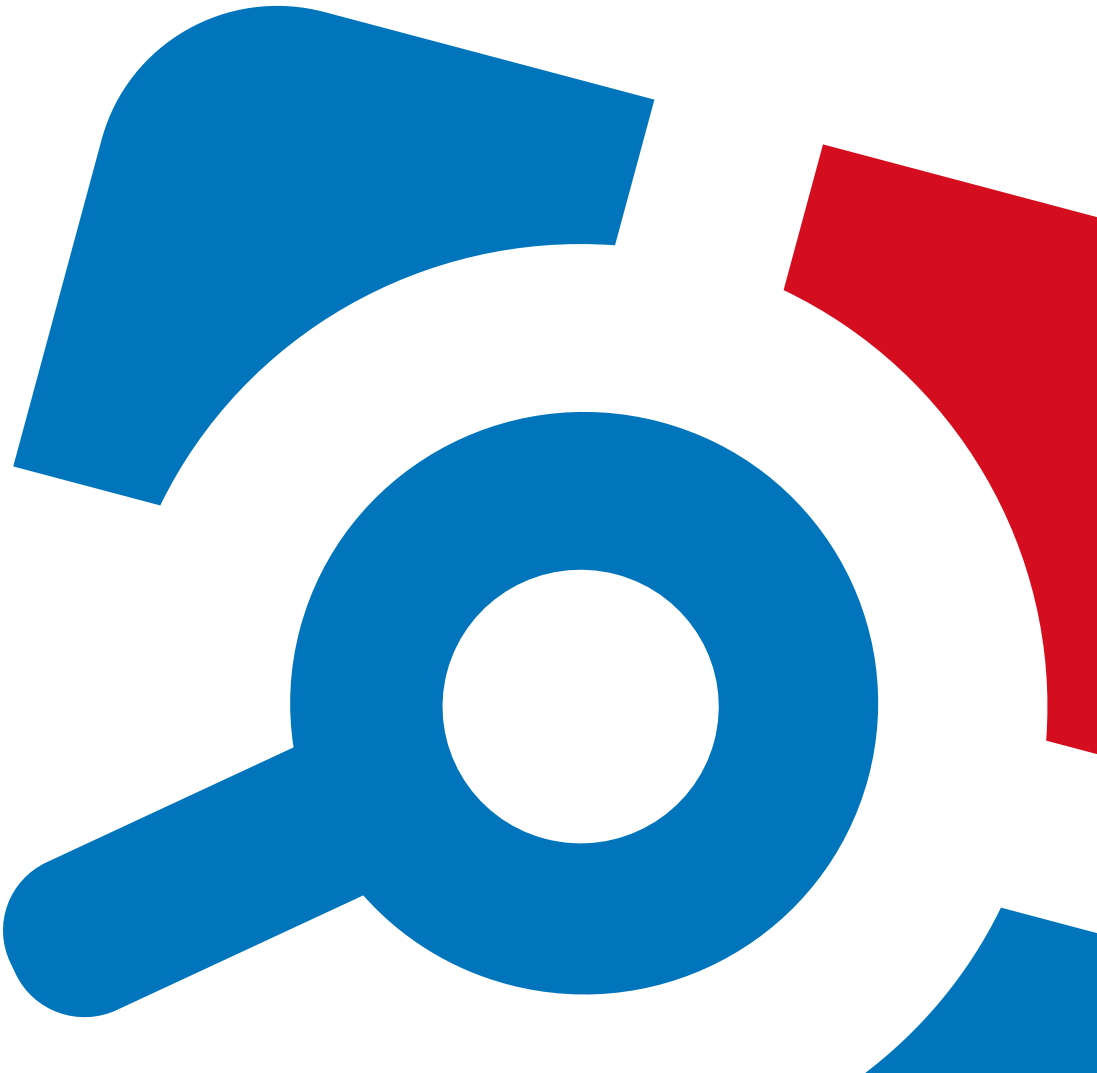
netwrix

Netwrix Auditor

Release Notes

Version: 10
9/14/2021



Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. What's New in 10

Create your personalized security experience

New features and improvements you'll get excited about

New: Customizable home screen

Personalize your security experience — Gain instant access to the most relevant information: Check your company's risk levels and activity trends, view alerts, and access your favorite reports and other information right from the main screen, so you can make swift decisions about your organization's security posture and quickly answer questions about it.

New: Data sensitivity tags in alerts

Reduce the time to detect incidents involving sensitive data — Detect critical threats faster by setting up alerts that will be triggered whenever sensitive documents are accessed, modified or deleted in a suspicious manner.

New: Data sensitivity tags in search

Speed response to threats to sensitive data — Make security investigations more efficient by easily filtering out all activity that isn't related to sensitive data. That way, you can focus on what happened to critical data during the incident and formulate the best response faster.

New: Reporting on SQL Server data reads

Know who's reading the sensitive data in your SQL Server — Hold your privileged users accountable for their actions, such as reading information they are not supposed to. As a result, you can deter behavior that could lead to data leakage, speed security investigations, and prove to auditors that only authorized users view the confidential information you store in SQL Server.

New: State-in-Time reports for Azure AD

Gain control over your Azure AD users and their roles — Mitigate the risk of a security incident and easily prove to auditors that you're following compliance requirements and industry practices by easily getting detailed information about your Azure AD users and their roles whenever you need it.

New: Reporting on SharePoint Online externally shared data (including new risk in Risk Assessment)

Identify and eliminate security gaps in SharePoint Online — Spot important security gaps in your SharePoint Online, such as documents that have been shared with external users or that can be accessed by everyone in the organization. Use interactive risk dashboards and detailed reports to see how you can close these gaps to reduce the risk of a breach.

Other notable improvements

1. New: Alerts Overview dashboard for monitoring alert statistics
2. New: State-in-Time data collection for modern authentication-only tenants in Exchange Online
3. New: Before and after values for attribute changes in Azure AD

4. New: Reporting on changes to local users and creations of users and groups in VMware
5. New: Support for VMware vSphere 7.0
6. New: Support for Nutanix Files 3.7 and 3.8
7. New: Auditing of SQL content changes (INSERT, UPDATE, DELETE) without triggers
8. New: Event-based collection of Windows Local User and Group changes
9. New: Support for Azure AD and Exchange Online in GCC and GCC High environments

+ Other enhancements that improve Netwrix Auditor usability and performance.

2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 10. For each issue, there is a brief description and a workaround or a comment if available.

2.1. General

ID	Issue Description	Comment
160222	After upgrading to Netwrix Auditor 9.95 you may need to wait for 24 hrs (until data collection daily cycle is completed) for the **User Accounts - Attributes** report to display all data as designed.	The report may be empty until *parentCanonicalName* property is collected and stored to the audit database. The following information based on related properties may be not reported properly: ◦ Account locked (*accountLockedOut*) ◦ Password expired (*pwdExpiringTime*) ◦ User cannot change password (*cannotChangePassword*) The following information will not be reported: ◦ Parent OU/container (*parentCanonicalName*) ◦ Manager (*managerDisplayName*) ◦ Manager email address (*managerEmail*) ◦ Street address (*streetPoBox*) ◦ Last modified (*whenChanged*)
158106	Netwrix Auditor Event Log Manager: the setup fails to	

ID	Issue Description	Comment
	copy remote distributed modules. Error details: *The process cannot access the file because it is being used by another process.*	
88793	If a Monitoring Plan includes multiple AD domains containing groups with the same name, then Search using *Who—In Group* filter without specified domain name will return the results for one domain only.	To search within certain domain using this filter, specify filter value in the *domain\group* format.

ID	Issue Description	Comment
132274	Nutanix does not send SMB notification in case the file was changed using some text editors, like Notepad, WordPad, etc. Some other editors work fine (e.g. MS Word). As a result, NDC does not detect file changes, and re-index for changed file does not start automatically. So, it will be re-indexed during the next scheduled re-index task (1 week by default).	

2.2. Netwrix Auditor for Active Directory

ID	Issue Description	Comment
10831	Since the AD Configuration partition is common for all domains in a forest, any change to this partition will be reported by the product for each of the audited domains. The name of the user who made the change will only be displayed for the domain where the change was made. Product reports for other audited domains will show the "System" value in the "Who" column.	Ignore entries with the "System" value in the "Who" column for other domains.
11090	If changes to group membership are made through Exchange Control Panel, the product will report on addition and deletion of all group members in addition to these changes.	
13619	If a change is made to the audited domain through Microsoft Exchange installed in another domain, the originating workstation for such changes will be reported as "Unknown".	
14291	If changes to Active Directory objects are made through	

ID	Issue Description	Comment
	Exchange Management Console or Exchange Control Panel, the "Workstation" field in reports showing the computer from which a change was made may contain several workstations.	
31008 31046	Netwrix Auditor reports the scheduled task or service start as an interactive logon.	
63500	The Administrative Group Members report does not show administrative group members beyond the monitored domain (e.g., child domain users).	

2.3. Netwrix Auditor for Exchange

ID	Issue Description	Comment
11537	If a user is added through Active Directory Users and Computers, and then a mailbox is created for this user through the Exchange Management Console within a short period of time (less than 10 minutes), the product will show duplicate entries for the mailbox creation event in the "Who" column. One change will show the Exchange name of the account under which a user was created, and the other—the name of the user who created a mailbox.	Ignore the duplicate entry with the Exchange account in the "Who" field.
11110	For Microsoft Exchange, changes to text strings that have line breaks will contain the before and after values only for the text fragment before the line break. The fact of the change itself will be reported for the whole text string.	Check the resulting value through Active Directory Users and Computers or other tools.
10897	The product does not report on changes made on an Exchange with the Edge Transport role.	
10590	For Microsoft Exchange, changes to the inetOrgPerson object type will be reported in the Exchange audit reports with the "user" value in the "Object Type" column.	
10431	If a previously disconnected mailbox is reconnected to a user, the Exchange reports will display the mailbox GUID instead of a canonical user name in the "What" column. If, as a result of this operation, the email address of this user is modified, this change will be reported in the Active	To get a canonical user name in an Exchange report, look for the "User" attribute in the "Details" field of the reconnected mailbox change entry.

ID	Issue Description	Comment
	Directory reports with the Exchange name in the "Who" column.	To get the "Who" value for the email address change entry, open Exchange report for the same time period and look for the entry reflecting the mailbox reconnection event. The user who reconnected the mailbox is the same user who initiated the email address change event. You can match the email notification entry with the mailbox reconnection entry by comparing the Object Path field in the Active Directory report with the User attribute in the "Details" field of the Exchange report.

2.4. Netwrix Auditor for Office 365

ID	Issue Description	Comment
–	When monitoring Exchange Online, *Add/Remove mailbox* actions will not be reported if mailboxes are created by the cloud services as a result of the user's license assignment. (The assignment of the license is reported by Netwrix Auditor for Azure AD.)	For *Add/Remove mailbox* actions to be reported, they must be created / removed via the PowerShell, using the `New-mailbox` or `Remove-mailbox` cmdlet.

2.5. Netwrix Auditor for File Servers (Windows File Server, EMC, NetApp, Nutanix Files)

ID	Issue Description	Comment
128593	For Nutanix file server: effective permissions (as a combination of NTFS and Shared permissions) are not calculated properly for the local Administrators group	

ID	Issue Description	Comment
	members.	
126202	For Windows file server: if a mount point is a shared folder, then the objects in its root will be initially collected by Netwrix Auditor and appear as processed by *System* account.	During the next data collections, all actions for these objects will be monitored in a normal way.
126198	Netwrix Auditor for Windows File Server does not audit the mount points targeted at the subfolder of a file share.	To process such mount points, in the monitored item settings provide network path to the target subfolder.
2871 762 42760	For NetApp 8.3.1 (or earlier) and EMC Isilon systems Netwrix Auditor may skip empty files creation and newly created folders in reports and activity summaries.	
30698 30847	If you switch native log format (EVTX and XML) on a NetApp 8.3.1 (or earlier) file server, you will receive errors on data collections until the first change event is captured and log is created. These errors can be ignored. If you performed a switch when the data collection was in progress you will receive an error stating that the log cannot be read. After a switch, Netwrix Auditor will not be able to get data from the previously used log.	
9450 9208 8887	When monitoring NetApp8.3.1 (or earlier), viewing an object's security properties may be reported as a change to these properties.	
34787	When monitoring NetApp 8.3.1 (or earlier), if an audit configuration error occurred within previous 11 hours, further data collection statuses may be **Working** and **Ready** even if this error persists. Netwrix Auditor automatically checks audit settings every 11 hours irrespective of scheduled or on-demand data collections, and writes a single notification into the Netwrix Auditor System Health log. Scroll down the log to see the error/warning.	To keep data collection status up-to-date, it is recommended to run data collections less frequently (e.g., twice a day—every 12 hours). To resolve configuration error: • Enable automatic

ID	Issue Description	Comment
		audit configuration. • Fix the error manually if this error is related to insufficient object permissions. • Add a problem object to omitcollect.txt to exclude it from monitoring.

2.6. Netwrix Auditor for Oracle Database

ID	Issue Description	Comment
158579	When adding Oracle Database instance or Wallet item to monitoring plan, Netwrix Auditor shows the following error: "Failed to install one or more required components."	Restart the Netwrix Auditor for Oracle Database Audit Service.

2.7. Netwrix Auditor for SharePoint

ID	Issue Description	Comment
1549	SharePoint Central Administration URL specified on monitoring plan creation cannot exceed 80 characters.	If your SharePoint Central Administration URL exceeds 80 characters, create a short name and specify it in the **Alternate Access Mappings**, and create a Site Binding in IIS for SharePoint Central Administration v4.
12683	When a lot of SharePoint changes are made within a short period of time (15-20 changes per second), some events may be lost and not reflected in audit reports and Activity Summaries because of the default IIS recycle settings (the IIS Worker Process that accumulates data on changes is restarted before all data is written to the Audit Database).	Modify the default IIS recycle settings to keep data when the process is restarted. For details on how to configure recycling, refer to the following Microsoft article: Recycling Settings for an Application

ID	Issue Description	Comment
		Pool.
12883	The timestamp for SharePoint farm configuration changes in audit reports and Activity Summary emails is the time when Netwrix Auditor generates the daily Activity Summary, not the actual event time.	
13445	The following changes are reported by the product with the "Unknown" value in the "Who" column: • Automatic creation of SharePoint groups on site creation if it uses unique permissions instead of inheriting them • All changes made under the "Anonymous" user if the security policy permits such changes	
13918	The following changes are reported with the "SHAREPOINT\system" value in the "Who" column: • Changes made under an account that belongs to Farm Admins • Changes made under an account that is a Managed account for the Web Application Pool • Changes made under an account that is specified in the User Policy of the modified Web Application with the **"Operates as a system"** option enabled • Changes resulting from SharePoint Workflows	
13977	The "Workstation" field is not reported for content changes if they were made in one of the following ways: • Through powershell cmdlets • Through the **Site settings** → **Content and Structure** menu • Through Microsoft servers and Office applications integrated with SharePoint • Through SharePoint workflows • Through the **Upload Multiple Files** menu option • Through the **Open With Explorer** menu option • Through a shared folder • Deletion of items through the context menu	

ID	Issue Description	Comment
33670	Netwrix Auditor does not report on changes to lists, list items, and web sites that had occurred before these objects were removed.	

2.8. Netwrix Auditor for SQL Server

ID	Issue Description	Comment
182794	When the NDC Provider integration module is configured, Netwrix Auditor incorrectly applies data categories to SQL Server tables in case when Netwrix Data Classification has been upgraded to the next version.	Workaround: Navigate to the Netwrix Data Classification web console and re- index your SQL Server source manually; or wait until the product completes planned re-indexing.
7769	Removal of a SQL Job together with unused schedules is reported with the "System" value in the "Who" column.	
6789	With the **Audit data changes** option enabled, when you try to perform the UPDATE/INSERT/DELETE operations in an audited database, an error is returned stating that the statements cannot be executed because the database owner SID cannot be resolved or SIDs do not match. **NOTE:** Database backup and restore may lead to unresolved or not matching SIDs.	For detailed information about the issue and for a solution, refer to the following Netwrix Knowledge base article: An error is returned stating that you have problems accessing an audited database.
25667	Netwrix Auditor shows the same workstation name in reports and search results for all changes made to an object within the data collection period (24 hours for default data collection schedule or between two manual launches) even if changes were made by different users and from different workstations.	
155774	The 'Object Permissions in SQL Server' and 'Account Permissions in SQL Server' reports will not show the ALTER (SERVER_ROLE) capability for the privileged users in SQL Server 2008 R2 due to that SQL Server version implementation.	
139588	The 'Object Permissions in SQL Server' and 'Account	

ID	Issue Description	Comment
	Permissions in SQL Server' reports will not show the RESTORE capability for the database owner.	
139554	Permissions for INFORMATION_SCHEMA granted via *master db* will not be reported in the 'Account Permissions in SQL Server' report.	
155179	State-in-time data for some system tables may not be collected properly.	
145577	Windows principals and windows_membership data will not be included in the state-in-time snapshot when collecting data on the group having members who belong to the outgoing trust domain.	

2.9. Netwrix Auditor for VMware

ID	Issue Description	Comment
160233	Netwrix Auditor for VMware will not collect data on Failed Logon event in case of incorrect logon attempt through VMware vCenter Single Sign-On.	
168911	When creating a state-in-time snapshot, Netwrix Auditor for VMware will not collect data on AD users if these users' permissions were granted via membership in their Primary Group.	

2.10. Netwrix Auditor for Windows Server

ID	Issue Description	Comment
134683	When calculating "Servers with unauthorized antivirus software" risk metric value, Windows 2016/2019 machines where pre-installed Windows Defender is running are considered a risk factor. They will be also considered a risk factor when the "Antivirus Baseline" filter in the "Windows Server Inventory" report is applied.	If you install a third-party antivirus product, you should uninstall Windows Defender as recommended by Microsoft. Otherwise, there will be two antiviruses running: Windows Defender and

ID	Issue Description	Comment
		third-party solution. In this case, Netwrix Auditor will treat Windows Defender as a main anitvirus, and related calculations will be performed accordingly.
102460	When calculating "Servers with unauthorized antivirus software" risk metric value, Windows 7 machines where pre-installed Windows Defender is running are considered a risk factor.	Microsoft Action Center does not classify Windows Defender on Windows 7 machines as antivirus software (see this article for more information). Use fully-featured antivirus software, e.g. Kaspersky Internet Security, ESET File security, Microsoft Security Essentials, etc.
12743	Some registry changes may be reported as *who=system* or *who=computer account*.	
12745	Software upgrade is reported by the product as two consecutive changes: software removal and software installation. The entry for software removal will have the "System" value in the "Who" column.	Look for the user name in the entry for software installation to determine who performed the upgrade.
	User Activity	
12763	Links to video recordings will not open from reports saved in the doc/xls format, or reports received by subscription and attached to emails in one of these formats.	Save reports in the PDF format and select this format when configuring a subscription to a report.
12807	On Windows 8.1/Windows Server 2012, the information on the launch of Windows Store (Metro-style) applications is not written to the detailed activity log (reports metadata), as applications in a tile-based interface do not have application descriptions or window titles. Therefore, data search or positioning inside video files will be unavailable for such applications. A video recording session will not start before the user accesses their desktop for the first time.	

ID	Issue Description	Comment
12451	Video capture of an RDP session will be terminated if this session is taken over by another user.	

3. What Has Been Fixed

This section lists issues that were known in the earlier versions and have been fixed in Netwrix Auditor 10.

Issue	Description
Ticket 175256, 182087	After upgrade from the version 9.7, Netwrix Auditor for Windows Server is unable to collect data from the target servers with the **Network traffic compression** option enabled.
Ticket 181745	Netwrix Auditor for Windows Server is stuck while reading empty or corrupted reader buffer file.
Ticket 181895	Netwrix Auditor for VMware Health log contains the following error: "*Failed to discover membership of <account> because object or item referred to could not be found.*" when trying to collect state-in-time data. The reason is empty AD logon name.
Ticket 182598	Netwrix Auditor for Windows Server. The Netwrix Auditor Health log contains the following error: "*Software install & remove data provider failed: The system cannot find the file specified.*".
Ticket 183162	Netwrix Auditor for File Servers. The "*Folder permission*" state- in- time report takes much longer to generate regardless of a snapshot size.
Ticket 183741	Netwrix Auditor for File Servers. The Netwrix Auditor Health log contains the following error: "*Cannot establish a connection to a Compression Service (0x80070035 The network path was not found)*". The reason is that the product tries to install compression service to a server previously removed from an Active Directory domain.
Ticket 183957	Netwrix Auditor for SharePoint Online. The Netwrix Auditor Health log contains the following error: "*Unable to parse the following event: {...} Skip this event*".
Ticket 169002	The Netwrix Auditor for Windows Server Health log contains the following error: 'User credentials cannot be used for local connections'.

Issue	Description
Ticket 172655	The Netwrix Auditor for Windows Server Audit Service crashes.
Ticket 176268	Netwrix Auditor for Windows Server. The 'There is not enough space on the disk' error for a single monitoring plan affects statuses of all Windows Server monitoring plans.
Ticket 176705	Netwrix Auditor for File Servers generates multiple activity records on permission changes.
Ticket 176753	Netwrix Auditor for SharePoint Online does not report on site deletions.
Ticket 177572	Netwrix Auditor for VMware Health log contains the following error: 'Failed to fetch membership of group.'
Ticket 180612	Netwrix Auditor for File Servers fails to parse some EMC Unity events.