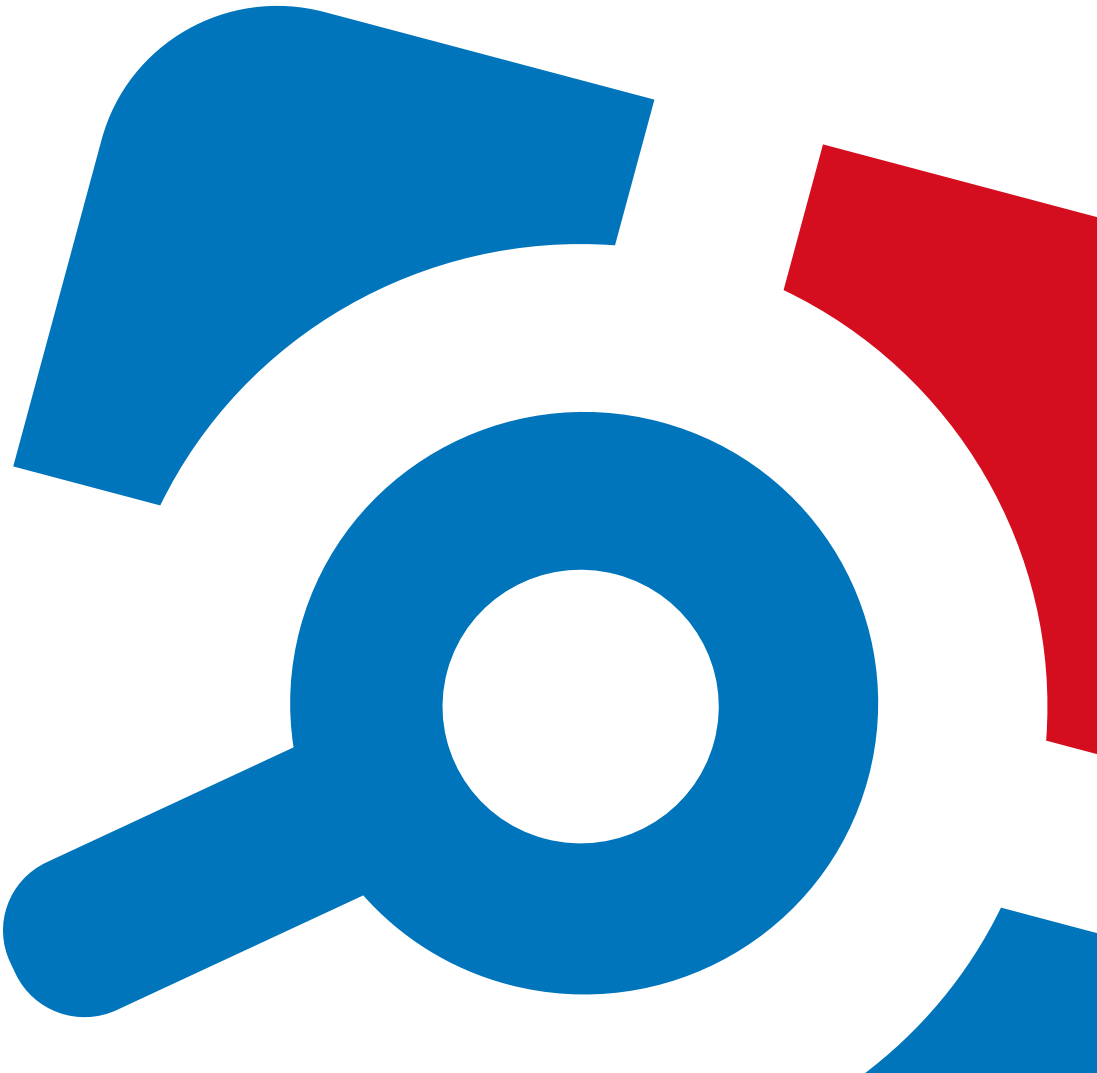
netwrix

Netwrix Auditor

Release Notes

Version: 9.0
7/3/2017



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 9.0

Shield Your IT Environment from Ransomware and Malicious Insiders

Netwrix Auditor 9.0

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

New: Alerts on threat patterns – Enable immediate response to ransomware and aberrant insider activity

Safeguard your data against ransomware with instant threshold-based alerting on file server activity. Also, stay on top of other suspicious behavior patterns and security violations across your Active Directory, file servers, SharePoint, databases and more, to ensure fast response to external attacks and insider threats. Simply choose from a list of predefined alerts or use the flexible criteria to specify your own pattern of behavior that you consider risky.

For example, the new alerts can help you in scenarios like these:

- A user has just modified a hundred files within a minute — could that be ransomware in progress?

  Take action immediately to prevent the ransomware from spreading.

- There's a spike in failed activity above your usual baseline?

  Investigate thoroughly to determine whether there is a legitimate reason for it.

- There's a change in a critical database no one is supposed to touch?

  Fix it before it leads to a data breach or a critical mistake based on erroneous data.

- A member of the Design team has just accessed an Accounting folder?

  It's time for a serious talk.

- An AD admin has just logged on to a production database?

  He'd better have a ticket for that.

New: Add-on for Cisco—Identify and block threats to your network infrastructure

Gain pervasive visibility into the activity around your network devices, which is normally minimal, so you can spot any outliers and prevent malicious actors from taking control over your traffic. With the free **Netwrix Auditor Add-on for Cisco**, you can now minimize the risk of network sniffing and other nefarious attacks aimed at monitoring or manipulating the traffic to and from your network, or masking illegitimate access to your critical systems.

Get the jump on threats like these:

- Are there multiple failed logons from a single account?

  Check whether someone is trying to brute-force your administrative credentials on a network device.

- Has your admin logged on from an invalid IP address?

  Investigate whether that admin account has been compromised.

- Has someone just changed a routing rule?

  Make sure the change does not put your data at risk.

New: Role-based access control—Granularly restrict access to security intelligence

Establish and enforce segregation of duties and a least-privilege model, as recommended by industry best practices and required by many security regulations. Intuitive, fine-grained controls enable you to easily ensure that your various IT and business teams have exactly the right access to Netwrix Auditor's security intelligence and settings.

New: Out-of-the-box compliance reports—Slash preparation time for audits by 50% or more

Relieve the burden of compliance and impress the auditors during your next check with out-of-the-box reports aligned with compliance controls. Netwrix Auditor now provides out-of-the-box compliance reports mapped to the specific requirements of GDPR, CJIS, FERPA, NERC CIP and GLBA, in addition to the common regulatory standards supported earlier.

New: Enhanced support for EMC Isilon appliances—The new Netwrix Auditor for EMC is now compatible with the latest versions of EMC Isilon, including 8.0.0.0 and 8.1.0.0.

+ More than 30 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 9.0. 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.	

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

ID	Issue Description	Comment
		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.

2.3. 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, folder creation is reported with the "System" value in the "Who" column. Folders created from a command prompt or in FAR Manager are not reported at all.	
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 be reported with the "System" value in the "Who" column.	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.	

ID	Issue Description	Comment
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, 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

ID	Issue Description	Comment
		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: • 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	

ID	Issue Description	Comment
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	
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	

ID	Issue Description	Comment
	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 9.0.

Issue	Description
	Update 1
New	Added support for EMC Isilon 8.0.0.0 and 8.1.0.0.
New	Added support for VMware vSphere 6.5, vSphere Hypervisor 6.5, and vCenter Server 6.5.
	9.0
47665	Netwrix Auditor collects incomplete data for NetApp filer, if NetApp logs contain special symbols that should not be used inside XML tags.
44902	Netwrix Auditor freezes while generating Logon Activity Summary.
45720	Netwrix Auditor encounters issues while processing Logon Activity data and resolving logon names. In order to optimize data collection, custom parameters were added to the product configuration.
43608	Active Directory alerts experience delays since Netwrix Auditor freezes while processing adevt files. Skip Account Management events to accelerate processing of root domains.
43950	The following error occurs when setting empty permissions for a file or folder: "Error while parsing SDDL strings (event ID 4670)".
44052	Data collection for File Servers completes with the following error: "System.ArgumentException: An item with the same key has already been added".
44513	The "TimeoutExpired" exception occurs since Netwrix Auditor for File Servers collects event log data even if change monitoring is disabled for the specified auditing scope (only state-in-time is enabled). State-in-time snapshot fails to be uploaded to the Audit Database.
45133	Netwrix Auditor retrieves incomplete list of available servers for auditing event logs.
45142	Netwrix Auditor for File Servers is unable to upload the state-in-time snapshot to the Audit Database where some file objects have ACE type value SDDL_OBJECT_ACCESS_ALLOWED.
45192	When auditing non-owner mailbox access, the maximum number of queried mailboxes is limited by 1000 per database. The limit is updated to 5000 by default. Create a custom registry key value to modify the limit: HKLM\SOFTWARE\Wow6432Node\Netwrix

Issue	Description
	Auditor\Non-owner Mailbox Access Reporter for Exchange\GetMailboxResultSize.
45531	Improve generation of report subscriptions that export data in csv.
45716	Netwrix Auditor does not update internal Audit Database views.
46018	The Netwrix Auditor for File Servers Core Service consumes 100% of CPU on the target server during data collection.
42331	Netwrix Auditor cannot retrieve the maximum password age for accounts with fine-grained password policies applied.
43379	Netwrix Auditor does not collect information on logon activity recorded by read-only DCs.
43608	Active Directory alerts experience delays since Netwrix Auditor freezes while processing adevt files. Accelerate processing of child domains.