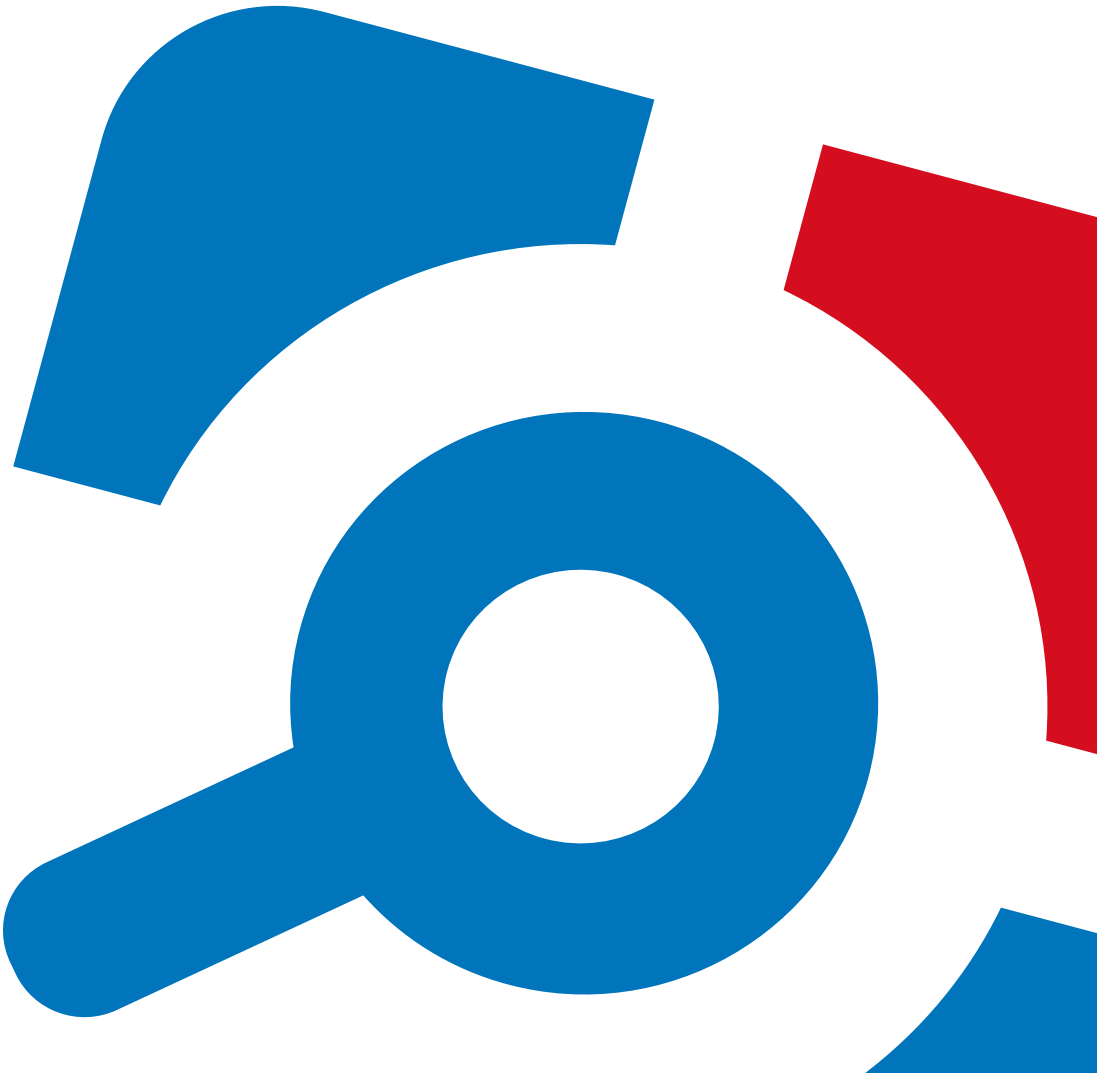
netwrix

Netwrix Auditor

Release Notes

Version: 8.0
6/1/2016



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

#completevisibility into hybrid cloud IT infrastructures to protect your data at rest regardless of its location

Regardless of data location—gain complete visibility into access, security changes and actions

- **Cloud**: Meet the all-new Netwrix Auditor for Office 365, which delivers visibility into changes to security settings and non-owner mailbox access in Microsoft Exchange Online.
- **Storage appliances**: Expand your visibility into changes and data access in storage appliances. The new Netwrix Auditor for EMC supports EMC Isilon as well as VNX and VNXe, and the new Netwrix Auditor for NetApp supports all the latest versions of Data ONTAP, including 8.3.2.
- **Windows-based file servers**: See the effective permissions for your data at rest with the new Netwrix Auditor for Windows File Servers, which analyzes both NTFS and share-level permissions.
- **SharePoint**: Establish audit controls over your most critical data. With Netwrix Auditor for SharePoint, you can now select specific documents and track who reads them.

File Analysis reports—make better information management decisions for unstructured data

New predefined reports enable you to quickly detect excessive access rights, overexposed data, and suspiciously high numbers of reads, modifications and failed access attempts. Get answers to questions such as:

- Who has access to data they shouldn't have?
- How are permissions assigned—directly or via groups?
- Who owns what data?
- Which file types are used most frequently?
- Have there been any unusual spikes in file reads, modifications or failed access attempts?
- Are there any empty folders or duplicate or stale files?

RESTful API—endless integration, auditing and reporting capabilities

- Data in: Centralize auditing and reporting by feeding Netwrix Auditor with audit data from any existing on-premises or cloud applications. All of your audit data will be centrally stored and ready for search and reporting.
- Data out: Get the most from your SIEM investment by feeding more granular audit data into your HP Arcsight, Splunk, IBM QRadar or other solution, thus increasing the signal-to-noise ratio. Moreover, you can also feed the granular audit data from Netwrix Auditor into critical IT processes, such as change management or ticketing, to further automate and streamline operations.

See how you can benefit from the RESTful API with examples of Amazon Web Services and HP ArcSight integration.

On-premises, virtual or cloud—deploy Netwrix Auditor wherever you need it

In addition to traditional on-premises deployment, Netwrix Auditor now offers two new deployment options that can speed time-to-value by getting you up and running in just 15 minutes:

- Virtual: Download our VMware Ready™ virtual appliance, which is ready to run on Microsoft Hyper-V and VMware hypervisors.
- Cloud: Visit the Microsoft Azure, Amazon, CenturyLink or VMware marketplace to deploy Netwrix Auditor in the cloud.

+ 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 8.0. 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 File Servers

ID	Issue Description	Comment
287162	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 the "System" value in the "Who" column, or not report at all if the **Basic mode (large servers)** option is enabled.	

ID	Issue Description	Comment
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. To resolve audit configuration error:

ID	Issue Description	Comment
		• 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.
31390	On Windows 10, 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..."	

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	

ID	Issue Description	Comment
	Netwrix Auditor generates the daily Change 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 • 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	

ID	Issue Description	Comment
	items, and web sites that had occurred before these objects were removed.	

2.6. Netwrix Auditor for SQL Server

ID	Issue Description	Comment
3133 7688 7769 7871	The following changes are reported with the "System" value in the "Who" column: • Backup operations • Removal of an SQL Job together with unused schedules • Database restore from backup to a new database	
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	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	

ID	Issue Description	Comment
12795 13365	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/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.	
32282	After upgrading from a previous version of Netwrix Auditor, DNS Server, DNS ZONE, and DNS Records changes for the last 24 hours might be lost.	To prevent data loss, run data collection before upgrade and right after upgrade.

3. What Has Been Fixed

This section lists all issues that have been fixed in Netwrix Auditor 8.0.

Issue	Description
	8.0 Update 2
35697	When auditing Active Directory, Netwrix Auditor freezes when trying to process membership changes (approximately 3 millions).
35953	Netwrix Auditor cannot start data collection for Logon Activity. Error: Invalid pointer.
35951	The " 0x80070534 No mapping between account names and security IDs..." error occurs when auditing Logon Activity. Netwrix Auditor cannot resolve user names formatted according to X.509 standard.
35610	The "0x80040204 Cannot convert the attribute data type" error appears on Netwrix Auditor Administrator Console start up.
35517	Disk space issues may occur since Netwrix Auditor does not clear Logon Activity data from its internal repository.
35209	Netwrix Auditor does not collect data on database content changes if SQL Server and database collations are case sensitive (e.g., SQL_Latin1_General_CP850_BIN2).
35167	Netwrix Auditor does not collect data on database content changes if tables contain non-Unicode symbols.
33372	In some cases, Netwrix Auditor reports incorrect changes when auditing SQL Server.
35709	Netwrix Auditor Integration API cannot write Activity Records with the Workstation property located in any other position except the last.
35513	The MSP.xml file is overwritten during the Netwrix Auditor upgrade.
n/a	Fixed issues related to group membership reports for SQL Server 2014.
	8.0 Update 1
Added	JSON support for Netwrix Auditor Integration API.
Added	HTTPS support for Netwrix Auditor Integration API.
Added	Netwrix Auditor downloads and installs Microsoft SQL Server 2014 SP1 Express with Advanced Services.

Issue	Description
33684	Netwrix Auditor triggers a database mirroring error when uploading a snapshot to the Audit Database.
33754	Netwrix Auditor should have an option to support both data and management interfaces for auditing NetApp clusters.
33372	In some cases, Netwrix Auditor reports "Who" as "system" when auditing SQL Server.
33096	Improve data collection and filtration for DFS.
34434	Unable to generate the "Groups Members" report for Active Directory containing 6,000+ groups and 180,000+ users.
35064	Netwrix Auditor is unable to store data to the Audit Database if port was specified during SQL Server configuration.
	8.0
32185	Netwrix Auditor reports changes to local account on SQL Server as System in the Who column.
33916	Improve performance for simultaneous processing of multiple file shares.
33199	Netwrix Auditor unable to collect audit data when a Managed Object for auditing NetApp filer appliances contains too many file shares (about 1500 and more). The following error occurs: More data is available.
32471	The HideEmailAdditionalInfo registry key should hide the "Inactive Users in Active Directory Report" title in the Inactive Users emails.
32445	The HideEmailAdditionalInfo registry key should hide the "Password Expiration Report" title in the Password Expiration emails.
32177	Exchange reports contain old data taken from the AAL events.
32018	All userAccountControl changes in AAL events are reported as Set-Mailbox.ResetPasswordOnNextLogon. The mapping is incorrect.
31811	Netwrix Auditor for Windows Server cannot process a server with a currently stopped DNS service.
31812	Netwrix Auditor for File Servers shows old data in reports and daily Change Summaries. This happens because the product cannot process events containing mojibake or not-readable symbols in the file paths (AutoCAD-related issue) and shows data since the last successful

Issue	Description
	data collection.
31362	Netwrix Auditor for Windows Server Omitcollectlist.txt does not work properly for DNS entries.
31747	Netwrix Auditor cannot process NetApp Clustered Data ONTAP 8.3.1 logs. Error: LastStoredEvent for server %servername%: 0 01/01/0001 00:00:00.
32015	Netwrix Auditor may fail to detect a log hosted on the file share that is not within first 20 file shares in NetApp Clustered Data ONTAP appliance.
32017	Netwrix Auditor receives information about first 20 volumes on NetApp Clustered Data ONTAP, the rest of volumes are skipped from processing, therefore, changes made to file shares in these volumes are not reported.
32105	Improve AAL events processing.
31058	Data is no longer specified after clicking Back-Forward in Active Directory Object Restore wizard.