# SailPoint IdentityIQ

Version: 8.0.1.3000

# File Access Manager v8.0.1 Service Pack 3 Deployment Guide

**Copyright and Trademark Notices.**

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

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

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

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

# Table of Contents

# List of Figures

# List of Tables

# Table of Revisions

Table 1 Table of Revisions

| Document Version # | Description | Author | Date |
|---|---|---|---|
| 1.0 | First Release | SailPoint | 7 February 2020 |
| 2.0 | Second Release | SailPoint | 26 June 2020 |
| 3.0 | Third Release | SailPoint | 30 October 2020 |

# 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

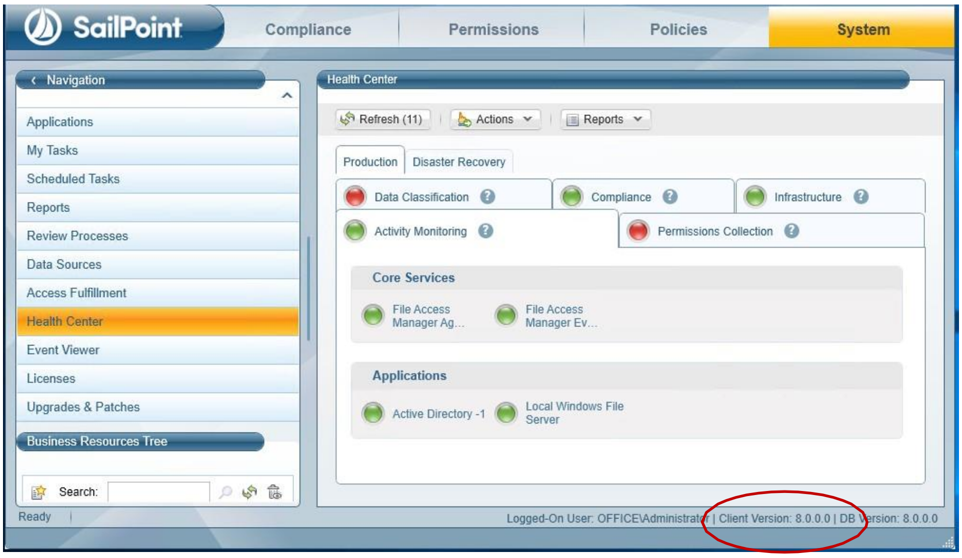
Starting from version 6.1, SecurityIQ (FAM) Service Packs deployment is done automatically. Service Packs are deployed by the File Access Manager update deployment mechanism. By simply uploading a Service Package through the Administrative Client, and pressing a button to initiate the deployment, the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



Logged-On User: OFFICE\Administrator | Client Version: 8.0.0.0 | DB Version: 8.0.0.0

**Figure 1 Application Monitors Screen**

File Access Manager version numbers are represented by a four-section number, e.g., 8.0.1.3000.
The first two sections represent major releases. File Access Manager 8 GA release number is 8.0.0.0. whereas, File Access Manager 8.1 release will be represented by the number 8.1.0.0.
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 Manager0 8.0.1 Service Pack 3 version number is 8.0.1.3000.
The Database version number will be updated with every service pack. For File Access Manager 8.0.1 Service Pack 3, the database version number is 8.0.1.3000.
The Client version number will be updated if the service pack includes changes to the Administrative Client. For File Access Manager 8.0.1 Service Pack 3, the database version number is 8.0.1.3000.

Infrastructure components, such as Elasticsearch and RabbitMQ will retain the same version number, unless and update to the actual infrastructure components is applied, in which case their version number will be updated as well. 8.0.1 Service Pack 3 does not include any updates to such infrastructure components.

## Versions included in this release:

Table 2 File Access Manager Component Version Details

| Component | Version |
|---|---|
| File Access Manager Database | 8.0.1.3000 |
| File Access Manager Elasticsearch | 5.1.1 |
| File Access Manager RabbitMQ | 3.7.4 |
| File Access Manager API | 8.0.1.3000 |
| File Access Manager Web Client | 8.0.1.3000 |
| File Access Manager Administrative Client | 8.0.1.3000 |

# Backup Measures

Backups are important. Having the original deliverable readily available, will allow you to quickly and easily roll-back 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 object 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 Service Pack 3 the Backup folder would be {%FILE_ACCESS_MANAGER_HOME%}\Backup\8.0.1.3000

# Chapter 2: Support Matrix

Table 3 IdentityIQ File Access Manager Server Support Details

| System | Supported Versions |
|---|---|
| IdentityIQ File Access Manager Servers | Windows 2012R2/2016/2019 |
| Workstation | Windows 8 and above |
| Browser | IE 11, Edge, Firefox, Chrome, Safari |
| Database | MS SQL Server 2012/2014/2016/2017 |

# Chapter 3: Deploying Version 8.0.1 Service Pack 3

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

4. Service Pack Deployment

   a. Upload the Service Pack through the Administrative Client

   b. Kick-Off the Service Pack deployment

   c. Verify successfully deployment

5. Post Deployment Steps

## Pre-upgrade Steps

1. Copy the "CollectorSynchronizerCertificateAssignmentTool" folder Included in the *File Access Manager v8.0.1.3000 Package* "tools" folder and place it on the server hosting the Collector Synchronizer service.

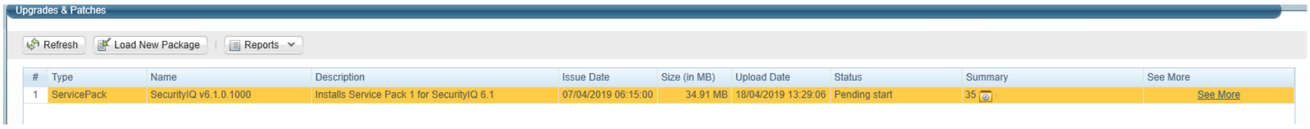
2. From the "CollectorSynchronizerCertificateAssignmentTool" folder, run "CollectorSynchronizerCertificateAssignmentTool.exe" with a user with administrative privileges on the server. Make sure the result is successful (the output window should show Success rather than Failure).

**Note:** The Certification Assignment Tool requires the location of the CollectorSynchronizerServiceHost.exe executable, and assumes the service and executable are located at the “%SAILPOINT_HOME%\FileAccessManager\CollectorSynchronizer\” path. In some case, for example on environments upgraded from SecurityIQ 6.1, the service executable may be located on a different path. If that is the case in your environment please set the “collectorSyncExePath” app.config key to the correct path, in the CollectorSynchronizerCertificateAssignmentTool.exe.config application configuration file, under the app.settings tag.

**Note:** If you have already applied Service Pack 2 for File Access Manager 8.0.1 prior to this service pack – this step can be skipped. Applying Service Pack 2 is **not** a pre-requisite to applying Service Pack 3.
All Service Packs are cumulative.

## Service Pack Deployment

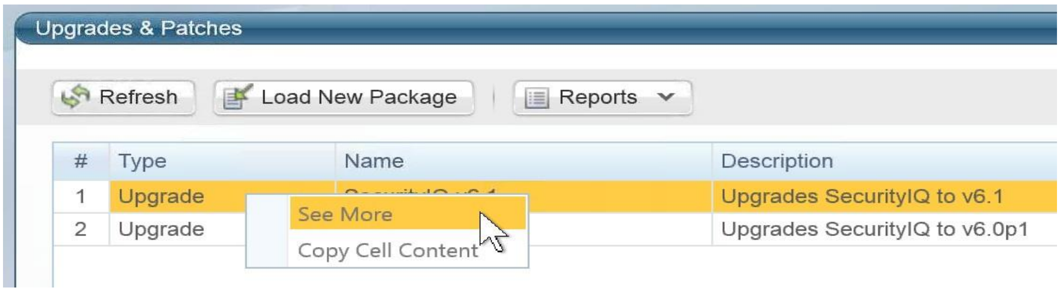
1. Extract the “File Access Manager v8.0.1.3000.zip” installation package.
2. Navigate to the “Service Pack 3” folder.
3. Log into the IdentityIQ File Access Manager Administrative Client
4. Click **System** >> **Upgrades & Patches** >> **Load New Package**
   This will open the **Load Package** dialog.
5. Press **Browse** and load the file “**File Access Manager v8.0.1 Service Pack 3.wbxpkg**” from the Service Pack folder.
6. Press **Upload Package**.
   The system will upload and validate the file. This might take a few minutes.
7. Once it is validated, press **Save**. This will add the upgrade package to the upgrades page.



| # | Type | Name | Description | Issue Date | Size (in MB) | Upload Date | Status | Summary | See More |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ServicePack | SecurityIQ v6.1.0.1000 | Installs Service Pack 1 for SecurityIQ 6.1 | 07/04/2019 06:15:00 | 34.91 MB | 18/04/2019 13:29:06 | Pending start | 35 | See More |

**Figure 2: Upgrades & Patches table**

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



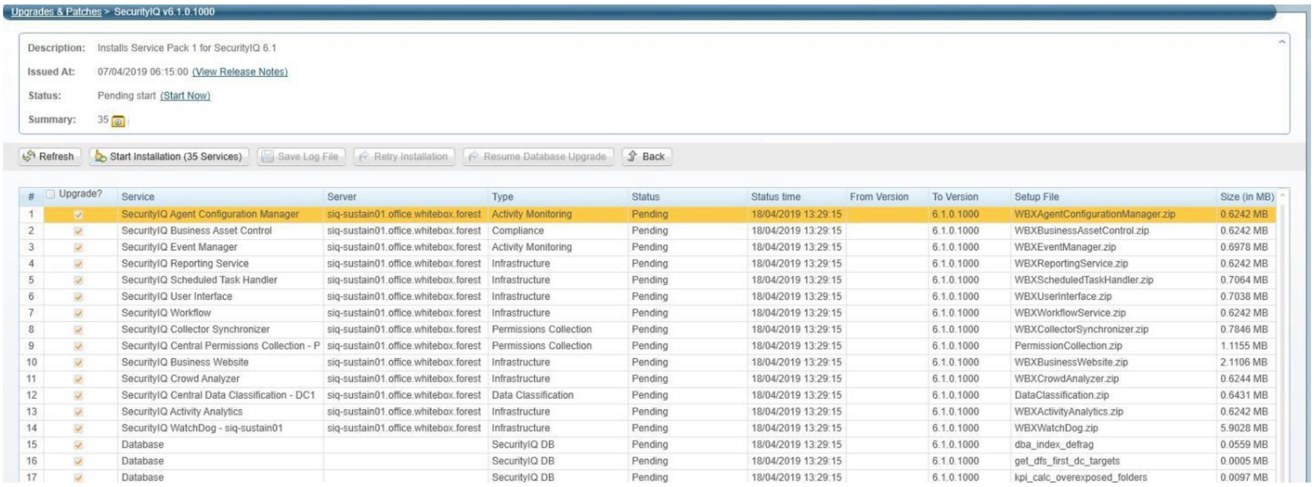
Upgrades & Patches

| # | Type | Name | Description |
|---|---|---|---|
| 1 | Upgrade | [illegible] | Upgrades SecurityIQ to v6.1 |
| 2 | Upgrade | | Upgrades SecurityIQ to v6.0p1 |

**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.



Upgrades & Patches > SecurityIQ v6.1.0.1000

Description: Installs Service Pack 1 for SecurityIQ 6.1

Issued At: 07/04/2019 06:15:00 (View Release Notes)

Status: Pending start (Start Now)

Summary: 35

| # | Upgrade? | Service | Server | Type | Status | Status time | From Version | To Version | Setup File | Size (in MB) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ☑ | SecurityIQ Agent Configuration Manager | siq-sustain01.office.whitebox.forest | Activity Monitoring | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXAgentConfigurationManager.zip | 0.6242 MB |
| 2 | ☑ | SecurityIQ Business Asset Control | siq-sustain01.office.whitebox.forest | Compliance | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXBusinessAssetControl.zip | 0.6242 MB |
| 3 | ☑ | SecurityIQ Event Manager | siq-sustain01.office.whitebox.forest | Activity Monitoring | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXEventManager.zip | 0.6978 MB |
| 4 | ☑ | SecurityIQ Reporting Service | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXReportingService.zip | 0.6242 MB |
| 5 | ☑ | SecurityIQ Scheduled Task Handler | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXScheduledTaskHandler.zip | 0.7064 MB |
| 6 | ☑ | SecurityIQ User Interface | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXUserInterface.zip | 0.7038 MB |
| 7 | ☑ | SecurityIQ Workflow | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXWorkflowService.zip | 0.6242 MB |
| 8 | ☑ | SecurityIQ Collector Synchronizer | siq-sustain01.office.whitebox.forest | Permissions Collection | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXCollectorSynchronizer.zip | 0.7846 MB |
| 9 | ☑ | SecurityIQ Central Permissions Collection - P | siq-sustain01.office.whitebox.forest | Permissions Collection | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | PermissionCollection.zip | 1.1155 MB |
| 10 | ☑ | SecurityIQ Business Website | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXBusinessWebsite.zip | 2.1106 MB |
| 11 | ☑ | SecurityIQ Crowd Analyzer | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXCrowdAnalyzer.zip | 0.6244 MB |
| 12 | ☑ | SecurityIQ Central Data Classification - DC1 | siq-sustain01.office.whitebox.forest | Data Classification | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | DataClassification.zip | 0.6431 MB |
| 13 | ☑ | SecurityIQ Activity Analytics | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXActivityAnalytics.zip | 0.6242 MB |
| 14 | ☑ | SecurityIQ WatchDog - siq-sustain01 | siq-sustain01.office.whitebox.forest | Infrastructure | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | WBXWatchDog.zip | 5.9028 MB |
| 15 | ☑ | Database | | SecurityIQ DB | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | dba_index_defrag | 0.0559 MB |
| 16 | ☑ | Database | | SecurityIQ DB | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | get_dfs_first_dc_targets | 0.0005 MB |
| 17 | ☑ | Database | | SecurityIQ DB | Pending | 18/04/2019 13:29:15 | | 6.1.0.1000 | kpi_calc_overexposed_folders | 0.0097 MB |

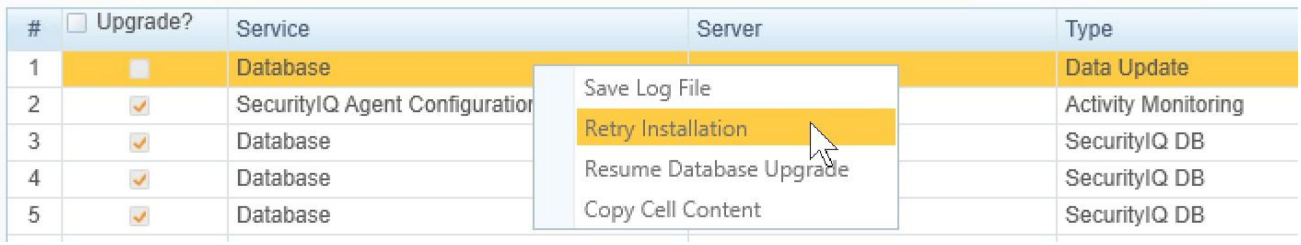
**Figure 4: Review Service Pack package - Details**

9. 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.



| # | □ Upgrade? | Service | Server | Type |
|---|---|---|---|---|
| 1 | □ | Database | | Data Update |
| 2 | ☑ | SecurityIQ Agent Configuratior | | Activity Monitoring |
| 3 | ☑ | Database | | SecurityIQ DB |
| 4 | ☑ | Database | | SecurityIQ DB |
| 5 | ☑ | Database | | SecurityIQ DB |

Figure 5: Retry installation line

10. Wait until all services have **Completed** or are in a **"Pending Restart"** status.

11. 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.

12. Wait until all services are in **"Completed"** status after restarting.

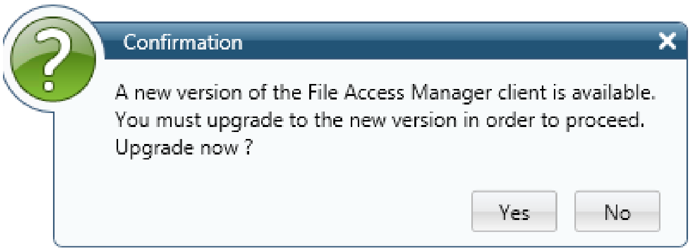
**Note: See** *Chapter 5: Troubleshooting* **for further suggestions and information.**

# Post Upgrade Actions

## 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.



Confirmation

A new version of the File Access Manager client is available.
You must upgrade to the new version in order to proceed.
Upgrade now ?

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 8.0.1.3000
The IdentityIQ File Access Manager Database version should be set to 8.0.1.3000

# Chapter 4: Important Information and Updates

## SIQSUS-11 Isilon Activity Monitor - Multiple Access-Zone and Tenant Isolation Support

File Access Manager Access Manager Isilon Connector now supports Activity Monitoring on Multiple Access Zones on the same Isilon Cluster, as well as full tenant isolation removing the need for System Access Zone access for tenants' Access Zones.

This change requires additional configuration settings in the Isilon Application Configuration.

Please refer to *Appendix A: Isilon Multiple Access-Zone and Tenant Isolation Support* for more details.

## SIQSUS-569 - Extend Isilon Multiple Access Zone Support to Permission Collection

This enhancement extends the support for Isilon Multiple Access Zones and tenant isolation to Permission Collection and the entire connector.

See Appendix A below for further details.

## SIQSUS-490 – Exchange Online Connector Full OAuth 2.0 Support

The File Access Manager Exchange Online Connector now offers Full OAuth 2.0 Authentication, removing the need to provide User/Password credentials, federated users limitation, adding support for MFA requirements, and support for multiple service accounts.

This change requires changes to your current Exchange Online configuration settings.

Please refer to Appendix C: Exchange Online Connector Full OAuth 2.0 Support for more details

## SIQSUS-491 - Azure AD Connector Full OAuth 2.0 Support

The File Access Manager Azure AD Connector now offers Full OAuth 2.0 Authentication, removing the need to provide User/Password credentials, federated users limitation, and adding support for MFA requirements.

This change requires changes to your current Azure AD configuration settings.

Please refer to *Appendix B: Azure AD Connector Full OAuth 2.0 Support* for more details.

## Data Classification Enhancements

Among many improvements and performance enhancements to the Data Classification modules, File Access Manager 8.0.1 Service Pack 3 introduces several parameters that help customize and adjust the Data Classification module to best fit your needs and optimize performance.

These parameters have been added to the DC_Parameter table and have default values, that maintain the current behavior.

Changes to these parameters will take effect only after a restart to the relevant Data Classification Engine.

| Parameter Name | Description | Possible Values |
|---|---|---|
| ContentType | Determines whether Data Classification should extract and index the files Content, Metadata (file properties), or both.<br>This is meant to increase granular control over indexing, as well as for Metadata classification of AIP protected files. | 0 – Content (Body) only<br>1 – Metadata only<br>2 – Both (Default) |
| ShouldNewPropertiesBeDisplayed | Determined whether new file properties (Metadata fields) automatically discovered during the scanning and indexing process, should be presented to the user as searchable fields and available attributes in rule constructions. | `'true'` – New property fields will be presented. (Default)<br>`'false'` – New property fields will not be presented. |
| MaxFileSizeMB | Determines the Maximum size (in Mega Bytes) for files to be included in the scanning and indexing process. Anything over this size will be excluded and listed in the DataClassification.FailedDocuments log. | 0 – 500<br>If 0 is selected only content under 1 MB will be indexed |

## SIQETN-2536 – Handling Business Resource paths longer than 4000 characters

SIQETN-2536 fixes a SQLServer in versions 2014 (and earlier) limitation.

File Access Manager uses a hashing mechanism to create a unique identifier for each Business Resource stored in the File Access Manager database. SQL Server databases hashing mechanism, in versions 2014 and earlier, is unable to process (hash) values with 4000 or more characters.
Though resources with paths of 4000 characters or longer are extremely rare, SIQETN-2536 is designed to handle that limitation.

SIQETN-2536 introduces an Application Configuration (app.config) key to the Permission Collection Engine that, when enabled, will ensure paths longer than 4000 characters are excluded from the applications' resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

The Application Configuration key - "excludeVeryLongResourcePaths" – accepts "True" or "False" values, to enable or disabled the exclusion, respectively. It is disabled (set to "False") and commented out, by default.

### Note: When enabled, resources with paths longer than 4000 characters *will* be excluded

When enabled, Business Resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is ***extremely*** rare.

### Note: You should not enable exclusion of long paths, unless you experience an issue.

The issue will manifest itself through the following error message in the Permission Collection Engine log file, and only if the File Access Manager SQLServer database is of version 2014 or earlier:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data
would be truncated.
```

In all other cases, this feature should not be enabled.

### Note: This enhancement is only relevant if the File Access Manager database is on SQLServer version 2014 or earlier.

In all SQLServer versions after 2014 – this is no longer a limitation, and no action is needed.

### Note: Service Pack 1 will automatically apply SIQETN-2536.

However, the configurable key is disabled by default, and will not affect current behavior, unless enabled.

## SIQETN-2329 - Update Site Collection Administrator / Secondary Owners Script - to address Move to SharePoint Service Administrator and GUID identifiers

Microsoft stopped using global SIDs as a group identifier and moved to Tenant specific GUID to represent Admin groups. In addition, with the drop of the Global Administrator role requirement, the FAM service account is no longer a member of the Company Administrators group, but a member of the SharePoint Service Administrator group instead, due to its the assignment of the SharePoint Administrator Role.

As a result, we needed to change the SIQUpdateOneDriveSecondaryOwners.ps1  to reflect that change. Since this is an external script, the change will not be applied automatically, and will need to be run manually, if you wanted to take advantage of that change, and the reduced necessary privileges.

### Note: Working environments are not required or recommended to apply this change.

Although possible, it is by no means required to apply that change and run that script.

# Chapter 5: Troubleshooting

## 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 reencrypted, 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 ❼ Tools ❼ 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 ❼ **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.

## Watchdog Services fail to upgrade on Windows Server 2008 R2 or earlier

**Problem: The Watchdog service fails to upgrade on Windows Servers of versions 2008 R2 or earlier or the watchdog upgrade stays in pending state for an unreasonably long time, and the WatchDogSelfUpgrade log file indicates a .NET Framework incompatibility, requesting to update the .NET Framework to version 4.5**

This issue may occur on servers without .NET Framework version 4.5 installed, or when an earlier version is installed.
Windows Servers of version 2008R2 and earlier, are more likely to experience this issue.
This pertains to only to servers ***monitored*** by File Access Manager
(File Access Manager components other than the Windows Activity Monitor, require Windows OS version 2012R2 or above)

**Suggested solution:**
This issue should not recur in Service Pack 1.
If you are experiencing these please contact SailPoint Support.

# Chapter 6: List of Released E-Fixes

The following E-Fixes are included in this Service Pack and will be automatically deployed by the Service Pack:

## Service Pack 1

### SIQETN-2292 - User Exit impersonation failure for Responses and Data Sources

Setting up a User Exit Data Source with user credentials doesn't run the process as the indicated user. A User Exit Response with credentials fails with an Access Denied error.

### SIQETN-2329 - Update Site Collection Administrator / Secondary Owners Script - to address Move to SharePoint Service Administrator and GUID identifiers

Microsoft stopped using global SIDs as a group identifier and moved to Tenant specific GUID to represent Admin groups. In addition, with the drop of the Global Administrator role requirement, the FAM service account is no longer a member of the Company Administrators group, but a member of the SharePoint Service Administrator group instead, due to its the assignment of the SharePoint Administrator Role.

### SIQETN-2562 - Microsoft has changed how groups are identified in AD

Microsoft has changed the internal group names from "c:0-.f|rolemanager|{SID}" to both "c:0-.f|rolemanager|{UID}" and "c:0t.c|tenant|{UID}" update to the permissions collection engines we required to handle the new way these internal groups are named.

### SIQETN-2576 - Dashboard Widgets Calculation Task Performance Enhancement

Another performance enhancement for the KPI Calculation procedure (which is part of the nightly Dashboard Widgets Calculation task).
Streamlined a hierarchical CTE responsible for retrieving resource children and added a missing NOLOCK to a DFS links query.

### SIQETN-2583 - Data Classification: Adding parameters to toggle content / metadata collection and auto-detection of file properties

Added several configurable parameters to the Data Classification parameters tables to customize behavior:

The ContentType parameter was added to control whether files' content, metadata or both are scanned.
The ShouldNewPropertiesBeDisplayed parameter was added to control whether automatically gathered file properties should be displayed as searchable fields.

### SIQETN-2586 - SharePoint Online Permission Collection fails - due to Site Collection fetching error (CSOM Dictionary Concurrency Contention)

CSOM Dictionary Concurrency Contention caused a problem with synchronization in setting the timeouts during permission collection was causing a task to fail prematurely. The timeout logic was updated to make the timer event check the status of the timer, before triggering a timeout. The timer event will not trigger a timeout event if the timer that it is associated with is stopped. All access to the CSOM libraries was brought into locks, and data transfer objects were introduced to transfer the permissions information from the collector to the engine.

## SIQETN-2601 - OneDrive Personal Drive Verification Step Timing Out, and Seeing Many 404s

Incorrect and / or inefficient calls during Personal Drive verification stages may cause crawl to time out due to throttling and extensive exceptions thrown from the OneDrive API. In addition to correcting and improving the calls, a new app.config key was added to bypass the verification steps in case it's not needed or causing problems

## SIQETN-2610 - Configuring Access Requests Reminders - reports errors when creating reminders for open Access Requests

Reported error is benign. Access Request reminders continues as designed.

## SIQETN-2611 - Access Fulfillment: If no Days of Week selected, AF tasks fail and report errors

When No Days of the Week selected in AF Commit Schedules, Errors Fill Up CollectorSynchronizer log.

## SIQETN-2617 - Various date-time fields on the Website display Invalid Date on different cultures

When the server on which the Business Website runs is set by default to a date-time format that doesn't match the English (US) format (because of language/culture settings), some date-time fields will display "Invalid Date" rather than a date-time string.

## SIQETN-2623 - NetApp Activity Monitor (CIFS) - Paths with tilde (~) can slow down processing

Activities occurring on paths containing tilde (e.g. \\naserver\~...) can significantly slow down processing of activities on a NetApp Activity Monitor (CIFS only). This is because paths with tilde are assumed to be truncated paths which match the legacy 8.3 format (e.g. PROGRA~1 for Program Files). When we encounter those, we try to convert then to regular paths which requires querying the remote VServer, causing delays.

## SIQETN-2629 - Add more granular control over Event Manager cached object expiration and Memory throttling

This is an Enhancement Request to allow for more Granular control over the Event Manager object caching expiration, as well as adding more granular statistics logging over cache component states in the statistics logs.

This was a result of an anomaly we observed where the Event Manager could reach a certain amount of memory and block any further Activity Monitoring because of that.

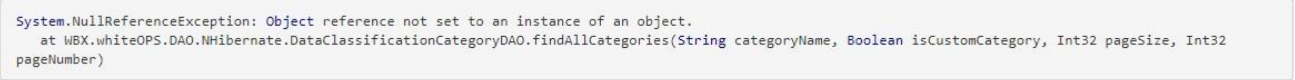
This feature is meant to (1) Add some more granular information to help identify what exactly is taking up memory - in terms of caching. (2) Add the ability to adjust the Threshold after which the Event Collector willl block - primarily meant for servers with high RAM capacity - so the threshold can be raised to a higher level to utilize more of the server's resources.

## SIQETN-2641 - OneDrive - SPOnline Performance & Throttling Enhancements

This enhancement encompasses several fixes and refactoring changes directed at improving the performance, throttling handling, resiliency and logging for the SharePoint Online and OneDrive connectors.

## SIQETN-2649 - Website Category Search fails in Data Classification Forensics page when SiqApi Debug is enabled

When logging level is set to DEBUG for SiqApi web app in IIS, the category search feature in the Data classification on forensics page will fail will following error:



```
System.NullReferenceException: Object reference not set to an instance of an object.
   at WBX.whiteOPS.DAO.NHibernate.DataClassificationCategoryDAO.findAllCategories(String categoryName, Boolean isCustomCategory, Int32 pageSize, Int32
pageNumber)
```

## SIQETN-2652 - NetApp CIFS Activity Monitor - Activity exclusion by folder doesn't work

When excluding activities by folder for NetApp CIFS Activity Monitors, activities for the excluded folders are still saved.

## SIQETN-2660 - User Scope - Data Owner notification for alerts should be sent to the users with the relevant scope and the "Data Owner" capability

“Data Owner” alert notifications were sent to all users whose scope contained the resource on which an alert was triggered, instead of only for Data Owners. The fix restricts the notification to Data Owners only.

## SIQETN-2662 - NHibernate Audit Interceptor throws exceptions when AuditField new_value is longer than 4000 characters

An Error indicating that a role description is exceeding 4000 characters appears in the UserInterface service logs.

The fix is to update AuditField type.

## SIQETN-2663 - SharePoint 2010 Activity Monitor fails to monitor events since 6.1 overhaul

In SecurityIQ (FAM) version 6.1, there has been a major overhaul in the way we access SharePoint data, so now we connect directly to the database and have implementations of the data structures in our code.

SharePoint 2010 has a different structure for the SPAuditEntry entity, which has one less property than the rest of the versions after it (2013, 2016 and 2019, which are currently supported, contain an extra AppPrincipalID property).

## SIQETN-2667 - My Reports Page Fails to Load when Report Owner User Does Not Exist

My Reports page on the Business Website does not load: shows no reports in the reports list and doesn’t not display any “error loading” or “loading failure” message on the website, if a personal report does not have an Owner user Id, or that the owner user id, does not exist as a FAM user.

## SIQETN-2668 - Bulk Installation template file throws an exception when multiple Event Managers are configured

Using the Bulk Installation function when having more than a single Event Manager yields an error generating the template file - rendering it impossible to use the Bulk Installation feature.

## SIQETN-2674 - Data Classification Forensics Page loads extremely slow when using filters such as rule, policy, and category

When using filter parameters such as policies, rules, or categories on the data classification forensics page, the page load time is extremely slow, and sometimes never returns.

## SIQETN-2678 - SPOnline O365 Groups Permission on Team Sites not being gathered

SharePoint Online Team Sites introduced a different approach to assigning permissions.
The existing method of local groups still exists, but it’s encapsulated by the Office 365 group that the Team Site is associated with (creating an Office 365 group creates a Team Site and vice versa). By default, group members are assigned Edit permissions, while group owners are assigned Full Control. The defaults can be changed by accessing the “Advanced permissions settings“, or by using PowerShell APIs. Through those methods, you can access the underlying logic of local groups as it is in legacy sites.
Currently, FAM/SecurityIQ is unable to expand the entities that represent the Office 365 group members and owners in Team Site local groups, meaning the permissions gathered on Team Sites are usually next to nonexistent.
To expand these entities, we’ll have to associate them with existing data from Identity Collection, which also means we’ll have to fetch group owners data from Azure AD.

## SIQETN-2679 - SIQETN-2679 - SQL Error: 'There is already an object named 'ra_deleted_roles_for_cleanup' in the database.', when applying 8.0.1

This issue only affects Upgrades of environment that have previously deployed the 6.1 Service Pack 2 Package.

Customer upgraded from 6.1 to 8.0 successfully. Then, when applying 8.0.1, they received this error:

Script execution error: 'An exception occurred while executing a Transact-SQL statement or batch.'SQL Error: 'There is already an object named 'ra_deleted_roles_for_cleanup' in the database.', Line: 1

## SIQETN-2685 - role_uid fields missing from ra_entitlement views - required for IIQ old integration

The role_uid field is used in the IIQ old integration - prior to the SCIM API, was removed from these views, as part of the RA views cleanup following the SCIM API development. The column was re-added to the relevant view to support ongoing IIQ integration processes, and for backward compatibility with previous IIQ versions.

## SIQETN-2688 - Activity Monitor files sometimes get removed by watchdog when service pack is being applied to new service

When installing an activity monitor for which there are service pack updates to apply, sometimes the process of applying that update fails and has the effect of removing all files from the activity monitor service folder.

## SIQETN-2697 - SharePoint OnPrem Crawler Fails when Analyze Permission on File is on - in case of Draft files

8.0 introduced changes to how files with unique permissions are handled.

In SharePoint, each "version" of the file is represented by a separate row in the Database, separated by the Level field - where:1 - Public2- Draft 255 - Checked Out.

SharePoint treats public, draft, and checked out files as separate records but considers them a single business resource. A file can be in one of the following states public, draft, checked out, public + checked out, or draft +

checked out. Since a file can have two records in the cases of public + checked out and draft + checked out one of them needs to be selected for our business resource object. Product will prefer the type with the lowest enumeration value according to public (1), draft (2), and checked out (255).

## SIQETN-2700 - SiqApi Call with potential SQL Injection vulnerability

The following API was identified as potentially vulnerable to SQL Injections:
/siqapi/campaignWizard/checkValidName
The endpoint, used to verify Campaigns names, accepts a name parameter, to identify a campaign with a specific name. An underlying non-parameterized SQL query can be abused for injecting warranted SQL code.

## SIQETN-2701 - EMC CEE Instance Cannot Connect to "Local" EMC BAMs

The File Access Manager EMC BAMs function as an RPC Server endpoint to the EMC CEE component. The option for a “Local” RPC Server was removed and is not re-instated.

## SIQETN-2702 - Cross-Site Scripting vulnerability in web-UI certain endpoints

The following endpoint were not protected against Cross-Site Scripting:

/siqapi/newAccessRequest

/siqapi/campaignWizard/saveCampaign

Both these endpoints accept free-text fields for the Access Request comment field, and the

Campaigns instructions. Lack of proper encoding and data validations made these vulnerable to JS injection, and are now protected against it.

## SIQETN-2704 - Agent Configuration Manager: Performance Enhancements and Optimizations

The Agent Configuration Service can fail to fulfill service calls because of NHibernate running out of available sessions in its session pool. Analysis reveals that the implementation of many of the ACM service methods is fetching much more information from the database than is required and is fetching much more often.

Using much slimmer DB calls using NHibernate projections and transforms and implementing in -memory caches where possible – reduces the load and duration on the session pools and overall optimize ACM performance.

## SIQETN-2722 - Access Fulfilment - Adding permission to a user without a display name fails

After setting up Access Fulfilment, trying to fulfil an Add Permission request for a user who doesn't have a display name seemingly results in success, but in fact the user is not added to the relevant group in Active Directory.

The Collector Synchronizer log shows an “Index-out-of-range” exception.

## SIQETN-2737 - Non unique result on permission collection because of multiple alt-uids

In cases of double migration, meaning migrating from domain A to domain B, and sometime later to domain C, the ra_role_alt_uids table will have two rows with the same uid for various roles.

The reason for that is that the alt_uids are saved in each role's sid history. After migrating from one domain to another and running an identity collection, a new role is created in FAM, as well as an additional row in ra_role_alt_uids, with an alt_uid that already exists in that table.

This causes a situation where a permission is collected for a role that no longer exists in FAM, but its identifier is still logged through the SID history support. Trying to fetch unique results for roles with multiple entries fails the query.

### SIQETN-2741 - After Removing Permission Coll Eng from Server Installer, all Collectors are No Longer Visible in Collector Installation Manager

Upon removing a Permission Collection Engine, which was never fully installed, from the FAM configuration (via the Server Installer) any and all collectors installed on that SAME machine/server (of wherever the removed Perm Coll Eng was added) become no longer visible in the Collector Installation Manager.

This happens for collectors ALL collectors on that same server - regardless of if they were installed before or after that engine is added. Once removed, all collectors disappear - even if they were not added for that engine.

### SIQETN-2743 - Identity Collection Task fails when synchronizing users without last login date change

Identity Collection task will fail, with the message below appearing in the Collector Synchronizer log file, when the Identity Collection synchronizes users with no last login date, or with a login date that did not change since the last run.

### SIQETN-2756 - Merging large number of Root BRs fails on timeout

During a crawl, if the number of root shares is relatively large - merging the root BRs may time-out, failing the crawl task.

### SIQETN-2757 - DEC Test Connection for DEC set with Specific Server does not retain specific server definition

During the “Test Connection” operation the information about a Specific Server Configuration is not retained.

In cases where just that server is accessible (for instance, only one server enables SSL communication) - this may fail the Test Connection operation on the DEC configuration screen, and results in a “The Server is not Operational” in the logs. This does not affect the DEC operation itself, or any Identity Collection that may rely on the DEC definition, as the definition is collected and persistent in the database  correctly.

## Service Pack 2

### SIQETN-2416 - Exchange Online BAM - MessageBind operation deprecated

Microsoft is in the process of deprecating the MessageBind operation for Exchange Online.
The new operation type that replaces the MessageBind is _MailItemsAccessed_.
The MailItemsAccessed is valid for all LogonTypes: AdminAudit, AuditDelegate, and AuditOwner.

### SIQETN-2468 - Bulk Re-assignment during Certifications Not Fully Re-Assigning All

Access Certification Campaign Bulk re-assignment refactoring and performance enhancement, to prevent timeout and incomplete re-assignment operations for large scale campaigns.

## SIQETN-2486 - Box BAM - optimize event reading and processing to prevent delay

Several performance enhancements to the Box Activity Monitor, improves parallel processing in both fetching and processing events.

## SIQETN-2491 - SharePoint Online/OneDrive allow Configurable URL/Root Domain

O365 *dedicated* tenants may have custom URLs for their SharePoint Online and OneDrive environments.
This fix add support for such customer URLs.
This fix only applies for O365 *Dedicated Tenant* environments.

## SIQETN-2525 - HDS Activity Monitor Improvements

The following enhancements were made to the HDS Activity Monitor:

1. Deletion of cached open events occur based on how long they've existed (TTL) rather than arbitrarily at an interval.
2. TTL and deletion interval are configurable.
3. Failure to fetch HNAS shares at any point does not delete the shares cache already in memory.
4. The log reader thread is now stopped along with the service, to avoid leaving the process up after the service is down.
5. Notifications about close events not being matched to open events are now reported as warnings rather than errors.

## SIQETN-2681 - OneDrive BAM - Not Finding Owner ID with Custom Tenant URL Configured

It is possible (but not common) for a SharePoint Online/OneDrive for Business customer to have a custom Tenant URL/Domain. Together with SIQETN-2491, we added the ability to configure these custom URL.
This fix keeps the domain configurable, while adding back in the proper format for parsing the URL within the OneDrive event, so that the events that are retrieved from OneDrive use the correct URL pattern.
These fixes only apply for O365 *Dedicated Tenant* environments.

## SIQETN-2763 - Generic Table Support for Activity Monitoring - Forensics & Reports

After setting up a Generic Table Activity Monitoring, issues in displaying Activities Forensics and creating Activity Reports may occur, such as Loading Failed on the Activities Forensics screen and null errors in the Reporting log.

## SIQETN-2766 - Threshold Alert "Details" filter does not include correct User Information

When creating a threshold alert for activities performed "by the same user", and then viewing the activity results from the alert details when clicking "View activities", the user is not included in the filter used for the activities detailed view, presenting activities from other users as well.

## SIQETN-2768 - SharePoint crawl ignores host-named site collections with same host-name

SharePoint host-named collections that share a host-name are not found when a crawl is executed.
Despite this failure the crawl completes in a successful state.

## SIQETN-2771 - SharePoint permission collection loads all resources within a site collection at once

SharePoint permission collector loads extensive permissions hierarchy, on initial BR load, which may cause timeouts during permission collection.

## SIQETN-2778 - OneDrive Crawling Unique File Level Permissions is missing throttling support

Recent additions to support throttling detection and back-off for OneDrive did not include the crawl for File level with unique permissions when detecting whether to include the file in the crawl resource results.

## SIQETN-2780 - OneDrive crawling can timeout while verifying mailboxes as part of fetching roots

To eliminate uninitialized or decommissioned personal drives which will throw a 404 File Not found during crawl, we query each mailbox during the roots collection crawl step to exclude those personal drives.
This increases the number of API calls during the roots fetching step relative to the number of personal drives.
Timeouts may occur during this stage in large environments.

## SIQETN-2788 - Exchange Online Crawl failure to create initial PowerShell session causes task cleanup error and subsequent task failures

When the initial PowerShell session cannot be created during EXO crawler initialization, the subsequent cleanup throws an exception, causing the cleanup task to fail to complete, and subsequent tasks on the same engine to fail to start.

## SIQETN-2789 - Data Classification fails to complete (hangs) when processing file with long path

When data classification indexes a resource with a very long file name / path, an exception is encountered which causes the completion response to fail to send to the engine and therefore the task will not complete.

## SIQETN-2795 - SharePoint On-Prem Activity Monitor seemingly not monitoring due to performance issues

SharePoint On-Prem Activity Monitor might seem to not be monitoring at all, due to a performance issue causing it to take a while to parse a certain type of activity.

## SIQETN-2796 - Exchange Online Connector Does Not Handle Apostrophes (') Well

Exchange Online crawling and permissions collection throw an error on mailboxes /users with apostrophes in the name.

## SIQETN-2798 - Well Known SID lookup misses in Exchange OnPrem Activity Monitor causes excessive errors and slows event processing

Access Certification Campaign Bulk re-assignment refactoring and performance enhancement, to prevent timeout and incomplete re-assignment operations for large scale campaigns.

## SIQETN-2803 - Activities Website's Forensic Screen and Reports Fail on Elasticsearch Queries Timeouts

Activities Forensics Screen throws a timeout error, when trying to fetch available values for filter fields, and when querying results, if the scope time frame is too large.

### SIQETN-2813 - Data Classification - OutofMemory error can occur when not all indexing is cancelled on task stop

It's possible for an OutofMemoryException to occur when re-running a Data Classification task because the previous task does not get completely cancelled and memory allocations are not completely cleared out.

### SIQSUS-11 – Isilon Activity Monitor - Multiple Access-Zone and Tenant Isolation Support

See Appendix A below for further details.

### SIQSUS-127 – DropBox Activity Monitor Refactoring – V2 Schema Support

The DropBox Activity Monitor was refactored to support the DropBox V2 API schema, in additional to several performance enhancements.

### SIQSUS-491 – Azure AD Connector Full OAuth 2.0 Support

See Appendix B below for further details.

### SIQSUS-544 – Added Support for increases session Concurrency in FAM API

Session Factory session now allows for more efficient session concurrency.

## Service Pack 3

### SIQSUS-490 – Exchange Online Connector Full OAuth 2.0 Support

See Appendix C below for further details.

### SIQSUS-569 - Extend Isilon Multiple Access Zone Support to Permission Collection

This enhancement extends the support for Isilon Multiple Access Zones and tenant isolation to Permission Collection and the entire connector.
See Appendix A below for further details.

# Appendix A: Isilon Activity Monitor - Multiple Access-Zone and Tenant Isolation Support

## Description

**Important!** Service Pack 3 completes the tenant Isolation and deprecation of the Management API dependency. Starting File Access Manager 8.0.1 Service Pack 3, File Access Manager provides full support for multiple-access zones, and full tenant isolation, across all its Isilon connector components.

File Access Manager now offers Tenant Isolation and Full Capabilities for Multiple Access-Zones on Isilon Clusters. With the addition of the Activity Monitoring and Permission Collections capabilities for Multiple Access-Zones within an Isilon Cluster and removing the dependency on the Administrative (System)-Zone-based OneFS API, each Access Zone within the cluster functions as an independent Isilon Application within FAM, with the complete set of FAM capabilities.
This enhancement marks the transition in approach from a Cluster-Oriented to a Zone-Oriented configuration. The new configuration will allow users to easily configure applications per Access Zone settings, now allowing for multiple Access Zones on the same cluster to be created with ease.

With the deprecation of the dependency on the Management API, this new mode of access simplifies the configuration setting, and only requires knowledge, connectivity and access rights of and to the managed Access Zone. This allows for a complete delegation of the configuration, administration and monitoring of an Isilon Access Zone to the tenant owner, removing the need for centralized management. Tenant Isolation and management is critically valuable in multi-tenant hosted environments, where such isolation enhances data privacy and autonomous management.

The new configuration also simplifies setting Access Zone and Management API (optional) settings, through the Application Configuration Wizards, settings that were previous set through application setting files.

### General Description

This enhancement brings full tenant isolation, and full capability support for multiple access zones on the Isilon Cluster, treating each Access Zone as a separate entity.

**Important! ALL** existing Isilon application will continue to function, with no changes required from current users. This enhancement requires some configuration changes be made for the new capabilities to become available and take effect. However, no configuration changes are required, if multiple access zone support is not required in your environment, and all currently configured application will continue to operate as always.

# Configuration Changes

Configuration changes included in this enhancement are:

- The following fields were added to the configuration as new (optional) fields:
  - **Storage Cluster Name** – The name of the clustered as it is registered with the CEPA Server
  - **Access Zone** – The name of the Access Zone as it is configured on the Isilon Cluster
- New Tenant Isolation Fields (optional)
  - **Use OneFS API** – Enables / Disable access to the OneFS API, and reversely, Disable / Enables tenant Isolation. OneFS API is located only on the System Zone and is used by the Permission Collection and Activity Monitor components of the Isilon Connector to fetch Share Information as well as Local Users and Roles for each individual Access Zone.
    Unchecking this will disable The Activity Monitor access to the API and the information will be collected solely using the SMB protocol, and access only the managed Access Zone.
  - **Management IP** – If access to the OneFS API is enabled, this field specifies the location of the Management API (System Access Zone). This field accepts IP addresses and / or any resolvable DNS name (FQDN or otherwise).
  -

## Note! App.Config Settings Keys will be deprecated in the next FAM release

The **Access Zone** and **Management IP** app.config settings keys, in the Activity Monitoring services configuration files, that were being used until now to configure Non-System Access Zone Applications in FAM, are replaced by the **Access Zone** and **Management IP** application configuration fields. These are available through the application configuration wizard. Although these app.config keys are still considered in FAM's 8.1 and 8.0.1 releases, they will be deprecated on the next FAM release.

To allow users time to adjust their configuration, and to minimize the effort required by our users, we continue to support these app.config keys through the 8.0.1 and 8.1 releases.
However, we strongly recommend that these setting be adjusted now to use the Application Configuration through the Application Configuration Wizard, to ensure successful future upgrades, and the continuous uninterrupted operation of the FAM environment.

**The same app.config settings, on the Isilon Permission Collection services, will be replaced by a separate enhancement, and currently should be kept set.**

## Note! All Activity Monitors for Access Zones of the Same Cluster must be installed on the same File Access Manager server

Due to limitations of the CEPA architecture, all Activity Monitor Services, monitoring Access Zones of the same cluster, must be installed on the same File Access Manager Server.

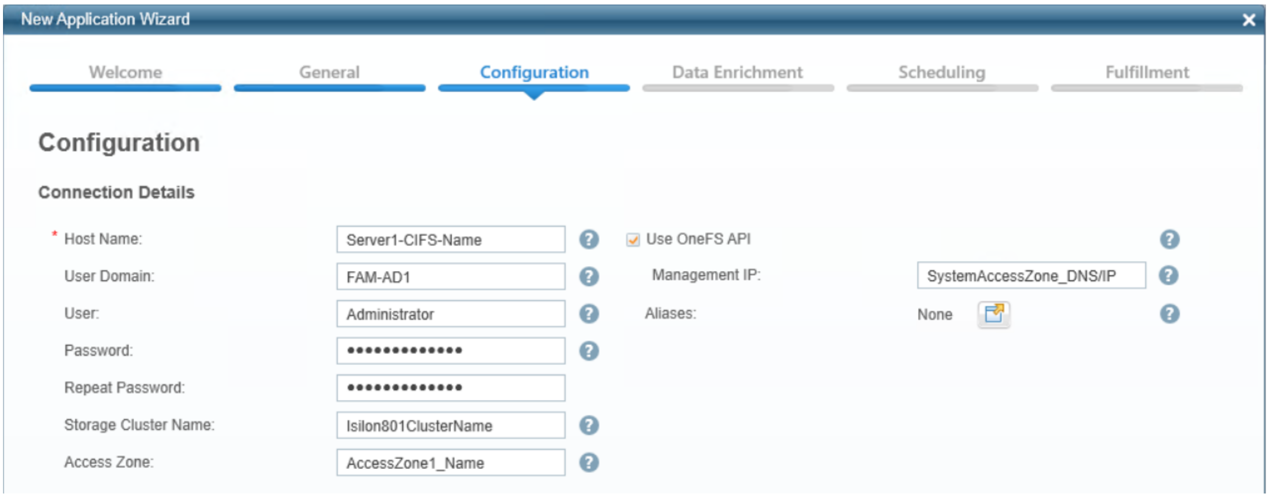
The File Access Manager Isilon Activity Monitor is a multi-instance service, i.e. a Single Service serves multiple instances of the Activity Monitor, e.g., for the different Access Zones. As a result, only a single service will be created (and appear in the Windows Services list), however, this single service will create activity monitors instances for all the Isilon Access Zones it is configured to monitor.

There is no limitation to the number of *Clusters* that can be monitor by a single File Access Manager Service. Although all monitors for Access Zones of the same cluster must reside on the same File Access Manager server, Activity Monitors for other clusters and their Access Zones can also be installed on the same File Access Manager server, provided that sufficient resources are allocated for that machine.

We recommend that instances will be added gradually, and resources be allocated appropriately to accommodate for the increase in activity volume, as the scope of the monitored environment grows, and more Activity Monitors are added to the server.

# Configuration (Screenshots)

## 1. Application Configuration Wizard

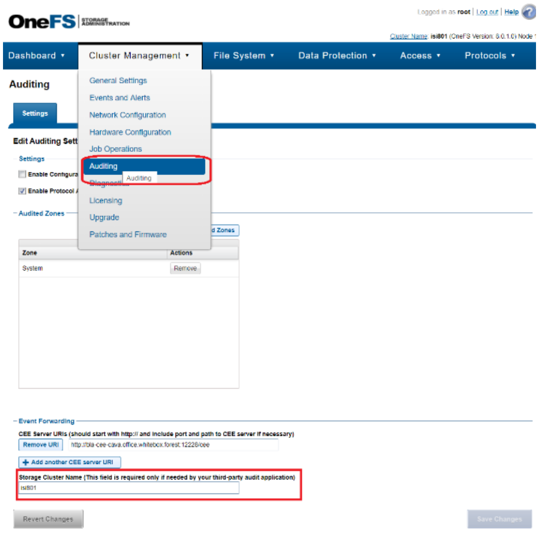


Configuration

Connection Details

| | | | |
|---|---|---|---|
| * Host Name: | Server1-CIFS-Name | ☑ Use OneFS API | |
| User Domain: | FAM-AD1 | Management IP: | SystemAccessZone_DNS/IP |
| User: | Administrator | Aliases: | None |
| Password: | ••••••••••••• | | |
| Repeat Password: | ••••••••••••• | | |
| Storage Cluster Name: | Isilon801ClusterName | | |
| Access Zone: | AccessZone1_Name | | |

- **Host Name** - The File Server's name users connect to it - its CIFS Name. This will be used by the SMB (CIFS) protocol.
- **User's Domain, Name & Password** – The Service Account dedicated for FAM, defined in the pre-requisite section of the Isilon Connector Deployment Guide
- **Storage Cluster Name -** The name configured in the Auditing section of the Isilon OneFS Admin Console (under the Cluster Management >> Auditing settings tab)



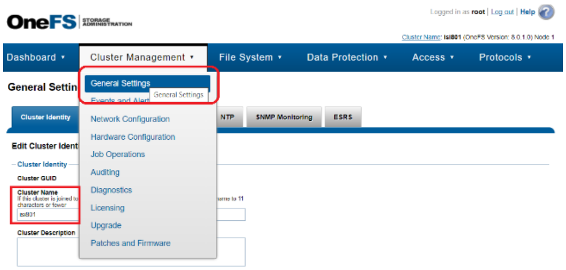
CEE Server URIs (should start with http:// and include port and path to CEE server if necessary)

http://bla-cee-cava.office.whitebox.forest:12228/cee

Storage Cluster Name (This field is required only if needed by your third-party audit application)

isi801

or if not configured, the name of the Isilon Cluster itself (under Cluster Management >> General Settings)

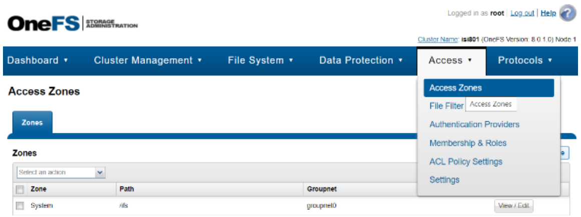


Cluster Name

If this cluster is joined to ... name to 11 characters or fewer

isi801

- **Access Zone -** The name of the Access Zone as it is configured in the Isilon Cluster configuration, in the Access section of the Isilon OneFS Admin Console (under Access >> Access Zones)

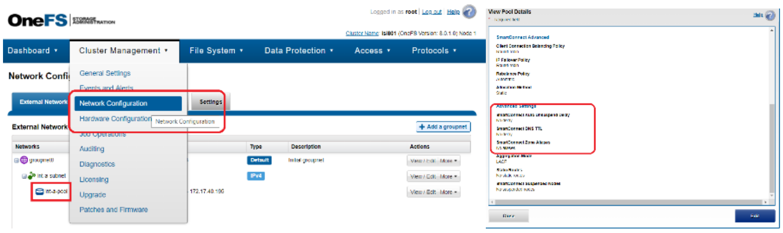


| Zone | Path | Groupnet |
|---|---|---|
| System | /ifs | groupnet0 |

- **Use OneFS API** – Enables / Disables access to the OneFS API.
  The Isilon OneFS Admin Management API is only available through the System Access Zone.
  The Management API is used by the Isilon Connector to fetch Share Information and Local Users, Groups and Roles information, and required access to the System Access Zone to that end.
  With the New Isilon Connector, access to the Management API is no longer required for Activity Monitoring, and is skipped by default, using native SMB Access to the managed Access Zone instead.
  However, you can choose to keep the old configuration and keep access the Management API on the System zone, to retrieve Share and Local Identities information.

- **Management IP** – The IP address or DNS name of the Management Interface (the System Access Zone).
  If access to the OneFS API is enabled (by checking the **Use OneFS API** checkbox, see above),
  this field specifies the location of the Management API (System Access Zone).
  This field accepts IP addresses and / or any resolvable DNS name (FQDN or otherwise).

- **Aliases** – SmartConnect Zone Aliases used as alternative DNS Names for the CIFS Server. All aliases must be provided to ensure that all activities performed on that server, through all access paths, are monitored by File Access Manager.
  These are available under the IP Pool Settings, in the Network Configuration section of the Isilon OneFS Admin Console (under the Cluster Management >> Network Configuration tab)



# Appendix B: Azure AD Connector Full OAuth 2.0 Support

## Description

File Access Manager now offers full support of standard OAuth 2.0 Authentication for the Azure AD connector.

The new authorization sequence will direct the user through a standard Microsoft O365 consent flow, to grant the File Access Manager Azure AD Connector app the privilege to acquire and refresh access tokens.

The new authentication method replaces the previous Basic Authentication flow, that required admins to provide user and password credentials.

- The Azure AD Connector now uses only fully modern authentication methods, and does not require Legacy Authentication methods be enabled, tenant-wide, or otherwise.
- The Azure AD Connector supports any user as a delegated account (the granting account), including users with Multi-Factor Authentication requirements enabled, and is no longer limited by Microsoft's restrictions on Federated Accounts
- The Azure AD Connector Supports internal Token Management and will be responsible for managing and renewing its own tokens.

### General Description

This enhancement brings full OAuth support to the Azure AD Identity Collector, instead of the legacy user and password approach.

This means the configuration will resemble other connectors for cloud applications such as OneDrive.

- Configuring the Identity Collector, instead of providing a user name and a password, you will click on a link that sends you to a Microsoft login page.
- Enter the relevant user credentials and give your consent for the File Access Manager Azure AD O365 Application to access your directory data.
- You will then copy the resulting Authorization Code to the appropriate field, which will then be used to generate the first access token.
- The access token will be used in all requests to the tenant's Azure AD and will be automatically refreshed when needed.
- **Note!** This enhancement requires multiple manual steps that must be followed carefully. This enhancement will also require you to reconfigure the AzureAD Identity Collector and go through the configuration wizard to generate access tokens and switch over to modern authentication flow.
- This will not recreate the identity collector, and current AzureAD information will remain intact.

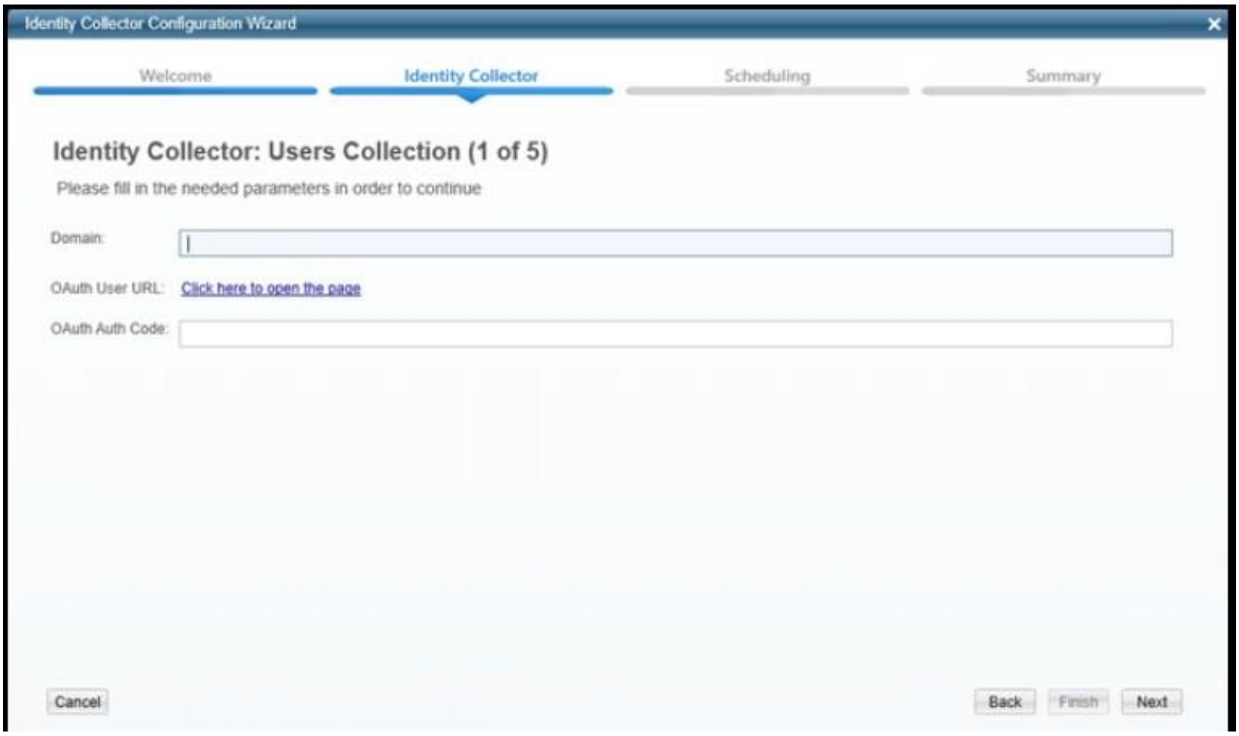
# Deployment Instructions

1. As part of this Service Pack Pre-Upgrade steps, you should have run the "CollectorSynchronizerCertificateAssignmentTool" utility that is attached as part of this package.
   Please refer to the *Pre-Upgrade* section in *Chapter 3: Deploying Version 8.0.1 Service Pack 3* and perform the pre-upgrade steps if you have not yet done so.
2. **Important!** Without completing this step, the Azure AD Identity Collectors will not work.
   1. Open the Administrative Client, edit your Azure AD Identity Collectors and follow the wizard to completion.
   2. The screen called "Identity Collector: Users Collection (1 of 5)" has undergone some modifications, so make sure to click on the "OAuth User URL" link and follow the instructions.
3. **Optional:** Run Identity Collection for Azure AD and make sure the task completes successfully.
4. **Optional:** Run Identity Collection for Azure AD again after two hours and make sure the task completes successfully.

# Configuration Steps (Screenshots)

## 2. Identity Collector Configuration Screen

In the Identity Collector Configuration Wizard enter your O365 Domain name then click on the "OAuth User URL" link to generate an Authorization Code



Identity Collector: Users Collection (1 of 5)

Please fill in the needed parameters in order to continue

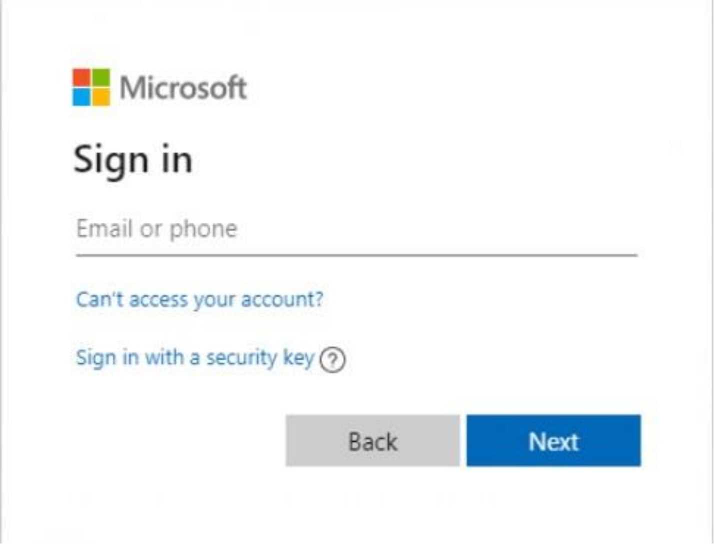
Domain:

OAuth User URL: Click here to open the page

OAuth Auth Code:

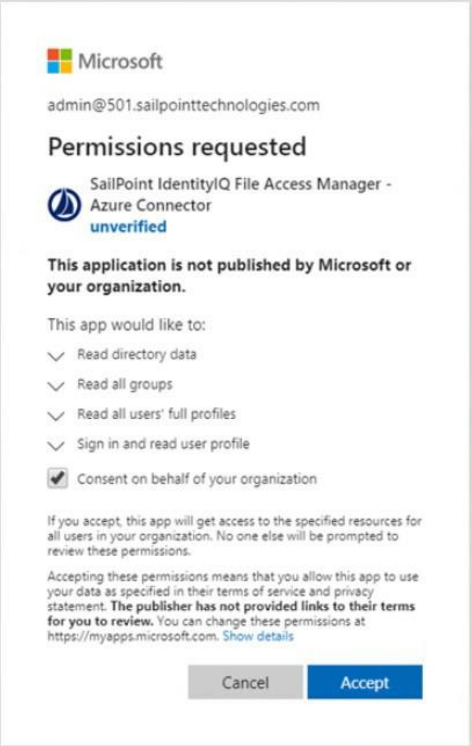
## 2. MS O365 Login Screen

You will then be redirected to the Microsoft O365 Login Screen Login with the user that should be used by the Identity Collector



## 3. MS O365 Application Consent Screen

You will then be prompted to consent to granting access to the File Access Manager Azure Connector Accept to receive an Authorization Code and continue with generating the Access Token



Microsoft

admin@501.sailpointtechnologies.com

Permissions requested

SailPoint IdentityIQ File Access Manager - Azure Connector
unverified

**This application is not published by Microsoft or your organization.**

This app would like to:

- Read directory data
- Read all groups
- Read all users' full profiles
- Sign in and read user profile

☑ Consent on behalf of your organization

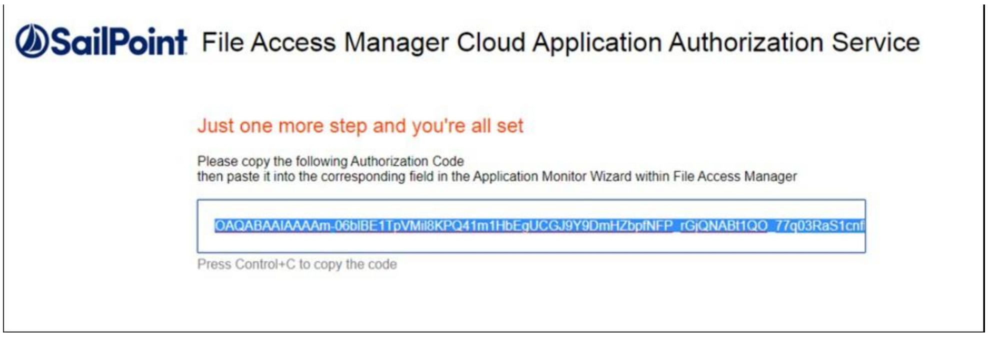
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

## 4. MS O365 Application Consent Screen

A final redirect will lead you to the File Access Manager Cloud Application Authorization Service, and will present the received Authorization Code

- Copy that code and past it in the Auth Code field in the Identity Collector Configuration Wizard screen
- Click next and complete the Identity Collector configuration flow.



SailPoint File Access Manager Cloud Application Authorization Service

Just one more step and you're all set

Please copy the following Authorization Code
then paste it into the corresponding field in the Application Monitor Wizard within File Access Manager

OAQABAAIAAAAm-06bIBE1TpVMil8KPQ41m1HbEqUCGJ9Y9DmHZbpfNFP_rGjQNABt1QO_77q03RaS1cnf

Press Control+C to copy the code

# Prerequisites

## Permissions

The File Access Manager Azure AD Connector Requires the following permissions:

- Directory.Read.All – This Permission grants **read only** access to AAD contents (by default, all domain users can read all AAD data)

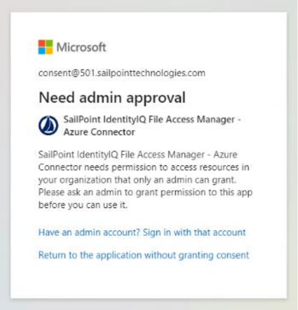
## Administrator's Consent Requirements

To grant a third-party application (ISV) with the Directory.Read.All permission requires an administrator consent, which can be given by users with one of the following roles:

- Global Administrator (Company Administrator).
- Application Administrator.
- Cloud Application Administrator.

Hence, during the ***initial configuration*** phase (while generating the token for the first time), the service account dedicated to the File Access Manager Azure AD Connector, must have one of the above-mentioned roles.
Once consent is given, the role can be removed from the user.

The Consent flow will appear different for users with different roles.
Non-admin user trying to access the consent screen will be presented with the following screen:



Microsoft

consent@501.sailpointtechnologies.com

Need admin approval

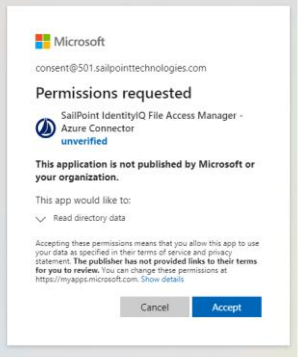
SailPoint IdentityIQ File Access Manager - Azure Connector

SailPoint IdentityIQ File Access Manager - Azure Connector needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account

Return to the application without granting consent

Application Administrators trying to access the consent screen, will be presented with a request to consent and grant the File Access Manager Application the Read Directory Data permissions:



Microsoft

consent@501.sailpointtechnologies.com

Permissions requested

SailPoint IdentityIQ File Access Manager - Azure Connector
unverified

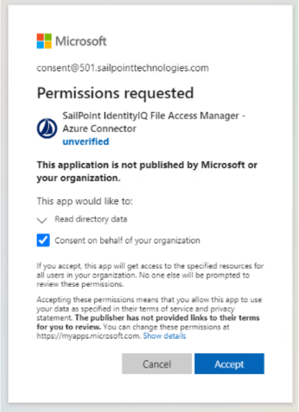
**This application is not published by Microsoft or your organization.**

This app would like to:

Read directory data

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Users with the Global Administrator role trying to give consent to an application will be presented with a screen containing an additional checkbox (Consent on behalf of your organization):



Microsoft

consent@501.sailpointtechnologies.com

Permissions requested

SailPoint IdentityIQ File Access Manager - Azure Connector
unverified

**This application is not published by Microsoft or your organization.**

This app would like to:

- Read directory data

☑ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

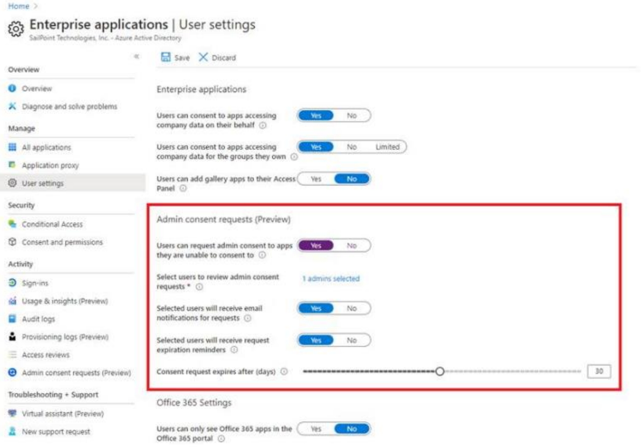
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

This extra checkbox consents to give permissions to the application on behalf of all other users in the organization, thereby ensuring no other user would have to explicitly give consent to the app to run on its behalf.
File Access Manager does not require this checkbox to be checked, as our application only needs to run on behalf of the consenting user.
Checking this option is optional, and not mandatory.

## Avoiding the Administrative Roles Grant

To avoid granting an administrative role the service account, even if only for the duration of the consent sequence, you may use Azure's "Admin Consent Requests". This relatively new feature lets non-admin users indirectly give consent to application that require admin consent by requesting an admin's authorization.

This feature can be enabled on the tenant's level, and allows setting one of the three above-mentioned administrator roles as a reviewer:



Home >
Enterprise applications | User settings
SailPoint Technologies, Inc. - Azure Active Directory
Save
Discard
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Consent and permissions
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Admin consent requests (Preview)
Troubleshooting + Support
Virtual assistant (Preview)
New support request

Enterprise applications

Users can consent to apps accessing company data on their behalf: [✓ Yes] No

Users can consent to apps accessing company data for the groups they own: [✓ Yes] No Limited

Users can add gallery apps to their Access Panel: Yes [✓ No]

Admin consent requests (Preview)

Users can request admin consent to apps they are unable to consent to: [✓ Yes] No

Select users to review admin consent requests *: 1 admins selected

Selected users will receive email notifications for requests: [✓ Yes] No

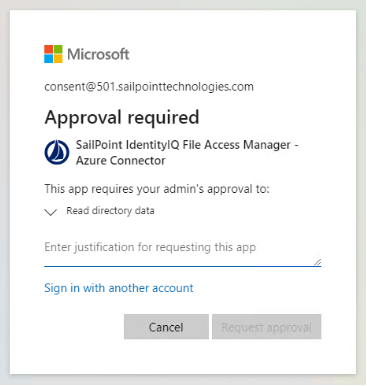
Selected users will receive request expiration reminders: [✓ Yes] No

Consent request expires after (days): 30

Office 365 Settings

Users can only see Office 365 apps in the Office 365 portal: Yes [✓ No]

When users without one of these administrative roles go through the normal consent flow, they will be presented with the screen:



Microsoft

consent@501.sailpointtechnologies.com

Approval required

SailPoint IdentityIQ File Access Manager - Azure Connector

This app requires your admin's approval to:

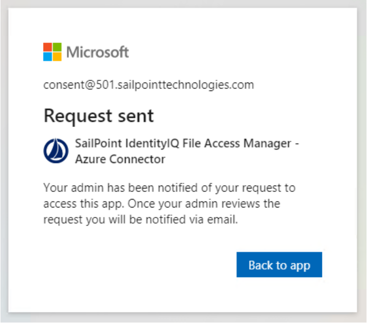
- Read directory data

Enter justification for requesting this app

Sign in with another account

The requested is required to provide a justification for granting consent to the application and a request is sent to the administrator listed in the configuration as reviewers.

When clicking on "Request approval" to continue, the following screen appears:



consent@501.sailpointtechnologies.com

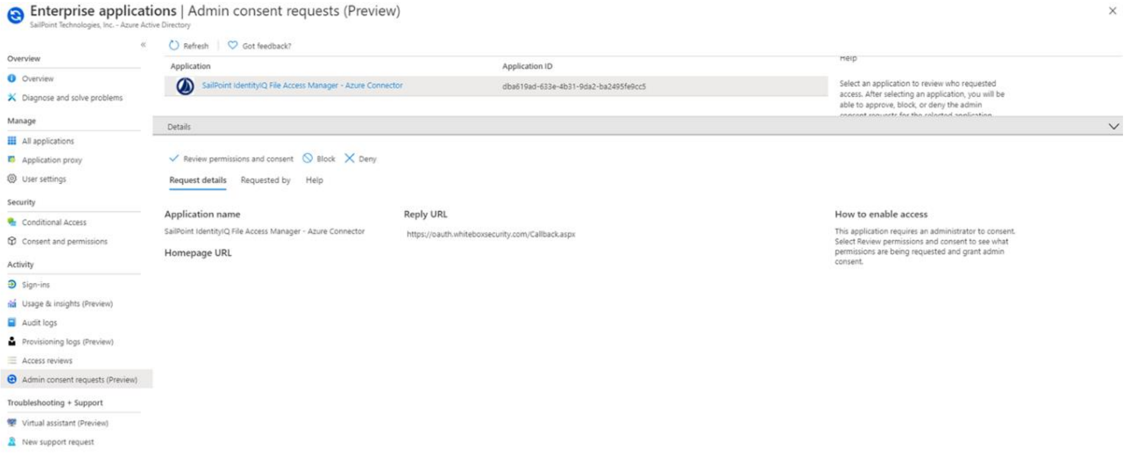
Request sent

SailPoint IdentityIQ File Access Manager - Azure Connector

Your admin has been notified of your request to access this app. Once your admin reviews the request you will be notified via email.

Clicking on "Back to app" would just return an "access denied" error as access was not yet granted.
This screen can be safely closed while waiting for admin consent.

The reviewing administrator will either receive an email notifying them of the request, or have to go to the "Admin Consent Requests" screen and check for new requests:


Enterprise applications | Admin consent requests (Preview)
SailPoint Technologies, Inc. - Azure Active Directory
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Consent and permissions
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Admin consent requests (Preview)
Troubleshooting + Support
Virtual assistant (Preview)
New support request
Refresh
Got feedback?
Help
Details
Review permissions and consent
Block
Deny
Request details
Requested by
Help

| Application | Application ID |
|---|---|
| SailPoint IdentityIQ File Access Manager - Azure Connector | dba619ad-633e-4b31-9da2-ba2495fe9cc5 |

Select an application to review who requested access. After selecting an application, you will be able to approve, block, or deny the admin consent requests for the selected application.

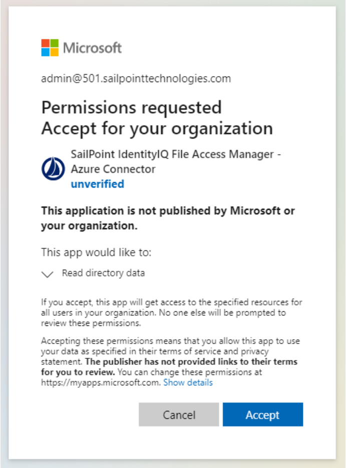
Application name
SailPoint IdentityIQ File Access Manager - Azure Connector

Reply URL
https://oauth.whiteboxsecurity.com/Callback.aspx

Homepage URL

How to enable access
This application requires an administrator to consent. Select Review permissions and consent to see what permissions are being requested and grant admin consent.

To approve a request, the administrator will go through the "Review permissions and consent" flow, where they will be presented with the familiar consent screen:



admin@501.sailpointtechnologies.com

Permissions requested
Accept for your organization

SailPoint IdentityIQ File Access Manager - Azure Connector
unverified

**This application is not published by Microsoft or your organization.**

This app would like to:

Read directory data

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

After an administrator "Accepts", non-administrator users can will have to go the through token generation sequence again. However, this time the consent screen will be skipped entirely, and the flow will lead directly to the Authorization code.

**Note:** This method gives consent to the app on behalf of the entire organization, similar to when a Global Administrator ticks the checkbox to enables the Consent on behalf of your organization, as described above.

# Appendix C: Exchange Online Connector Full OAuth 2.0 Support

## Description

File Access Manager now offers full support of standard OAuth 2.0 Authentication for the Exchange Online connector. The new authorization sequence will direct the user through a standard Microsoft O365 authentication flow, to grant the File Access Manager service account the privilege to acquire and refresh access tokens.

The new authentication method replaces the previous Basic Authentication flow, that required admins to provide user and password credentials.

- The Exchange Online Connector now uses only fully modern authentication methods, and does not require Legacy Authentication methods be enabled, tenant-wide, or otherwise.
- The Exchange Online Connector now supports the use of multiple service accounts, for both the Permission Collection and Activity Monitoring modules, to utilize larger API access quotas and minimize delays caused by Microsoft O365 Rest APIs quotas, throttling and back-off algorithms.
- The Exchange Online Connector supports any user as a delegated account, including users with Multi-Factor Authentication requirements enabled, and is no longer limited by Microsoft's restrictions on Federated Accounts
- The Exchange Online Connector supports internal token management and will be responsible for managing and renewing its own tokens.

### General Description

This enhancement brings full OAuth support to the Exchange Online Connector, instead of the legacy user and password approach.

File Access Manager uses the Microsoft official ADAL library to generate and refresh OAuth tokens.

- Configuring the Exchange Online Connector, instead of providing a user name and a password, you will click on the plus sing (+) next to the relevant token manager component, to generate a new OAuth Access Token.
- You will then be redirected to a standard Microsoft O365 login screen.
- Enter the relevant service account credentials and login.
- The Microsoft ADAL library will then initiate a PKCE Authorization Code Flow to generate the initial OAuth token, that will then be encrypted and stored as part of the Exchange Online application configuration.
- The access token will be used in all requests to the tenant’s O365 Exchange environment and will be automatically refreshed when needed.
- Multiple service accounts can be used to generate tokens for both the Permission Collection and Activity Monitoring modules.
- The same service accounts can be used for both modules; however, this is not recommended as the service account API call quota would be shared across the two modules, which will increase the likelihood of exceeding the API call quota and encountering throttling issues.
- **Note!** This enhancement requires multiple manual steps that must be followed carefully. This enhancement will also require you to reconfigure the Exchange Online Connector, go through the configuration wizard to generate access tokens and switch over to modern authentication flow.
- This will not recreate the application, and current Exchange Online information will remain intact.

# Deployment Instructions

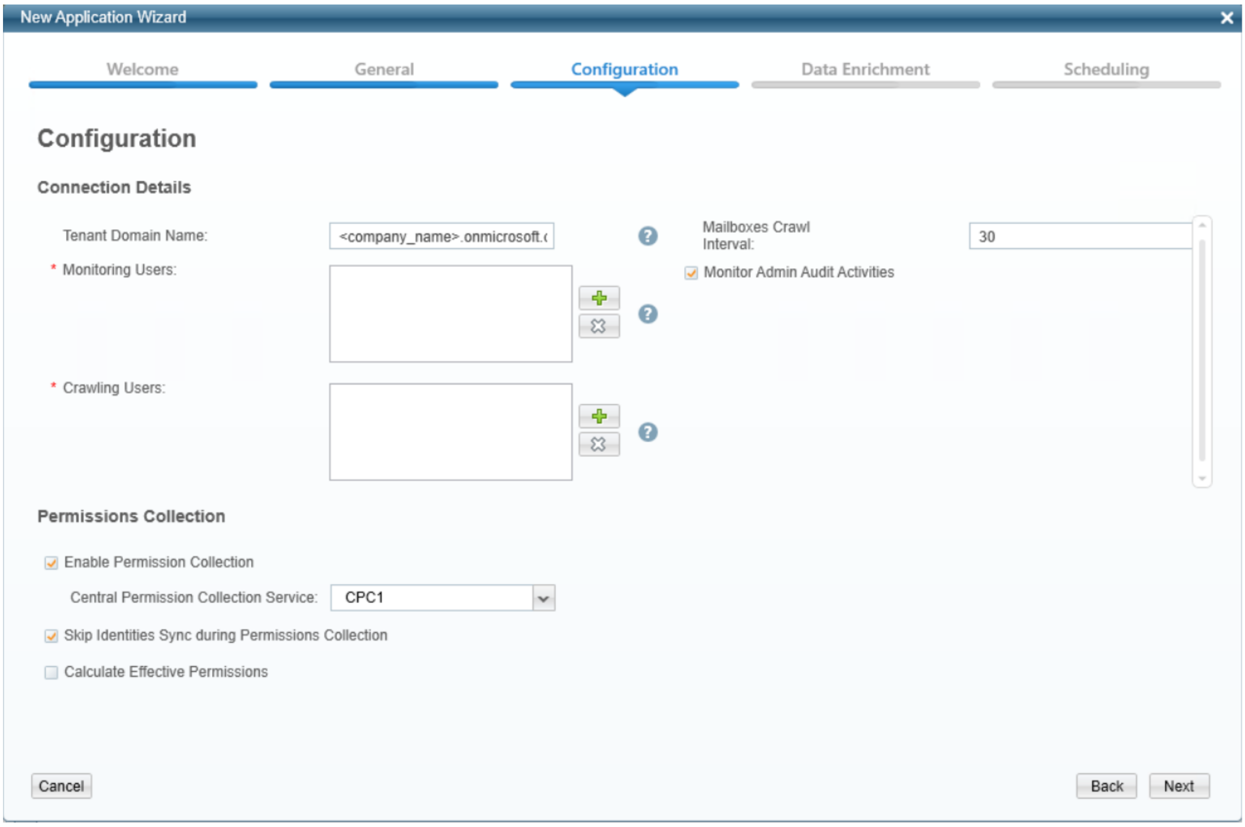
**Important!** Without completing this step, the Exchange Online Connector will not function properly.

1. Open the Administrative Client, edit your Exchange Online Application and follow the wizard to completion.
2. The main “Configuration” screen has undergone some modifications.
   Make sure to fill in the “Tenant Domain Name” field and use the Add and Remove buttons of the Token Management component to add and remove tokens.
3. **Optional:** Run a Crawl and Permission Collection tasks and make sure the tasks complete successfully.
4. **Optional:** Ensure the Exchange Online Activity Monitor is running and that events are displayed in the Activity Forensics screen on the File Access Manager Business Website.

# Configuration Steps (Screenshots)

## 1. The Exchange Online Application Configuration Screen

In the New/Edit Application Wizard enter your O365 Tenant Domain name, then use the “Add Token” button of the Token Management Component - marked by the green Plus sign (“+”) – to login using the File Access Manager service account and generate OAuth Tokens



Configuration

Connection Details

Tenant Domain Name: <company_name>.onmicrosoft.(

Mailboxes Crawl Interval: 30

☑ Monitor Admin Audit Activities

* Monitoring Users:

* Crawling Users:

Permissions Collection

☑ Enable Permission Collection

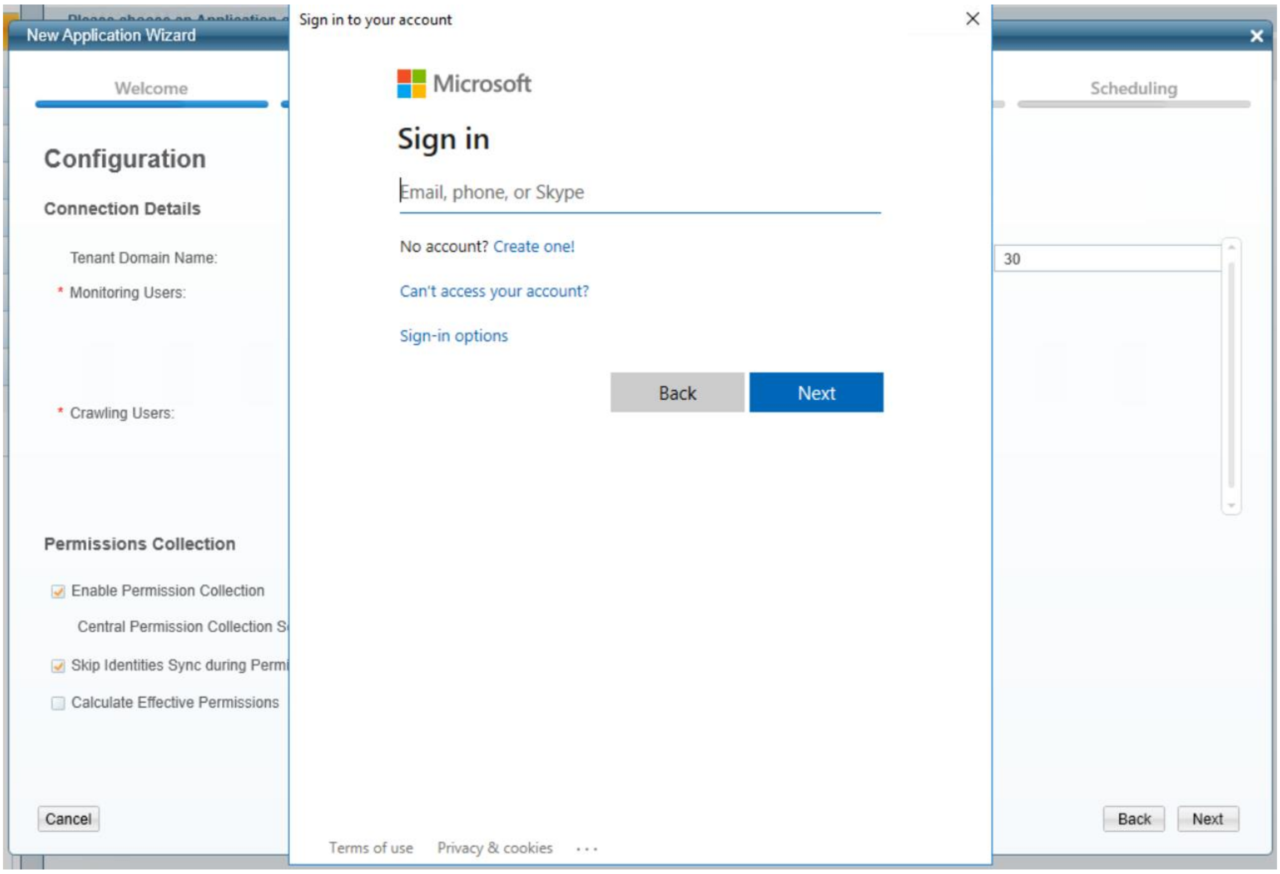
Central Permission Collection Service: CPC1

☑ Skip Identities Sync during Permissions Collection

□ Calculate Effective Permissions

## 2. MS O365 Login Screen

You will then be redirected to the Microsoft O365 Login Screen.
Login with the Service Account that should be used by the Exchange Online Connector.



Sign in to your account

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

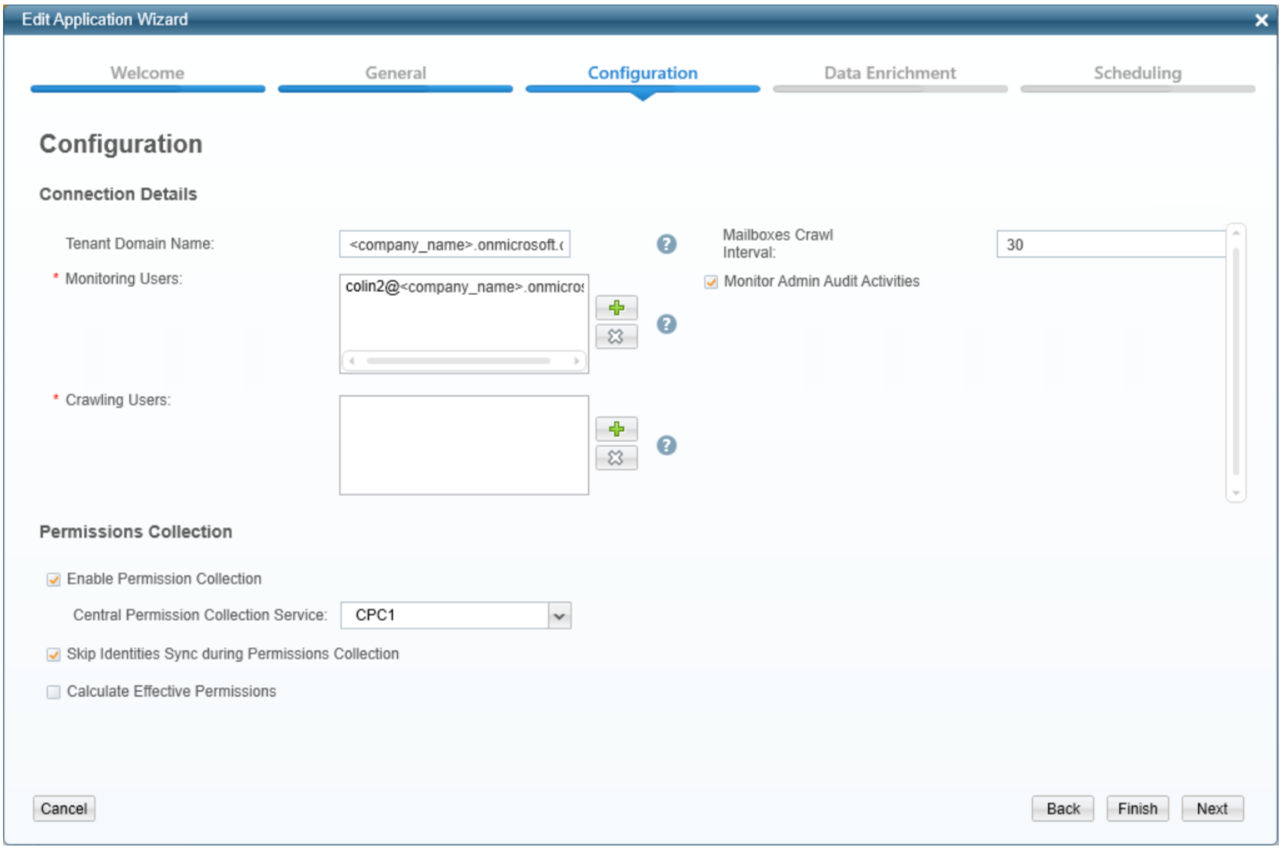
Sign-in options

## 3. The Token Management Component

Upon a successful login of the Service Account, an OAuth Access Token for the Service Account will be generated, encrypted and added to the Exchange Online Application Configuration.

Although the Service Account name is presented in the Token Management Component, credentials are not persisted as part of the Application Configuration. File Access Manager persists the OAuth tokens exclusively.

The Service Account is extracted dynamically from the generated token, solely for display purposes.



Configuration

Connection Details

Tenant Domain Name: <company_name>.onmicrosoft.(

* Monitoring Users: colin2@<company_name>.onmicros

* Crawling Users:

Mailboxes Crawl Interval: 30

☑ Monitor Admin Audit Activities

Permissions Collection

☑ Enable Permission Collection

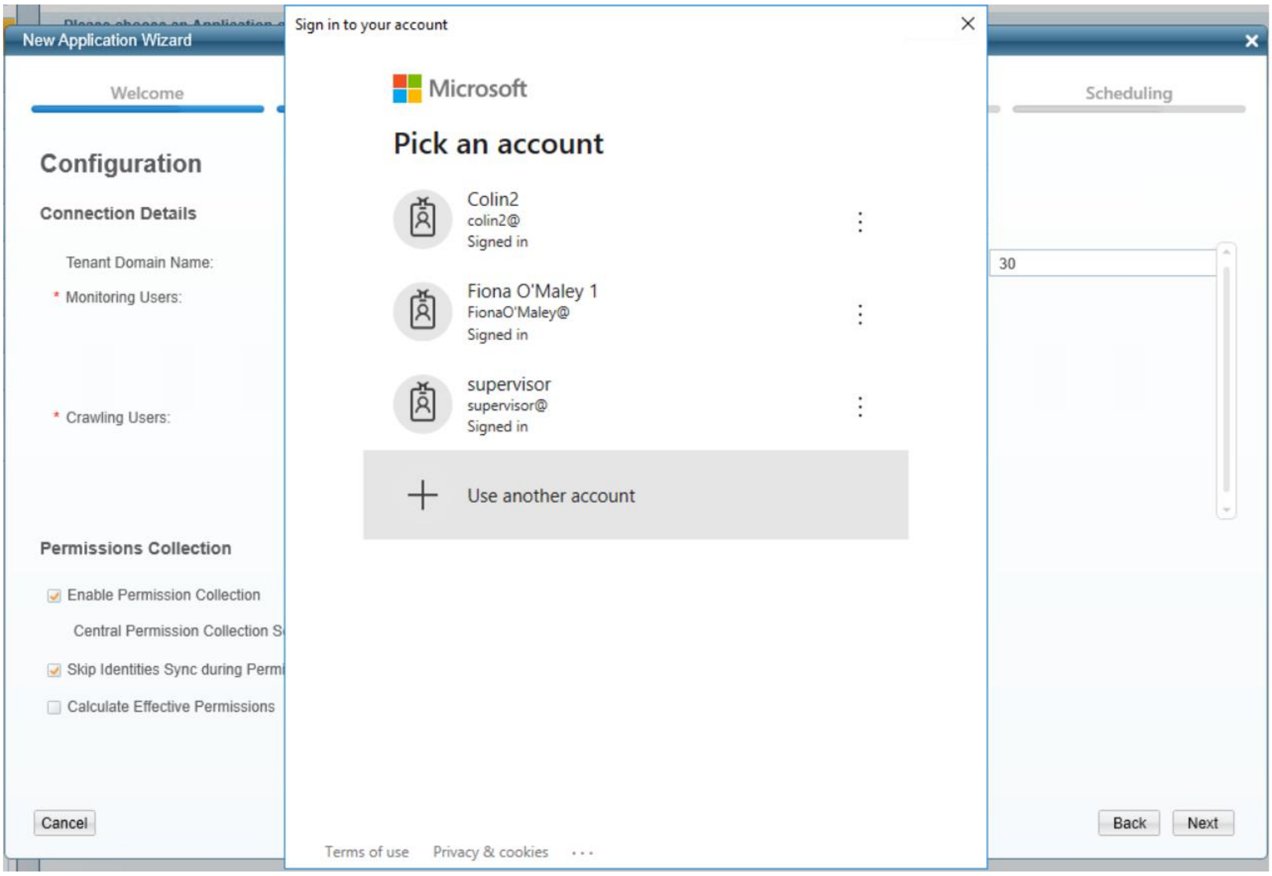
Central Permission Collection Service: CPC1

☑ Skip Identities Sync during Permissions Collection

□ Calculate Effective Permissions

## 4. Multiple Service Account Support

Use the “Add” and “Remove” buttons of the Token Management Component to manage the service accounts to be used by the Permission Collection and Activity Monitoring modules of the Exchange Online Connector. Multiple Service Accounts can be added as desired – to increase API call capacity and avoid throttling issues. Multiple service accounts can be used to generate tokens for both the Permission Collection and Activity Monitoring modules.
The same service accounts can be used for both modules; however, this is not recommended as the service account API call quota would be shared across the two modules, which will increase the likelihood of exceeding the API call quota and encountering throttling issues.



New Application Wizard

Configuration

Connection Details

Tenant Domain Name:

* Monitoring Users:

* Crawling Users:

Permissions Collection

☑ Enable Permission Collection

Central Permission Collection S

☑ Skip Identities Sync during Permi

☐ Calculate Effective Permissions

30

Sign in to your account

Microsoft

Pick an account

Colin2
colin2@
Signed in

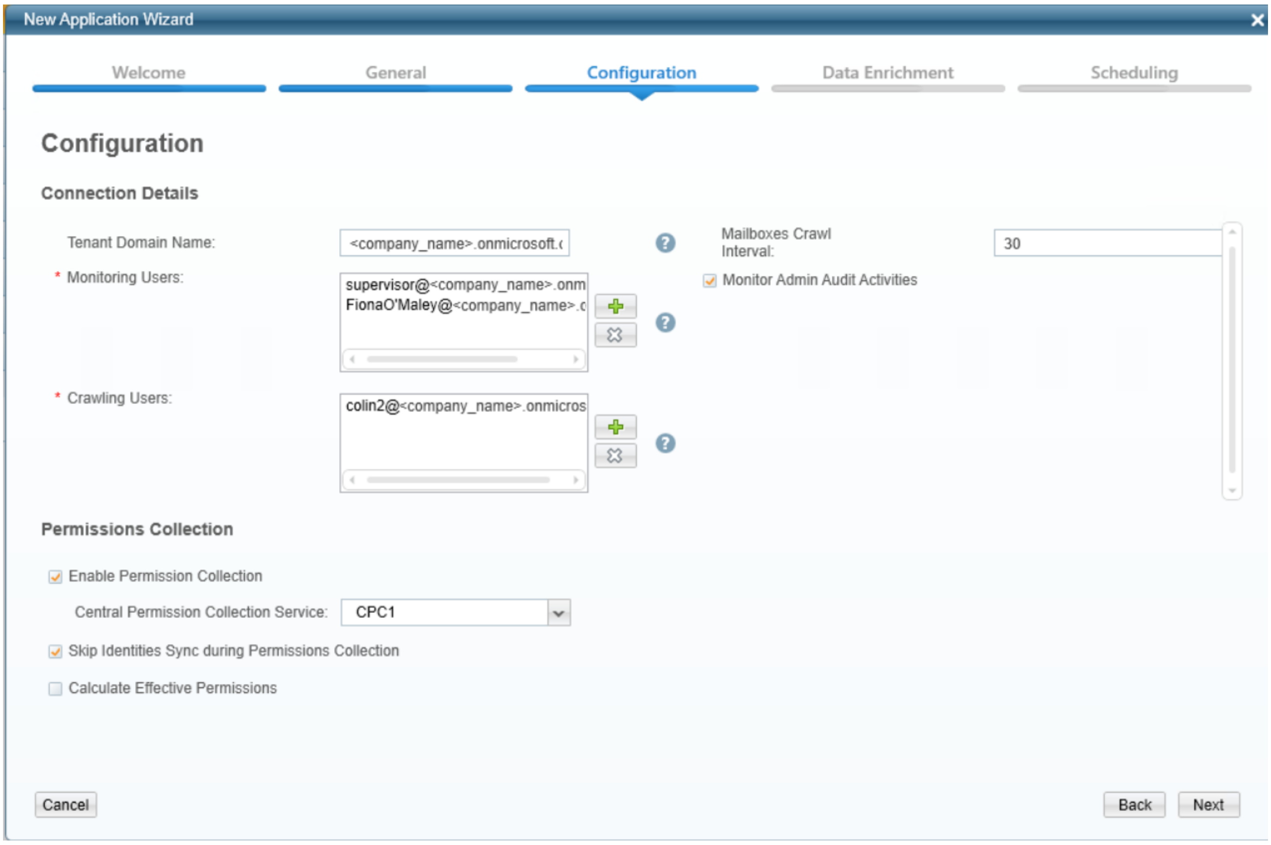
Fiona O'Maley 1
FionaO'Maley@
Signed in

supervisor
supervisor@
Signed in

+ Use another account

## 5. Complete the Configuration

Once you’ve added all the service accounts to the configuration, a list of all associated account will appear in the Token Management Components.
Follow the wizard instruction to complete the configuration.



Configuration

Connection Details

Tenant Domain Name: <company_name>.onmicrosoft.c

* Monitoring Users: supervisor@<company_name>.onm
FionaO'Maley@<company_name>.c

* Crawling Users: colin2@<company_name>.onmicros

Mailboxes Crawl Interval: 30

☑ Monitor Admin Audit Activities

Permissions Collection

☑ Enable Permission Collection

Central Permission Collection Service: CPC1

☑ Skip Identities Sync during Permissions Collection

□ Calculate Effective Permissions