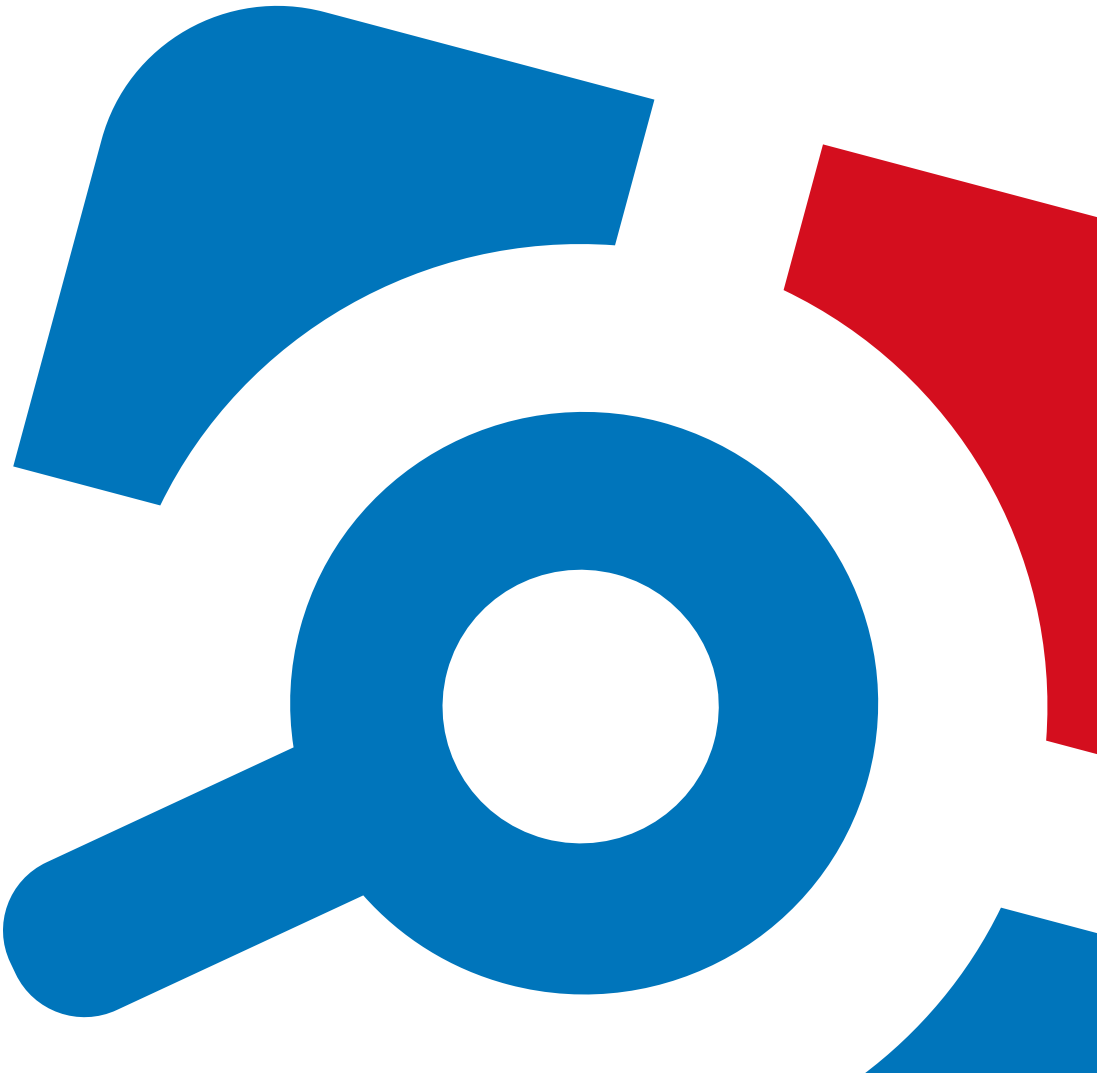
netwrix

Netwrix Auditor

Release Notes

Version: 9.5
1/11/2018



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.

© 2018 Netwrix Corporation.

All rights reserved.

Table of Contents

1. What's New in 9.5

Identify, assess and reduce risks to your IT infrastructure and data

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

New: Risk Assessment—Close security holes by identifying and prioritizing risks

Jump-start your risk mitigation program with a bird's-eye view of your security posture that pinpoints high-risk areas in your IT environment that need your immediate attention. Use this actionable information to adjust your security controls and thereby improve your security posture.

For example, assess your environment for the following risks:

- Excessive provisioning of administrative rights
- Overly broad assignment of data access rights
- Stale user and computer accounts
- Accounts with passwords that are empty or never expire

New: Behavior Anomaly Discovery—Improve detection of malicious insiders and compromised accounts

Spot data security threats that might otherwise stay concealed for a long time. An interactive behavior anomalies dashboard identifies the users with the most suspicious behavior over time by aggregating alerts on threat patterns and their associated risk scores. You can easily investigate the context of any anomalous action to enable an informed response.

For example, Netwrix Auditor's use cases for behavior anomaly discovery include:

- Account compromise and hijacking
- Privileged account abuse
- Data theft by a departing employee
- Cyber sabotage by a malicious insider

New: Permission Analysis—Scrutinize who has access to what

Gain peace of mind and ensure regulatory compliance by enforcing good access hygiene. Make certain that access rights are in strict accordance with the least-privilege principle to limit the reach of both human and automated attacks.

- **Netwrix Auditor for Active Directory**

  Analyze effective permissions for important resources to spot unnecessary access rights. Remove them to mitigate the risk of privilege abuse and limit the damage that malware can inflict.

- **Netwrix Auditor for Windows Server**

Stay informed about who has access to your critical servers by checking on local users and groups regularly. If you detect any deviations from your security policy or a known good baseline, quickly restrict access to minimize your attack surface.

New: API-Enabled Integrations—Speed incident response and maximize visibility into your Linux environment

Streamline incident detection and response workflows and expand visibility across your IT environment using free, ready-to-use add-ons.

- **Add-on for ServiceNow Incident Management**

  Speed incident response by immediately kicking off the resolution process whenever a suspicious event is detected. This smart integration uses information from Netwrix Auditor's alerts to automatically create detailed tickets in your ServiceNow ITSM and provide initial incident support, enabling faster and more accurate incident investigation.

- **Add-on for Privileged User Monitoring on Linux and Unix Systems**

  Promptly identify and respond to improper behavior across your *nix systems by gaining full control over temporary privilege elevations via the SUDO command and OpenSSH remote sessions.

- **Add-on for Generic Linux Syslog**

  Spot, investigate and block threats to your Linux environment with a single-pane view of what's happening there. Stay alert to risky behavior patterns, such as multiple authentication failures or failed attempts to run the SU command.

New: Custom Report Subscriptions—Stay informed about your specific security and compliance concerns

Easily ensure that your organization's specific security and compliance requirements are continuously met by creating custom reports using Interactive Search and having them sent to you or other stakeholders on a regular basis. Prove your compliance in minutes by simply having these custom reports saved in a particular folder and granting auditors access to that folder when they come.

+ More than 20 additional enhancements that improve usability, performance and scalability

2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 9.5. For each issue, there is a brief description and a workaround or a comment if available.

2.1. 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.	
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).	

2.2. 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 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

ID	Issue Description	Comment
		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.

2.3. Netwrix Auditor for Windows File Servers, EMC, and NetApp

ID	Issue Description	Comment
2871 762 42760	For NetApp, EMC VNX/VNXe and Isilon, Windows DFS and failover cluster, Netwrix Auditor may skip empty files creation and newly created foldersin reports and activity summaries.	
6462	If you switch between the active and the passive node on a clustered file server, the changes that took place between the last data collection and the switch will not be reported.	If you plan a switch, manually launch a data collection (click the **Update** button in your plan page), wait until data collection completes, and then perform the switch. If the switch is unplanned, contact Netwrix Technical Support.
30698 30847	If you switch native log format (EVTX and XML) on a clustered 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.	

ID	Issue Description	Comment
34787	When monitoring NetApp, EMC VNX/VNXe and Isilon, Windows DFS and failover cluster, 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 an 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). 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.	

2.4. 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.

ID	Issue Description	Comment
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: • 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.	

2.5. 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.	

2.6. 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 Vista/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 customer issues that have been fixed in Netwrix Auditor 9.5.

Issue	Description
	Update 2
New	Support for EMC Unity.
Ticket 250020: Item 64038	User Activity video recordings show part of user's screen if custom scaling display settings are set on the target computer.
Ticket 250949: Item 65490	Netwrix Auditor for Windows Server returns the "Out of memory" error when auditing terminal servers with a large number of users.
Ticket 248453: Item 64562	Netwrix Auditor for EMC reports on false positives Read and / or Modify Failed Attempts when changing permissions to a file or folder.
Ticket 250969: Item 66275	Netwrix Auditor for Logon Activity fails to collect data if there are unavailable Domain Controllers in the target domain.
Ticket 247354: Item 63229	Missed Workstation field for Lockout activity records in alert emails.
Ticket 250726: Item 66553	Netwrix Auditor for Azure AD is unable to collect audit data due to throttling limits in Azure Active Directory. "AF429: Too many requests " error fix.
Ticket 250965: Item 66452	Netwrix Auditor for Active Directory creates too many temporary folders from Exchange powershell connections in the Windows Temp folder.
Ticket 249641: Item 66702	Long processing of changes by Netwrix Auditor for Active Directory in the environment with slow DirSync connections.
Ticket 250565: Item 64865	The product fails to update SQL databases correctly after upgrade from Netwrix Auditor 9.0 to 9.5.
Ticket 251347: Item 66814	Netwrix Auditor for Active Directory is unable to upload state-in-time snapshot to a mirrored SQL database due to a constraint conflict.
Bug 66798	The product does not upload new predefined alerts after upgrade from Netwrix Auditor 9.0 to 9.5.
Bugs 64825, 64583	The "Folder and File Permission Details" State-in-time report does not show correct effective permissions.

Issue	Description
	Update 1
64055	Netwrix Auditor failed to process multiple subscriptions to custom reports.
63774	After the upgrade from 7.0 to the next versions up to Netwrix Auditor 9.5, the state-in-time functionality enables automatically for **Windows Server** data source.
64587, 64587, 64593, 64688, 64143, 63683	The IT Risk Overview report improvements.
63727, 63990	Netwrix Auditor for File Servers— **The Folder Permissions** report improvements.
	9.5
New	Added the ability to specify State-in-time reports generation interval more than 24 hours.
New	Error reporting improvements for File Servers Compression Service.
New	File Servers performance improvements for State-in-time data collection.
New	Netwrix Auditor Password Expiration Notifier and Netwrix Auditor Inactive User Tracker now allow creating several monitoring plans for one domain. With several monitoring plans, you can apply specific settings to each organizational unit individually.
New	Support for Exchange Server 2016 Cumulative Update 6, 7.
New	Netwrix Auditor now checks SharePoint audit settings and collects data on changes and activity in parallel threads.
New	Side-by-side data collection for multiple SharePoint site collections.
61670	Netwrix Auditor encounters the OutOfMemory exception when collecting SQL Server snapshot.
60226	Netwrix Auditor for SharePoint Core Service uses incorrect log level messages: "DEBUG" instead of "INFO".
58750	Netwrix Auditor returns 500 Internal Error when retrieving activity records with a help of Netwrix Auditor Add-on for CEF Export.
58675	Netwrix Auditor for VMware fails to collect data if any event contains

Issue	Description
	unknown argument.
58351	Netwrix Auditor encounters an error when processing file server objects - Netwrix Auditor cannot match the local and network paths when the whole disk is being monitored as a share.
56929	Netwrix Auditor for SQL Server supports increased timeouts for DML operations.
56875	Netwrix Auditor encounters an error if a shared security descriptor was corrupted or removed.
56755	Netwrix Auditor is unable to upload the Active Directory state-in-time snapshot to a share-based Long-Term Archive.
56609, 56693	Netwrix Auditor for File Servers stability improvements.
56291	The Kaspersky Security Center 10 blocks Netwrix Auditor on Windows Server 2008 R2.
56288	While collecting data, Netwrix Auditor for File Servers is now able to process directories with nesting up to 200 levels. Omitlists fixed for directories with nesting up to 1500 levels.
56155	While collecting File Servers data, Netwrix Auditor cannot process cyclically nested groups.
55998	When monitoring User Activity, Netwrix Auditor cannot exclude Organizational Units from being audited.
55360	Netwrix Auditor encounters an exception while collecting and processing NetApp ONTAP 9.1P3 adevt files.