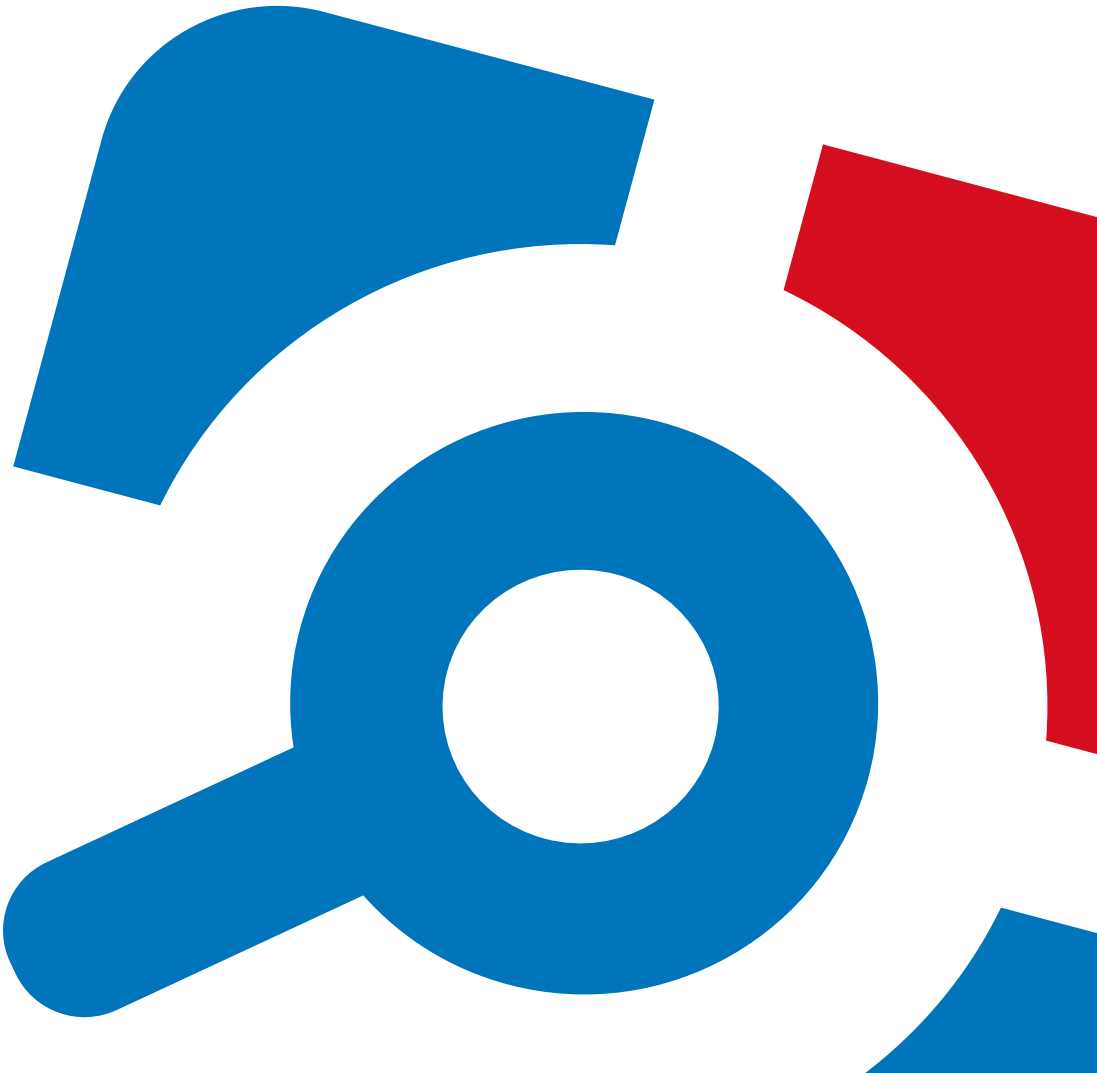
netwrix

Netwrix Auditor Data Discovery and Classification

Release Notes

Version: 9.7
11/28/2018



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.

1. Netwrix Auditor Data Discovery and Classification Overview

Netwrix Auditor's Data Discovery and Classification gives you complete visibility into where your sensitive files are, what content is inside them, who can access these files and who actually uses them. With this actionable information, your risk, compliance and data security officers and IT security pros can prioritize their efforts and secure data in accordance with its value or sensitivity. Your organization will be able to mitigate the risk of PII, PHI, PCI and IP being stored outside dedicated locations, and apply controls and policies consistently and accurately, ensuring both data security and regulatory compliance.

With Netwrix Auditor Data Discovery and Classification, you can identify, classify and secure sensitive data on Windows file servers, EMC storage devices and NetApp filer appliances.

Major benefits:

- Gain a high-level view of the sensitive data you store
- Discover sensitive data stored outside of a secure dedicated location
- Streamline regular attestations of access rights to sensitive data
- Detect unauthorized activity that might threaten your sensitive data

2. What's New in Netwrix Auditor Data Discovery and Classification

- The new multi-server DDC Collector deployment mode and various performance optimizations enable support for extra-large file repositories. Now you can scan and classify up to 32 million files. Main operational improvements are: optimized speed of database usage, refined DDC Provider data delivery mechanism , speeding of Data Discovery and Classification reports, and more.
- Improved classification accuracy for sensitive cardholder data, personal and financial information using industry-standard validation algorithms (Luhn, IBAN – Mod 97/10, Verhoeff). Out-of-the-box classification rules for the major payment systems (Visa, Mastercard, American Express), Social Security Numbers and IBAN account numbers have been augmented to perform additional checksum verification on identified matches to significantly reduce the number of false positive classifications.
- Added optional regex validation using proximity clues (specific text patterns before or after the match) to enable context-based fine-tuning of regular expression classification rules.
- Added core Australian identification patterns (passport number, AMN, etc.) to the standard PII taxonomy.

3. Known Issues

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

ID	Issue Description	Comment
Bug 99686	Shortly after upgrade, you may receive the error in **Netwrix Auditor System Health** log (Event ID 4408). This error occurs when the product cannot upgrade DDC Collector database to the latest version. In this case, Data Discovery and Classification reports might be temporarily unavailable.	Ignore this error, the product returns to normal. It takes a while.
98669	Data Discovery and Classification reports displayed incorrectly if an item is duplicated in several monitoring plans.	These issues will be fixed in future updates of Netwrix Auditor Data Discovery and Classification. To avoid such scenario, make sure you do not have duplicated items.
98544	Data Discovery and Classification reports displayed incorrectly if a monitoring plan contain duplicated items.	
82050	The following error may occur while Data Discovery and Classification reports generation: "String or binary data would be truncated. The statement has been terminated".	This error occurs if file share path is too long. Workaround: When configuring DDC Collector and Netwrix Auditor data sources, provide shorter path to the monitored file share (not as of root folder).
76343	If different time zones are set on the computers where DDC Collector and Netwrix Auditor reside, the **Classification session** parameter is displayed incorrectly in Data Discovery and Classification reports.	The **Classification session** parameter in reports shows local time of the computer where DDC Collector resides.
76337	If taxonomy name in DDC Collector console contains comma (,) a user cannot subscribe to any Data Discovery and Classification report.	