File Access Manager

Release Notes

Version: 8.3 Revised: March 30, 2022

Contents

File Access Manager Release Notes

Server Support Information

System	Supported Versions
File Access Manager Servers	Windows 2012R2 / 2016 / 2019 / 2022
Workstation	Windows 7 and above
Browser	IE11, Edge, Safari, Chrome, Firefox
Database	MS SQL Server 2012 / 2014 / 2016 / 2017 / 2019

New Features

Data Subject Access Requests - DSAR Campaign Workflows

Introducing Data Subject Request Campaign Workflows. A new screen under the **Compliance** menu enables the following:

- Creating and running a DSAR request, defining the parameters and purpose (The purpose depends on the user request, and determines the final outcome of the process. The defined purposes are: Information disclosure, data redaction, and data deletion)
- Performing searches for personal identifiable information (PII)
- Performing bulk background searches of multiple DSARs
- Sharing results with stakeholders for additional verification and approval
- Tracking requests, providing additional access context
- Performing data removal and / or redaction, as requested
- Verifying the actions
- Generating reports and exporting the results

  File Access Manager supports DSAR for different purposes. DSAR Purposes depend on the requester reason for submitting the request, and effect the request handling workflow.

  - Information Disclosure
  - Data Redaction
  - Data Deletion

Background

Recent Regulation requires organizations to identify and detect personal identifiable information, such as name, address / location, SSN, IDs, email addresses, account #, etc.

Additionally, organizations are required to provide requesters the ability to:

- Receive the information in the form of an electronic file, with other PII information redacted.
- Perform changes and modifications to the information.
- Request that information be obfuscated or deleted - what is known as “the right to be forgotten”.

These requests are called Data Subject Access Requests, or DSARs

Data Privacy Toggle within Application Wizard

All applications that support Data Classifications now have a new toggle within the Application Wizard. A new toggle has been incorporated for applications that support Data Privacy.

This privacy task will be executed by Data Classification Engines. Admins can choose to use the same engine as used in the Data Classification task or use a different engine for the privacy task.

Federated Accounts Support with AWS S3 Connector

The AWS S3 Bucket Connector can now associate Active Directory Federated Accounts with their effective access on AWS Resources and assumed IAM Roles.

Steps on how to integrate the AWS S3 connector with Active Directory can be found in the AWS S3 Buckets Connector guide in the section titled "Active Directory Integration with AWS".

SQL Server Events Backup Toggle

Admins can now disable aspects of event backups to save space in SQL or to improve performance when saving and deleting events.

The new configuration options can be found in the Activities chapter of the Administrator Guide.

Google Drive Shared Drive Support

If members are assigned to shared drives that exist in the domain, a Shared Drive tree root will represent those resources.

See the "How is Google Drive Mapping Converted to a Business Resources Tree" section in the Google Drive Connector Guide.

Unattended Collectors Installation

The Collector Bulk Installer installs and uninstalls Windows File Server Activity Monitors, Permission Collection, and Data Classification Collectors in an unattended fashion. It simplifies the installation process when many services need to be installed.

The Unattended Collectors Installation Guide goes into detail about unattended installation.

Business Website Custom IIS Settings

Administrators can now configure custom IIS settings and set the Business Website's name, port, and installation folder location, on a system-wide level.

For information on how to configure custom IIS settings, please see the File Access Manager Installation Guide.

New Connectors

Azure Files

This connector enables you to use File Access Management to access and analyze data stored in Azure Files. This connector supports permissions collection, data classification, and automated governance processes.

Enhancements

Data Classification reports

Sensitive Data reports maximum size limitation was adjusted to the system wide maximum report size setting, with a maximum cap of 1M records.

Data Classification Policy Updates

The following Data Classification policies have been updated:

- GDPR
- ICD
- PII

The following changes were made to Rules and Policy Objects:

- The EU Phone Number policy rule was split to individual rules per EU country
- Updated the IBAN verification algorithm
- Updated the Canadian SIN# verification algorithm
- Updated ICD Terms based on new WHO definitions
- Updated credit card regular expressions