of-the-box alerts include those that help you detect suspicious activity and inform you on critical changes to your environment. The alerts contain pre-configured filters and in most cases you only need to enable an alert and select who will receive notifications.

To...	Do...
Enable / disable an existing alert	<ol style="list-style-type: none"> 1. Select an alert from the list and enable it using the slider in the Mode column. 2. Double-click the selected alert and specify alert recipients or set a risk score want to include an alert in Behavior Anomalies assessment. You can go on with a score suggested by Netwrix industry experts or fine-tune it to fit your organization's priorities. Refer to Risk_Score for detailed instructions on how to configure scoring settings. 3. Review and update filters. For some alerts you should provide filter values, such as group name or user.
Modify an existing alert	<ul style="list-style-type: none"> • Select an alert from the list and click Edit.
Create a new alert from existing	<ul style="list-style-type: none"> • Select an alert from the list and click Duplicate at the bottom of the window.
Remove an alert	<ul style="list-style-type: none"> • Select an alert from the list and click  in the right pane.
Find an alert	<ul style="list-style-type: none"> • Use the Filter by tags option to find an alert by tags associated with this alert. <p>OR</p> <ul style="list-style-type: none"> • Use a search bar in the upper part of All Alerts window to find an alert by its name or tag.

5.3. Configure a Response Action for Alert

Upon the alert triggering, you can instruct Netwrix Auditor to run a command, a script or other executable file that will perform a remediation action, open a ticket with the organization help desk, and so on.

← Password Reset
Home > All Alerts > Password Reset

General
Recipients
Filters
Thresholds
Risk Score
Response Action

Take action when alert occurs
☒ On

Run: C:\scripts\upload.cmd

With parameters: Enter parameters (optional)

Working directory: Enter path to working directory (optional)

Options: ☒ Write data to CSV file Limit row count in a file to: 10

Credentials: By default Netwrix Auditor uses the LocalSystem account to run the executable file.
☒ Use custom credentials

User name: enterprise\wnorris

Password:

Command line preview:
C:\scripts\upload.cmd (CsvFile)

[Test run](#)

Note: {CsvFile} - path to csv-file containing activity records.

[Save & Close](#) [Save](#) [Discard](#)

netwrix

For that, configure the required settings in the **Response Action** tab of the alert properties.

1. Turn the switch **On** if you want a response action to be taken when the alert occurs.
2. In the **Run** field, specify the path to the executable file (.exe, .cmd, .bat; for .ps1 files see step 3 below). The file must be located on the machine where Netwrix Auditor server runs.
3. In the **With parameters** field, enter the parameters to be used by the executable file. Use space character as a separator.
 - To run .exe, .cmd and .bat files, you can enter the path to your command-line or batch file directly in the **Run** field, for example:

Take action when alert occurs
☒ On

Run: C:\response\upload.cmd

With parameters: 200

- To run .ps1 files, you will need to enter the path to *powershell.exe* and path to your script. For example:
 - In the **Run** field, enter `C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe`
 - In the **With parameters** field, enter
-File <path_to_your_ps_script>

Take action when alert occurs

☒ On

Run:

With parameters:

NOTE: Unless you select to **Write data to CSV file**, Netwrix Auditor will also pass the following parameters to the command line:

- *AlertID* — alert ID
- *RecordID* — ID of the activity record that triggered the alert

Selecting **Write data to CSV file** will change this behavior, as described [Writing data to CSV file](#) section below.

4. In the **Working directory** field, specify path to the working directory of the executable file on Netwrix Auditor server.

If you leave this field empty, then the path to the file specified in the **Run** field will be used as a working directory. As shown in the example with the *.ps* file, this may be the system directory. So, to avoid system directory cluttering, it is recommended not to leave the **Working directory** field empty but to explicitly specify the directory where your executable file is located, or a dedicated directory for that purpose. In the latter case, make sure the directory exists on Netwrix Auditor server.

5. **Write data to CSV file** — select this option if you want Netwrix Auditor to locate the activity records associated with the alert, and write the record fields and their values in a structured way to a *.csv* file. For each new alert being created, this option is selected by default, as well as for the predefined alerts installed with Netwrix Auditor.

NOTE: After the upgrade, all alerts with previously configured response action will have this option cleared.

6. **Limit row count in a file to <N>** — limit the number of rows (activity records) to be written to a single *.csv* file. Enter a value from 1 to 1000.

NOTE: Learn more about how these options work in [Writing data to CSV file](#) section.

7. By default, the executable file will be launched under the *LocalSystem* account. If you want to use another account, select the **Use custom credentials** checkbox and specify user name and password. Make sure this account has **Log on as batch job** privilege.
8. The resulting command line including executable file name and execution parameters will appear in the **Command line preview**:
 - If you selected to **Write data to CSV file**, the command line will include *{CsvFile}*, i.e. the file path
 - Alternatively, the command line will include *{AlertID}* and *{RecordID}*, i.e. related IDs

9. **Test run** — if you click this button, the executable file will be run with the specified parameters on Netwrix Auditor server. This can be helpful, for example, if you want to ensure script operability before the related alert is triggered.

NOTE: As there is no actual alert triggering in this case, sample alert ID and sample activity record ID will be passed to the executable file. If you selected to write data to CSV file, a sample file will be created and populated with these sample IDs.

To be able to perform the test run, current user account (logged on to Netwrix Auditor client) must have local **Administrator** privileges on Netwrix Auditor server where the executable file is located.

After the test run, you will get a notification message with the exit code. Typical values are as follows:

- **0** — the response action completed successfully
- Any other value — the response action was not a success

It is strongly recommended to apply similar logic if you plan to use custom exit codes in your response action script.

NOTE: Same exit codes will be returned by response action regular runs.

If the action is not a success (exit code is not 0), the program will try to perform response action again (up to 200 times) with increasing time interval.

5.3.1. Writing data to CSV file

In Netwrix Auditor 9.7, just the alert ID and activity record ID were passed to the executable file in order to locate the associated data in the database. With this approach, to retrieve the activity record field values (required for service ticket creation or other response actions), a user needs to perform a number of API requests. Also, consider that for every alert triggering, the response action will be launched once, retrieving a single activity record per launch. Using CSV files simplifies and optimizes this data retrieval process.

Starting with Netwrix Auditor 9.8, to pass certain activity record fields to the executable file, you can instruct the program to write the fields and their values in a structured way to a CSV file.

Here is an example of a CSV file structure:

Alert ID	"Record ID"	"Alert name"	"Alert description"	"Action"	"Object type"	"Data source"	"What"	"Where"	"Who"	"When"	"Monitoring plan"	"Item"	"Workstation"	"MAC"	"Details"
"2442f87a-f74d-4f86-b1b1-9cc9726f18c0"	"2019031213344932 27245D8ECC4C84250 A62601EA4B8A74F5"	"My alert"	""	"Added"	"alert test"	"Netwrix API"	"what"	"Where"	"Me"	"13196871284 00000000"	"Monitoring plan 8 API"	"Item (Integration)"	""	""	"Property changed from "15" to "80"

The number of activity records retrieved per every response action launch will be only limited by user (see below for details). If the number of records associated with the alert exceeds this limit, the program will create multiple CSV files, storing data in chunks.

For example, if there are 50 records associated with the alert (e.g., *"Scanning threat is detected on network device"* alert), and the number of records for one CSV is set to 10, the program will create 5 CSV files, with 10 records in each chunk. Also notice that the response action will be launched once for every such chunk (5 times in this example), and will retrieve multiple activity records per launch (not more than the specified limit, i.e. 10 records in this example).

A CSV file is named using the timestamp and GUID and stored in the subfolder of Netwrix Auditor working folder (by default, *%ProgramData%\Netwrix Auditor\AuditCore\AuditArchive\AlertsToolLauncher\Csv*). Note that a CSV file will exist only while the executable file is running – after the execution is completed, the CSV file will be deleted. So if you plan, for example, to obtain some data from that file for further processing, you may need to copy it to a permanent location in a timely manner, e.g., using a script.

6. IT Risk Assessment Overview

To help you identify configuration gaps in your environment and understand their impact on overall security, Netwrix Auditor offers a dashboard with a number of metrics and drill-down reports on IT risk assessment. They pinpoint the weak points in your IT infrastructure such as overly broad assignment of access rights, loose password policies, and stale accounts. This information will help you to take corrective measures in the required area, ensuring the IT risks stay in the safe zone.

Risk assessment dashboard can be accessed by clicking the **Risk assessment** tile in the main window of Netwrix Auditor. For details about using the dashboard, see [IT Risk Assessment Dashboard](#).

For details about metrics calculation, see [How Risk Levels Are Estimated](#).

Looking for real-life use cases and walk through examples? Check out Netwrix training materials. Go the [IT Risk Assessment videos](#).

6.1. Providing Data for Risk Assessment

To provide data for metrics and reports that belong to different categories, you will need to configure monitoring plans that will process related data sources. These monitoring plans should have at least one item added. See the following table for the certain reports:

Category	Report name	Collect data from
Users and Computers	User accounts with "Password never expires"	AD domain
	User accounts with "Password not required"	AD domain
	Disabled computer accounts	AD domain
	Inactive user accounts	AD domain
	Inactive computer accounts	AD domain
	Servers with Guest account enabled	Windows Server
	Servers that have local user accounts with "Password never expires"	Windows Server

Category	Report name	Collect data from
Permissions	User accounts with administrative permissions	AD domain
	Administrative groups	AD domain
	Administrative group membership sprawl	Windows Server
	Empty security group	AD domain
	Site collections with the "Get a link" feature enabled	SharePoint farm
	Sites with the "Anonymous access" feature enabled	SharePoint farm
	Site collections with broken inheritance	SharePoint farm
Data	Files and folders accessible by Everyone	Windows File Server
	File and folder names containing sensitive data	Windows File Server
	Potentially harmful files on file shares	Windows File Server
	Direct permissions on files and folders	Windows File Server
	Documents and list items accessible by Everyone and Authenticated Users	SharePoint farm
Infrastructure	Servers with inappropriate operating systems	Windows Server
	Servers with under- governed Windows Update configurations	Windows Server
	Servers with unauthorized antivirus software	Windows Server

6.2. Required Monitoring Plan Settings

To provide data needed for risk assessment, the related monitoring plan must be set up to store data to the audit database.

Also, consider that all risk metrics and related reports require state-in-time data to be collected. You can select the relevant option when creating a new monitoring plan, as described in the [Settings for Data Collection](#) section. For the existing plan, refer to the procedure below.

To verify the necessary settings of the existing plan

1. Select the monitoring plan you need and click the **Edit** button.
2. In the right pane of the dialog displayed, select **Edit settings** from the **Monitoring plan** section.
3. Go to the **Audit Database** section and make sure that **Disable security intelligence ...** checkbox is cleared. This will instruct Netwrix Auditor to store data to both Long-Term Archive and audit database:

The screenshot shows the 'Plan Settings' dialog box with the 'Audit Database' section selected in the left sidebar. The main area is titled 'Specify the database to store your data'. A checkbox labeled 'Disable security intelligence and make data available only in activity summaries' is circled in red. Below this, there are fields for 'Database' (containing 'Netwrix_Auditor_File_Server_Audit'), 'SQL Server instance' (containing 'STATIONNASRV\SQLEXPRESS'), 'Authentication' (a dropdown menu set to 'Windows authentication'), 'User name', and 'Password'. At the bottom, there are three buttons: 'Save & Close', 'Save', and 'Discard'. The Netwrix logo is in the bottom right corner.

4. Save the settings and return to the window with the monitoring plan details. Make sure you have at least one monitored item in the plan. If necessary, add an item.

5. Select the data source you need (for example, Active Directory) and click **Edit data source** from the **Data source** section on the right.

← AD Monitoring

Home > Monitoring Plans > AD Monitoring

Data source	Status	Last activity time
Active Directory	Enabled	10/12/2018 7:12:01 PM
enterprise.local (Domain)	Ready	
+ Add item		

Monitoring plan

Edit settings

Delegate

Update

Data source

+ Add data source

Edit data source

Remove data source

Item

+ Add item

Edit Item

Remove Item

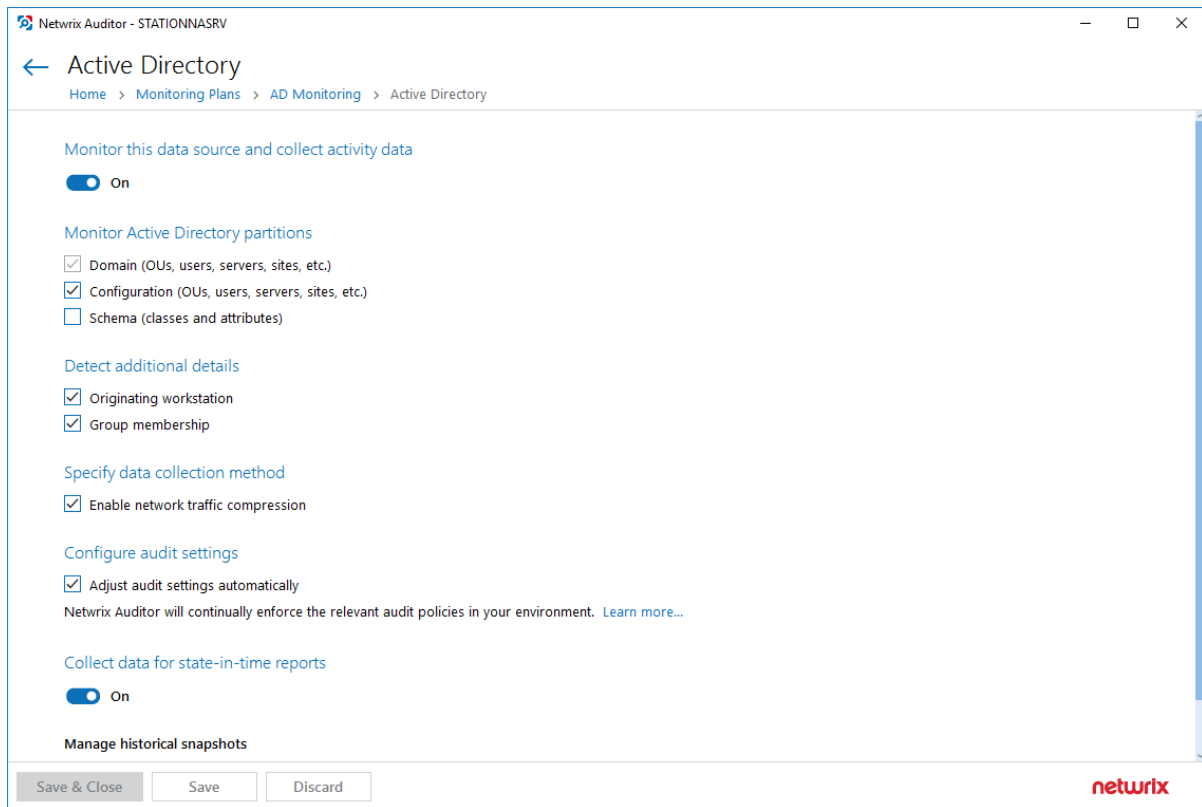
Intelligence

Search

View reports

netwrix

6. Make sure that:
 - a. **Monitor this data source and collect activity data** is switched **ON**.
 - b. **Collect data for state-in-time reports** is switched **ON**.



7. Save the settings and close the dialog.

6.3. IT Risk Assessment Dashboard

To access the **Risk Assessment** dashboard, click the corresponding tile in the main window. The IT risks are grouped into the following categories:

- Users and Computers
- Permissions
- Data
- Infrastructure

Within each category there are several key metrics identified by Netwrix industry experts who also suggested formulas for calculating metrics values. Risks are assessed against these metrics and displayed with the color indicators in accordance with the level:

- High — red
- Medium — yellow
- Low — green

Risk Assessment Overview

Home > Risk Assessment Overview

Filters | Not set

Type to filter risks

Risk name	Current value	Risk level	Details
Users and Computers			Permissions Risk metrics in this category are related to privilege elevation and improper user right assignment in your organization. For each selected metrics you can view a detailed report to determine which settings or security practices you should adjust to reduce the risks for your infrastructure.
User accounts with Password never expires	9	High (6 - unlimited)	
User accounts with Password not required	1	Medium (1 - 2)	
Disabled computer accounts	20% (1 of 5)	High (3% - 100%)	
Inactive user accounts	80% (8 of 10)	High (1% - 100%)	
Inactive computer accounts	20% (1 of 5)	High (3% - 100%)	
Servers with Guest account enabled	33.3% (1 of 3)	High (1% - 100%)	
Servers that have local user accounts with "Password neve...	100% (3 of 3)	High (99% - 100%)	
Permissions			
User accounts with administrative permissions	20% (2 of 10)	High (3% - 100%)	
Administrative groups	12.3% (8 of 65)	High (3% - 100%)	
Administrative group membership sprawl	66.7% (2 of 3)	High (0% - 100%)	
Empty security groups	75.4% (49 of 65)	High (2% - 100%)	
Site collections with the "Get a link" feature enabled	0% (0 of 5)	Low (0% - 30%)	
Sites with the "Anonymous access" feature enabled	20% (1 of 5)	Low (0% - 30%)	
Site collections with broken inheritance	40% (2 of 5)	Medium (30% - 60%)	
Data			

Subscribe Export

netwrix

After reviewing general risks assessment results in each category, you can drill-down to details covered in the underlying report— for that, double-click the selected metric or use the **View Report** button.

6.3.1. Customizing Metrics for Your Organization

Default threshold values for risk levels are set in accordance with recommendations of Netwrix industry experts, as described in [How Risk Levels Are Estimated](#). They can be, however, easily customized to reflect your organization's internal security policies and standards. For that, do the following:

1. In the dashboard pane, select the metric you need and in the **Actions** section on the right click **Modify thresholds**.
2. In the dialog displayed, specify new threshold values for risk levels.

- Click **OK** to save the settings and close the dialog.

Modify Risk Threshold Values

Currently, risk level for "User accounts with administrative permissions" is **High** with metric value of **7.1%**. Enter new threshold values to use when assessing risk levels.

■ Low: 0 - %

■ Medium: unused

■ High: - 100 %

Also, for several metrics the **Customize risk indicators** command is available.

For metric...	Use Customize risk indicators command to...
<i>File and folder names containing sensitive data</i>	Edit the list of words you consider to be indicators of sensitive content if detected in the file or folder name.
<i>Potentially harmful files on file shares</i>	Edit the list of extensions you consider to be indicators of potentially harmful files detected in the file share.
<i>Servers with inappropriate operating systems</i>	Edit the whitelist of permitted OS versions. Any other OS version will be considered a risk factor.
<i>Servers with unauthorized antivirus software</i>	Edit the whitelist of permitted antivirus tools. Any other antivirus will be considered a risk factor.
<i>Administrative group membership sprawl</i>	Edit the whitelist of permitted accounts that can be the members of local administrative groups. Any other account will be considered a risk factor.

NOTE: New settings will be applied/risk level thresholds will be refreshed after the next data collection session.

6.3.2. Delivering Assessment Results as a File

You can create a subscription to periodically receive IT risk assessment results by email or using a file share. For that, in the dashboard window click **Subscribe** and configure the necessary settings. See [Create Subscriptions](#) for more information.

You can also save current results to a PDF file, using the **Export** button in the dashboard window.

6.4. How Risk Levels Are Estimated

As mentioned, dashboard and built-in reports give you a bird's eye view of the following high-risk areas:

- User and computer accounts
- Permissions
- Data
- Infrastructure

Within each area, Netwrix Auditor industry experts identified risk categories and suggested guidelines for them. For example, if the number of administrative accounts in your organization is less than 2%, the risk should be considered insufficient. If the value is between 2% and 3%, the risk is moderate, while any value that exceeds 3% should be considered a high risk. These guidelines are based on security best practices and analytical data.

The product compares your environment configuration against these metrics and assigns a risk level to each category. The risk levels in each category determine the overall risk level for the area you review. The following risk levels are used:

Risk level	Color	Comments
Low	Green	Keep monitoring your environment on a regular basis.
Medium	Yellow	Proactively mitigate risks and adjust your workflows before a breach occurs.
High	Red	Respond to the threat as soon as possible.

Calculation formulas for each metric are provided in the table below.

NOTE: The following signs are used to define risk level intervals and threshold values:

- > —More than, exclusive
- ≥ —This value or more, inclusive
- = —Equals
- < —Less than, exclusive
- ≤ —This value or less, inclusive

- [] —Inclusive interval
- () —Exclusive interval
- [) or (] —Half-closed interval, where 1 value is inclusive and the other is exclusive or vice versa.

Risk	Assessment formula	Default risk level thresholds
Users and computers		
User accounts with "Password never expires"	Number of enabled user accounts with Password never expires property set	<ul style="list-style-type: none"> • 0 — Low • [1 - 5] — Medium • > 5 — High
User accounts with "Password not required"	Number of enabled user accounts with Password not required property set NOTE: Interdomain trust accounts are excluded from total count.	<ul style="list-style-type: none"> • 0 — Low • [1 - 2] — Medium • > 2 — High
Disabled computer accounts	Number of disabled computer accounts / Overall number of computer accounts (%)	<ul style="list-style-type: none"> • ≤ 1% — Low • (1% - 3%) — Medium • ≥ 3% — High
Inactive user accounts	Number of inactive but enabled users / Overall number of enabled user accounts (%)	<ul style="list-style-type: none"> • 0% — Low • (0% - 1%) — Medium • ≥ 1% — High
Inactive computer accounts	Number of inactive but enabled computer accounts / Overall number of enabled computer accounts (%)	<ul style="list-style-type: none"> • 0% — Low • (0% - 3%) — Medium • ≥ 3% — High
Servers with Guest account enabled*	Number of servers with enabled Guest account / Overall number of servers (%)	<ul style="list-style-type: none"> • 0% — Low • (0% - 1%] — Medium • >1% — High
Servers that have local user accounts with "Password never expires"*	Servers that have local user accounts with Password never expires / Overall number of servers (%)	<ul style="list-style-type: none"> • 0% — Low • >0% — High

Permissions

Risk	Assessment formula	Default risk level thresholds
User accounts with administrative permissions	Number of administrative accounts / Overall number of accounts (%)	<ul style="list-style-type: none"> • $\leq 2\%$ — Low • (2% – 3%) — Medium • $\geq 3\%$ — High
Administrative groups	Number of administrative groups / Overall number of groups (%)	<ul style="list-style-type: none"> • $\leq 2\%$ — Low • (2% – 3%) — Medium • $\geq 3\%$ — High
Administrative group membership sprawl*	Number of Windows servers whose Local Administrators Group members differ from those specified in the whitelist / Overall number of servers (%)	<ul style="list-style-type: none"> • 0% — Low • $>0\%$ — High
Empty security groups	Number of security groups without members / Overall number of security groups (%)	<ul style="list-style-type: none"> • $\leq 1\%$ — Low • (1% – 2%) — Medium • $\geq 2\%$ — High
Site collections with the "Get a link" feature enabled	Number of site collections with the Get a link feature enabled / Total number of site collections (%)	<ul style="list-style-type: none"> • $\leq 30\%$ — Low • (30% – 60%) — Medium • $\geq 60\%$ — High
Sites with the "Anonymous access" feature enabled	Number of sites with the Anonymous access feature enabled / Total number of sites (%)	<ul style="list-style-type: none"> • $\leq 30\%$ — Low • (30% – 60%) — Medium • $\geq 60\%$ — High
Site collections with broken inheritance	Number of site collections with broken inheritance / Total number of site collections (%)	<ul style="list-style-type: none"> • $\leq 30\%$ — Low • (30% – 60%) — Medium • $\geq 60\%$ — High
Data		
Files and folders accessible by Everyone	Files and folders shared with <i>Everyone</i> security group / Overall number of shared folders (%)	<ul style="list-style-type: none"> • $\leq 1\%$ — Low • (1% – 5%) — Medium • $\geq 5\%$ — High

Risk	Assessment formula	Default risk level thresholds
File and folder names containing sensitive data	Number of files and folders with names that suggest they contain sensitive data	<ul style="list-style-type: none"> • 0 — Low • 1 — Medium • > 1 — High
Potentially harmful files on file shares	Number of detected harmful files	<ul style="list-style-type: none"> • 0 — Low • 1 — Medium • > 1 — High
Direct permissions on files and folders	Number of shared objects with at least one direct permission / Overall number of shared objects (%)	<ul style="list-style-type: none"> • 0% — Low • (0% - 5%) — Medium • ≥ 5% — High
Documents and list items accessible by Everyone and Authenticated Users	Number of documents and list items shared with the <i>Everyone</i> and <i>Authenticated Users</i> groups / Total number of documents and list items (%)	<ul style="list-style-type: none"> • ≤25% — Low • (25% - 50%) — Medium • ≥50% — High
Infrastructure		
Servers with inappropriate operating systems*	Number of Windows servers with OS not included in the whitelist / Overall number of servers (%)	<ul style="list-style-type: none"> • 0% — Low • >0% — High
Servers with under-governed Windows Update configurations*	Number of servers with Windows Update configuration source set to Local Settings AND/OR with auto-update set to Not configured or Disabled / Overall number of servers (%)	<ul style="list-style-type: none"> • 0% — Low • >0% — Medium
Servers with unauthorized antivirus software*	Number of Windows servers with antivirus tools not included in the whitelist / Overall number of servers (%)	<ul style="list-style-type: none"> • 0% — Low • >0% — High

* -here the *Overall number of servers* means the number of Windows servers for which data collection was a success. That said, this count may vary across the risks. In such a case, it is recommended to examine Netwrix Auditor health log and omit lists.

7. Behavior Anomalies

Netwrix Auditor enables you to detect behavior anomalies in your IT environment, such as activity surges or mass deletions of archived data. As you investigate suspicious activity and review incidents, you can identify intruders or in-house bad actors who keep violating your company's security policies.

The behavior anomalies assessment extends the alerting functionality and provides both a high-level visualization and a detailed history of malicious user activity. While alerts notify you on a single or repetitive action almost immediately, the Behavior Anomalies dashboard accumulates this data over time and thus gives you the bird's eye view of activity patterns. With Behavior Anomalies, you can step beyond individual actions and investigate more complicated user behavior scenarios that might otherwise stay concealed for a long time.

On a high level, your behavior anomalies assessment workflow can be described as follows:

1. You create alerts on threat patterns specific to your company. You include these alerts in Behavior Anomalies assessment and associate a risk score with each alert. The score, that is between 1 and 100 points, reflects how critical the action is for your organization. Refer to [Risk Score](#) for detailed instructions on how to set a risk score for an alert.

Although Netwrix industry experts suggest risk scores for alerts that are provided out-of-the-box, you can easily tailor these scores to your organization needs and priorities. You can always adjust risk scores over time as you become more aware of behavior patterns and anomalous actions in your environment.

2. Each action that provokes an alert is treated as anomaly. Once the anomaly is detected, it appears on a dashboard's timeline and its risk score is added to the user's total score.
3. Every now and then, you review the Behavior Anomalies dashboard—the risk score timeline with anomaly surges, and the most active users. The general rule of thumb is: the more risk score points the user has the more he or she merits your attention. See [Review Behavior Anomalies Dashboard](#) for more information.
4. To learn more about user activity, you can drill-down to a user profile to review all alerts provoked by this user. As you review anomalies and mitigate risks, the user's total score reduces. See [Review User Profiles and Process Anomalies](#) for more information.

The purpose of the dashboard is to keep risks low and help you spot and address issues as they occur. The risk score assigned to a user does not qualify him or her as a bad actor but rather brings your attention to behavior patterns. Depending on the role in your organization, users might have different safe levels while you should make your priority to review the anomalies on time, stay focused, and proactively mitigate risks.

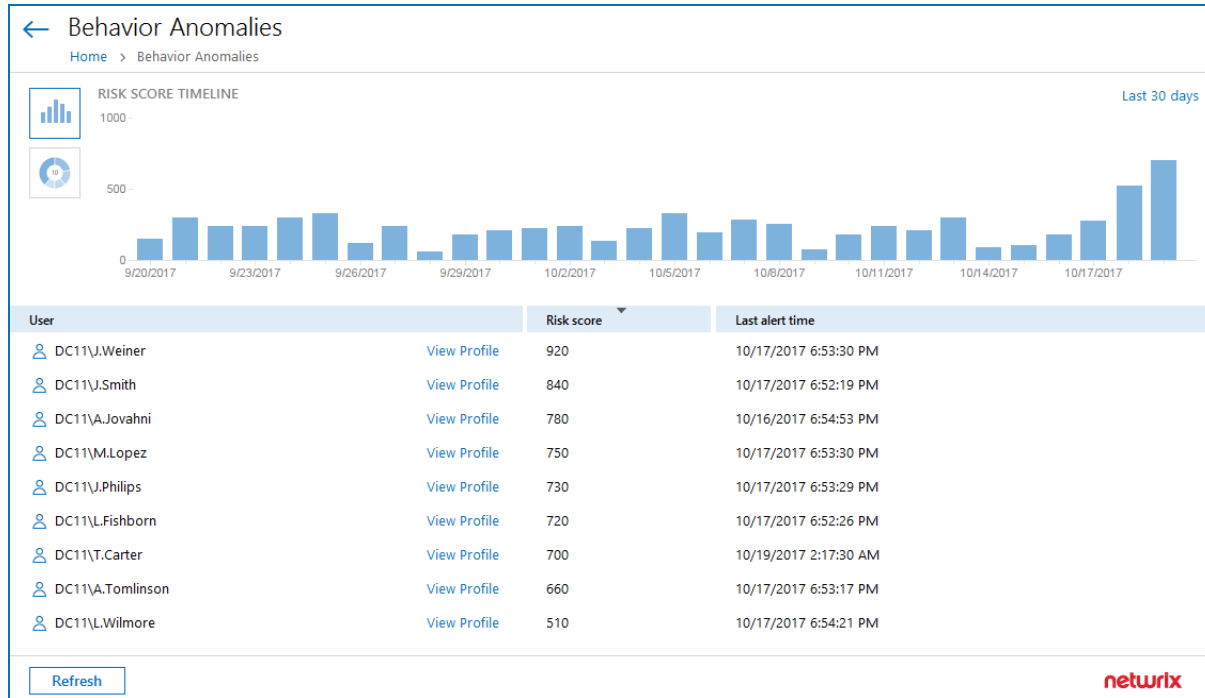
7.1. Review Behavior Anomalies Dashboard

NOTE: To review the Behavior Anomalies dashboard, process and filter anomalies in user profiles, you must be assigned the Global administrator or Global reviewer role in the product. See [Netwrix](#).

[Auditor Administration Guide](#) for more information.

To review the Behavior Anomalies dashboard

- On the main Netwrix Auditor page, navigate to **Behavior Anomalies**.



The dashboards includes the following sections:

- The **Risk score timeline** that helps you review anomaly surges over time.
- The **Risk score by top five users** chart that helps you identify the most active users. To see the chart, click the pie chart icon in the upper left corner of the page.
- The user list with all users who provoked alerts and their total risk scores.

Once you reviewed the general anomaly trend and identified users that merit your special attention, review their profiles and process anomalies. Click **View Profile** next to a user name to dive into user activity and investigate each action in details. See [Review User Profiles and Process Anomalies](#) for more information.

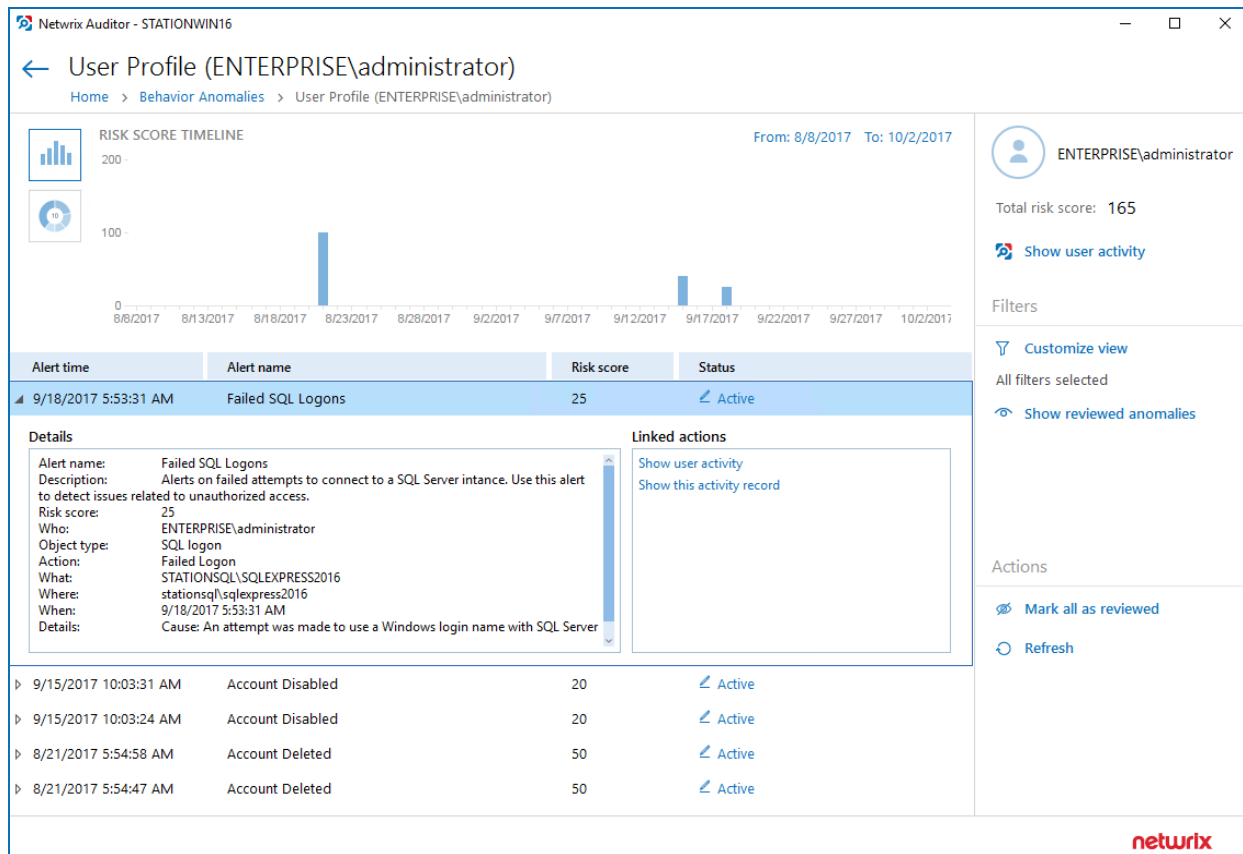
See [Review User Profiles and Process Anomalies](#) for more information.

7.2. Review User Profiles and Process Anomalies

The user profile enables you to investigate user behavior and take a closer look at anomalies.

To view a user profile

- On the **Behavior Anomalies** assessment dashboard, locate a user and click **View Profile** next to his or her name.



The user profile page contains the following sections:

- User data with the name and the total risk score. Click **Show user activity** below the total risk score, to launch the Interactive Search in a new window. Use it to see all user actions, including those that were not treated as anomalies.
- The **Risk score timeline** that demonstrates anomalous activity surges. Modify the timeframe to narrow down the results.
- The **Risk score by top five alerts** chart that outlines the most frequent anomalies provoked by user. To see the chart, click the pie chart icon in the upper left corner of the page.
- The anomalies list displays details for each anomaly: the alert that was triggered, the date and time, the risk score and anomaly status.

Double-click an entry to see more details: who did what, when and where the action was made, etc. Navigate to **Linked actions** and click **Show user activity** or **Show this activity record** to invoke Interactive Search and see all user actions or a specific action correspondingly.

NOTE: Netwrix Auditor shows only the top 2,000 anomalies. Modify the timeframe or hide reviewed anomalies, and then click **Refresh** to see more anomalies.

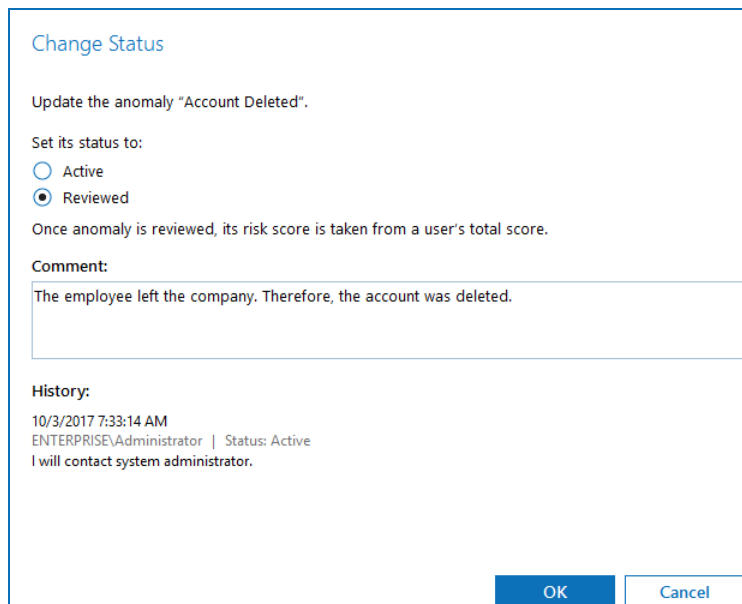
7.2.1. Process Anomalies and Reduce Risk Score

By default, the anomaly status is active and it indicates that the incident still requires some examination or is kept for further investigation. As you inspect anomalies and respond to threats, update statuses and add comments.

To change an anomaly status

1. Specify an anomaly from the list and click the **Active** link in the **Status** column.
2. In the **Change Status** dialog, set the status to *"reviewed"* and provide a justification.

NOTE: You can add comments without changing a status. This might be helpful if the anomaly remains active for a long period of time and you need even more time to examine it closely.



The image shows a 'Change Status' dialog box. At the top, it says 'Update the anomaly "Account Deleted".' Below this, it asks 'Set its status to:' with two radio buttons: 'Active' (unselected) and 'Reviewed' (selected). A note states: 'Once anomaly is reviewed, its risk score is taken from a user's total score.' There is a 'Comment:' section with a text area containing 'The employee left the company. Therefore, the account was deleted.' At the bottom, there is a 'History:' section showing a log entry: '10/3/2017 7:33:14 AM ENTERPRISE\Administrator | Status: Active I will contact system administrator.' At the very bottom are 'OK' and 'Cancel' buttons.

Once the anomaly is reviewed, it disappears from the timeline and chart, and its associated risk score is taken from user's total score. The reviewed anomalies supplement the status with the reviewer name and date (e.g., *Reviewed by CORP\Administrator (10/02/2017 10:12:03 AM)*).

You can always revert changes and assign the **Active** status back.

To process all anomalies

- In the **Actions** section, select **Mark all as reviewed**.

In this case, all anomalies that are currently in view will be set to *"reviewed"*. Perform this operation only with a proper justification. Since Netwrix Auditor shows only the top 2,000 anomalies, make sure to click **Refresh** to check if there are more anomalies to be reviewed.

NOTE: The anomalies that are excluded from view by filters are not affected by the **Mark all as reviewed** action. For more information about filters, see [Customize Anomalies List](#).

7.2.2. Customize Anomalies List

By default, all anomalies are in view. The **Filters** section helps you show or hide anomalies.

Click **Customize view** and clear the checkboxes next to alert names, if you do not want to see anomalies associated with them.

When you hide an alert from view, its associated anomalies will no longer be displayed on a timeline, chart, or in the list but the user total score will remain unchanged. Note that hidden anomalies cannot be reviewed in bulk with the **Mark all as reviewed** action.

Hide reviewed anomalies enables you to modify the anomalies list so that you can focus on active anomalies only. To see reviewed anomalies, click **Show reviewed anomalies**.

7.3. Behavior Anomalies Assessment Tips and Tricks

This topic contains various frequently asked questions as well as tips and tricks you might find helpful when configuring scoring settings and reviewing behavior anomalies.

- **The user has a high score and keeps provoking same alerts almost every day.**

Drill-down to the user profile and then click **Show user activity**. Review user actions and compare them to his or her job responsibilities. Does the user seem trustworthy? Are there any rights elevation or suspicious access attempts?

Try to review user tasks—you may find out that the anomaly the user keeps provoking is a genuine part of his or her daily routine. For example, the office staff should not reset passwords for other accounts while this is a basic task for a system administrator. In this case, review your alert settings and exclude the user from the alert filters.

- **Everyone in organization has a huge score**

Probably, you have configured too many alerts that turn behavior anomalies assessment into mess. It takes some time to learn what matters most to your organization and get accustomed to setting proper risk scores. Try to review your scoring settings regularly and adjust them when necessary.

- **Is anyone who is charge of "Failed..." anomaly a bad actor?**

Anyone can forget a password or accidentally try to access some data in a wrong folder. Such users are not subject to immediate prosecution unless they do not provoke repetitive alerts. The best practice is to review user profile after some time and check if there are any threat patterns in user behavior.

8. Subscriptions

Subscriptions enable you to schedule email delivery of a variety of reports or set of specific search criteria. Subscriptions are helpful if you are a rare guest of Netwrix Auditor and you only need to get statistics based on individual criteria. For example, an IT manager can easily provide auditors with weekly reports to prove compliance with regulations.

You can configure subscriptions to reports (including dashboards) risk assessment overview and interactive search.

8.1. Subscription to Reports

This subscription type has the following key features:

- Predefined change reports to monitor important cases for all data sources.
- State-in-Time reports to monitor data source state at a specific moment of time.
- Predefined User Behavior and Blind Spot Analysis report pack with complex logic to identify vulnerabilities (e.g., data access, suspicious files, etc.).
- Organization level reports to visualize what is happening in your environment.
- Reports with review status to track team workflow.
- Compliance reports to stay compliant with different standards.

8.2. Subscription to Search Results

This subscription type has the following key features:

- Flexible set of filters to modify search for your business use and create another subscription based on the existing one.
- Advanced filters to make your results context match.
- The **History** option to verify that the subscription is configured properly.
- On-demand delivery to send the subscription to a recipient at any moment.

8.3. Subscription to Risk Assessment Overview

This subscription type has the following key features:

- Risk assessment overview based on the latest state-in-time data to monitor the state of your Active Directory users and computers, as well as files and folders and other data at a specific moment.

- Automatically calculated metrics to identify risks and potential vulnerabilities (sensitive data, malicious files, etc.).
- Filters for monitoring plans and risk categories to receive exactly the data you need.
- Subscription options - delivery by email or upload to the specified file share.
- **History** option to verify that the subscription was configured properly and delivered successfully.
- On-demand delivery (**Run Now**) to send the subscription to a recipient at any moment.

NOTE: Subscription emails may vary slightly depending on the file delivery method and subscription type.

8.4. Subscription to Behavior Anomalies

This subscription type is similar to the predefined reports.

Review the following for additional information:

- Refer to [Create Subscriptions](#) for detailed instructions on how to create new subscriptions.
- Refer to [Review and Manage Subscriptions](#) for detailed instructions on how to manage subscriptions.

8.5. Create Subscriptions

NOTE: To create new subscriptions and manage existing subscriptions, you must be assigned the Global administrator or Global reviewer role in the product. See [Netwrix Auditor Administration Guide](#) for more information.

1. Do one of the following depending on subscription type:

To...	Do...
Subscribe to a report	On the main Netwrix Auditor page, navigate to Reports . Specify the report that you want to subscribe to and click Subscribe .
Subscribe to Behavior anomalies dashboard report	On the main Netwrix Auditor page, navigate to Behavior anomalies , then in the dashboard window click Subscribe .
Subscribe to search	<ol style="list-style-type: none"> 1. Navigate to Search and set appropriate search criteria. See Use Filters (Simple Mode) for more information. Click Search. 2. Navigate to Tools and select Subscribe.
Subscribe to risk assessment overview	On the main Netwrix Auditor page, navigate to Risk assessment and in the dashboard window click Subscribe .

2. On the **Add Subscription** page, complete the following fields:

Option	Description
General	
Subscription name	Enter the name for the subscription.
Report name	For report subscription —You cannot edit report name.
OR	
Email subject	For subscription to search and risk assessment overview —Specify email subject to identify subscription emails from Netwrix Auditor. For example, <i>"Successful read attempts on important file shares"</i> .
Send empty subscriptions when no activity occurred	Slide the switch to Yes if you want to receive a report even if no changes occurred.
NOTE: Available for report and search subscriptions only.	
Specify delivery options	<ul style="list-style-type: none"> • File format—Configure reports to be delivered as the pdf or csv files for search subscriptions; and pdf, docx, csv or xls files for report subscriptions.

Option	Description
<p>NOTE: Available for report and search subscriptions only.</p> <ul style="list-style-type: none"> • File delivery—Select delivery method: <ul style="list-style-type: none"> • Attach to email—Select this option to receive data as email attachments. <p>The maximum size of the attachment file is 50 MB. Attachments larger than 50MB will be uploaded to \\<NAservername>\Netwrix_Auditor_Subscriptions\$\LostAndFound\ folder on Netwrix Auditor server. They will be available for 7 days. Check the subscription email to get the files.</p> • Upload to a file share—Select this option to save data on the selected file share. Click Browse to select a folder on the computer that hosts Netwrix Auditor Server or specify a UNC path to a shared network resource. <p>NOTE: Make sure that the recipients have sufficient rights to access it and the Long-Term Archive service account has sufficient rights to upload reports. See Netwrix Auditor Installation and Configuration Guide for more information.</p>	
Other tabs	
Recipients	<p>Shows the number of recipients selected and allows specifying emails where reports are to be sent.</p> <p>Expand the Recipients list and click Add to add more recipients.</p>
Schedule	<p>Allows specifying report delivery schedule (daily, certain days of week, a certain day of a certain month).</p> <p>NOTE: By default, risk assessment overview and search subscription delivery is scheduled to 7.00 am daily, report subscription delivery - to 8.00 am daily.</p>
Filters	<ul style="list-style-type: none"> • For report subscription—Specify the report filters, which vary depending on the selected report. • For subscription to risk assessment overview—Select one or several monitoring plans and risk categories whose data you want to be included. By default, you will receive data on all risk categories, provided by all monitoring plans configured for risk assessment.

Option	Description
	<ul style="list-style-type: none"> • For search subscription—Specify filters in the same way as for search. See Apply Additional Filters for more information. <p>NOTE: For search subscription, you can also select a parameter to sort actions by and the sorting order.</p>
History	<ul style="list-style-type: none"> • Contains subscription generation details (intervals, status, last run time, start type). If the subscription failed, expand its details to understand and resolve error, then click the Try again link.
NOTE: For search and risk assessment subscriptions only.	<ul style="list-style-type: none"> • Allows for on-demand subscription delivery—for that, click Run Now. <p>On successful subscription generation you will receive the results that match your criteria for the scheduled period.</p>

8.6. Review and Manage Subscriptions

On the main Netwrix Auditor page, navigate to **Subscriptions** to review a list of your subscriptions.

Name	Type	Status	Mode	Recipients	Schedule	
Active Directory Changes and Activity	Search	✓ Completed	On	admin@corp.local	Weekly	×
Subscription to the 'All Activity with Review Status' report...	Report	✓ Scheduled	On	supervisor@corp.local	Daily	×
Subscription to the 'All User Activity' report	Report	✓ Scheduled	On	helpdesk@corp.local	Daily	×

The table below provides instructions on how to manage your subscriptions.

To...	Do...
Browse subscriptions	Type the target subscription name in the search bar in the upper part of the Subscriptions window and click the Search icon to review results.
Enable or disable subscriptions	Pick a subscription and select On or Off in the Mode column.
Modify subscriptions	Select the subscription that you want to modify and click Edit at the bottom of the Subscriptions window. Update the subscription and save your changes.
Remove subscriptions	Click × icon next to the selected subscription.

Index

A

Alerts 56, 60
 Apply tags 57
 Configure 56
 Predefined alerts 60
 Risk score 59
 Search by tag 60
 Threshold-based alerts 58

B

Baselines 47
Behavior Anomalies
 Concept 76
 Customize view 80
 Dashboard 76
 Process anomalies 79
 Timeline 76
 User profile 77
Browse audit data 20

C

Custom reports 54

D

Dashboard 72
Diagrams 39

E

Enterprise Overview 39

F

Free Community Edition 12

H

How it works 11

I

Intelligence

 Enterprise Overview 39
 Reports 35
 Search 20

L

Launch 17

Licensing

 Product editions 12

O

Overview 7

R

Reports

 Baselines 47
 Change management 38
 Change reports 38, 43
 Change Review Status reports 38
 Changes with video 38
 Compliance 53
 Custom 54
 Dashboards 38
 Filtering 37
 How to find 35
 Organization Level reports 38, 42
 Overview diagrams 39
 Overview reports 38
 Reports for change management 50
 Reports with video 52

SSRS-based Reports 35

State-in-Time Reports 38, 45

Subscriptions 81

User behavior and blind spot analysis 48

Response action 60

Risk assessment 65, 69

Overview 65, 72

S

Saved searches 54

Search

Advanced 26

Browse data 20

Columns 25

Condition 29

Copy and paste 33

Export data 33

Filters 22

Include and exclude data 32

More filters 26

Save as report 54

Subscribe 81

Subscriptions 81

Create 82

Manage 85

T

Tags

Apply to alerts 57

W

Windows Server

Baseline reports 47