File Access Manager

Release Notes

Version: 8.2 Revised: July 18, 2021

Contents

IdentityIQ File Access Manager Release Notes

Release 8.2 Overview

Starting with v8.2, File Access Manager is Common Criteria certified.

Migrating Functionality from the Administrative Client Windows Application to the Website

Resource explorer with enhanced capabilities

New Application wizard

User scope change management

Automatic ownership assignment, and user scope change management

New Connectors

AWS S3 Bucket

Linux

Connectivity Changes

SAML-Based SSO Authentication

Full OAuth Support for all O365 Endpoints

Enhancements

Improvements in Reports - Including resource and ownership scope in Stale Data

Sub-resources scope added in most reports

New System Usage report

Platform

All File Access Manager Services now run on .NET Core

With the exception of the user interface and the admin client that require .NET Framework 4.7.2

Features Removed in this Version

Several legacy systems are no longer supported. see full list in Discontinued Features.

These systems will continue to be supported in earlier versions of File Access Manager (Formerly, SecurityIQ), according to the support matrix and official documentation for each release.

Server Support Information

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

New Features

New Connectors

AWS S3 Buckets

The AWS S3 Buckets connectors supports permissions analysis and governance processes, using modern authentication method connecting to an AWS accounts.

- Analyzing access privileges down to the file level.
- Analyzing access rights granted to identities in AWS under all accounts in the organization.
- Permissions analysis of IAM and bucket policies.
- Public access ACL level permissions.
- Region and OU filtering and searching for resources and accounts.

Linux

The Linux connector supports data classification, permissions analysis and its corresponding governance processes for all major Linux distributions

- Tested for the following versions:
  - Ubuntu versions 18.04 and 20.04
  - Red Hat Enterprise Linux versions 7 and 8
  - CentOS versions 7 and 8
- Governing access to resources, and analyzing permissions granted to users from NIS & AD identity stores as well as local users and groups.
- Analyzing native POSIX (UGO) permissions types and the more granular ACL permission model.
- Identifying sensitive and regulated information in files through data classification.

Full OAuth Support for all O365 Endpoints

File Access Manager Azure AD and O365 Connectors now offer Full OAuth 2.0 Authentication, removing the need to provide user / password credentials, and allowing the enforcement of MFA, conditional access and additional security requirements.

This change effects the following modules:

- Azure Active Directory
- Exchange Online
- SharePoint Online
    - Adding support for permission collection, in addition to the existing capabilities for activity monitoring
- OneDrive
    - File-level permission no longer requires user / password credentials

SAML-Based SSO Authentication

The File Access Manager login process can be integrated with any identity provider (IdP) supporting SAML 2.0-based authentication.

Detailed integration steps are available for the following providers:

- Azure
- Okta
- ADFS

Enhancements

.NET Core Migration

All File Access Manager services now run .NET Core, with the exception of the user interface and the admin client that require .NET Framework 4.7.2

Verification Algorithms' For Data Classification Support Platforms

- When writing verification algorithms for data classification, the assembly must target .NET Standard 2.1 or .NET Core up to 3.1 These will be referred to as the supported .NET platform.

> Verification algorithm assemblies written in previous versions (in .NET Framework 4.5) must be removed, and re-written to target one of the supported .NET platforms as mentioned above, and uploaded again.

New Application Wizard Enhancements

In addition to migrating the application wizard to the website, the following changes were made:

The application logical containers were replaced with tags.

The tags are used for filtering and classifying applications.

Every application can contain multiple tags (As opposed to the logical containers).

Exiting containers are now represented by tags.

All newly created applications will be placed in a default "Applications" container in the Admin Client.

Modification of User Exit Data Source

- When creating a user exit data source, the fields Username, Domain, Password are now compulsory.

Permission Forensics

Permission Forensics filters with business resource name or business resource full path now support only the following operators:

- Any of
- Equals

The upgrade process will delete the operator and value fields for filters **with business resource name or business resource full path**. These should be filled in following the upgrade.

Filters for these fields will not offer the auto-complete feature.

Existing filters with operators that are no longer supported will be highlighted and prompt for changing the filter query.

SCIM API

The Permission SCIM endpoint was added a classification category filter, for retrieving permission sets associated with a specific data classfication category.

Stale Data Report

Two enhancements were added to the Stale Data Report template:

- A Resource Level Scope – Similar to the Activity Report template, this adds the ability to produce a report on a single or multiple resource with or without their sub-resources.
- Data Owner Filter – Allows users to filter report results (based on scope) by the following:
    - Any resource with a Data Owner
    - Any resource without a Data Owner
    - Any resource with specific Data Owners

Data Classification

Composite Rules

A change in a composite rule will no longer trigger a new composite calculation task.

Composite rule calculation will run on classification results from a single application.

Monitored Actions Migration

File Access Manager supports the following two modes for Activity Monitoring:

- Full Learning Mode – Activity Monitoring is enabled for all resources, and all actions are monitored.
- Semi-Learning Mode – Activity Monitoring is enabled for selected Top-level resources. This mode allows selecting the types of audited / monitored actions. (Everything below the selected top-level resources in their hierarchy will inherit the same settings),

Full Scope for Compliance Manager and Auditor Roles

The Compliance Manager and Auditor capabilities now have full scope, and can view and manage all resources, in all applications.

Previously, full scope was enabled only for the Administrator capability.

There is no change in the actions included in these capabilities and the functionality available to them.

Import User Scope

The Import User Scope functionality supports changes and adjustments to existing scopes. New imports will not override existing scopes and manually-set data owners, but will retain or adjust the existing scope assignments based on the specified action.

There is also a new "Action" field within the Import User Scope display. The four possible actions related to a resource include Add, Remove, Clear, and Data Owner.

The Data Owner action will automatically add the Data Owner capability to the assigned user, in addition to adding the scope.

One-way Trust Corrections

Corrections to one-way Active Directory domain trusts synchronization and improvements to the trusted domain enumeration order. This change should only impact users that utilize and have previously configured one-way trusts within File Access Manager. These changes may incur some changes to your current File Access Manager set up and may require some further actions by File Access Manager Administrators. See One-Way Trust Corrections in 8.2 and upcoming 8.1 SP4 in Compass for further details.

Features Moved to the Website

The following features have been rewritten and added to the IdentityIQ File Access Manager website. The corresponding features were removed from the IdentityIQ File Access Manager Administrative Client as part of a phase out of this interface.

“Date Sources” Page

Website path

Admin > Data sources

Moved from Admin Client path

File Access Manager > Data Sources

Description

A data source is a table containing data accumulated from various sources, including internal File Access Manager reports, for use in various system locations

Manage Normalized Resources

Managing normalized resources lets you view, add or remove resources to normalize, per application, determine how to handle inexact permissions matches during a normalization process, and run or schedule a report of normalized resources.

To access the normalized resources - select from the dropdown menu on the row of the required application, on the Applications page.

> As part of the conversion, the csv file format for bulk set / remove of normalization files was changed. The csv file format should be in UTF-8 encoding (in previous versions the csv file uploaded into the Administrator Client had to be in Unicode)

“Data Dictionary” Page

Website path

Admin > Permissions Management > Data Dictionary Fields

Moved from Admin Client path

Application > Configuration > Permissions Management > Manage Data Dictionary

Description

Manage the data dictionary fields - attributes to define the data types in the system. The user can add new data dictionary types for Users, Groups, Business Resources, and Permission Type. Each data type has a separate list of data fields

“SMTP Account Configuration” Page

Website path

Settings > General > SMTP Account

Moved from Admin Client path

Applications > Configuration > General Configuration > File Access Manager SMTP Account

Description

Used to configure the connection to the organization email server to send notifications, reports, and reminders to users.

An additional field of "From" has been added to the configuration page. This is a unified From field that replaces the current From field from all the Email responses.

The upgrade process will take the report response From field as the unified email From value.

“Applications" Page and Wizards

Website path

Admin > Applications

Moved from Admin Client path

Applications

Description

Rebuilding the Application page from the administrative client and adding it to the website.

The Application page is used for configuring applications to be used as sources in File Access manager.

The new data grid displays all the applications in a single table, showing the options of File Access Manager for each application (Activity monitoring, permission collection, data classification, etc.)

Conversion Behavior

- In the conversion to 8.2, the parameter **logical container** in applications created in previous versions of IdentityIQ File Access Manager will be converted to **Tags**.

Modifications from Previous Versions

- In the Crawl scope configuration, when refreshing the list of top level resources, running the task will not clear the list of top level resources to exclude.

Discontinued Features

Installation

- The SMTP Account Configuration will no longer be prompted as part of the installation of the administrative client. The administrator will have to configure the connection to the organization email server using the SMTP account configuration page on the website.
- MS SQL 2008, 2008 R2 are no longer supported as a File Access Manager Database

Connectors

The following versions of connectors are no longer supported:

Windows file server 2008, 2008 R2, 2012

(Version 2012 R2 - will continue to be supported)

SharePoint 2010

Exchange 2010

SQL Server 2008, 2008R2, 2012

These legacy systems will continue to be supported in earlier versions of File Access Manager (Formerly, SecurityIQ), according to the support matrix and official documentation for each release.

Newer version of these systems will be supported by File Access Manager as managed application types, according to the product support matrix and official documentation available on Compass.

Generic Table connector no longer supports permission collection

Activity Monitor

When an activity from an unknown resource is detected, there is no longer the option to discard the activity ("No auto learning mode")

During the upgrade process, activity monitors that had this setting will be set to Store the Activity (Full learning mode)

Isilon Access Zone and Management IP app.config Setting Keys

App.Config Settings Keys will be deprecated in File Access Manager release 8.2

The Access Zone and Management IP app.config settings keys, in the activity monitoring and permission collection services configuration files, that were being used until now to configure Non-System Access zone applications in File

Access Manager , have been replaced with the Access Zone and Management IP application configuration fields, that are available through the application configuration wizard. See EMC Isilon Connector Configuration guide for further details.

Upgrade Considerations

Verification algorithm assemblies of data classification written in previous versions (in .NET Framework 4.5) must be removed, and re-written to target .NET Standard 2.1 or .NET Core up to 3.1, and uploaded again.