SailPoint IdentityIQ

Version: 8.0

File Access Manager Release Notes

IdentityIQ File Access Manager Release Notes

These are the release notes for IdentityIQ File Access Manager, version 8.0.

The release notes contain the following information:

- New Features
- Enhancements
- Discontinued features
- Upgrade considerations
- Known issues

Server Support Information:

System	Supported Versions
IdentityIQ File Access Manager Servers	Windows 2012/2012R2/2016 / 2019*
Workstation	Windows 7 and above
Browser	IE11, Edge, Safari, Chrome, Firefox
Database	MS SQL Server 2008R2/2012/2014/2016/2017*

* Support for this version was added in release 8.0 of IdentityIQ File Access Manager

New Features

Terminology changes in 8.0

With the rebranding of SecurityIQ to **IdentityIQ File Access Manager**, the terms below have been converted to fit the IdentityIQ terminology and schema. Some of the legacy terms might still appear in some of the application screens and the accompanying documentation.

IdentityIQ File Access Manager release 8.0 is the next release following SecurityIQ release 6.1

IdentityIQ File Access Manager term	Legacy term
IdentityIQ File Access Manager	SecurityIQ
Capability	Role*
Right	Permission*

* These terms are still in use in the IdentityIQ File Access Manager Admin Client.

Disaster Recovery

Support of a parallel disaster recovery environment with a one-step failover from Production to the Disaster Recovery environment and back.

Each server can be designated as either Production or Disaster Recovery. For each service and collector installed the user assigns a Production server, and, an optional Disaster Recovery server.

User Rights and Scope Management

This release introduced a new concept to the File Access Manager web client: Role-based user access management. The File Access Manager administrator can now determine **what** a user can do in the File Access Manager (rights and capabilities), and **which business resources** each user can view (user scope).

The administrator can create capabilities (sets of user rights) to fit their needs, in terms of screens the user can access, and actions the user can perform on each screen.

The user scope can be added individually or uploaded from a file via a scheduled task to maintain a fully up to date list.

You can assign “Full Scope” to a user – thus granting access to everything.

Assigning AD Groups to Capabilities

You can now assign Active Directory groups to capabilities, thus granting the entire group access to IdentityIQ File Access Manager. Previously it was necessary to add each member individually.

Data Classification

OCR capability for Data Classification

The Data Classification has been extended to identify text within image files using optical character recognition. This will enable identifying sensitive data over text embedded in scanned documents, pictures etc. This will help enforcement of the existing Data Classification rules over a wider set of content.

The OCR process should be configured carefully to concentrate the scanning on business resources that are likely to contain sensitive data.

New file extensions identified by Data Classification

The classification engine reads file content, based on the file extension.

The following file extensions were added to the Data Classification:

Text: csv (Comma Separated Values files)

Image (See OCR above): jpeg, jpg, tif, tiff, gif, png, wmf, emf, bmp,

File-Level permission collection

Cloud application storage enables maintaining permissions below a folder (or similar) level.

File level permission collection was added to the following applications:

- One Drive
- SharePoint Online

This capability is set to inactive by default for performance reasons.

Security Enhancements

Allow using external CA issued certificates

Expanding our current self-signed certificate mechanism to allow external certificates.

New Connectors

CIFS Connector

A generic CIFS connector which can be renamed per deployment.

This connector supports Crawl, Permission Collection and Data Classification.

This connector does not include local users/groups when collecting permissions.

MS SQL Connector

The SQL connector enables connection to an MS SQL resource. The connector supports crawling, and permissions collection. This connector does not perform actual direct activity monitoring as other File Access Manager connectors do. It can be configured to analyze user generated activity data for use within File Access Manager.

CTERA connector

CTERA provides cloud gateway services to organizations. This new connector for CTERA connects to a CTERA master gateway. It supports crawling, permission collection, and data classification.

Windows file server

The Windows File Server connector has been expanded to support Windows Server 2019

New IdentityIQ File Access Manager APIs

DataClassificationCategories

The API retrieves a list of all File Access Manager Data Classification categories. An optional filter of category enables calling a single category record.

DataClassificationResults

For each resource requested, this endpoint returns an object including the file name, policy, rule, and categories that triggered the classification for this file, as well as the number of times a category match was found. This endpoint supports DFS addresses, if the DFS applicationId is requested.

Capabilities

The API retrieves a list of capabilities, including the capability description, the rights each capability includes, and associated users and groups. Optional filters include capability, right, and user names.

KPIs

The API returns the count and score of KPIs calculated in IdentityIQ File Access Manager. This is a read only endpoint.

IdentityIQ File Access Manager Web Client New Features

Localization expanded to include these additional languages:

- Traditional Chinese/ZH-TW
- Swedish/sv-se
- Dutch/nl-nl
- Danish/da

Filtering Campaigns by current status

Filtering expanded to include all campaign statuses, when selecting running, completed, or failed campaigns.

Audit Log

IdentityIQ File Access Manager now stores all activities in the web client to an audit log on a database. Administrators can run a report to view and export all or part of this audit log.

Enhancements

Updates to IdentityIQ File Access Manager APIs

businessResource Endpoint

New filter parameter: *parentResourceId*. When used, the filter will return the first level under the parentResouceId. If it is empty, the filter will return the top level only.

Updated filter parameter: *parentApplicationID*. from this release it can be sent alone. If so, the endpoint will return the top-level resources of the specified application.

Permissions Endpoint

New filter parameter: userUniqueIdentifier added alongside groupUniqueIdentifier to return the permissions of the user or group on each business resource.

Installation process

Supporting Strict CLR Security when connecting to an SQL Server 2017 and above. The new option **"Assemblies Certificate checkbox"** in the installation screen will import a certificate into the Master database.

Notification of new File Access Manager Releases

When there are new software updates for IdentityIQ File Access Manager, the system will send an email to the application administrator to notify them.

Auto-retry of tasks

The user can now set an auto-retry for failed tasks. The setting is done in the web client per task type. By default, some task types are set to auto retry twice. A full list is in the documentation.

Data Classification can read unencrypted metadata of encrypted files

The Data Classification module supports reading unencrypted metadata from encrypted files.

IdentityIQ File Access Manager Web Client enhancements

Updated web client URLs

The IdentityIQ File Access Manager web client was renamed to: [server]/identityiqfam

The API documentation has been renamed to: [server]/identityiqfamapi/docs/

Menu navigation updates

The IdentityIQ File Access Manager is in process of migration to a new design of the user interface. Screens will be transferring to the new design over the next few releases.

1) **Settings → * Exclusions menus**: Unifying these menus to be under the menu item

Settings → Account Exclusions

- Goals Exclusions (Previously called "Data Owner Exclusions")

- Alert Exclusions
- Sensitive Account Exclusions

2) The tabs under **Settings→General** have been expanded to a full screen and are accessible via a submenu under **Settings → General**.
   - Path Display
   - Overexposed Resources
   - Task Auto Retry
   - API Authentication

Data Ownership

Bulk Data Owners Import removed from the admin client
User Scope Import added to the web client

Removed the Resources → Dashboard screen Data Ownership widget from the user Dashboard

To access the KPI data for any owned resources, simply grant the user the right to access the **Dashboard → Data Owner** screen.

(Note: This does not grant data owner capability. Only access to the screen)

Reports

Add filter for 'Number of matches' in all Classified Data report templates

Added a filter to the Data Classification report templates by number of matches – larger or smaller than a given match count.

Process improvements

The stale data calculation was enhanced to include more methods of determining when a business resource was last accessed.

Performance improvements

Avoid Activity Duplication for Windows file servers

Activities are now listed under the share that the activity was executed in. We no longer duplicate the activity in case there is an overlapping share.

First Crawl Time

Significant improvements in the crawl code. The first crawl time is improved by approximately 40%.

Supported environment

Added / verified support to install the IdentityIQ File Access Manager on the following environments / platforms:

- SQL Server 2017
- Windows server 2019

Connectors

SharePoint server connector verified to support SharePoint 2019

Discontinued Support and Features

This section lists main features that have been removed from the menus compared to the previous release. Features were moved / removed / renamed mostly for the following reasons:

- Renaming features, menus and terms as part of the rebranding to IdentityIQ
- Part of the ongoing migration features from the admin client to the web client
- Rearranging and relocating features to improve performance and user experience

Event Manager

Cancel the BR creation in the Event Manager service

The Event Manager no longer creates a new resource when an activity is identified on an unknown resource. The activity will still be stored.

Data Owner related features discontinued

The concept of Data Owners has been revisited in this release. The following features and actions will no longer be available:

Bulk Data Owners Import removed from the admin client

Bulk upload of user scope is now available via the User Scope import in the web client.

Intra-service communication

IdentityIQ File Access Manager services no longer have an option to use non-SSL communication

SecurityIQ for Oracle ERP Connector

As mentioned in release 6.1 - This connector has reached end of life and will no longer be supported.

SecurityIQ for SAP ERP Connector

As mentioned in release 6.1 - This connector has reached end of life and will no longer be supported.