SailPoint IdentityIQ

Minor Release Version: 8.0.1

File Access Manager Release Notes

IdentityIQ File Access Manager Release Notes

These are the release notes for IdentityIQ File Access Manager, version 8.0.1.

The release notes contain the following information:

- New Features
- Enhancements

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 8.0.1 of IdentityIQ File Access Manager

Minor Release overview

This minor release of IdentityIQ File Access Manager focuses on:

- UI enhancements to make the flow and configuration more intuitive
- Unattended installation of File Access Manger services across many servers
- Custom script fulfillment
- One Drive sharing
- Tracking Active Directory authentication
- Migrating the Permission Forensics and Task Management screens from the administrative client to the web application.

New Features

IdentityIQ File Access Manager Web Application New Features

Task Management: Scheduled Tasks and Tasks (previously known as My Tasks) screen moved from the Admin Client to the web application

The screens **My Tasks** and **Scheduled Tasks** were removed from the Admin Client, and added to the web application. The new screens in the web application have enhanced filtering and actions from the task tables themselves.

Installation note: When installing File Access Manager for the first time, the "Identity Sync" task has to complete its operation in order to get a list of users who can log into the web application. You can follow the progress of this task on the Health Center in the admin client. (The task status is generally displayed in the web application which you cannot access before this task has completed.)

Unattended installation of File Access Manger services across many servers

The installation can now be performed on multiple servers by running the File Access Manager installer wizard once, and then running installation commands via a distribution tool or other method.

The services to servers mapping is stored in the database, and the application creates a command file for the users to configure per installation server.

Enhancements

Custom access fulfillment request

Adding automatic fulfillment of unmanaged BRs via user script.

Until this release, unmanaged resources required a manual process of adding or revoking permissions. This is available in access requests and campaigns.

Crawler inclusion and exclusion lists simplified

- A new panel in the application definition screen is used to identify the top level resources for applications. This screen can be used to exclude top level resources from the crawl process.
- Create a list of resource paths to include or exclude from the crawl process from within the crawler configuration tab. This can be used instead of the regex exclusion entry.

Error message clarifications

Added details and clarification to some of the error messages and log messages following customer requests.

IdentityIQ File Access Manager Web Application enhancements

Moved "Task Auto Retry" from the General top menu to Task Management top menu

Screens and functionality moved from the admin client to the web application

Screens and functionality are in process of being migrated from the administrator client to the File Access Manager web application. Where possible, the functionality remains unchanged.

Permissions Forensics screen (Rewritten from the administrative client)

The Permission Forensics screen lets the user monitor and analyze the user and group permissions

- Create queries to analyze the permission of specific groups of users
- Save and share queries for selecting users and groups
- Generate reports
- Run permission scans
- Revoke explicit permissions of users.

Task Management screens (Rewritten from the administrative client)

- Tasks
- Scheduled Tasks
- Task Auto Retry

Connectors

Exchange: Added support for Exchange 2016 installation on Windows server 2016

In previous versions this combination of installation required a workaround, due to a Microsoft issue. This involved installing an additional Client Access Service (CAS) on a non-2016 Windows Server, and configuring the IdentityIQ File Access Manager Exchange Application Monitor to access that CAS server.

Exchange 2016 installed on Windows Server 2016 can now be connected directly to the File Access Manager Exchange connector.

Active Directory: Added failed logon attempt EventIDs to AD connector

Added the ability to capture EventIDs 4625, 4740, and 4771 for failed logon attempts from Active Directory.

Added support for SharePoint version 2019

Extended the support of SharePoint server connector to version 2019

Google Drive connector updated to support V2 of the API

Upgraded from the depreciated version 1 of the API to version 2

One Drive – Added new types for shared permissons

Added permission types for users who gained permissions through sharing links:

- Share for view only
- Share for Edit