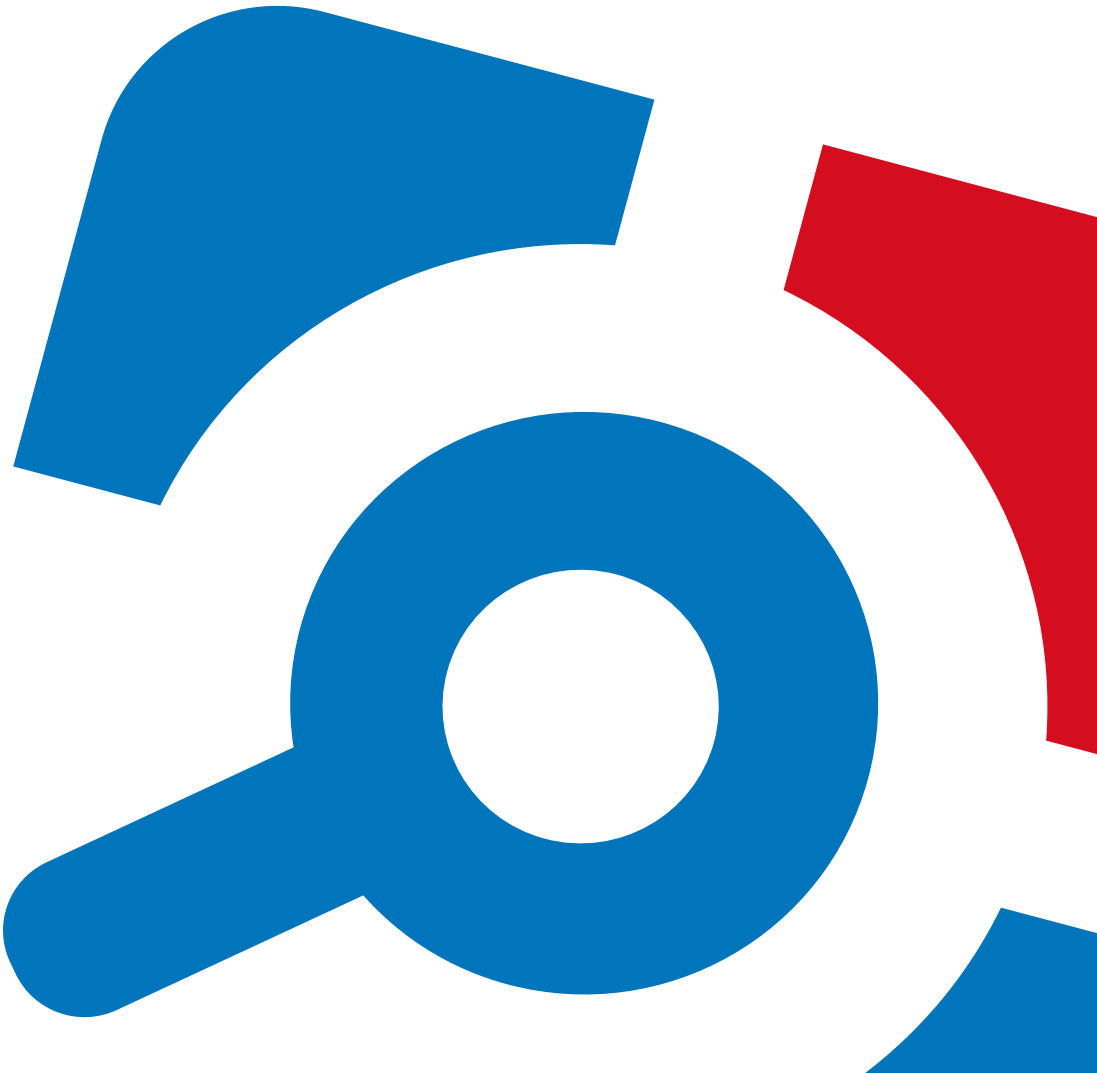
netwrix

Netwrix Auditor

Release Notes

Version: 8.5
12/1/2016



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 8.5 4
2. Known Issues 6
2.1. General 6
2.2. Netwrix Auditor for Active Directory 6
2.3. Netwrix Auditor for Exchange 7
2.4. Netwrix Auditor for Windows File Servers, EMC, and NetApp 8
2.5. Netwrix Auditor for SharePoint 10
2.6. Netwrix Auditor for SQL Server 12
2.7. Netwrix Auditor for Windows Server 12
3. What Has Been Fixed 14

1. What's New in 8.5

Detect & Investigate Abnormal User Behavior with 360-degree Visibility

The only visibility and governance platform for hybrid cloud IT infrastructures

#completevisibility into activity across hybrid cloud IT infrastructures for threat detection and data access governance

New: Secure identities and data in the cloud

- **Azure AD:**

  Solidify AD security—even if your identities reside in the cloud. The all-new **Netwrix Auditor for Azure AD** delivers actionable intelligence about what's going on in Azure Active Directory, enabling you to detect and investigate unauthorized changes to security settings, privilege escalation and suspicious access to Azure applications in time to make a difference.

- **Office 365:**

  Support your move to the cloud with proper security controls over your SharePoint data. The enhanced **Netwrix Auditor for Office 365** provides security intelligence about user behavior in SharePoint Online, so you can easily identify inappropriate data access and promptly take steps to prevent leaks of sensitive information.

New: Protect your structured data against exfiltration

- **Oracle Database:**

  In addition to visibility into unstructured data, gain control over database activity to detect, investigate and remediate threats to structured data. The new **Netwrix Auditor for Oracle Database** gives you visibility you can trust into what users and DBAs are doing in your Oracle databases, so you can quickly spot anomalous behavior and take corrective or preventive actions before a data breach occurs.

- **SQL Server:**

  Harden the security of data in your Microsoft SQL environment. The enhanced **Netwrix Auditor for SQL Server** strengthens your control over highly privileged users, giving you confidence that you can detect any unauthorized access to your SQL databases.

New: User Behavior and Blind Spot Analysis—Detect insider threats or external attacks in progress

Spot anomalous access attempts, suspicious activity and abusive user behavior across multiple systems that would otherwise go unnoticed. With Netwrix Auditor, you can detect insider threats and cyber-attacks, identify bad actors and respond to incidents efficiently. The new **User Behavior and Blind Spot Analysis** capability enables you to easily answer questions such as:

- Has there been any abnormal access to sensitive data?
- Is anyone accessing stale data?
- Have there been any unusual spikes in failed activity?
- Who is active outside of business hours and what are they doing?
- Has anyone put harmful files on corporate data storage?
- Are there any files likely to contain credentials, Social Security numbers, PHI or other sensitive data?

... and more.

New: Add-on Store—Fully leverage your IT security ecosystem through seamless, bi-directional integration

Maximize the value of your existing security applications by feeding them granular audit data from Netwrix Auditor. Visit the Netwrix Auditor Add-on Store to discover new free add-ons for integrating with SIEM systems, such as Splunk, IBM Security QRadar, AlienVault USM, Solarwinds Log & Event Manager, Intel Security and LogRhythm.

+ 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 8.5. For each issue, there is a brief description and a workaround or a comment if available.

2.1. General

ID	Issue Description	Comment
27063	Netwrix Auditor cannot start data collection after reinstalling the product to a different location.	Perform the following steps: 1. Start **Task Scheduler**, select the **Task Scheduler Library** node. 2. Locate **Netwrix Auditor - {id xxx} - {id xxx}** tasks and select **Properties** for each task one by one. 3. Select the **Actions** tab and click **Edit**. 4. Update path to a Netwrix Auditor component (that goes before *\Netwrix Auditor*).

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.	Ignore entries with the "System" value in the "Who" column for other domains.

ID	Issue Description	Comment
	Product reports for other audited domains will show the "System" value in the "Who" column.	
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.	

2.3. 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.	

ID	Issue Description	Comment
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 "Object Name" 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 the mailbox reconnection entry by comparing the Object Path field in the Active Directory audit report with the User attribute in the "Details" field of the Exchange audit report.

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

ID	Issue Description	Comment
2871 762	Windows native audit does not write folder creation operations to the event log. As a result, Netwrix Auditor, which relies on native audit, will report these changes with	

ID	Issue Description	Comment
	the "System" value in the "Who" column, or not report at all if the **Basic mode (large servers)** option is enabled.	
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, or not reported at all if the **Basic mode (large servers)** option is enabled.	If you plan a switch, manually launch a data collection (click the **Run** button in Netwrix Auditor Administrator Console on your Managed Object page), wait until it has completed 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	If the **Basic mode (large servers)** option is enabled when auditing NetApp and Celerra, viewing an object's security properties may be reported as a change to these properties.	
19247	If you select a *Server**Share**Subfolder* for auditing, Change Summaries and reports will include data on *Server**Share*, and files and subfolders inside *Subfolder*, but will miss the information on *Subfolder* itself.	
34787	If an audit configuration error occurred within previous 11 hours, further audit data collection statuses may be OK event 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.

ID	Issue Description	Comment
		To resolve audit 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 auditing.

2.5. Netwrix Auditor for SharePoint

ID	Issue Description	Comment
1549	SharePoint Central Administration URL specified on Managed Object 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 Change 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 email Change Summaries is the time when Netwrix Auditor generates the daily Change Summary, not the actual event time.	

ID	Issue Description	Comment
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 • 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 **Database Content Audit** 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 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	Look for the user name in the entry for software

ID	Issue Description	Comment
	installation. The entry for software removal will have the "System" value in the "Who" column.	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/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 all issues that have been fixed in Netwrix Auditor 8.5.

Issue	Description
	8.5 Update 2
Added	Support for OneDrive for Business (as a part of SharePoint Online auditing).
42605	The "OutOfMemory" exception occurs while generating a Change Summary email for Windows Server.
42569	Active Directory issues: • Provide ability to filter out accounts from search results, reports, and Change Summaries. Omituserlist.txt is created to support this functionality. • To reduce data collection time, provide ability to limit membership data collection to specified global catalogs. Membershipservers.txt is created to support this functionality.
42768	Logon Activity issues: • Netwrix Auditor is unable to copy adevt files from DCs if the connection to DC interrupts. • The system disk is running out of space because Logon Activity unzips its temporary files there. • Netwrix Auditor is unable to compress and decompress adevt files which original (not compressed) size exceeds 4 GB.
	8.5 Update 1
39995	When auditing non-owner mailbox access, Netwrix Auditor does not report names for archive mailboxes, just their GUIDs.
39286	The "OutOfMemory" exception occurs when auditing non-owner mailbox access.
39341	The following error occurs when auditing Windows Server with network traffic compression enabled: "Netwrix.WSA.AgentService.exe. ... Error while deleting closed session...: System.IO.DirectoryNotFoundException: Could not find a part of the path...".
36736	Subscription to the "All VMware Changes" that is scheduled for delivery once a week contains a report with incomplete data (for one day instead of a week).

Issue	Description
40029	When auditing file servers, Netwrix Auditor must omit actions made by Backupadmin to improve performance and prevent timeout exceptions.
40502	Netwrix Auditor fails to generate a Change Summary if the logon name contains supplementary characters (e.g., Amharic, Chinese, Korean, etc.)
	8.5
36375	When auditing Active Directory, Netwrix Auditor cannot process membership information (approximately 10 million changes per user/service). The omiteventuserlist.txt omit list is created to exclude these accounts.
36471	Netwrix Auditor does not collect logon activity data from DCs running Windows Server 2008.
36154	For environments with Exchange Resource Forest, Netwrix Auditor mailbox access reports show user's SID instead of account name in the Who column.
36301	Netwrix Auditor is unable to save Activity Records to the Audit Database if some field (e.g., Who) contains more than 255 characters.
3133 7688 7871	The following SQL Server changes are reported with the "System" value in the "Who" column: • Backup operations • Database restore from backup to a new database
31390	When auditing Windows 10-based file servers, Netwrix Auditor cannot collect membership information for the System Managed Accounts Group group. Error: "The following error has occurred while enumerating local users and groups..."
35684	Netwrix Auditor does not audit event logs containing a low line character (_) in their names.
38062	The following error occurs when auditing EMC Isilon OneFS 7.2.1.1: "Error while parsing event line <root type="object"><id type="string">...<createResult type="string"> SUPERSEDED</createResult>".
38063	The following error occurs when auditing EMC Isilon 7.2.1.1: "... Characters with hexadecimal values 0xFFFE and 0xFFFF are not valid."