



File Access Manager

Release Notes

Version: 8.3 Revised: March 30, 2022

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive Identity” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Contents	ii
File Access Manager Release Notes	3
Server Support Information	3
New Features	3
Data Subject Access Requests - DSAR Campaign Workflows	3
Data Privacy Toggle within Application Wizard	4
Federated Accounts Support with AWS S3 Connector	4
SQL Server Events Backup Toggle	4
Google Drive Shared Drive Support	4
Unattended Collectors Installation	4
Business Website Custom IIS Settings	4
New Connectors	4
Enhancements	5

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