

Netwrix Auditor

Release Notes

Version: 9.9
1/31/2020



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. What's New in 9.9	4
2. Known Issues	5
2.1. General	5
2.2. Netwrix Auditor Data Discovery and Classification	5
2.3. Netwrix Auditor for Active Directory	5
2.4. Netwrix Auditor for Exchange	6
2.5. Netwrix Auditor for File Servers (Windows File Server, EMC, NetApp, Nutanix Files)	7
2.6. Netwrix Auditor for SharePoint	9
2.7. Netwrix Auditor for SQL Server	10
2.8. Netwrix Auditor for Windows Server	11
3. What Has Been Fixed	13

1. What's New in 9.9

Visibility platform for user behavior analysis and risk mitigation in hybrid environments IT Risk Assessment

Don't let attackers sneak around in your IT infrastructure

New: Netwrix Auditor for Office 365 – Untangle SharePoint Online permissions. Strengthen security and prove compliance to auditors with enhanced visibility into who has access to what in SharePoint Online and OneDrive for Business.

New: Netwrix Auditor for Office 365 – Enhance transparency and security of your Exchange Online environment. Identify users that have access rights beyond what they need. Spot improper delegation and reduce data exposure in a few clicks.

New: Netwrix Auditor Netwrix Auditor for VMware – Detect unauthorized attempts to log on to your ESXi hosts and vCenter servers that could indicate an intrusion attack. Ensure that each successful logon to your virtual environment is fully authorized.

New: Netwrix Auditor for Active Directory – Watch your cloud applications for security threats. Reduce the risk of attackers taking control of the cloud applications your business relies on. Strengthen your access controls by detecting unauthorized AD FS logon attempts and getting actionable intelligence about them.

New: Netwrix Auditor Add-on for CyberArk Privileged Access Security – Keep the keys to your IT environment safe. Detect and investigate unauthorized activity across Privileged Session Manager and Enterprise Password Vault, including Central Policy Manager.

New: Netwrix Auditor Self-Audit – Audit modifications of your configuration files, monitoring plans, data sources and audit scope. Log each local and remote launch of the product, so you can keep administrators accountable for their actions and comply with PCI DSS, ISO 27001 and other regulatory standards.

Improved: Enterprise Overview dashboard and reports for your audited systems – Understand which of your critical IT assets requires attention in a flash with a 360-degree graphical view of what's happening across your IT systems.

+ Other additional enhancements that improve usability and performance.

2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 9.9. For each issue, there is a brief description and a workaround or a comment if available.

2.1. General

ID	Issue Description	Comment
88793	If a Monitoring Plan includes multiple AD domains containing groups with the same name, then Search using <i>Who—In Group</i> 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 <i>domain\group</i> format.

2.2. Netwrix Auditor Data Discovery and Classification

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).	

2.3. 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	

ID	Issue Description	Comment
	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 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).	

2.4. 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	

ID	Issue Description	Comment
	type will be reported in the Exchange audit reports with the "user" value in the "Object Type" column.	
10431	<p>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.</p> <p>If, as a result of this operation, the email address of this user is modified, this change will be reported in the Active Directory reports with the Exchange name in the "Who" column.</p>	<p>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.</p> <p>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.</p>

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 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	During the next data collections, all actions for

ID	Issue Description	Comment
	Netwrix Auditor and appear as processed by <i>System</i> account.	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), EMC VNX/VNXe and Isilon systems Netwrix Auditor may skip empty files creation and newly created folders in reports and activity summaries.	
30698 30847	<p>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.</p> <p>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.</p>	
9450 9208 8887	When monitoring NetApp 8.3.1 (or earlier) and EMC, viewing an object's security properties may be reported as a change to these properties.	
34787	<p>When monitoring NetApp 8.3.1 (or earlier) , EMC VNX/VNXe and Isilon systems, if an audit configuration error occurred within previous 11 hours, further data collection statuses may be Working and Ready even if this error persists.</p> <p>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.</p>	<p>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). Or contact Netwrix Support to enable more frequent audit checks.</p> <p>To resolve configuration error:</p> <ul style="list-style-type: none"> • Enable automatic audit configuration. • Fix the error manually if

ID	Issue Description	Comment
		<p>this error is related to insufficient object permissions.</p> <ul style="list-style-type: none"> • Add a problem object to omitcollect.txt to skip it from processing and monitoring.

2.6. 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 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: <ul style="list-style-type: none"> • 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 	

ID	Issue Description	Comment
	security policy permits such changes	
13918	<p>The following changes are reported with the "SHAREPOINT\system" value in the "Who" column:</p> <ul style="list-style-type: none"> • 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	<p>The "Workstation" field is not reported for content changes if they were made in one of the following ways:</p> <ul style="list-style-type: none"> • 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 	
33670	Netwrix Auditor does not report on changes to lists, list items, and web sites that had occurred before these objects were removed.	

2.7. Netwrix Auditor for SQL Server

ID	Issue Description	Comment
7769	Removal of a SQL Job together with unused schedules is reported with the "System" value in the "Who" column.	

ID	Issue Description	Comment
6789	<p>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.</p> <p>NOTE: Database backup and restore may lead to unresolved or not matching SIDs.</p>	<p>For detailed information about the issue and for a solution, refer to the following Netwrix Knowledge base article:</p> <p>An error is returned stating that you have problems accessing an audited database.</p>
25667	<p>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.</p>	

2.8. Netwrix Auditor for Windows Server

ID	Issue Description	Comment
134683	<p>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.</p> <p>They will be also considered a risk factor when the "Antivirus Baseline" filter in the "Windows Server Inventory" report is applied.</p>	<p>If you install a third-party antivirus product, you should uninstall Windows Defender as recommended by Microsoft.</p> <p>Otherwise, there will be two antiviruses running: Windows Defender and third-party solution. In this case, Netwrix Auditor will treat Windows Defender as a main antivirus, and related calculations will be performed accordingly.</p>
102460	<p>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.</p>	<p>Microsoft Action Center does not classify Windows Defender on Windows 7 machines as antivirus software (see this article for</p>

ID	Issue Description	Comment
		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 <i>who=system</i> or <i>who=computer account</i> .	
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.	
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 9.9.

Issue	Description
Update 2	
Ticket 285332: Item 147765	In Netwrix Auditor for Windows Server, Host Service (<i>Netwrix.WSA.HostService.exe</i>) crashes if Local Administrator permissions are missing on any of the monitored hosts.
Bug 150105	Stored procedure <i>dbo.nwxsqlcr_tracestartup</i> does not support logon traces enabling for Netwrix Auditor for SQL Server.
Update 1	
New:	Optimized Netwrix Auditor virtual appliance configuration: pre-configured monitoring plan for User Activity monitoring is now disabled by default.
New: Item 146388	Netwrix Auditor for Azure AD provides the ability to search and alert on sign-ins from IPs or locations outside the list of permitted ones (whitelist).
Ticket 278352: Item 140072	Netwrix Auditor shows 'Access Denied' error on the Activity record details pane for the Activity Records containing a large number of changed attributes.
Ticket 280755: Item 140157	Netwrix Auditor for User Activity reports 'Could not find a part of the path' warnings for missing video files.
Ticket 280736: Item 140266	For the folders with symbolic links, Netwrix Auditor for File Server incorrectly shows permissions in state-in-time reports.
Ticket 279055: Item 141009	For different folders with equal NTFS permissions, Netwrix Auditor for File Servers incorrectly shows permissions in state-in-time reports.
Ticket 282986: Item 143933	Too long processing of <i>vim.event.HostSubSpecificationUpdateEvent</i> vSphere Web Services API event during Netwrix Auditor for VMware data collection.

Issue	Description
Ticket 280561: Item 143188	Private Bytes and Handles leaks occur in Netwrix Auditor for User Activity when using custom credentials in Custom location of session recordings setting.
Ticket 282899, 282417: Item 142174	Netwrix Auditor for Azure AD reports failed logons for the data processing account.
Ticket 283893: Item 145178	Netwrix Auditor for Office 365 partially collects SharePoint Online snapshot due to a throttling error: <i>'The remote server returned an error: (429) Too many requests.'</i>