SailPoint IdentityIQ

File Access Manager v8.5 Service Pack 1 Deployment Guide

Version: 8.5 SP1
Revised: May 22nd, 2026

Table of Contents

Table of Contents

List of Figures

IMPORTANT

Please read this Deployment Guide carefully as this is a unique installation and requires special considerations.

This version of FAM supports new installations as well as seamless upgrades from version 8.5 only (.NET 8 required).

This 8.5 package is NOT applicable for versions prior to 8.4 SP7 of FAM. You will need to update to 8.5 and only then can it be applied.

Microsoft's SQL Server 2012, 2014 and 2016 are no longer supported, make sure to upgrade to a supported version before applying this Service Pack.

Chapter 1: Planning Your Service Pack Deployment

What is a Service Pack?

Service Packs are cumulative packages containing all released E-Fixes to date since the last Major or Patch release. Service Packs allow customers to stay up to date with the latest bug fixes and performance enhancements, with minimal down time and without the need to upgrade. Service Packs only update the File Access Manager components for which bug fixes or performance enhancements were issued, while the rest of the system remains untouched.

Service Packs Deployment Process

Starting from version 6.1, SecurityIQ (FAM) Service Packs deployment is done automatically. Service Packs are deployed by the File Access Manager update deployment mechanism. By simply uploading a Service Package through the Administrative Client, and pressing a button to initiate the deployment, the Service Pack will be deployed and will automatically update all relevant File Access Manager components.

All File Access Manager components, including Web Sites, Administrative Clients, Core Services, Activity Monitors, Permission Collection and Data Classification Engine and Collectors, Watchdogs and the File Access Manager Database, will be updated – provided that the service pack contains update for the specific component.

The only exception to that is the File Access Manager Collector Manager – used to deploy Collectors and Activity Monitoring Agents – which is a standalone application, and will need to be updated manually, if an update is available.

Version Numbers

The current version number is displayed on the bottom right corner of the Administrative Client screen.

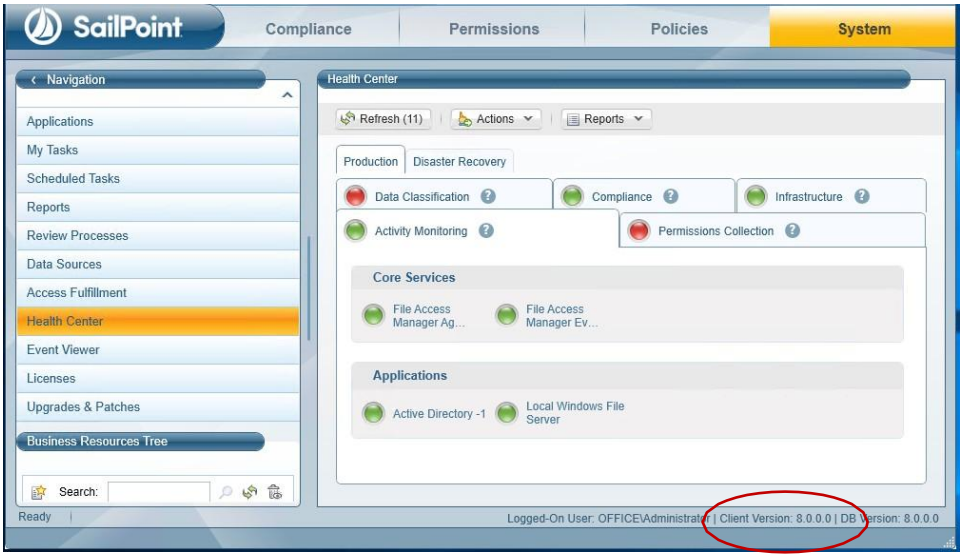


Figure 1 Application Monitors Screen

File Access Manager version numbers are represented by a four-section number, e.g., 8.5.0.1000.
The first two sections represent major releases. File Access Manager 8 GA release number is 8.0.0.0. whereas File Access Manager 8.5 release will be represented by the number 8.5.0.0.
The next section represents Patch Releases, e.g., File Access Manager 8.0P1 version number is 8.0.1.0.
Service Pack updates are reflected in the last section, and so File Access Manager 8.5 Service Pack 1 version number is 8.5.0.1000. This does not apply to this release as it being a major version of FAM.
The Database version number will be updated with every service pack. For File Access Manager 8.5 Service Pack 1, the database version number is 8.5.0.1000.
The Client version number will be updated if the service pack includes changes to the Administrative Client. For File Access Manager 8.5 Service Pack 1, the Client version number is 8.5.0.1000.

Infrastructure components, such as Elasticsearch and RabbitMQ will retain the same version number, unless an update to the actual infrastructure components is applied, in which case their version number will be updated as well. 8.5 majorly includes updates to RabbitMQ, Elasticsearch, Server Installer and more.

Versions included in this release:

Table 2 File Access Manager Component Version Details

Component	Version
File Access Manager Database	8.5.0.1000
File Access Manager Elasticsearch	8.19.4
File Access Manager RabbitMQ	4.2.3
File Access Manager SCIM API	8.5.0.1000
File Access Manager REST API	8.5.0.1000
File Access Manager Business Website	8.5.0.1000
File Access Manager Administrative Client	8.5.0.1000
File Access Manager Data Classification	8.5.0.1000
File Access Manager Permission Collection	8.5.0.1000
File Access Manager Activity Analytics	8.5.0.1000
File Access Manager Agent Configuration Manager	8.5.0.1000
File Access Manager Collector Synchronizer	8.5.0.1000
File Access Manager Crowd Analyzer	8.5.0.1000
File Access Manager Event Manager	8.5.0.1000
File Access Manager Reporting Service	8.5.0.1000
File Access Manager Scheduled Task Handler	8.5.0.1000
File Access Manager User Interface	8.5.0.1000
File Access Manager Watchdog	8.5.0.1000
File Access Manager Workflow Service	8.5.0.1000
File Access Manager Activity Monitor	8.5.0.1000

Backup Measures

Backups are important. Having the original deliverable readily available will allow you to quickly and easily rollback changes if needed. One of the great things about Service Packs is that they allow for small surgical changes to be made to the system, by changing only what is necessary. For that reason, they are also easy to roll back, provided that backup measures have been taken.

Database

As a rule, we recommend that regular backups be performed on the IdentityIQ File Access Manager database.

Service Packs can occasionally require changes to the database, either in the form of content modification on specific tables or in the form of schema changes to the tables and objects in the database.

In the case of schema changes, we recommend that a copy of the original database object be taken. The simplest way of doing that is creating a backup object with a different name, using the script of the original object. In most cases, that would entail generating a Create script of the original object and renaming the object name in the script before execution.

You can consult your DBA on how to create such backup objects.

Other Components

The IdentityIQ File Access Manager updates' deployment mechanism creates a backup for every component updated by the service pack. Once the Service Pack package is loaded and its deployment started, before any changes are made, a backup copy of the updated component is taken and stored in the designated Backup folder. The Backup folder is located under the SailPoint home directory (set by the SAILPOINT_HOME environment variable and is by default at C:\Program Files\SailPoint\). A folder bearing the Service Pack name will be created in the main Backup folder, and a backup of each of the updated components will be created.
For 8.5 the Backup folder would be %FILE_ACCESS_MANAGER_HOME%}\Backup\8.5.0.1000} (*the contents of the folder will be related to the pre-upgraded version*).

Chapter 2: Support Matrix

Table 3 IdentityIQ File Access Manager Server Support Details

System	Supported Versions
IdentityIQ File Access Manager Servers	Windows 2016/2019/2022/2025
Workstation	Windows 8 and above
Browser	Edge, Firefox, Chrome, Safari
Database	MS SQL Server 2017/2019/2022

Chapter 3: Deploying Version 8.5 Service Pack 1

The deployment process consists of the following steps:

1. Downloading the Service Pack from this Compass Location
2. Read the Service Pack deployment guide thoroughly.
3. Pre-deployment Steps; since 8.5, .NET 8 is a must for this version, please make sure to follow the instructions accordingly if needed.
4. Service Pack Deployment
    a. Upload the Service Pack through the Administrative Client
    b. Kick-Off the Service Pack deployment
    c. Verify successfully deployment
    d. Update Client Installer with the latest version
    e. RabbitMQ update (mandatory)
    f. Elasticsearch update (mandatory)
5. Post Deployment Steps

Pre-upgrade Steps

Install FAM 8.5 Prerequisites.

This version of FAM **does not require** any Prerequisites to be executed prior to the actual installation (regardless of whether they were applied previously on any 8.4 Service Pack at all).

Install EXO PowerShell module.

For those who use Exchange Online Connector please follow the installation prerequisites section: **Chapter 4, SIQSUS-881 – Modernize EXO Connectivity v3.0.** , if not used, please continue.

Install .NET 8 (if needed)

IMPORTANT NOTE: DO NOT uninstall or remove any older version of .NET either before or during the upgrade process (including ALL FAM servers) as this could make your installation of FAM fail.

Before starting the installation, gather the required data, open the required ports, and set up the servers, as described. File Access Manager requires the latest ASP.NET Core 8.0.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime.

You can download the latest 8.0.x Hosting Bundle version from here.

Run apps - Runtime ⓘ

ASP.NET Core Runtime 8.0.6

The ASP.NET Core Runtime enables you to run existing web/server applications. **On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.**

IIS runtime support (ASP.NET Core Module v2)
18.0.24141.6

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS		Arm64 | x64
Windows	Hosting Bundle | x64 | x86 | winget instructions	Arm64 | x64 | x86

Caution: Without completing these steps, the installation will fail.

All servers hosting File Access Manager services, including all Activity Monitors must, have .NET 8.0.x installed as a prerequisite for the installation.

The administrative client computer and Business Website service server must contain .NET Framework 4.7.2

Note: .NET Core and .NET Framework 4.7.2 can be installed on the same server.

Verifying .NET Settings

Complete the following steps to verify the version of .NET Core:

1. Open a CMD window.
2. Execute the following command:

a. dotnet --list-runtimes

The output should consist of at **least** these two:

- Microsoft.AspNetCore.App 8.0.x

- Microsoft.NETCore.App 8.0.x

If the command did not execute or the two runtimes mentioned above are not in the output list, reinstall or repair the hosting bundle.

IMPORTANT NOTE: DO NOT uninstall or remove any older version of .NET either before or during the upgrade process (including ALL FAM servers) as this could make your installation of FAM fail.

> Note: .NET Core and .NET Framework 4.7.2 can be installed on the same server.

- **Ensure .NET 8 has been installed at some point.**
- Extract the "File Access Manager v8.5.0.1000.zip" installation package.
- **If this is a fresh FAM deployment, navigate to the "File Access Manager v8.5.0.1000" folder that has been just uncompressed; the Server and Collector installers will be found there to proceed with the normal installation (no further steps from this section are needed).**
- **If this is an UPGRADE of FAM**, log into the IdentityIQ File Access Manager Administrative Client,
- Click **System** >> **Upgrades & Patches** >> **Load New Package**
  This will open the **Load Package** dialog.
- Press **Browse** and load the file "**File_Access_Manager_v8.5.0.1000.wbxpkg**" from the Service Pack folder.
- Press **Upload Package**.
  The system will upload and validate the file. This might take a few minutes.
- Once it is validated, press **Save**. This will add the upgrade package to the upgrades page.

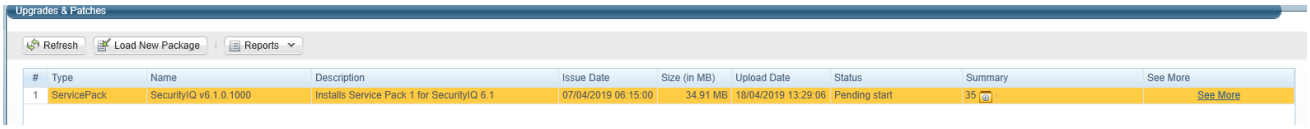


Figure 2: Upgrades & Patches table

- Right click the upgrade package and select **See More** from the menu.

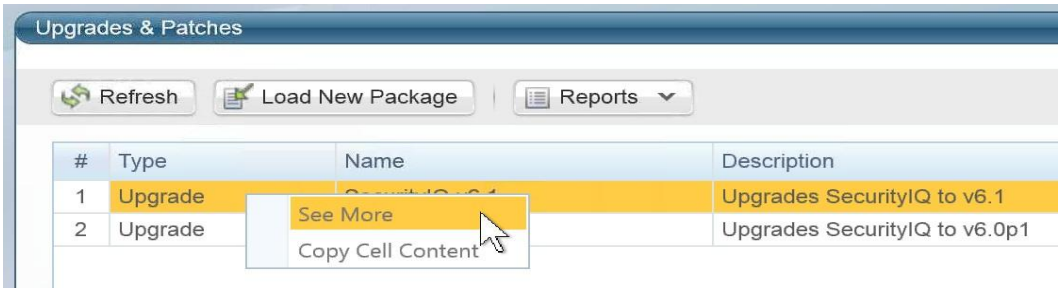


Figure 3: Expand Service Pack package - Details

This will open the upgrade detail panel, showing a list of the upgrade steps included in this package.

Each installation line is listed in "Pending" state when it is added to the upgrade/installation list.

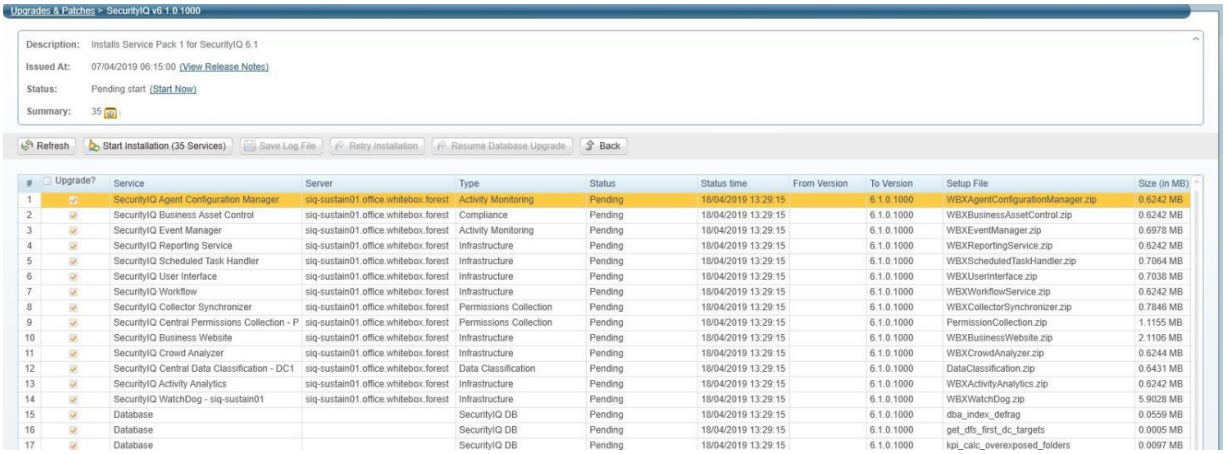


Figure 4: Review Service Pack package - Details

- Click **Start Installation** and **Confirm** to start the installation process.

The Service Pack deployment process runs a series of prerequisites checks before the Database update begins. Then proceeds to perform the Database updates.
Following the Database updates, the first component to be updated will be the Watchdog Service, installed on the server hosting the User Interface core service.
Following that, all other components will be updated.

What if an update line fails?

If a script or a component update fails, right-click the failed line in the **System/Upgrade and Patches** screen and click **Save** to save the log file. The system will download the log file where you can see error messages describing the issues.

After you fix the issue, right-click the failed line and click **Retry** to rerun the script and continue the upgrade process.

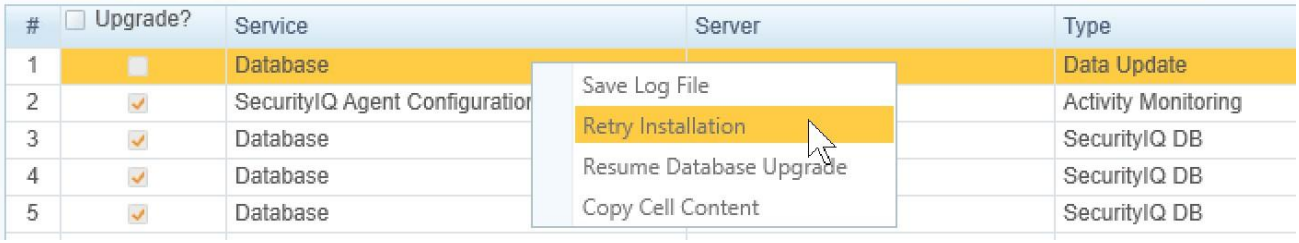


Figure 5: Retry installation line

- Wait until all services have **Completed** or are in a **"Pending Restart"** status.
- If one of the services is in a **"Pending Restart"** status, restart the server on which this service is installed.

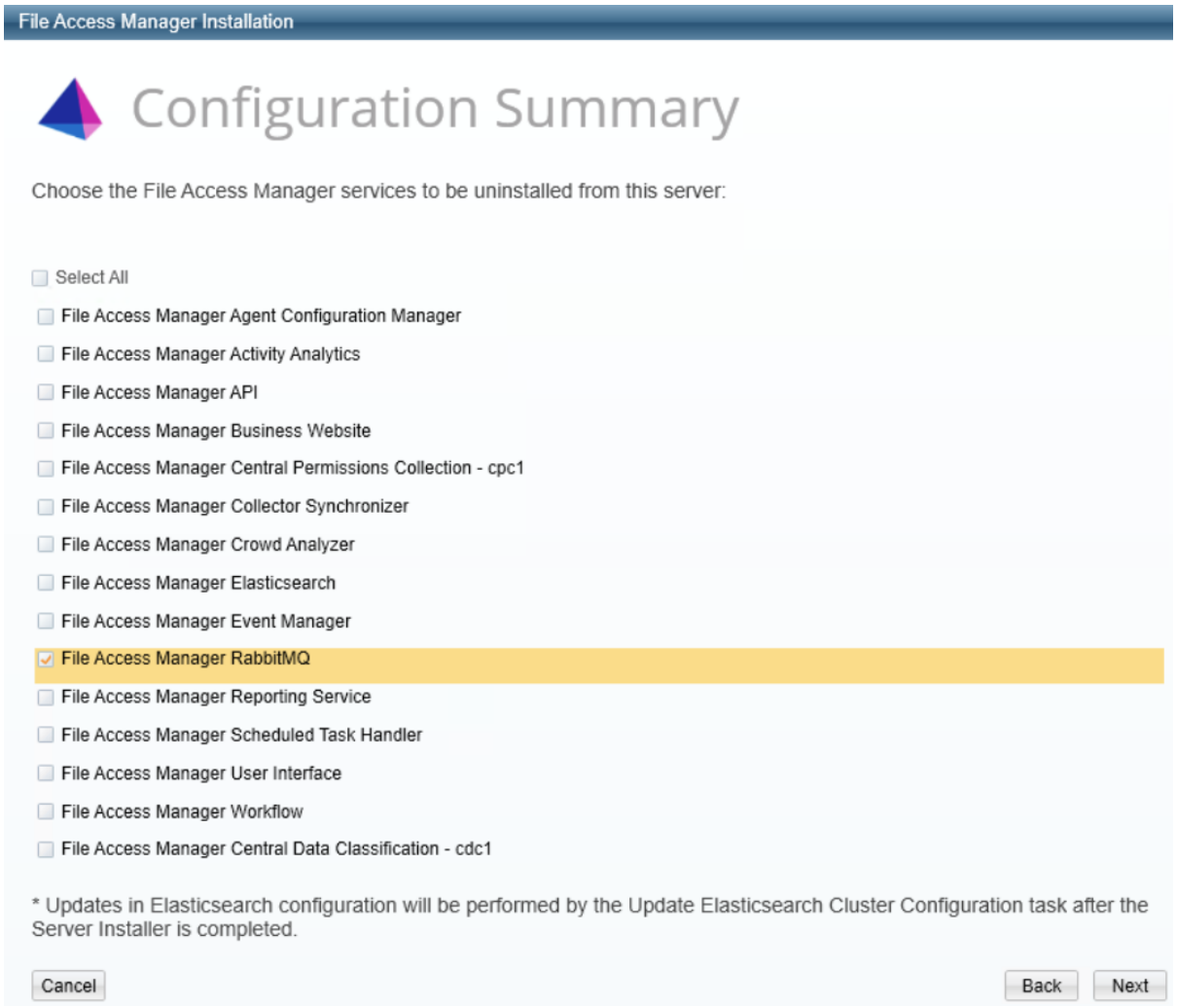
  The Service Pack update will continue automatically after restarting.
- Wait until all services are in **"Completed"** status after restarting.

Note: See *Chapter 5: Troubleshooting* **for further suggestions and information.**

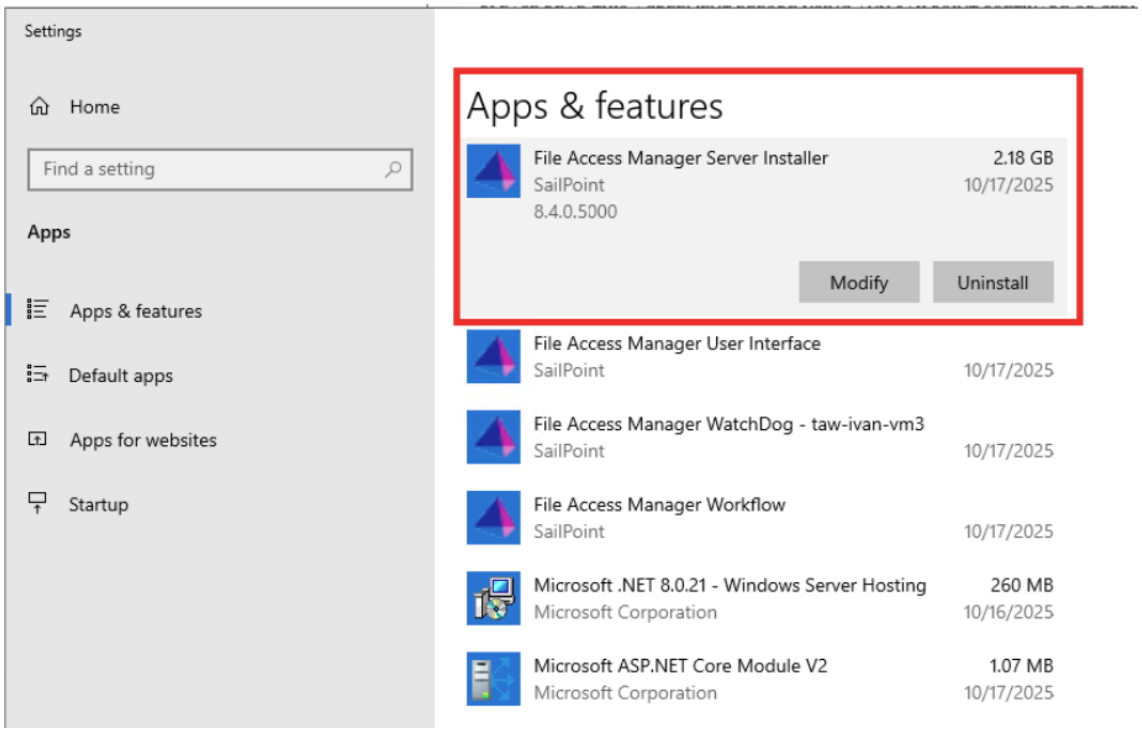
RabbitMQ update to 4.2.3

NOTE: This update is mandatory for this version of FAM 8.5 SP1 and can be applied to any 8.5 Environment.

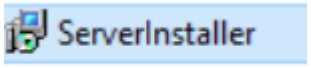
1. Make sure 8.5 SP1 upgrade (WbxPkg) has been already applied successfully.
2. Uninstall RabbitMQ using **current** Server Installer.



3. Once RabbitMQ has been uninstalled, uninstall the current Server Installer by using Add & Remove Programs. This is needed to avoid any conflict with the **8.5.0.1000** Server Installer to be installed in step number 5.

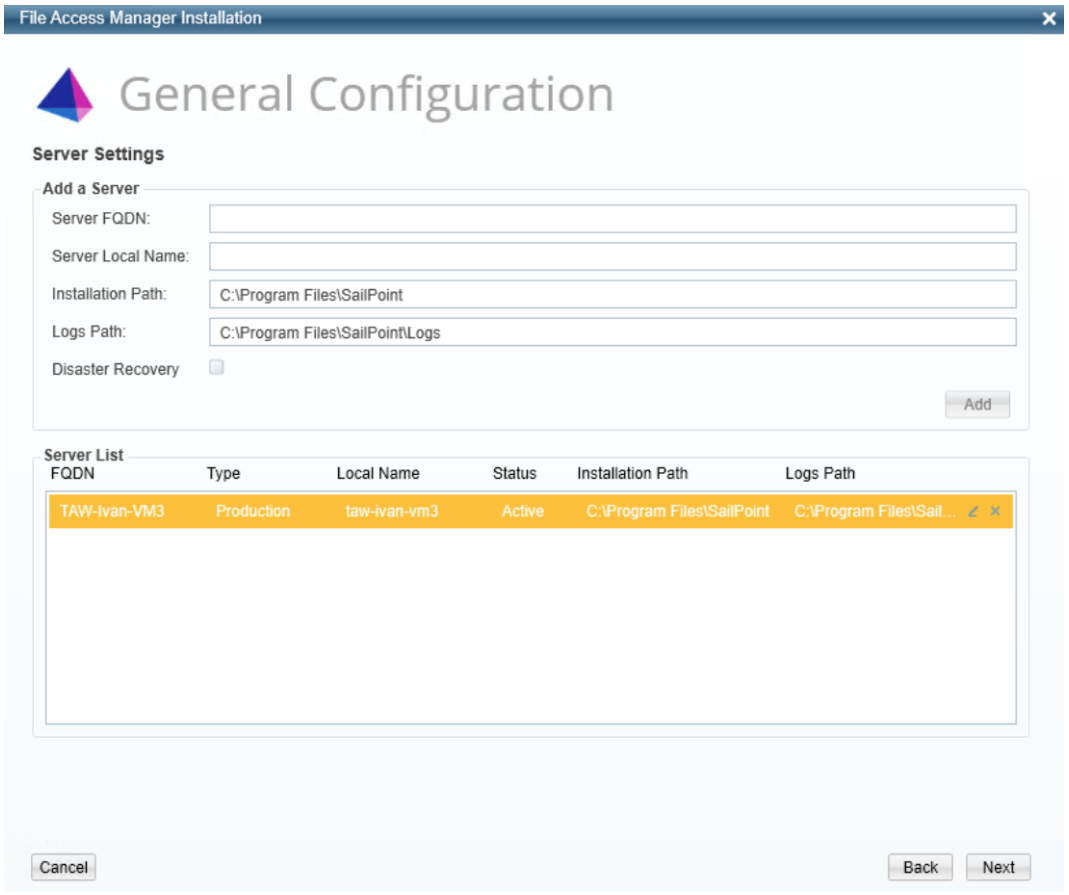


4. Stop All FAM Services.
5. Run ServerInstaller (8.5.0.1000 version) by double clicking from the installation files.

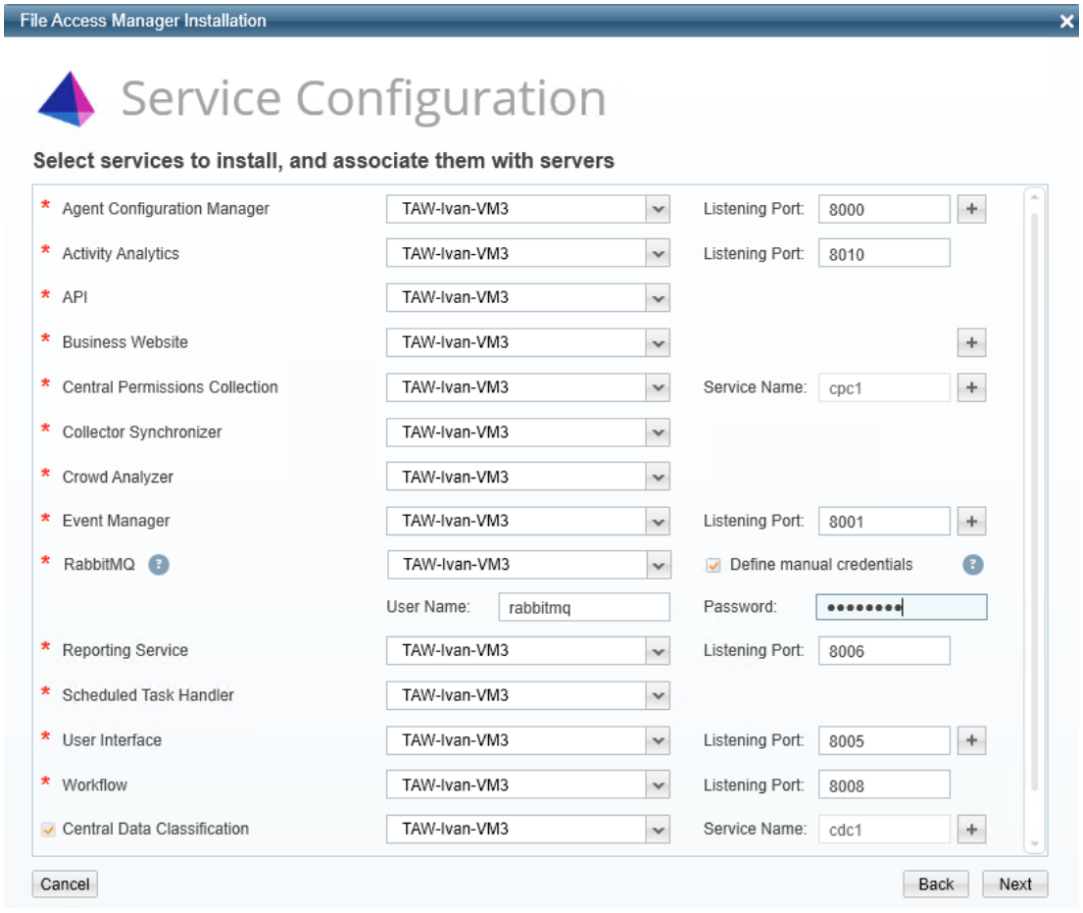


6. Once installed, open Server Installer and select the Create option:

7. Select Current Server Installation.

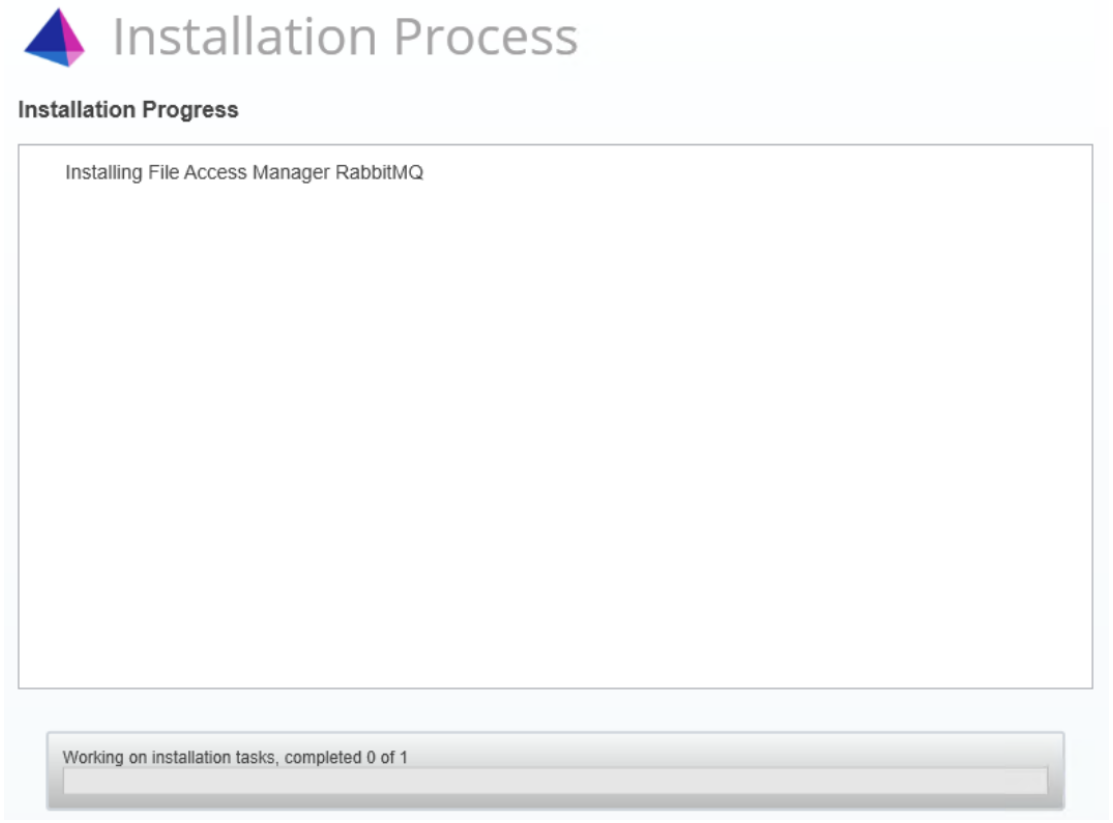


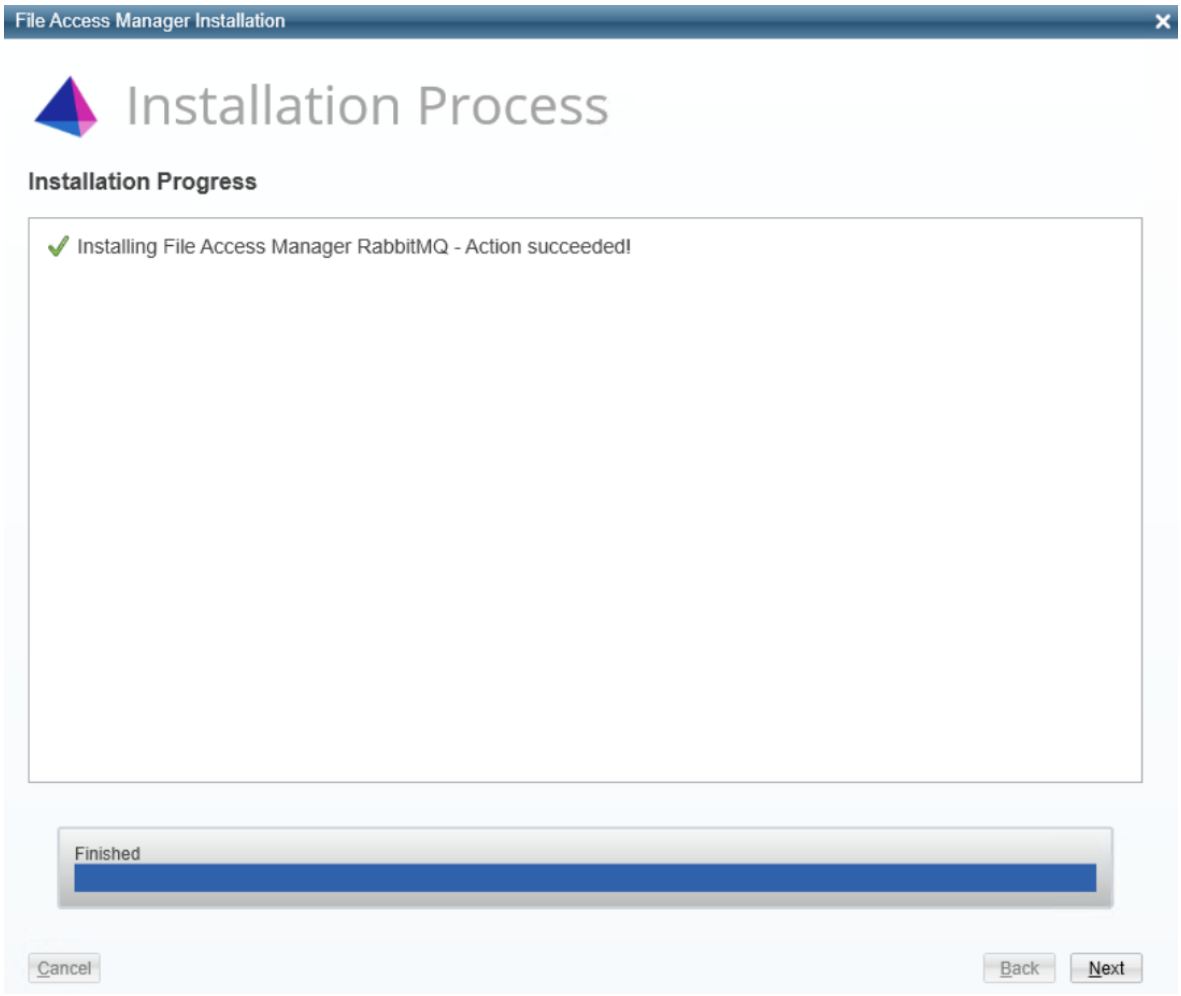
8. Define RabbitMQ Credentials into the existing Server.



9. Proceed until the end to execute Pending Installations (RabbitMQ):


File Access Manager Installation
Configuration Summary
Congratulations, You have finished the configuration stage.
Please choose an action:
Save Configuration Only
Save Configuration and Perform current Server's Installation Tasks:
- Installation of File Access Manager RabbitMQ
* Updates in Elasticsearch configuration will be performed by the Update Elasticsearch Cluster Configuration task after the Server Installer is completed.
* A command file "Installation_Command.txt" for unattended installation will be created under the Server Installer folder.
Cancel
Back
Next


Installation Process
Installation Progress
Installing File Access Manager RabbitMQ
Working on installation tasks, completed 0 of 1



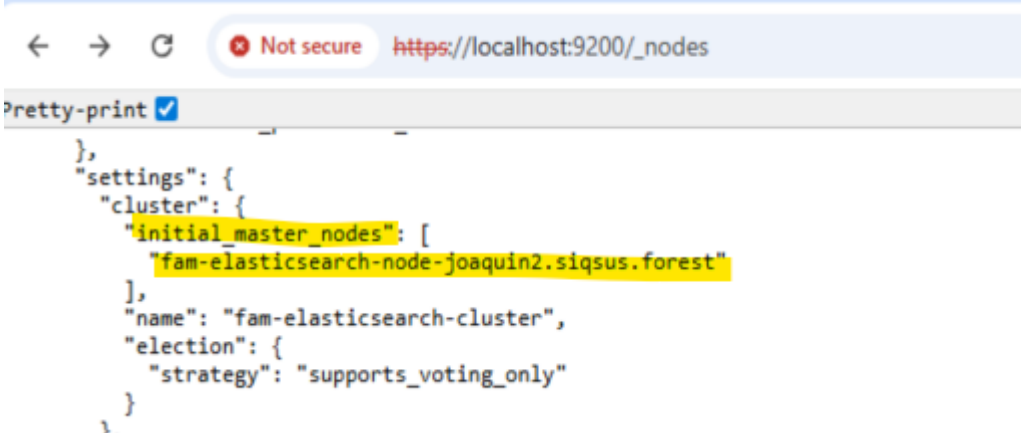
10. Start All FAM Services following the recommended order as usual. At this point, RabbitMQ is now using the updated version.

    Note: If needed, Erlang folder (usually found at *X:\Program Files\erl-24.3.2*) can be manually removed in case it is still present after the upgrade.

ElasticSearch upgrade to 8.19.4

Like RabbitMQ, ElasticSearch must be upgraded by following the next steps:

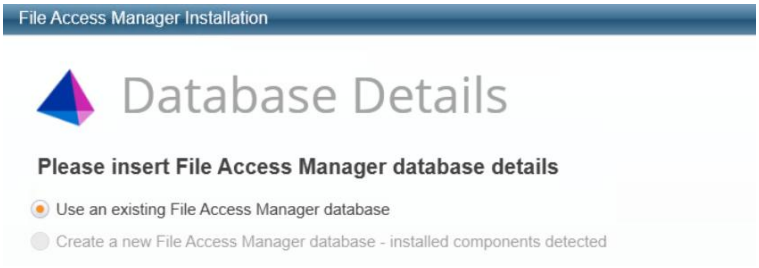
1. **If clustering is present**, please make sure to:
   a. Verify the initial_master_nodes (https://elastic_url:9200/_nodes)



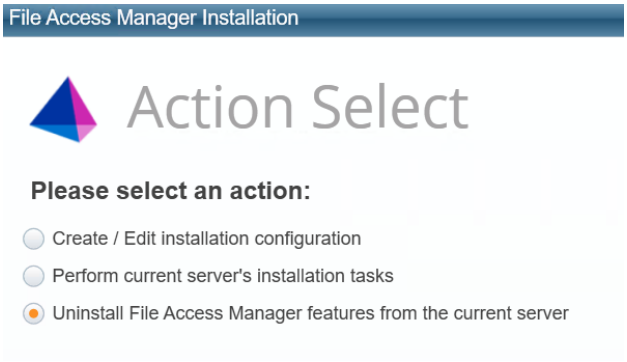
b. Uninstall all the servers in the cluster using Server Installer (next steps).

2. Open the Server Installer as an Administrator and choose the Use Existing File Access Manager Database option.

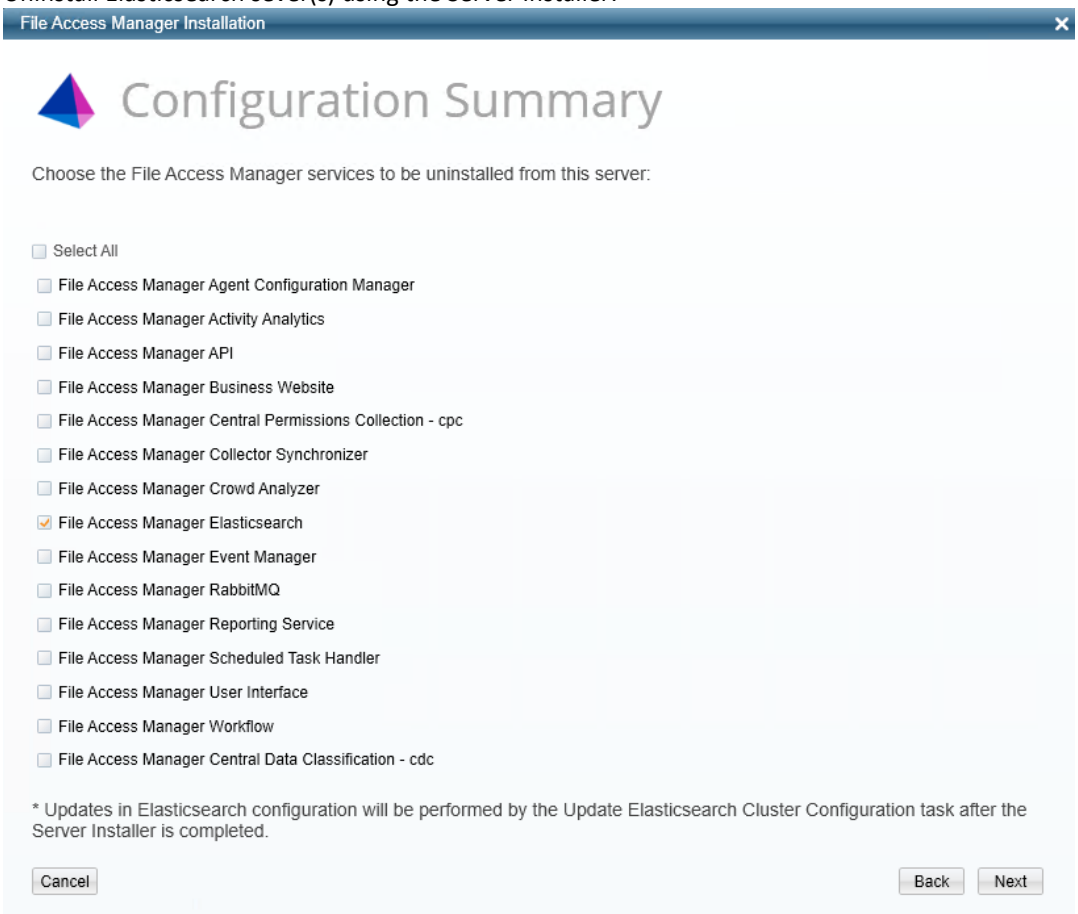
3. Insert valid database information and select Next



4. Select Uninstall FAM Features and select Next.

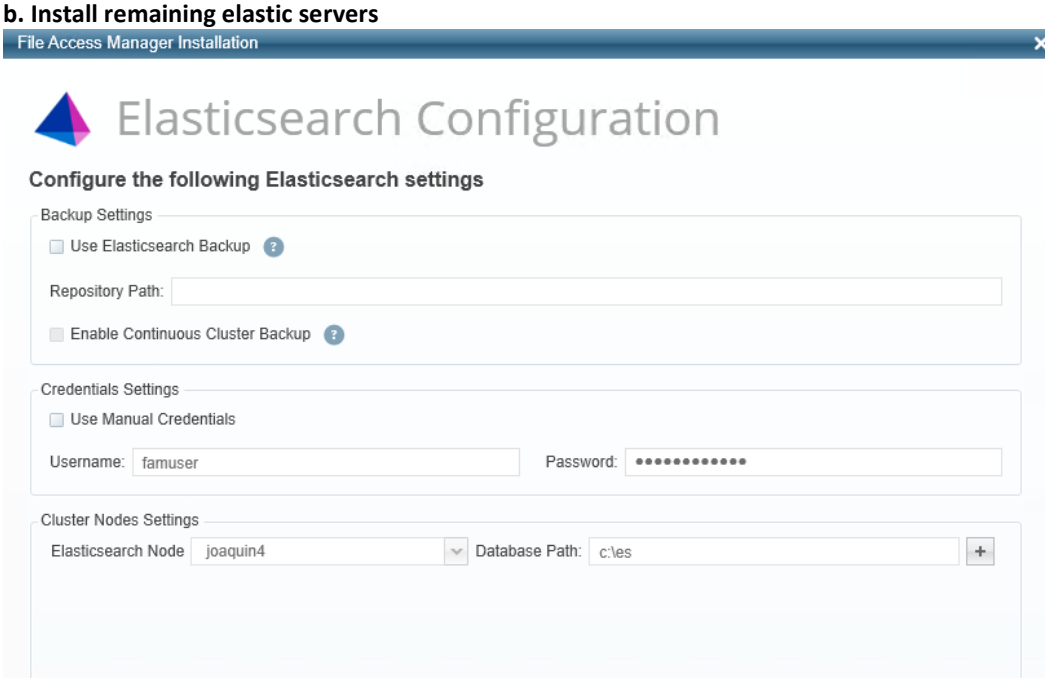


5. Uninstall Elasticsearch sever(s) using the Server Installer:



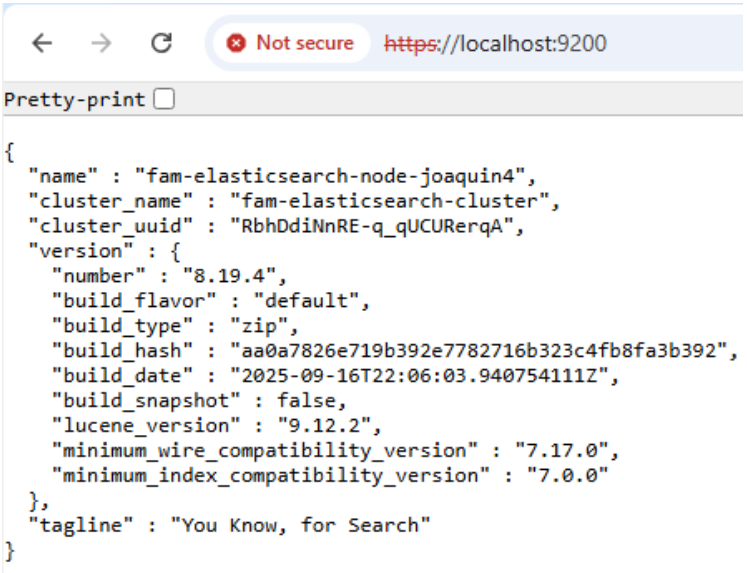
6. Once uninstalled, reopen Server Installer as Admin and using the same FAM DB information, define ElasticSearch details (creds, server names, etc.).

If ES clustering is present:
a. First install the initial_master_node
b. Install remaining elastic servers



7. Once Server Installer concludes with the installation, ES 8.19.4 version will be installed at FAM's server.

8. Verify the ES version (8.19.4) by accessing ES API:



Post Upgrade Actions

File Access Manager UI Upgrade (IISReset needed)

Due to recent UI changes and to avoid any cache conflicts, please run as an Administrator an *iisreset* command using either PowerShell or Command Prompt window (this can also be made using the IIS administration window):

iisreset /restart

IdentityIQ File Access Manager Client Upgrade

Please close and re-open all File Access Manager Administrative Client applications.

On the first run of the IdentityIQ File Access Manager administrative client after an update, a popup message displays, requesting that you update the client. During the update, you will be required to reenter the server on which the User Interface Service is installed.

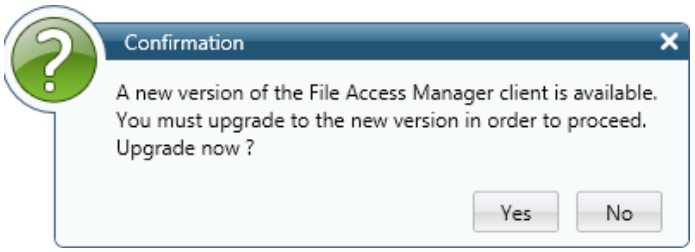


Figure 4: Message - Update File Access Manager Client

Validate the Service Pack update

To validate the installation, and verify that the correct version was installed, check in the Windows Add/Remove programs in the control panel.

The versions of the IdentityIQ File Access Manager components should be set to 8.5.0.1000
The IdentityIQ File Access Manager Database version should be set to 8.5.0.1000

Note: See "Versions included in this release:" for a full list of components updated.

Optional: Uninstall .Net Core 3.1

After you have completed the installation, you optionally can uninstall .NET Core 3.1

Navigate to the Control Panel > Programs > Uninstall a program

Locate corresponding .NET Core 3.1.x program, right-click > Uninstall

Chapter 4: Important Information and Updates

SIQSUS-1484 - Improvement Crawl Task - Cache LiteDB taking a lot of time to read when file grows without limit

Optimizing Crawl Performance: New Configuration Setting for LiteDB Cache

During the crawl process in File Access Manager, the crawler may utilize the disk as a temporary cache (writing data to a LiteDB file) when server memory nears capacity. While this ensures the crawl continues, allowing this cache file to grow indefinitely can eventually slow down read operations and impact overall crawl performance.

To provide better control over this process, a new setting has been introduced to the Permission Collection Service configuration file:

<add key="crawlerCachedDbMaxFileSize" value="0"/>

- Default Behavior (0): By default, no file-size limit is enforced. The system will use a single cache file, which may become large.
- When to Adjust: If you observe that crawl collection has become slow, accompanied by high memory usage and a very large LiteDB file in the permission collection service folder, we recommend setting a file size limit.
- Recommended Value: For optimal performance, a limit between 1000 and 1500 MB is recommended.

Make sure to restart CPC Service to obtain latest configuration after the configuration change is made.

SIQDEV-20726 – Stale Data capabilities for FAM

File Access Manager offers Stale Data detection capabilities, to help organizations identify clusters of unused data, based on real activity-based usage data, as well as file-level metadata. Stale Data information is important in guiding organizations' governance efforts.

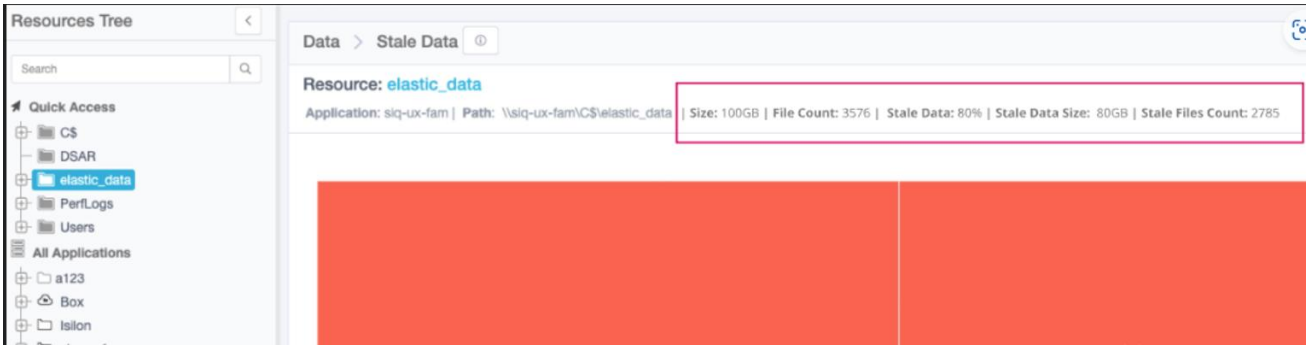
Understanding where stale data reside can lead organization to areas where access is granted unnecessarily, and data is kept and maintained without being used, which can be exploited by attackers. Stale Data is often forgotten and overlooked during governance process, precisely because of the fact it’s not being used. Some of this data may be sensitive, available on company resources as a sitting duck, increasing the likelihood of an incident or a breach.

Remediating stale data, by archiving, deleting or otherwise handling it, can reduce the organization attack surface, and well as reduce hosting costs. Information about the unused data in FAM is aggregated to surface clusters of stale data, with the lowest level of granularity being a business resource (effectively, a folder). Information about stale data is available now as part of the Resources views under the Stale Data tab, in Stale Data and Resource Usage report, and in forensics views.

This will allow admins to get more granular information about files and content that have not been accessed, down to the file level. In addition, it will enable admins and IT teams to leverage existing backup solutions to further archive, backup and / or dispose of that data - based on FAM’s initial work.

Overall Description:

- As part of File Access Manager resource discovery task, the crawl will now collect and aggregate the number and total size of stale files (files that have not been accessed for X long) within a folder. These numbers (# of stale files and the size of stale files) - will include all the resources sub-resources - calculus is based on Folders, not on individual files.
- Stats will be calculated for all resources whose last accessed data is older than 3 months.
- Information about the stale data will be added to resource, and will be presented in both the Resources tab Data view, and the Resource Explorer (see below) - including:
  - Size: XXX KB/MB/GB/TB/PB
  - File Count: XXXXX
  - Stale Data: XX%
  - Stale Data Size: XX KB/MB/GB/TB/PB
  - Stale Files Count



- The Resources “Data” Tab now shows the aggregated value for the resources including all sub resources.
- In the Resource Explorer (under Admin > Application > Manage Resources) administrators would be able to navigate to any resource (on CIFS applications) - and start an archival task:

1. Go to applications → … → Manage Resources.

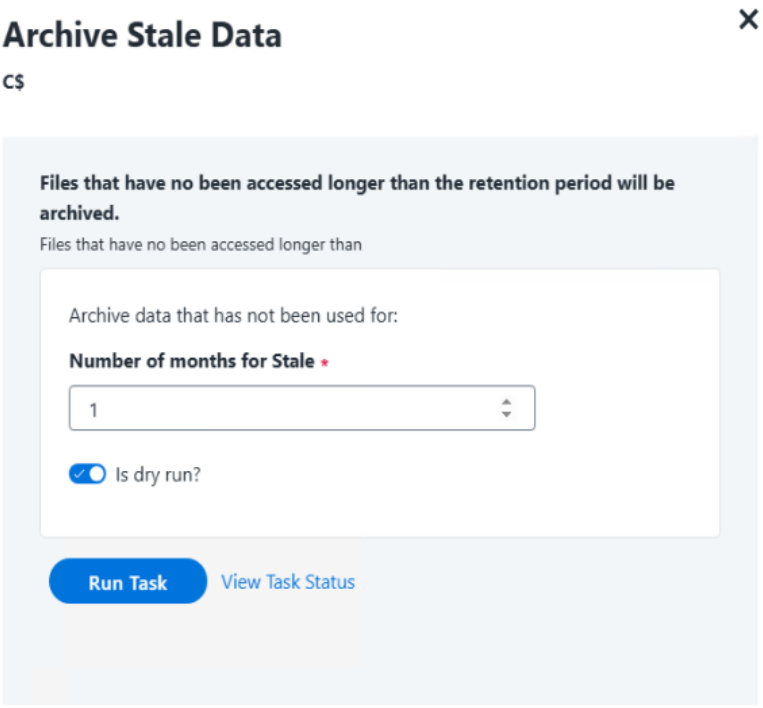
2. If user has Administrator permission, it will see the new button “Archive Stale Data“.

3. After Clicking the button, slide pop up will appear displaying next fields
   i. Number of months for Stale: number of months a file has not been accessed to be considered Stale, Default value: 12

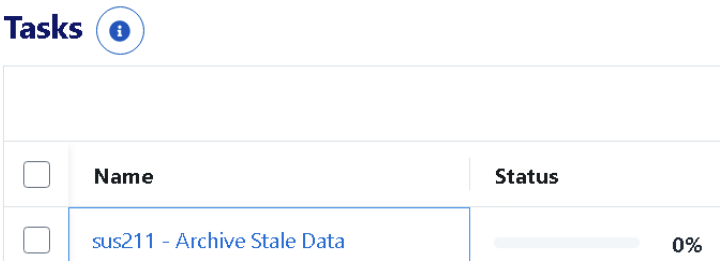
   Task uses days to compare last access date on stale files:

Current date - File last access date >= Number of months * 30 days

4. Is dry run? True if process will run and just get the list of files to move into a log file, False will move the Stale files
5. Save: Will update in the database the number of months value for this application
6. Run task: Will start the Archive Stale Data task execution

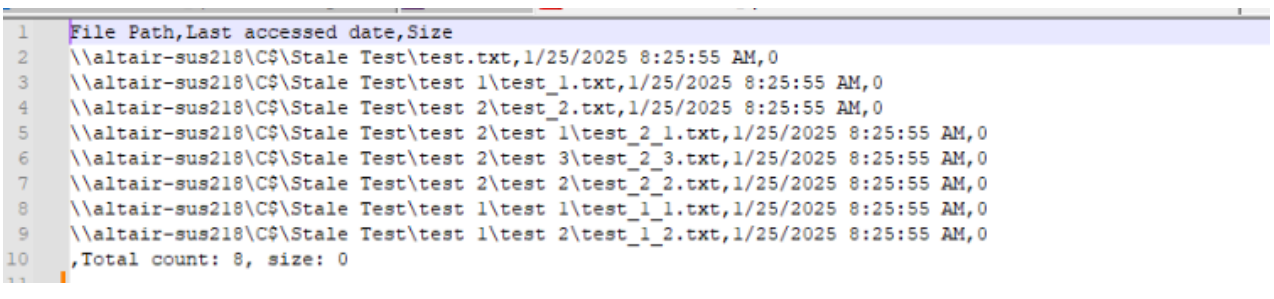


7. Admins can view the task progress, by clicking on the “View Task Status” link - that will lead them to the Task Details screen with a filter to the specific task



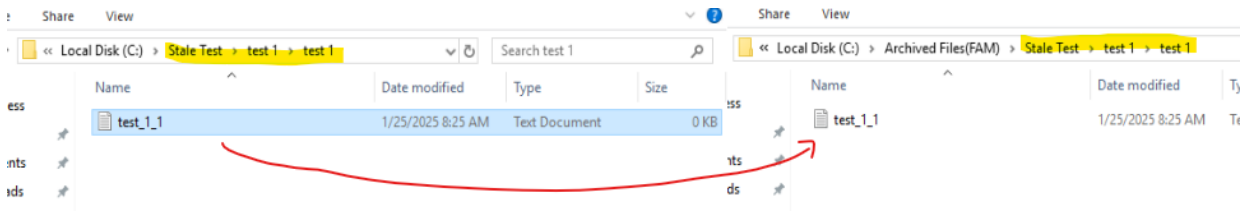
8. Once completed, Admins will be able to get the current archived files log - by searching in the SailPoint logs regular folder.
9. Run task: Will start the Archive Stale Data task execution
10. Search for file “PermissionsCollection.Archive Stale Data Successful Documents Details.csv“

    File will include the list of files that will be moved by task when Dry run is set to False



```
File Path,Last accessed date,Size
\\altair-sus218\C$\Stale Test\test.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 1\test_1.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 2\test_2.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 2\test 1\test_2_1.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 2\test 3\test_2_3.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 2\test 2\test_2_2.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 1\test 1\test_1_1.txt,1/25/2025 8:25:55 AM,0
\\altair-sus218\C$\Stale Test\test 1\test 2\test_1_2.txt,1/25/2025 8:25:55 AM,0
,Total count: 8, size: 0
```

11. If Dry Run set to False, Task will move the files to the “Archived Files (FAM)” folder.



Archival Process description:

- Under the selected resource root a new folder called “Archived Files (FAM)” will be created.
- The Stale Data task will traverse the resource, and all sub resources - like a mini crawl - and go over all the files within each resource.
- Any files found that has not been accessed for more than the retention period - will be moved to the “Archived Files” folder - while retaining the relative path(!).
    - That is, if I found “file X.yyy” to be stale under the path: “Root Resource \ Folder 1 \ Folder 2 \ Folder 3” it will be moved to the location “Root Resource \ Archived Files (FAM)\ Folder 1 \ Folder 2 \ Folder 3\file X.yyy”. Where “Folder 1 \ Folder 2 \ Folder 3\” represent the relative path.

- Any file found and moved will be reported in the log, including the found Last Accessed Date.
- Any failures to move / archive the file - will also be reported in the log.
- The Stale Data task will report on the progress of Resources Completed out of Resources Traversed.
- The Stale Data task will report a summary at the end of the number of files that were moved, and the total size of files that were archived.

Currently Supported Applications:

- File Servers and NAS Devices supported CIFS / SMB Protocols only:
    - Windows, NetApp, Isilon, Celera / Unity, HDS, Azure File, Generic CIFS

SIQDEV-20715 – NTLM Authentication Proxy support

Previous to version 8.4 Service Pack 5, FAM did not support Proxy Authentication capabilities, the only out-of-the-box proxy available configurations were the proxy URL and whitelisting of sites where proxy is not used. This translated into certain limitations like not being able to read and make use of User and Password values to be able to authenticate itself against a Proxy.

FAM Proxy Configurator Tool

To ensure a correct setup, a new support tool is included on this release, it oversees setting the values in the selected alternative, as well as encrypting the password value (if needed), and performing basic testing of the provided settings.

Now, this latest version of FAM provides two options to securely store forementioned credentials:

Using Windows Environment Variables

ALL_PROXY – the proxy server used on HTTP and/or HTTPS requests in case HTTP_PROXY and/or HTTPS_PROXY are not defined.

Example: 10.10.10.10:8080

NO_PROXY – a comma-separated list of hostnames that should be excluded from proxying.

Example: SOME.DOMAIN.COM,LocalFAMServer1,LocalFAMServer2

USER_PROXY – Username for Proxy NTLM authentication.

PWD_PROXY – Password for Proxy NTLM authentication (encrypted by the FAM Proxy Configurator Tool(included)).

BOL_PROXY – Either enables or disables the Proxy usage for intranet addresses.

Using Windows Credential Manager

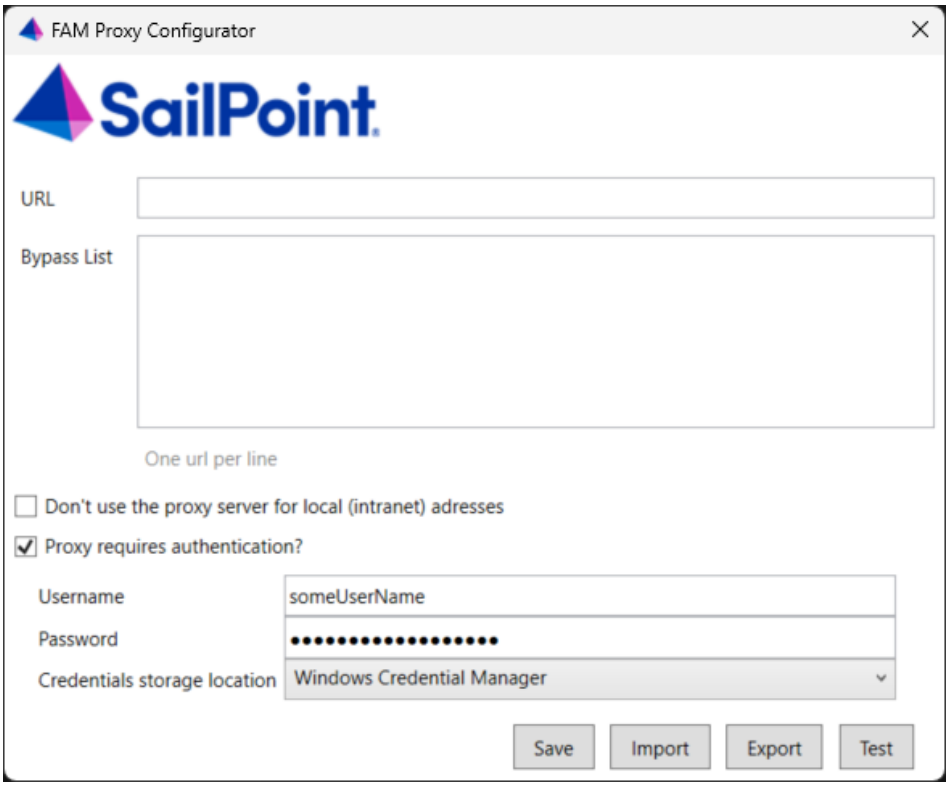
Another option is to make use of Windows Credential Manager. These specific values need to be configured on the FAM server(s) hosting the Engine/collector/Collector Sync services.

NOTE: This Tool must be executed using Admin credentials if Windows Credential Storage option is selected.

Please note that after creating these credentials (regardless of the store location), the corresponding FAM services must be restarted for the changes to take effect.

SIQDEV-20716 – NTLM Authentication Proxy Configurator Tool

We added an NTLM Authentication Proxy Tool to support/configure the actual values to be used as Credentials by the Proxy if NTLM Authentication is being used.



- **Url**: Proxy server name or IP address and port (optional).

This setting corresponds to the environment variable **ALL_PROXY**

- **Bypass List**: To avoid the use of the proxy server when visiting certain websites, enter the ending of the website address in the exception list (_for example, *.contoso.com*_).

  For multiple websites, type each website address per line. The * is a wildcard so any website addresses that end with the website address listed will bypass the proxy server. This setting corresponds to the environment variable **NO_PROXY.**

- **Do not use the proxy server for local (intranet) addresses**: We recommend you select this check box unless your organization requires the proxy server to be used for intranet addresses.

  This setting corresponds to the environment variable **BOL_PROXY**.

For further details on the Tool, please refer to the Readme.pdf file included with it.

SIQETN-3331 – Privacy scan getting stuck due to RabbitMQ duplicates

Data Privacy Scan task suffered from RabbitMQ messages being resent from DC engine due to intermittent connection generating some duplicate DB records, *KeyNotFoundException* being thrown caused FAM's thread to break and task get stuck.

This now have been fixed and DPS Task and RabbitMQ resiliency are now reassured.

SIQSUS-1312 – Exchange Online (EXO) updates for Cmdlet deprecation

On September 15th, 2024, Microsoft deprecated certain Exchange Online Admin Cmdlets that were used by File Access Manager Exchange Online integration. The deprecation of these Cmdlets ONLY affects the Activity Monitoring functionality of the File Access Manager Exchange Online integration. The four cmdlets in the Exchange Online V3 module that Microsoft deprecated are:

- Search-AdminAuditLog
- Search-MailboxAuditLog
- New-AdminAuditLogSearch
- New-MailboxAuditLogSearch

These cmdlets are no longer be available for use at this date, FAM code changes were made to switch to a Search-UnifiedAuditLog cmdlet instead to access audit logs. If not addressed, this could lead to disruptions in this specific functionality of File Access Manager for Exchange Online.

For more details, visit Microsoft's announcement.

SIQSUS-1315 – Remove Oracle JDK in replace of AdoptOpenJDK

File Access Manager 8.4 Service Pack 5 replaces all Oracle JDK assets with Adoptium's Temurin JDK 17 (Latest LTS supported by ElasticSearch 8.2.2.) Latest Releases | Adoptium.

New installations of File Access Manager 8.4 Service Pack 5 will deploy Adoptium's Temurin JDK by default, in support of the File Access Manager Elasticsearch deployment. Upgrades of existing deployments must follow the deployment instructions provided with the product documentation, using the new File Access Manager Server Installer, included

with Service Pack 5. For further info, please refer to the Pre-Upgrade Steps section.

SIQSUS-1318 – Enable FAM's Memory Protected Extraction by default

Out-of-the-Box Data Classification setting *useProtectedExtraction* default value as true. In previous versions it is disabled by default.

As a note, with this enabled setting, FAM creates a memory configuration based on available memory when DC task starts. Then it checks and adjusts memory usage while running to prevent out of memory exceptions.

SIQDEV-20711- FAM's upgrade to .NET 8

Starting with 8.4 Service Pack 4, FAM has been upgraded to make use of the latest Long Term Support .NET Framework version, which is 8. More information regarding this update can be found here on the prerequisites list as it needs to be installed prior to any FAM-related installation task for this upgrade.

SIQSUS-880- Data Classification Policy Scope Isolation

Now, FAM applications can have a delta scan that should be based on the set application scope of the policy.

- Delta Scan: The DC task will only scan recently modified folders (last modified updated from last crawl).
- Full Scan: The DC task will re-scan all folders in the DC scope.

After a full Data Classification scan, only changed folders detected after a crawl will be scanned on the next DC run. A full re-scan of all folders will only occur if active DC policies, rules or policy objects are changed.

If a policy change occurs that would only result in results being removed, a full scan will not be triggered. This is an optimization because of the expensive cost of running a DC task.

SIQSUS-880 fixes an issue introduced in v8.4 with the new policy scope feature, where a particular policy can be restricted to a particular application(s) or application type(s). Since we use a global last changed policies timestamp, the problem is that it will trigger a full DC re-scan when a DC policy/rule/object is changed even if it is outside the scope of that application.

The fix for SIQSUS-880 is to add a [last_updated] column to [dc_policy] table, as well as an [ocr_enabled_last_updated] column to the [bam] table. This way we have fine-grained knowledge of when a particular DC policy has changed and so can correctly calculate the last modified policies timestamp for a particular application based on it's given policy scope and active policies only and will not be affected by changes to policies outside of it's scope.

Internal rules of when to consider a policy updated:

- If a policy/rule/object is changed or created, but the object is not active and part of an active policy within the policy scope of a particular application, it will not trigger a full re-scan.

- If a new policy is created, but does not yet have any rules, a new DC full re-scan will not be triggered, as only active policies with at least one active rule are considered when computing the last changed policies timestamp just before a particular DC task run.

SIQETN-3295 – DFS Crawl improvements

Crawl issues (like uncaught exceptions) have been fixed within DFS stored procedures along with some performance improvements.

Also, in some cases, temp tables were not being removed/renamed generating extra burden to the DB. As a safety measure, moved the deletion of the temp tables at the end of the Workflow to ensure they are always deleted.

SIQETN-3297 – Data Privacy Scan ElasticSearch query improvements

Improved performance on Data Privacy Scan by reducing the number of searches/queries made to ElasticDB.

On Data Privacy Scan, when saving to Elastic, the process was searching for changes, deleting BR IDs, updating and inserting records, to improve it, the process now deletes the records and inserts the records.

Also, added enhancements to the help with the Save process, by avoiding any search bigger than 2GB from ElasticSearch, which was causing issues within ES.

SIQSUS-879 - Data Classification OOTB Policy Optimization

Updated RegEx expressions for IBAN and ICD rules to reduce false positives and address common use cases - by tuning current OOTB rules and expanding inter-rule relations to achieve more complex, and accurate data detection.

1. ICD - Codes A00-Z99 policy regex updated to include optional decimal point and one or two digits.
2. EU IBAN policy regex updated to get the most accurate results.

SIQSUS-1034 - Groups query for IIQ Correlation

The FAM Classifications Aggregation task now has a new "Query Type" argument that provides a choice between the FAM SCIM service that is used to aggregate classifications:
1. The legacy API that aggregates classifications via FAM Permissions
2. A new, more efficient API that aggregates classifications via FAM Groups

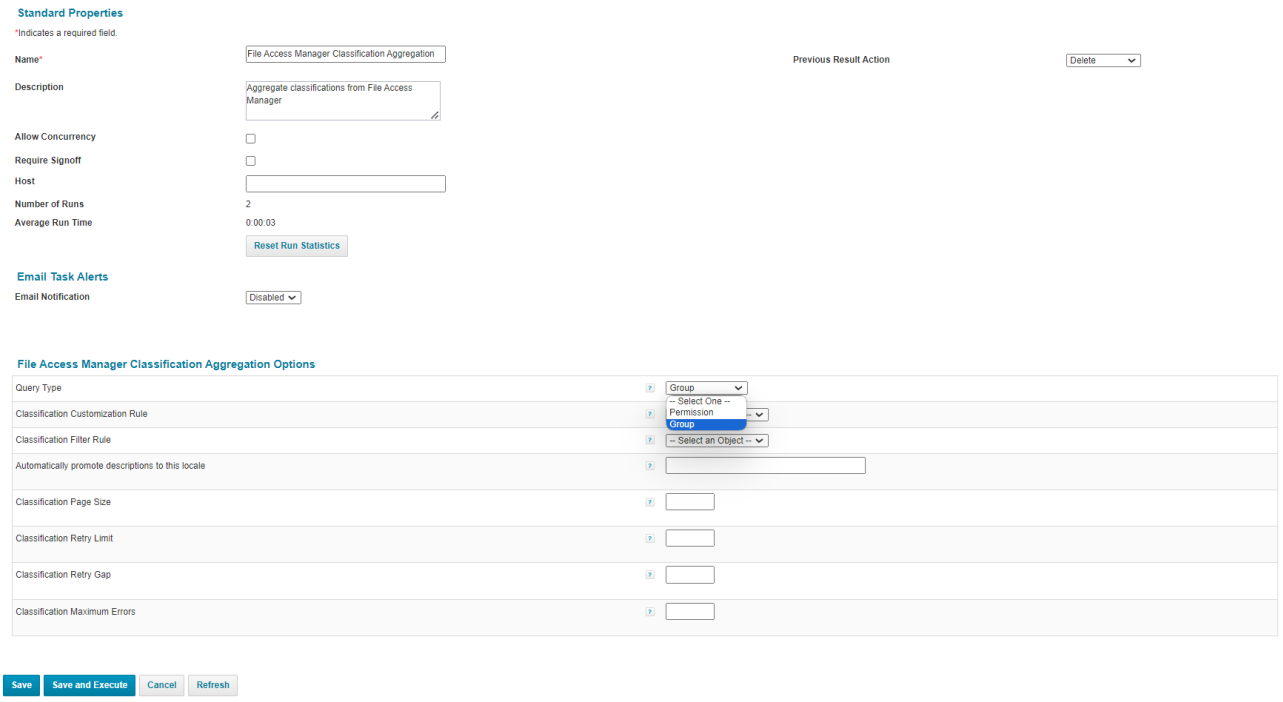
NOTE: This option is enabled in the following IIQ versions: *8.2p6, 8.3p4, *8.4p1, 8.5 (those w/ an asterisk have been already released).

There is a new feature in the IIQ FAM Classification task that is now exposed. The Classification Filter Rule is used to narrow the scope of Classifications for the task. Like most rules, it accepts a SailPointContext and a Logger. The return value is a QueryOptions that contains a Filter that is used to generate the SCIM query. The Filter is not as feature-rich as a traditional Hibernate Filter. It supports "and" operations but not "or". If expression values include reserved URL characters, they need to be encoded.

The Page Size is now configurable on the task. This argument specifies the number of records that we fetch with each SCIM call to FAM.

Several arguments have been added to the FAM Classification task to allow users to adjust its tolerance. They are as follows:

- Retry Limit: The number of times that we retry a failed query before giving up and moving on.
- Retry Gap: The number of milliseconds that we wait before retrying a failed query.
- Max Errors: The number of times that we give up on retrying individual queries before giving up on the task entirely.



NOTE: These enhancements require the import of the following file to expose the new configuration options for the task:
- New installations: WEB-INF/config/init-fam.xml
- Existing installations: WEB-INF/config/patch/identityiq-fam-8.4p1.xml

For more detailed information please reach out to IIQ Support Teams.

SIQETN-3284 – DB Cleanup Task performance optimization.

FAM's Database Cleanup Task is a crucial maintenance job that users can trigger or schedule as needed. The primary goal of this task is to ensure that FAM's DB remains in optimal conditions. It encompasses various processes such as tables maintenance (including temporal ones), rebuilding DB indexes, cleaning up some other stuff not used anymore like old reports and Application Wizard Records, removing obsolete information related to deleted resources (e. g. DSAR information) from Elasticsearch, and more. Key optimizations include:

Rebuild DB indexes: Potentially long running process that may time out after the configured *rebuildIndexTimeLimitMinutes* setting.

- Some DB Store Procedures were optimized to be executed and the progress of it can be tracked.
- Now the process reports how many indexes were rebuilt.
- If the process did not complete in the elapsed time, mark the task log entry as a warning.

Remove deleted resources privacy records from ElasticSearch repository and Database: Potentially long running process that was not cancelable, even if the task is cancelled the process kept running in the background.

- The process is now cancelled as expected.
- Added a new config setting (*removeDsarRecordsTimeLimitMinutes*) that allows the configuration of a timeout for this step of the process and honor it in execution. To adjust setting, complete the following steps:
    1) Stop the FAM Scheduled Task Handler Windows Service.
    2) Navigate to FAM's installation path and locate the *ScheduledTaskHandlerServiceHost.dll.config* within the *\SailPoint\FileAccessManager\ScheduledTaskHandler* path.
    3) Update the *removeDsarRecordsTimeLimitMinutes value* accordingly.
    4) Start the FAM Scheduled Task Handler Windows Service.

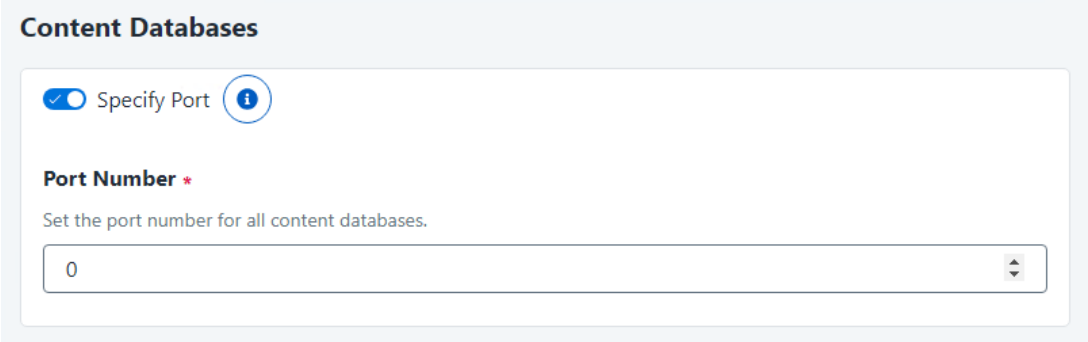
SIQSUS-1036 – Incorporate Custom DB Ports for SharePoint Content DBs into SP Configuration.

Support was added to allow for a custom port definition of the SharePoint content databases during its configuration.

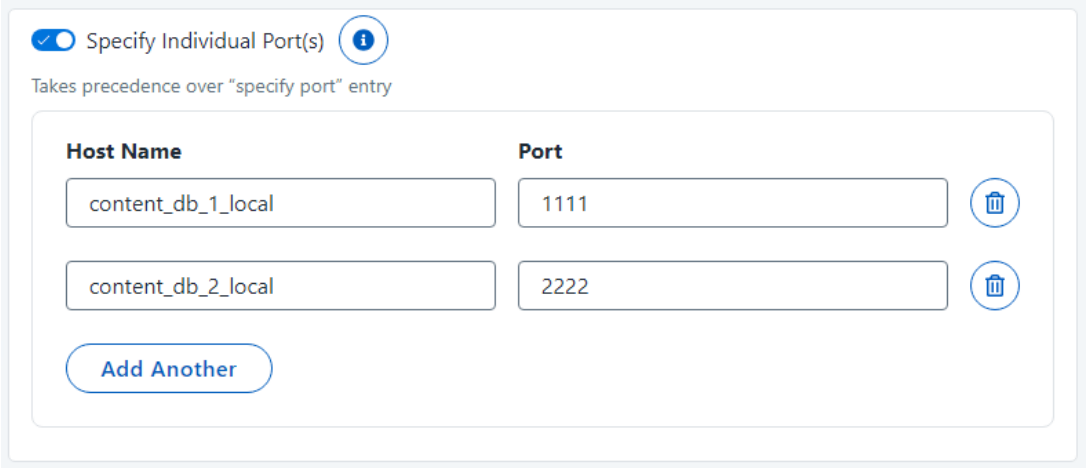
In a future Service Pack we are looking to include the ability to auto-detect the SharePoint Content Databases. Currently they need to be manually entered.

In the SharePoint application configuration screen the User will now have the following options:

Toggle option to specify All Content Database ports. Utilize this option if all Content Databases share same port number.



Individual Ports numbers per DB/Host. Utilize this option if Content Databases use different ports.
Note: If Content Database does not have the port specifically defined it will default to port entered in “Specify Port” section.



SIQETN-3118 – Enhance Data Classification Skipped Document Log Messages.

Updated the error description to include both the actual file size and the metadata file size:

> *Skipping content of file {filePath} because it is too large.*
> *The extracted content size { computedFileSize } MB. exceeds the max file size.*
> *Metadata reported size = { fileSize } MB.*

SIQETN-3119 – Summarize Failed Documents During Data Classification in Task Details.

The purpose of this report is to improve the visibility and clarity of failed documents during the data classification

process. The summary is divided in 2 general sections:

Settings section:

Setting	Description
BAM	Business unit name
Task	Name of the task
Agent	Name of the agent
Start time	Starting date time of the task
End time	Ending date time of the task
Elapsed time	Time it took for task time to complete
Excluded formats	DC_Parameters.FormatsToExcludeFromIndex
Formats to Index	DC_Parameters.FormatsToIndexAsDocuments
Archive formats	DC_Parameters.ArchiveFormats
Max file size	DC_Parameters.MaxFileSizeMB

Note: Parameters that do not have a value or are null in DC_Parameters will not be included.

Errors sections
Errors are grouped in categories, with the title being the type of error and the error count of that category:

- { CATEGORY_NAME } ({ ERROR_COUNT } items)

All errors include the timestamp when they occurred, a brief description of the error and the file name it applies to

- IvalidOperation (1 item)
2023-07-27T17:23:20 | Invalid operation for file [_corrupt_doc_file_.docx]

Applicable categories

Category	Description
FileIsEncrypted	*(Hyland)*. File is encrypted
FileIsLocked	*(Hyland)*. File is locked or in use
FileNotFound	*(Hyland)*. File was not found
FileNotReadable	*(Hyland)*. File is not readable
General	*(Hyland)*. General error
InvalidOperation	*(Hyland)*. The operation is invalid for this type of object
MaximumFileSize	File size exceeds the maximum configured size
OutOfMemory	*(Hyland)*. Out of memory
OpenError	*(Hyland)*. Error opening the file
OutOfMemory	*(Hyland)*. Corrupt file
WrongType	*(Hyland)*. Attempt to open file with wrong type

NLog configuration
A new log file definition for the report is needed for the summary report.

Target definition:

```
<target
        name="failedDocumentsDetailsLogFile" xsi:type="File"
        keepFileOpen="true" concurrentWrites="false"
        fileName="${environment:SAILPOINT_HOME_LOGS}\DataClassification_[AGENT_NAME].Failed Documents Details.log"
        archiveNumbering="DateAndSequence" archiveDateFormat="yyyy-MM-dd" maxArchiveFiles="10" archiveEvery="Day"
        archiveAboveSize="31457280"
        layout="${message}"
        />
```

Rule definition

```
<logger name="FailedDocumentsDetails"
    minlevel="Error"
    writeTo="failedDocumentsDetailsLogFile" final="true" />
```

Sample report:

```
------------------------------------------------------------------------------------------------------------------------
              BAM: BOX Data Classification
             Task: BOX Data Classification - Data Classification Scheduler
       Agent name: cdc1 Collector 1
       Start time: 2023-07-27T17:23:14
         End time: 2023-07-27T17:45:52
     Elapsed time: 00:22:38.4701005
  Formats to index: docx;doc;xls;ppt;xml;cs;txt;htm;html;sql;xlsx;js;pptx;pdf;csv;json
   Archive formats: zip;tar;gz;rar;7z
     Max file size: 200MB


- InvalidOperation (2 items)
    2023-07-27T17:23:20 | Invalid operation for file [New Word Doc.docx]
    2023-07-27T17:29:13 | Invalid operation for file [Test.docx]

- FileNotReadable (2 items)
    2023-07-27T17:35:19 | File [DSAR_TestFiles\~$ckData_docx.docx] is not readable
    2023-07-27T17:45:44 | File [~$SIQ-Backend Sanity - Automation Candidates - 2022-20220628.xlsx] is not readable
```

SIQETN-3250 - Box and OneDrive permission collection invokes stored procedure to create user_role tables excessively.

Performance improvements have been made to Box and OneDrive Permission Collection tasks to decrease runtime.
NOTE: These improvements can be found in other Permission Collection tasks, not just Box or OneDrive.

SIQSUS-881 – Modernize EXO Connectivity v3.0

Microsoft will soon be deprecating legacy remote PowerShell sessions for exchange online.

For new tenants, basic authentication will be disabled by default on June 1, 2023, and will be forcefully disabled for all tenants by October 2023.

Microsoft is recommending all tenants to move all scripts, unattended or otherwise, to migrate to using the new Exchange Online PowerShell V3 module. The module name is ExchangeOnlineManagement, and it is also sometimes referred to as shorthand of EXO module, or EXO V3 module.

Microsoft advertises this new module as being more secure (built-in support for modern authentication), more reliable (handles transient failures with built-in retry), and more performant.

For more details consult Microsoft documentation here:
https://techcommunity.microsoft.com/t5/exchange-team-blog/announcing-deprecation-of-remote-powershell-rps-protocol-in/ba-p/3695597
https://techcommunity.microsoft.com/t5/exchange-team-blog/exchange-online-powershell-v3-module-general-availability/ba-p/3632543

8.4 SP1 Exchange Online Connector now utilizes the new V3 Module.

New Module Installation Prerequisite:
The new module will need to be manually installed by the customer on any machines running Exchange Online tasks:

Activity Monitoring and the Permission Collection engine. The command to installs the latest version of the module and should be run from an elevated administrator PowerShell prompt:

```
Install-Module -Name ExchangeOnlineManagement -MinimumVersion 3.1.0 -Scope AllUsers -Force -AllowClobber
```

The above command will install the latest stable version and will be included in the FAM documentation for this connector. Note that any upgrades of the EXO module will require a restart of the relevant activity monitoring and permission collection services, since it will have loaded different versions of internal module libraries.

To check which version of EXO module is installed, run:

```
Get-InstalledModule
```

Optimized Get-EXO* Cmdlets

We are now using the new Get-EXO* cmdlets where possible:

- Get-EXOMailbox (to replace Get-Mailbox)
- Get-EXOMailboxFolderPermission
- Get-EXOMailboxFolderStatistics
- Get-EXOMailboxPermission
- Get-EXOMailboxStatistics
- Get-EXORecipient
- Get-EXORecipientPermission

Mailbox Folder Statistics Collection Now Opt-In To Address Performance

As an optimization, we will make collecting the following statistics optional:

- LastLogonTime - Updates business_service_last_used table.
- ItemCount - Updates files_count in business_service table.
- TotalItemSize - Updates size in business_service table.

While this data may be useful to some customers, the performance penalty of collecting it causes crawls to run an order of magnitude slower, as a separate REST call must be made for each mailbox after getting the initial root collection. This will now be disabled by default but can be re-enabled by setting crawlCalculateSize from Never to Always row in bam_configuration_value table for matching bam and can create row if it doesn't exist. (There is precedent for this change as Exchange On-Prem already has this backend hidden switch but is always on.)

Exclude Internal Folders "SubstrateHolds" and "DiscoveryHolds"

Hidden folders created internally by Microsoft named SubstrateHolds and DiscoveryHolds are excluded from crawl results.

Memory Usage

Microsoft has noted usage of the new EXO V3 module does create a memory leak. Over time, across many re-runs of an Exchange Online crawl or permission collection task, you may experience a gradual increase in memory usage of the Permission Collection engine service.

There is a note about it on the Microsoft EXO module about page:

> ⓘ Note
>
> Frequent use of the **Connect-ExchangeOnline** and **Disconnect-ExchangeOnline** cmdlets in a single PowerShell session or script might lead to a memory leak. The best way to avoid this issue is to use the *CommandName* parameter on the **Connect-ExchangeOnline** cmdlet to limit the cmdlets that are used in the session.

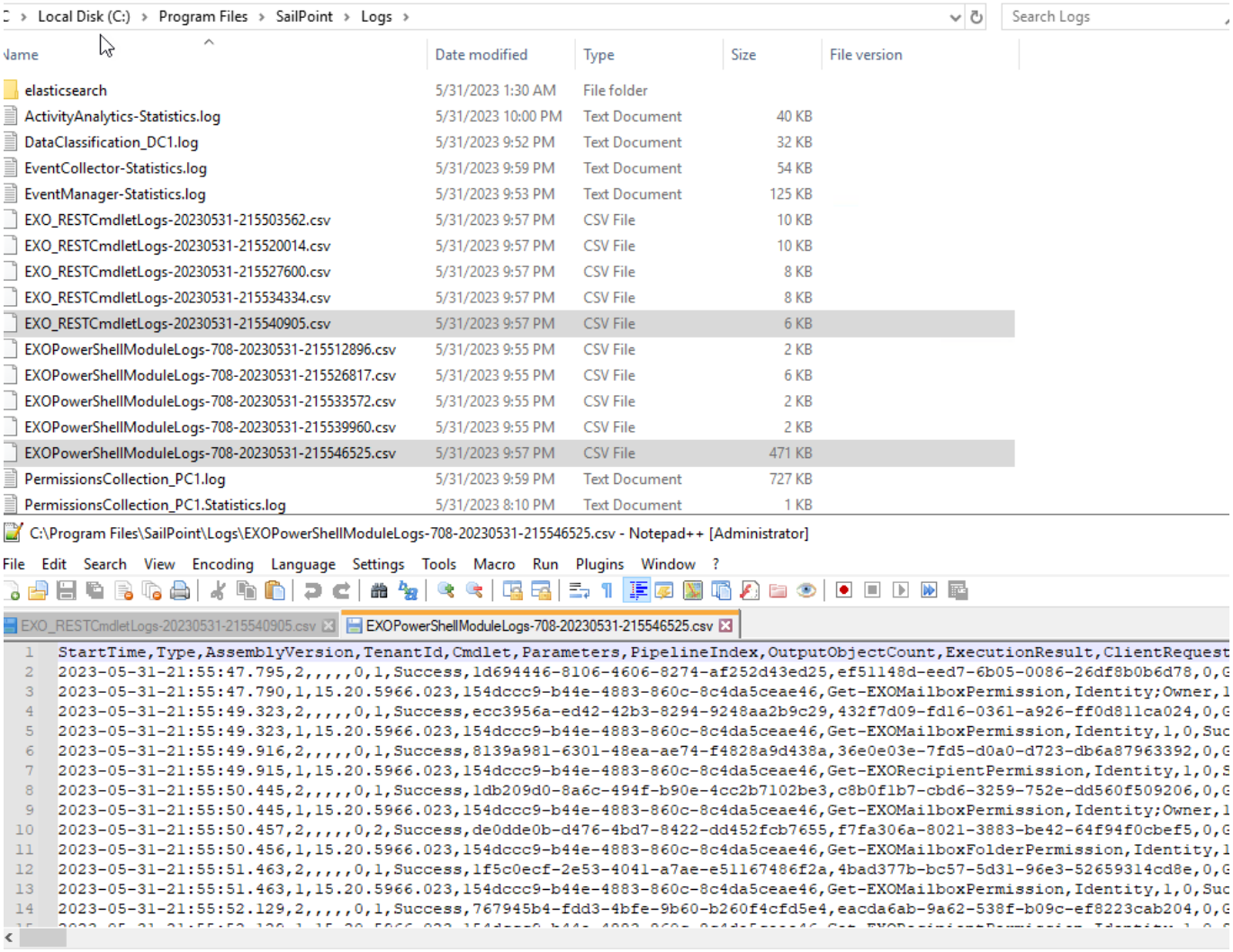
We are using the CommandName parameter to import any needed REST cmdlets to reduce memory usage. When this is corrected by Microsoft, we will include Microsoft updates/recommendations into the upcoming Service Pack.

Overall Performance

With focused efforts on improving the speed of the crawl, we have made adjustments to no longer fetch statistic by default. Internal testing efforts see a decreased in the crawls time to completion.

Logging and Configuration

There is a way to enable Microsoft internal EXO V3 module logging by editing the NLog configuration file.
Setting **writeTo="logFile"** will enable this logger and new logs will be created beginning with EXO.



This may be useful to quickly capture and report Microsoft bugs, as EXO V3 is still undergoing development and stability fixes and should not yet be considered mature.

References:

[Connect to Exchange Online PowerShell]
[Deprecation of Remote PowerShell (RPS) for New Exchange Online Tenants]
[Welcome to the Microsoft Tech Community]
[App-only authentication in Exchange Online PowerShell and Security & Compliance PowerShell]
[Use C# to connect to Exchange Online PowerShell]

SIQETN-3194 – IIQ SCIM API - Allow for more than 100K results to be returned in Permission Forensics Call

This feature is applicable to customers that utilize integration with IIQ and FAM.

Prior to this change, IIQ API queries would return a maximum number of one hundred thousand results.

This change increases the query's index limit to ten million. Restructuring was completed to improve performance and two additional indexes have been introduced to improve query plans.

Please note these queries still may require a significant time to return results. Additional work is planned for upcoming Service Packs (for both IIQ and FAM) to improve the performance of the results.

SIQETN-3204 – Support custom port configuration for SharePoint On Prem Content Databases

These changes will allow for custom port use for the SharePoint Content databases.

In order to enable this piece of functionality in your environment the following script should be applied to your specific FAMDB with the help of your DBA and SailPoint's Support team.

Please make sure to create a Backup of the DB prior to any changes.

```
DECLARE @bam_id int = -1,
      @port nvarchar(max) = '1433'
IF EXISTS (
            SELECT 1
            FROM whiteops.bam_configuration_value
            WHERE bam_configuration_id = @bam_id
              AND name = 'hasSpecificContentDatabasePort')
BEGIN
            UPDATE whiteops.bam_configuration_value
            SET [value] = 'True'
            WHERE bam_configuration_id = @bam_id
              AND [name] = 'hasSpecificContentDatabasePort'
END
ELSE BEGIN
            INSERT INTO whiteops.bam_configuration_value
            VALUES (@bam_id,  'hasSpecificContentDatabasePort', 'True')
END
IF EXISTS (
            SELECT 1
            FROM whiteops.bam_configuration_value
            WHERE bam_configuration_id = @bam_id
              AND name = 'specificContentDatabasePort')
BEGIN
            UPDATE whiteops.bam_configuration_value
            SET value = @port
            WHERE bam_configuration_id = @bam_id
              AND [name] = 'specificContentDatabasePort'
END
ELSE BEGIN
            INSERT INTO whiteops.bam_configuration_value
            VALUES (@bam_id,  'specificContentDatabasePort', @port)
END
```

After the script has been applied, the output should be this at the whiteops.bam_configuration_value table:

785	24	hasSpecificConfigDatabasePort	True
786	24	specificConfigDatabasePort	41232

Note - FAM only supports a single custom port for the Content Databases. If multiple content databases are used, they all should be utilizing the same custom port.

SIQSUS-850 – Migration to Microsoft Graph API

Microsoft made an announcement of their intentions to deprecate Azure AD Graph API starting June 2023: https://learn.microsoft.com/en-us/graph/migrate-azure-ad-graph-overview

With this announcement, the service pack now supports Microsoft Graph API.

Necessary steps:

After the upgrade has complete, please reissue new Authorization codes for:

- Azure Active Directory Identity Collector
- SharePoint Online application
- OneDrive application

If you need help performing this, please submit a support ticket. Or reference the ***8.4*** documentation to view details around Microsoft Cloud endpoints for further details.

If you are not utilizing any of the above, there are no needed changes which need to be performed.

Considerations:

A list of resources that are accessed by File Access Manager using the REST graph API include:
https://graph.windows.net/{tenant_domain_name}/tenantDetails
https://graph.windows.net/{tenant_domain_name}/users
https://graph.windows.net/{tenant_domain_name}/users/{user_id}
https://graph.windows.net/{tenant_domain_name}/groups/{group_id}
https://graph.windows.net/{tenant_domain_name}/directoryRoles
https://graph.windows.net/{tenant_domain_name}/directoryRoles/{role_id}

Please be aware of these changes and adjust access accordingly. Please reference ***8.4*** documentation to view details around Microsoft Cloud endpoints for further details.

Chapter 5: Troubleshooting

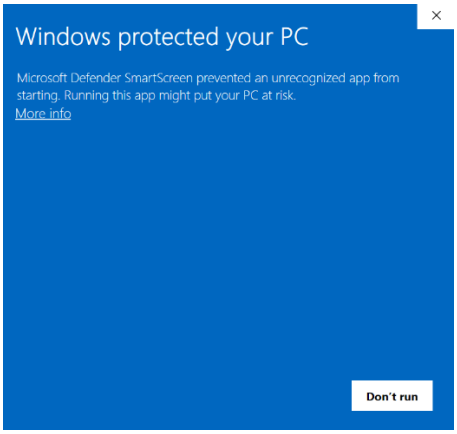
Windows SmartScreen Warning

Problem: During a fresh install during an MSI install, you receive a warning with the message "*Windows Protected your PC*":

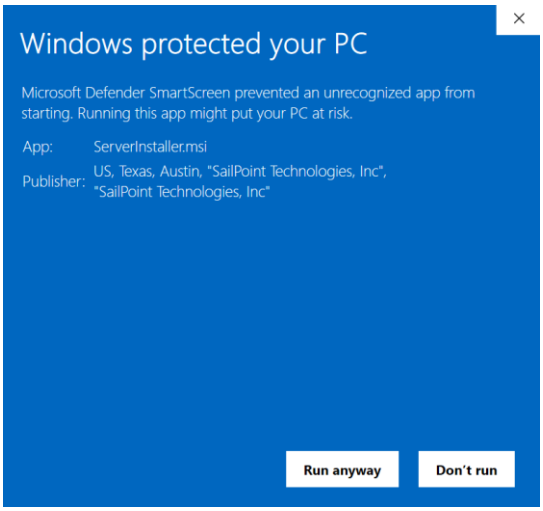
The problem is likely that the Code Signing Certificate used to build the MSI installers does not have the necessary general audience approval. This happens when brand new Certificates are used to have binary files signed and released to the general market. This warning is safe to ignore as long as the Publisher details correspond to SailPoint's.

Suggested solution:

1) Press the More Info link shown in the warning screen.



2) In the next screen, click on Run anyway button so installation can begin.



3) The installation should continue as usual. This warning only happens once. Subsequent attempts to use MSI files will not throw a similar warning.

Upgrade Package Loading Fails

Problem: During the package upload step, you receive a warning with the message "*Loading the package failed due to the following error: Signature is not valid*":

The problem is likely that the machine hosting the User Interface service does not have the necessary Root Certificate (or is missing part of the Certification Chains leading up to the root) to validate the signature of the upgrade package.

Suggested solution:

1. To resolve the issue you should check that the machine hosting the User Interface service contains the root certificate named "DigiCert Assured ID Root CA", which has a serial# 0C:E7:E0:E5:17:D8:46:FE:8F:E5:60:FC:1B:F0:30:39.
   If this root certificate is missing, it can be downloaded from https://www.digicert.com/digicert-root-certificates.htm and installed as a trusted root certificate manually.

2. Another reason for this error would be that the machine hosting the User Interface service has been configured so that updating root certificates is disabled. To fix this, set the registry value HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate to 0, and retry uploading the upgrade package.
   This will allow Microsoft to restore the missing root certificate during validation.

NHibernate configuration

Problem: During the upgrade, the NHibernate configuration file or registry key do not display on one of the machines:

Suggested solution:

1. Copy the "hibernate.cfg" from another server to \SailPoint\Nhibernate.

2. Copy the "[HKEY_LOCAL_MACHINE\SOFTWARE\whiteboxSecurity]" key from another machine to this machine.

3. Run the ResetDBPassword utility, to reencrypt the database password with the current server's certification

   a. Make sure the SecurityIQ Home environment variable is set to the correct location

   b. Ensure that the folder named "External Tools", containing the "makecert.exe" executable, or copy that folder from the Core Services server (the server hosting the User Interface service), and place it in the SecurityIQ Home directory

   c. Ensure that the folder named "ServerInstaller" exists in the "%SECURITYIQ_HOME%\File Access Manager" path, and within that folder you can locate the "Tools" directory or copy it from the Core Services server.

   d. Navigate to the "DBResetPassword" folder

   e. In a Command Line window (cmd) from the "DBResetPassword" directory path, run the following command:

```
C:\Program Files\SailPoint\File Access Manager\Server
Installer\Tools\DBResetPassword>
DBResetPassword.exe {YourPasswordGoesHere}
```

f. After the NHibernate file is re-encrypted, resume the manual uninstallation and installation of the remaining service on that server.

Business Website

Problem: You encounter an "Access Denied" error message while logging in to the Business Website after the upgrade

Suggested solution:

1. Navigate to the wwwroot folder on the server hosting the Website at C:\inetpub\wwwroot).
2. Verify that the IdentityIQFAM and SiqApi folders are in the wwwroot folder.
3. If these folders are in the wwwroot folder, but there are still problems with the Business Website, contact support.
4. If these folders are **not** in the wwwroot folder, perform the following steps:
5. Open the Internet Information Service (IIS) manager (Server Manager ➔ Tools ➔ Internet Information Service (IIS) manager).
6. Select the Application Pools node.
7. Verify that the IdentityIqFamV1_ApplicationPool, IdentityIqFamV2_ApplicationPool and SiqApi_ApplicationPool are missing from the Application Pools node.
8. Create the new application pools, (naming them IdentityIqFamV1_ApplicationPool, IdentityIqFamV2_ApplicationPool and SiqApi_ApplicationPool), with the following parameters: .Net CLR Version: .Net CLR Version v4.0.30319 Managed pipeline mode: Integrated
9. Check the "**Start application pool immediately**" checkbox.
10. For each application pool, navigate to Advance Settings (Right-click ➔ **Advanced Settings**)
11. Under Process Model, set the "**Identity**" parameter to **LocalSystem**.
12. Under Recycling set the "**Regular Time Interval (minutes)**" to **720**.
13. From the Site panel (on the left), navigate to **IdentityIQFAM**, and click on it.
14. Click "**Basic Settings**" on the right. If this option is not available, right click **IdentityIQFAM** (on the left) and select "Convert to Application".
15. On the newly opened screen, click **Select**, select the IdentityIqFamV1_ApplicationPool you created earlier, and click **OK** twice.
16. Double click "**Authentication**".
17. Enable "Windows Authentication" and disable all other authentication methods.
18. Repeat Steps 11-15 for the SiqApi site and SiqApi_ApplicationPool.
19. Reset the IIS using the iisreset command.

Business Website

Problem: You encounter the following error, in the File Access Manager Server Installer log, when trying to uninstall the Business Website:

```
Unable to uninstall service: WBXBusinessWebsite System.InvalidOperationException:
Sequence contains more than one matching element
```

Suggested solution:

1. Open the **Internet Information Services (IIS) Manager**
2. Expand the **Server Name**
3. Expand **"Sites"**
4. Expand **"Default Web Site"**
5. Select **"SecurityIQBiz"** and click **"Basic Settings"** on the right side
6. Click **"Select…"** then select **"SecurityIQ_ApplicationPool"** then click **OK**, then click **OK** again
7. Go to **"Application Pools"**
8. Select **"SecurityIQ_ApplicationPool"** and click **"View Applications"** on the right side
9. Right click **"/SecurityIQBiz/Whitebox_Rest"**, then click **"Change Application Pool"**, select **"DefaultAppPool"** and click **OK**
10. Right click **"/SecurityIQBiz/WhiteopsRest"**, then click **"Change Application Pool"**, select **"DefaultAppPool"** and click OK
11. Go to **"Application Pools"** and Confirm that the **"SecurityIQ_ApplicationPool"** application pool has only one application (in the **"Applications"** column)
12. Try to uninstall again.

Improper upgrade path

Problem: The improper upgrade path was taken. 8.3 SP4 was uploaded and upgraded was started but prerequisite of being on 8.3 failed.

Steps to "rollback" the failed installation.

PLEASE NOTE: whenever performing changes to the database we always recommend performing a backup prior to the changes and working with your DBA. We also recommend working with Professional or Expert Services to help perform these changes.

1. Find and note the *id* associated to the failed SP4 installation in the *whiteops.upgrade* table.
   - select * from whiteops.upgrade;
2. Run the following delete queries in order, updating the [[UPGRADE_ID_VALUE]] with the *id* value noted above.
   - delete from whiteops.upgrade_state where upgrade_component_id in (select id from whiteops.upgrade_component where upgrade_id = '[[UPGRADE_ID_VALUE]]');
   - delete from whiteops.upgrade_component_dependency where dependency_version = '8.3.0.4000';
   - delete From whiteops.upgrade_component where upgrade_id = '[[UPGRADE_ID_VALUE]]';
   - delete from whiteops.upgrade where id = '[[UPGRADE_ID_VALUE]]';
   - delete from whiteops.wbx_file where id not in (select file_id from whiteops.upgrade_component UNION select certificate_wbx_file_id from whiteops.installed_service);

3. Delete contents of the *%SAILPOINT_HOME%\Packages* folder

After the DB has been cleaned up and reloading the Client the 8.3 SP4 wbxpkg will no longer be listed in the 'Upgrades & Patches' screen. This allows for following a valid upgrade path to 8.3.0.000 and then retry SP4, Once FAM has been upgraded to at least 8.3.0.0000 there should be no issue reloading the SP4 wbxpkg and successfully completing the installation.

Chapter 6: List of Released E-Fixes

The following E-Fixes are included in this Release and will be automatically deployed:

Service Pack 1

SIQETN-2851 - Slow Performance in Data Classification Forensics page when using Resource filtering with DFS

Improved performance on page Forensics -> Data Classification search for DFS applications search.

SIQETN-3396 - Columns selection on Permissions Forensics filters doesn’t persist

Fixed Permissions Forensics filters feature; it now persists user's selections.

SIQETN-3398 - Failing to create a new campaign after deleting an application

New campaigns can now be created regardless of previous applications’ deletions.

SIQETN-3403 - The data area passed to a system call is too small exception on activity

FAM code is now catching and handling exception "data area passed to a system call is too small exception" on Activity Monitor for Windows file server.

SIQETN-3404 - Improve memory usage on Binary Serializer

Memory usage has been decreased by internally improving Binary Serializer FAM code implementation.

SIQETN-3406 - Task to start RabbitMQ server always fails

In certain situations, an Start Service error was thrown for RabbitMQ related service, this has been fixed.

SIQETN-3407 - Incorrect string encoding in SQL query

Fixed an issue where usernames containing underscores prevented Access Request submissions by correcting the username encoding logic.

SIQETN-3409 - FAM 8.4 QP- IDC Wizard - Joined Data Sources with similar headers selected as Remote Key - Remove both headers on Mapped Fields dropdown

Fixed an issue where selecting a Remote Key with similar headers across joined data sources during IDC setup.

SIQETN-3410 - FAM 8.4 - OP - Sharing Report - It is not possible to delete the first user we added to the list

Now all users can be deleted at the time the Report is shared.

SIQSUS-1311 - NFS 4.2 FAM Support

Support for NFS 4.2 is now implemented starting with this Service Pack, no new functionality has been added just pure support for this specific version.

SIQSUS-1478, SIQSUS-1479, SIQSUS-1480 - Assemblies FAM replacement/removal

FAM dependencies on CONCAT, COMPRESS and TO_LOWER_INVARIANT assemblies are now removed from the Product.

SIQSUS-1482 - FAM - ES upgrade to 8.19.4

Replacement for ES component with a newer version that helps to maintain into a tip-top condition.

SIQSUS-1484 - Improvement Crawl Task - Cache LiteDB taking a lot of time to read when file grows without limit

Adding a new setting for Permission Collection service, it will limit the size of LiteDB file when service is running out of memory and will cache the resources on disk during crawl.

SIQSUS-1485 - Telerik Security vulnerabilities on FAM Client application

Upgraded Telerik library (2024.4.1111) on FAM Client.

SIQSUS-1486 - FAM's Python libraries Upgrade

Upgraded Python(3.13.5) and Spacy library for Privacy Classification Task.

SIQSUS-1516 - FAM - RabbitMQ upgrade to 4.2.X

Replacement for RabbitMQ (4.2.3) component with a newer version that helps to maintain into a tip-top condition.

FAM 8.5.0.0

SIQETN-2868 - Over 2B Health Center Events causes Crawls to Fail with Arithmetic Overflow Error

Fixes a problem presented when there are more than 2 billion rows in the Health Center Events database table. There is a new step in the data cleanup process that will purge old records and reindex the table so it's always in a healthy state.

SIQETN-3249 - Not able to properly restrict protocols for RabbitMQ due to incorrect configuration

In certain cases, Campaign emails are not being sent due to an incorrect parameters usage. This has been fixed for this release.

SIQETN-3326 - SMTP client is deprecated needs replacement

In certain cases, Campaign emails are not being sent due to an incorrect parameters usage. This has been fixed for this release.

SIQETN-3352 - System.MissingMethodException during SCIM token validation

An issue has been fixed during any method call after the scim token authentication, an exception of type System.MissingMethodException is being generated in all versions of FAM that use .NET 6 and .NET 8.

SIQETN-3372 - FAM Server Installer not installing module V2 on IIS, if IIS was removed to reinstall website

Fix an error during website reinstallation that was generating an error within module V2.

SIQETN-3374 - FAM 8.4 Upgrade, error while trying to install Elastic 8 if customer have Activity monitors configured for windows file servers

Fixing error on server installer during upgrade from 8.3 to 8.4 and environment has Activity monitors installed.

SIQETN-3375 - RoleUsers and RoleHierarchy data sources configuration not updating

When a Data Source configuration is edited, e. g. user or password values, only the data sources for roles and users are updated, the data sources for RolesUsers and RolesHierarchy were not updated properly.

SIQETN-3376 - SPO PC: ACE.Identity is null

In certain cases, Campaign emails are not being sent due to an incorrect parameters usage. This has been fixed for this release.

SIQETN-3378 - Identity IQ FAM API throws a loop configuration error when calling the application endpoint

Fixed an error when detected at Identity IQ FAM API that causes a self-referencing exception when calling certain endpoints.

SIQETN-3379 - SPO: BS table is not updated when extended properties updated

Fixed a condition when a record's *field1* is updated in SPO, it cannot update existing/corresponding record in DB.

SIQETN-3381 - HTML injection validation for FAM alert emails

HTML injection will now be validated within FAM's email alert system/process.

SIQETN-3382 - Crawler gets stuck with error: LiteDB.LiteException: Document size exceed 16683050 limit

Permission Collector log is displaying an error during crawl; this is due to having folders with a huge number of Subfolders, record size depends on the full Path of directory and subdirectories complexity.

SIQETN-3386 - Getting configuration for SPO prevents from editing configuration

Fixing an error that appears when trying to edit SharePoint Online application.

SIQETN-3387 - Change ServerInstaller to use cabs de to MSI size limitations

MSI installers have a limitation of a max size of 2gb, now this is supported with the new changes in FAM size being exceeded.

SIQETN-3388 - Authentication Proxy discards variables information

When more than 1 proxy was configured by FAM code for Authentication Proxy management; the 2nd entry was not correctly read. This has been fixed.

SIQETN-3389 - REST API service crashes during heartbeat unhandled exception

Fix that prevents the Rest API service from going down when communication with the database fails during a health-check.

SIQSUS-1369 - Replace System.Data.SqlClient with Microsoft.Data.SqlClient

Now FAM uses a replaced System.Data.SqlClient with Microsoft.Data.SqlClient library to keep up with overall market updates.

SIQSUS-1376 - Vulnerabilities for Microsoft.IdentityModel.Tokens

Replacement for "Microsoft.IdentityModel.Tokens" with a newer version that helps with CVE-2024-21319.

SIQSUS-1421 - Vulnerabilities for NHibernate

Replacement for NHibernate library with a newer version that resolves several CVEs reported.

SIQSUS-1457 - RabbimtMQ upgrade to 4.1.X

Replacement for RabbitMQ component with a newer version that helps to maintain it in a tip-top condition.

SIQSUS-1462 - FAM Website not allowing to enqueue multiple Archive Stale Data Tasks

Second task never appears on tasks page when multiple are set up. This has been fixed.

SIQDEV-20726 - Stale Data capabilities for FAM

Stale Data capabilities have now been extended, please refer to Chapter 4 for further details.