

Netwrix Auditor Data Discovery and Classification Release Notes

Version: 9.5
8/2/2018



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.

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 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

Since the main release of Netwrix Auditor Data Discovery and Classification, several improvements have been added to the product. These improvements for Update 2 and Update 1 are listed below.

2.1. Update 2

With the latest fixes, file paths longer than 260 characters are supported when uploading data to *Netwrix_Categories* database.

2.2. Update 1

The following improvements were implemented:

- Significant boost in performance
- Improved and more accurate reporting
- DDC Provider is integrated with Netwrix Auditor and can be configured using a new Netwrix Auditor DDC Configuration tool
- Assistance with upgrading to the latest version of Netwrix Auditor Data Discovery and Classification

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
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).
82446	Shortly after first start, the Indexer component may have red status on the Dashboard tab in DDC Collector console.	Workaround: Restart the conceptIndexer service manually via Services snap-in.
81963	If Netwrix Auditor 9.6 used one account to connect to Audit Database and DDC Provider used another account to connect to the Categories database , after upgrade, Categories database upgrade may fail or DDC Provider may work incorrectly.	Consider one of the following workarounds: <ul style="list-style-type: none"> Grant the Database owner (db_owner) role on the Categories database to the Audit Database service account. Delete the Categories database and restart the Netwrix Auditor Management Service. The service recreates the database with required settings.
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.	

4. What Has Been Fixed

This section lists customer issues that have been fixed in Data Discovery and Classification 9.5.

Issue	Description
Bug 85728	Cannot process file paths longer than 260 characters when uploading data to <i>Netwrix_Categories</i> database.
Bug 81188	DDC Provider cannot process Sources if the "Anonymous Access Allowed" option disabled for files and folders.
Bug 79175	While processing large amount of files, DDC Provider cannot process files path to which contains special characters.
Bug 76475	The current version of Data Discovery and Classification does not support DDC Provider upgrade.
Bug 76389	The System Health dashboard displays the following Global message: IFilter for ".PDF" documents not found.
Bug 77580	In some reports, filtering by category may not be applied properly if you are processing large amount of data.
Bug 71524	Data Discovery and Classification reports may contain files and / or folders that have been removed.