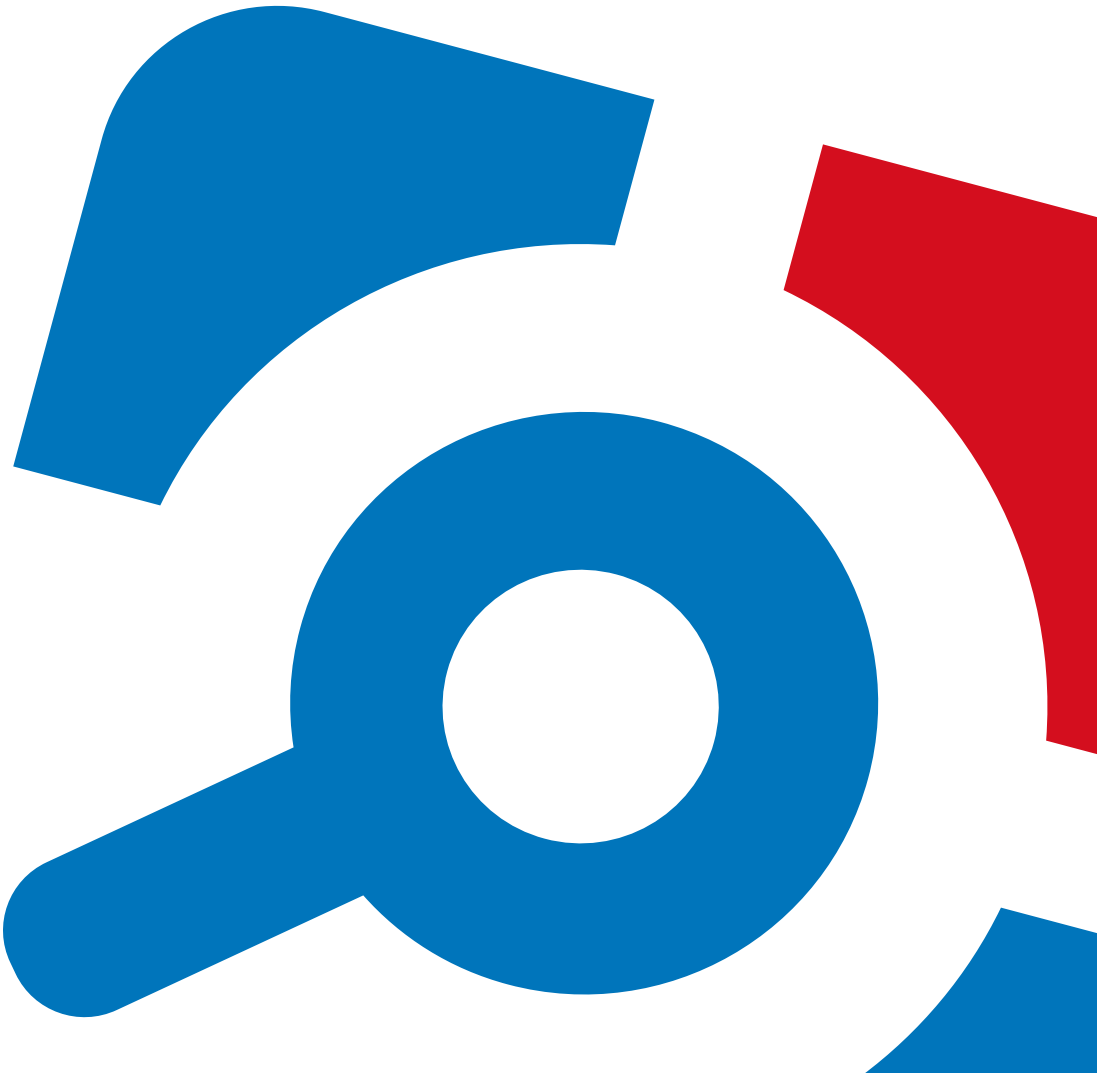
netwrix

Netwrix Auditor

Release Notes

Version: 9.7
12/13/2018



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 9.7

Detect and Block Attacks on Your Network Devices

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

New: Netwrix Auditor for Network Devices — Detect and investigate network security threats.

Reduce the risk of attackers taking control of your critical network infrastructure or insiders inadvertently or deliberately jeopardizing its security. Quickly catch whenever someone is trying to log into your Cisco or Fortinet devices and detect activity aimed at monitoring or manipulating the traffic to and from your network, or masking illegitimate access to your critical systems.

New: Visibility into SharePoint Permissions — Discover who has access to what on your SharePoint.

Untangle the permissions in your SharePoint and clearly see who has access to what data in your sites, know how these permissions were granted, and identify broken inheritance. Netwrix Auditor enables you to proactively mitigate the risk of insider misuse and reduce the reach of compromised accounts by streamlining the process of conducting regular privilege attestations and creating more manageable SharePoint environment.

New: User Profile — Immediately access account details to accelerate investigations.

Quickly determine whether there were legitimate reasons for activity you deem suspicious with key details about each suspect, including their full name, job title, manager, and AD group membership. This user profile is available side by side with the suspect's activity trail, enabling you to speed investigations and make more informed response decisions.

New: Automated Response — Respond to incidents in seconds, not days.

Speed threat mitigation and improve IT team productivity by having Netwrix Auditor alerts automatically trigger custom scripts. Use your deep knowledge of your organization's policies and use cases to craft the best response for each type of incident.

New: Customizable IT Risk Assessment Dashboard — Tailor IT risk assessment to your environment.

New: "In Group" Filter in Search and Alerts — Increase oversight of high-risk groups.

+ Numerous 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 9.7. 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 *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.

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 Exchange 2010 or 2013 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 2010 or 2013 Management Console or Exchange Control Panel, the "Workstation" field in reports showing the computer from which a change was made may contain several workstations.	

ID	Issue Description	Comment
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 2010, 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 2010, 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 Directory reports with the Exchange name in the "Who" column.	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. To get the "Who" value for the email address change entry, open Exchange report for the same time period and

ID	Issue Description	Comment
		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 Windows File Servers, EMC, and NetApp

ID	Issue Description	Comment
2871 762 42760	For NetApp, EMC VNX/VNXe and 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 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 NetApp and EMC, viewing an object's security properties may be reported as a change to these properties.	
34787	When monitoring NetApp, EMC VNX/VNXe and Isilon	To keep data collection

ID	Issue Description	Comment
	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. 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.	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. To resolve configuration error: • Enable automatic audit configuration. • Fix the error manually if this error is related to insufficient object permissions. • Add a problem object to omitcollect.txt to skip it from processing and monitoring.
53509	If you select a *\\Server\Share\Subfolder* for monitoring, Netwrix Auditor will also report on changes to *\\Server\Share* properties. Activity records will display the *Share* as object type, *\\Server\Share\Subfolder* in the What column, and *System* in the Who column.	

2.5. 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	Modify the default IIS recycle

ID	Issue Description	Comment
	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).	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: • 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	

ID	Issue Description	Comment
	• 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.	

2.6. 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.	
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.	

2.7. Netwrix Auditor for Windows Server

ID	Issue Description	Comment
12743 12765 12795 13365	The following changes will be reported with the "System" value in the "Who" column: • Changes to child registry keys (i.e., the keys that other keys link to). • For Windows 7/2008/2012, the "Who" column will contain the target computer name. • Creation of a new registry key if no value has been set for it.	
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.
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 9.7.

Issue	Description
	Update 1
New	Netwrix Auditor for Network Devices offers a set of predefined alerts on configuration changes, logon activity and hardware issues to help you ensure the network devices health.
New	To decrease infrastructure load, default behavior of Netwrix Auditor add-on for CEF Export will be modified so that it exports only activity records for the last month. So, this will be the default behavior for the following add-ons: for AlienVault USM, for IBM QRadar, for Intel Security, for LogRythm, for Solarwinds Log & Event Manager, for Splunk, for CEF Export and for Event Log Export.
New: Item 97358	Netwrix Auditor for Office 365, Netwrix Auditor for Active Directory and Netwrix Auditor for Exchange Servers support environments with '*Turn On Script Execution*' PowerShell policy set via Group Policy.
Ticket 266589: Item 100656	Netwrix Auditor for Oracle fails to work with more than one monitoring plan.
Ticket 265942: Item 100480	Netwrix Auditor for SQL Server fails to collect SQL Server logons if the '*hostname*' field in the original events is empty.
Ticket 264467: Item 97360	Netwrix Auditor for Windows Server failed to get a list of audited computers from the OU specified as the monitored item in the monitoring plan due to the system overflow error.
Ticket 259789: Item 84276	Netwrix Auditor for Windows Server failed to collect data from the log files with the long file names.
Ticket 258958: Item 82674	Netwrix Auditor for User Activity Video Recording fails with the '*Core.Common*' error and alike.
Ticket 263175: Item 97201	New: Netwrix Auditor for Active Directory supports disjoint namespace domains/forests.

Issue	Description
Ticket 252376: Item 78853	Netwrix Auditor for Office 365 fails to collect event data for the mailboxes, issuing exceptions.
Ticket 256801: Item 96319	If some DCs in the domain are unavailable, Netwrix Auditor for Windows Server may not be able to retrieve the list of computers from the OU specified as the monitored item in the monitoring plan.
Ticket 264299: Item 94481	Netwrix Auditor for Windows Server incorrectly reports server restart.
Ticket 262442: Item 94861	Netwrix Auditor for File Servers may fail to upload state-in-time snapshot to the database if the 'owner' attribute is empty for the file/folder.
Ticket 266344: Item 99687, 101132	If after the upgrade Netwrix Auditor for Network Devices service starts using the same listening port as used by Netwrix add-on for Cisco in the previous version, this leads to service crash.
Bug 99593	Netwrix Auditor for File Servers failed when trying to get remote server time, with the error '*0x80041010*' received from WMI.
Bug 98343	Netwrix Auditor for File Servers failed if the '**Combination of file and share permissions**' option was not selected in State-in-Time data collection settings.
Bug 93873	Automatic audit settings for Netwrix Auditor for File Servers do not include Audit Removable Storage policy on the target servers.
Bug 94243	'*Modified Time*' file attribute was not stored correctly to the database by Netwrix Auditor for File Servers, so "**Stale Data by Folder**" report did not display proper information.
	Netwrix Auditor 9.7
Ticket 254816: Item 85689	In some cases the Originating workstation information may be missing when Netwrix Auditor for Active Directory stores logon data to the database.
Ticket 261927: Item 87498	Netwrix Auditor for File Servers fails during snapshot incremental update.

Issue	Description
Ticket 260834: Item 92253	Netwrix Auditor for Active Directory fails to process large amount (2M+) of account lockout events, issuing the '*System.TimeoutException: The operation has timed out.*' error.
Ticket 260214: Item 92883	When auditing changes on a USB drive connected to a file server, Netwrix Auditor for File Servers incorrectly reports 'who/when' information for these changes.
Ticket 261335: Item 93725	If a newly created user account was immediately added to a group, Netwrix Auditor for Active Directory will report user addition to the group change partially (no information on actual group members).