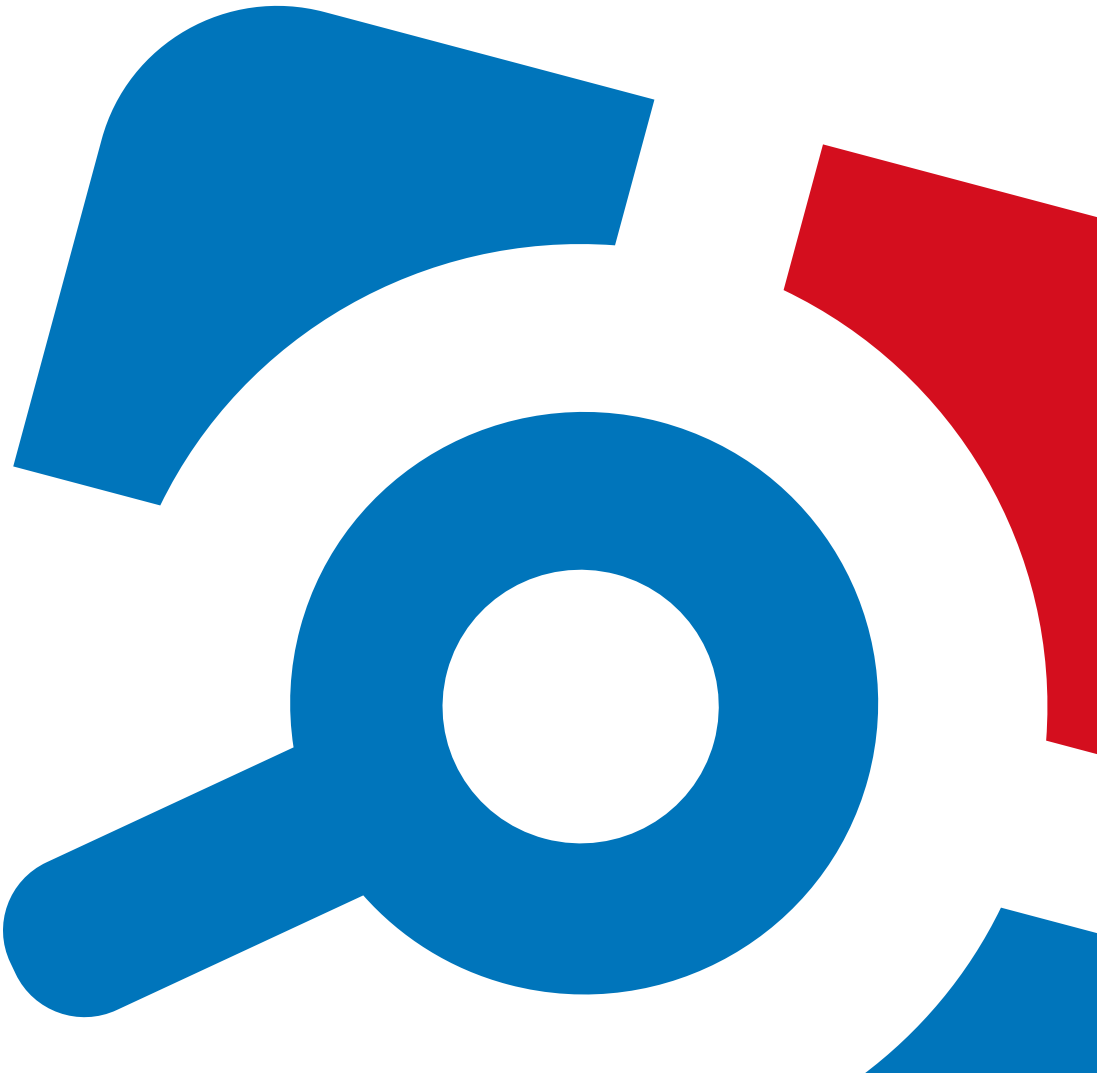
netwrix

# Netwrix Auditor

## Release Notes

Version: 9.8
7/12/2019



## 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 9.8 ..... 4
2. Known Issues ..... 5
2.1. General ..... 5
2.2. Netwrix Auditor for Active Directory ..... 5
2.3. Netwrix Auditor for Exchange ..... 6
2.4. Netwrix Auditor for Windows File Servers, EMC, and NetApp ..... 7
2.5. Netwrix Auditor for SharePoint ..... 8
2.6. Netwrix Auditor for SQL Server ..... 10
2.7. Netwrix Auditor for Windows Server ..... 10
3. What Has Been Fixed ..... 12

# 1. What's New in 9.8

## **Visibility platform** for user behavior analysis and risk mitigation in hybrid environments IT Risk Assessment

## Reduce Exposure of Your Windows Infrastructure and SharePoint Data

**New: Remediate security gaps on your critical Windows servers** — Identify weaknesses in your critical Windows Server infrastructure, such as servers with outdated operating systems or unsecure local accounts, and remediate them before they can be exploited.

**New: Reduce the exposure to threats in SharePoint** — Uncover security gaps in SharePoint that put you at risk of a breach of sensitive information, such as insecure sharing settings or large amounts of data accessible by global access groups.

**New: Data Discovery and Classification Edition** — Sensitive information discovery, classification and reporting is now available for SharePoint documents, lists and sites.

**New: Alerts on Threat Patterns** — Reduce alert fatigue and focus on high-priority incidents. Detect whenever someone is acting outside of working hours or a scheduled window so you can prioritize investigation of this unexpected activity. Identify and correct any access controls that are not working as desired by receiving alerts on activity generated by anyone other than members of the groups you expect, such as an AD admin modifying SQL Server configurations, a marketing team member accessing accounting files or a business user logging into a domain controller that only domain admins are supposed to access.

**Improved: Alert Response Actions** — Enables organizations to implement automated response actions on the incidents detected.

**Imporved: Netwrix Auditor for Network Devices** — Helps administrators to ensure the security of their networks and remediate downtime by supporting Palo Alto, SonicWall and Juniper devices.

**Improved: Netwrix Auditor for Windows Server** — Empowers security and compliance specialists to catch privileged users abusing their permissions before their actions result in a data breach. User session monitoring can be triggered by a session's start or more specific events, such as blacklisted application being launched or Run As events.

+ Numerous enhancements that improve usability and performance.

# 2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 9.8. For each issue, there is a brief description and a workaround or a comment if available.

## 2.1. General

| ID | Issue Description | Comment |
|---|---|---|
| 88793 | If a Monitoring Plan includes multiple AD domains containing groups with the same name, then Search using *Who — In Group* filter without specified domain name will return the results for one domain only. | To search within certain domain using this filter, specify filter value in the *domain\group* format. |

## 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.<br>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 Microsoft Exchange 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 Management Console or Exchange Control Panel, the "Workstation" field in reports showing the computer from which a change was made may contain several workstations. | |

| ID | Issue Description | Comment |
|---|---|---|
| 31008<br>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). | |

## 2.3. 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, 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, 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.<br><br>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.<br><br>To get the "Who" value for the email address change entry, open Exchange report for the same time period and |

| ID | Issue Description | Comment |
|---|---|---|
| | | 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 report with the User attribute in the "Details" field of the Exchange report. |

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

| ID | Issue Description | Comment |
|---|---|---|
| 2871<br>762<br>42760 | For NetApp 8.3.1 (or earlier), EMC VNX/VNXe and Isilon systems Netwrix Auditor may skip empty files creation and newly created folders in reports and activity summaries. | |
| 30698<br>30847 | If you switch native log format (EVTX and XML) on a NetApp 8.3.1 (or earlier) 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.<br>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<br>9208<br>8887 | When monitoring NetApp8.3.1 (or earlier) and EMC, viewing an object's security properties may be reported as a change to these properties. | |
| 34787 | When monitoring NetApp 8.3.1 (or earlier) , EMC VNX/VNXe | To keep data collection |

| ID | Issue Description | Comment |
|---|---|---|
| | and Isilon systems, if an audit configuration error occurred within previous 11 hours, further data collection statuses may be **Working** and **Ready** even if this error persists.<br><br>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 the error/warning. | 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.<br><br>To resolve configuration error:<br><br>• Enable automatic audit configuration.<br><br>• Fix the error manually if this error is related to insufficient object permissions.<br><br>• Add a problem object to omitcollect.txt to skip it from processing and monitoring. |

## 2.5. 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. |
| 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 |

| ID | Issue Description | Comment |
|---|---|---|
| | | 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:<br>• Automatic creation of SharePoint groups on site creation if it uses unique permissions instead of inheriting them<br>• 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:<br>• Changes made under an account that belongs to Farm Admins<br>• Changes made under an account that is a Managed account for the Web Application Pool<br>• 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<br>• 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:<br>• Through powershell cmdlets<br>• Through the **Site settings → Content and Structure** menu<br>• Through Microsoft servers and Office applications integrated with SharePoint<br>• Through SharePoint workflows<br>• Through the **Upload Multiple Files** menu option<br>• Through the **Open With Explorer** menu option<br>• Through a shared folder | |

| ID | Issue Description | Comment |
|---|---|---|
| | • 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 **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.<br><br>**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:<br><br>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 |
|---|---|---|
| 102460 | When calculating "Servers with unauthorized antivirus software" risk metric value, Windows 7 machines where pre-installed Windows Defender is running are considered a risk factor. | Microsoft Action Center does not classify Windows Defender as antivirus software (see this article for more information). Use fully-featured antivirus software, e.g. Kaspersky Internet Security, ESET File |

| ID | Issue Description | Comment |
|---|---|---|
| | | security, Microsoft Security Essentials, etc. |
| 102115 | When calculating "Servers with unauthorized antivirus software" risk metric value, machines with Sophos Endpoint Agent will be reported as having only disabled Windows Defender. | The reason is that Sophos Endpoint only disables Windows Defender without uninstalling it. |
| 12743 | Some registry changes may be reported as *who=system* or *who=computer account*. | |
| 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. |
| | **User Activity** | |
| 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 issues that were known in the earlier versions and have been fixed in Netwrix Auditor 9.8.

| Issue | Description |
|---|---|
| | **Update 3** |
| Ticket 275512: Item 123347 | Netwrix Auditor for File Servers fails when starting to collect data from NetApp storage (ONTAP 9.4 p2). |
| Ticket 276956: Item 124206 | Netwrix Auditor for File Servers fails to process data from NetApp storage system if items with the same name are included into different monitoring plans for the corresponding data source. |
| Bug 119512 | Sorting by "Expiration Date" field in the "User Account - Expired" report does not work properly. |
| Bug 121468 | After upgrading to version 9.8, path to *Netwrix_UAVR$* is changed automatically to the default one. |
| Bug 125854 | In the "Duplicate Files" report the monitoring plan default filter value now includes only one session instead of all existing sessions. |
| | **Update 2** |
| Ticket 275644: Item 120605 | Netwrix Auditor for Network Devices cannot send Activity Summary due to the following error:"*The request processing service has an unknown ID*". |
| Ticket 273735: Item 117534 | Netwrix Auditor for File Servers failed to upload state-in-time snapshot to the database while monitoring an AD container (OU) with a large number of servers. |