

Netwrix Auditor

Release Notes

Version: 9.6
6/15/2018



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 9.6	4
2. Known Issues	5
2.1. Netwrix Auditor for Active Directory	5
2.2. Netwrix Auditor for Exchange	6
2.3. Netwrix Auditor for Windows File Servers, EMC, and NetApp	7
2.4. Netwrix Auditor for SharePoint	8
2.5. Netwrix Auditor for SQL Server	10
2.6. Netwrix Auditor for Windows Server	11
3. What Has Been Fixed	12

1. What's New in 9.6

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

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

New: Health Status Dashboard—Look at your audit status through a single pane of glass.

Simplify maintenance and troubleshooting tasks with at-a-glance view on the product health, data collection performance, and storage capacity displayed in the dashboard widgets. Drill down to the detailed information on the critical issues and the aspects you are interested in:

- Activity records statistics
- Actionable live statuses for monitoring plans
- All Netwrix Auditor Health log events in a single place
- Database usage statistics
- Disk space usage rate for Long-Term Archive and working folder

To learn more, refer to [Health Status Dashboard](#).

New: Netwrix Auditor Health status email—A single email report sent daily to the persons operating Netwrix Auditor providing a whole picture of the audit status.

To learn more, refer to [Netwrix Auditor Health Summary Email](#).

New: Active Directory Membership Reports—Review security principals from other domains that are audited within one instance of Netwrix Auditor.

New: Streamlined Alerts—Fine-tune your alerts with live data in "Preview".

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

2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 9.6. 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	<p>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.</p> <p>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.</p>	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	<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</p>

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 folders in 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	<p>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.</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 an 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 this error is related to insufficient object permissions. • Add a problem object to omitcollect.txt to skip it from processing and monitoring.
53509	<p>If you select a <code>\\Server\Share\Subfolder</code> for monitoring, Netwrix Auditor will also report on changes to <code>\\Server\Share</code> properties. Activity records will display the <i>Share</i> as object type, <code>\\Server\Share\Subfolder</code> in the What column, and <i>System</i> in the Who column.</p>	

2.4. Netwrix Auditor for SharePoint

ID	Issue Description	Comment
1549	<p>SharePoint Central Administration URL specified on monitoring plan creation cannot exceed 80 characters.</p>	<p>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.</p>

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: <ul data-bbox="367 890 1057 1087" 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 security policy permits such changes	
13918	The following changes are reported with the "SHAREPOINT\system" value in the "Who" column: <ul data-bbox="367 1226 1057 1570" 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	The "Workstation" field is not reported for content changes if they were made in one of the following ways: <ul data-bbox="367 1709 1057 1917" 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	

ID	Issue Description	Comment
	<ul style="list-style-type: none"> • 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	<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	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	The following changes will be reported with the "System" value in the "Who" column:	
12765		
12795	<ul style="list-style-type: none">Changes to child registry keys (i.e., the keys that other keys link to).	
13365	<ul style="list-style-type: none">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 9.6 Update 1.

Issue	Description
New:	Support for VMware vSphere 6.7.
New:	Support for NetApp 9.2, 9.3.
New:	For Data Discovery and Classification edition - streamlined configuration of DDC Provider.
New:	Significant failover cluster auditing improvements and speedup.
Ticket 249373: Item 78855	If Netwrix Auditor for File Servers experienced issues accessing data collection agent while processing file servers with multiple shares, then the next data collection will be performed as initial.
Ticket 255997: Item 81375	File Server Auditing fails because of the NwFileStorageSvc service failure, leading to audit data loss.
Ticket 250458: Item 71274	Netwrix Auditor for File Servers cannot upload EMC Isilon storage system state-in-time snapshot to the database.
Ticket 256567: Item 80394	Netwrix Auditor for File Servers fails to save state-in-time snapshot if processing a file servers cluster.
Ticket 256031: Item 75693	Netwrix Auditor for Active Directory reports incorrect Logon Hours attribute values.
Ticket 258267: Item 81892	Netwrix Auditor is unable to upload historical state-in-time snapshot to SQL server database if using custom credentials specified in the Long-Term Storage settings.
Bug 80588	Netwrix Auditor for File Servers displays incorrect monitoring status ' <i>Take action</i> ' for the file share, although the corresponding error was successfully added to the list of monitoring exclusions (<i>omiterrors.txt</i> file).
Bug 77538	Netwrix Auditor for File Servers does not apply the exclusion listed in the <i>omitcollectlist.txt</i> file if the exclusion path contains Japanese characters.
Bug 77767	Netwrix Auditor for File Servers does not apply the exclusion listed in the <i>omitstorelist.txt</i> file if the ' <i>Who</i> ' field contains two slash characters.
Bug 76121	Cannot access Long-Term Storage on a network share using custom

Issue	Description
Bug 73662	credentials when trying to store state-in-time snapshot.
Bug 73662	If long file paths are shorten by File Explorer according to 8.3 file name format, then Netwrix Auditor for File Servers cannot properly collect Activity Records and state-in-time snapshots.
Bug 77838	Excessive warnings issued upon license expiration.
Bug 73431	Netwrix Auditor for File Servers cannot perform deferred process because the system cannot find the path specified.