



SailPoint IdentityIQ

Version: 8.2.0.4000

File Access Manager v8.2 Service Pack 4 Deployment Guide



Copyright ©2022 SailPoint Technologies, Inc., All Rights Reserved.

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.

Restricted Rights Legend.

All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

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. Government's Specially Designated Nationals (SDN) List; 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.

Copyright and Trademark Notices.

Copyright ©2022 SailPoint Technologies, Inc. All Rights Reserved. All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet web site are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint Technologies & Design," "SailPoint," "IdentityIQ," "IdentityNow," "SecurityIQ," "IdentityAI," "AccessIQ," "File Access Manager," "Identity Cube" and "Managing the Business of Identity" are registered trademarks of SailPoint Technologies, Inc. "Identity is Everything" and "The Power of Identity" are trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

Table of Contents

Table of Contents

Table of Contents	3
Chapter 1: Planning Your Service Pack Deployment.....	1
What is a Service Pack?	1
Service Packs Deployment Process.....	1
Version Numbers	1
Backup Measures.....	3
Chapter 2: Support Matrix	4
Support Matrix.....	4
Chapter 3: Deploying Version 8.2 Service Pack 4.....	5
Pre-upgrade Steps	5
Service Pack Deployment	6
Post Upgrade Actions	8
Chapter 4: Important Information and Updates	10
Chapter 5: Troubleshooting	10
Chapter 6: List of Released E-Fixes	13
Service Pack 4	13
Service Pack 3	14
Service Pack 2	17
Service Pack 1	19

List of Figures

Figure 1 Application Monitors Screen.....	1
Figure 2: Upgrades & Patches table.....	6
Figure 3: Expand Service Pack package - Details	7
Figure 4: Review Service Pack package - Details.....	7
Figure 5: Retry installation line	8
Figure 4: Message - Update File Access Manager Client	8

Chapter 1: Planning Your Service Pack Deployment

What is a Service Pack?

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

Service Packs Deployment Process

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

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

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

Version Numbers

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

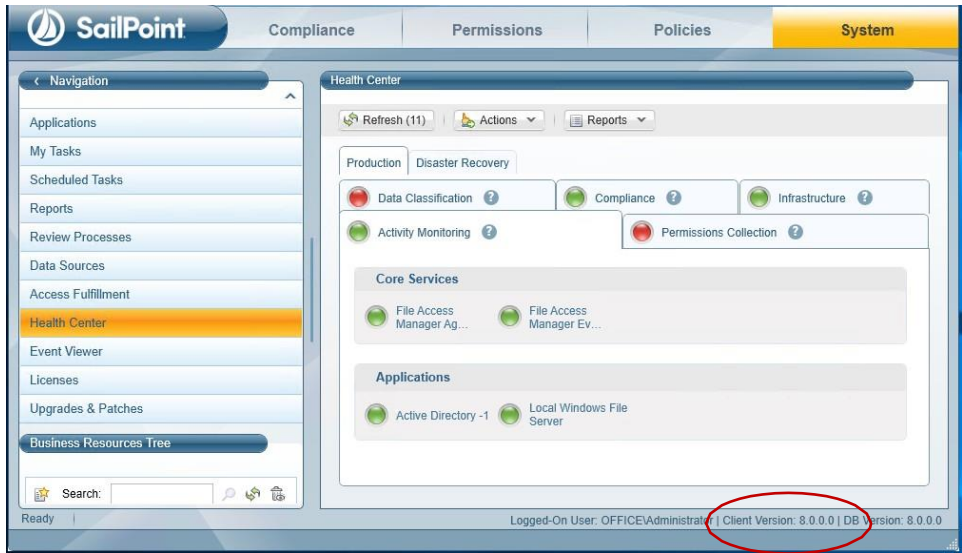


Figure 1 Application Monitors Screen



File Access Manager version numbers are represented by a four-section number, e.g., 8.2.0.4000. The first two sections represent major releases. File Access Manager 8 GA release number is 8.0.0.0. whereas, File Access Manager 8.2 release will be represented by the number 8.2.0.0. The next section represents Patch Releases, e.g., File Access Manager 8.0P1 version number is 8.0.1.0. Service Pack updates are reflected in the last section, and so File Access Manager 8.2 Service Pack 4 version number is 8.2.0.4000. The Database version number will be updated with every service pack. For File Access Manager 8.2 Service Pack 4, the database version number is 8.2.0.4000. The Client version number will be updated if the service pack includes changes to the Administrative Client. For File Access Manager 8.2 Service Pack 4, the database version number is 8.2.0.4000.

Infrastructure components, such as Elasticsearch and RabbitMQ will retain the same version number, unless an update to the actual infrastructure components is applied, in which case their version number will be updated as well. 8.2 Service Pack 4 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	8.2.0.4000
File Access Manager Elasticsearch	5.1.1
File Access Manager RabbitMQ	3.7.4
File Access Manager API	8.2.0.4000
File Access Manager Web Client	8.2.0.4000
File Access Manager Administrative Client	8.2.0.4000
File Access Manager Data Classification	8.2.0.4000
File Access Manager Permission Collection	8.2.0.4000
File Access Manager Activity Analytics	8.2.0.4000
File Access Manager Agent Configuration Manager	8.2.0.4000
File Access Manager Collector Synchronizer	8.2.0.4000
File Access Manager Crowd Analyzer	8.2.0.4000
File Access Manager Event Manager	8.2.0.4000
File Access Manager Reporting Service	8.2.0.4000
File Access Manager Scheduled Task Handler	8.2.0.4000
File Access Manager User Interface	8.2.0.4000
File Access Manager Watchdog	8.2.0.4000
File Access Manager Workflow Service	8.2.0.4000
File Access Manager Activity Monitor Connectors	8.2.0.4000

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 SP3 the Backup folder would be {%FILE_ACCESS_MANAGER_HOME%\Backup\8.2.0.4000

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 8.2 Service Pack 4

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

Log4J Vulnerability

Critical vulnerabilities in the log4j library used in the Elasticsearch component of File Access Manager were announced and are being tracked by CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, and CVE-2021-45105. Announcement can be found here: [Compass FAM Blog: File Access Manager log4j Remote Code Execution and Denial of Service Vulnerabilities](#)

SailPoint has reproduced these vulnerabilities and determined that File Access Manager is susceptible to remote code execution and denial of service vulnerabilities because of them.

These vulnerabilities can and should be immediately mitigated by updating the log4j library in the Elasticsearch instance that is part of the File Access Manager deployment to version 2.17.1 as documented in the content for the CVEs referenced above. An e-fix containing updated libraries and a README with installation instructions is included in the Service Pack deployment folder. The ElasticSearchLog4J.ps1 PowerShell script will remediate the vulnerabilities by replacing the vulnerable .jar files with libraries which do not contain the vulnerability.

Steps to apply the PowerShell script are as follows:

1. Login to the Elasticsearch server
2. Extract Log4jPatch.zip to your folder of choice
3. Open PowerShell as administrator
4. Navigate to the folder you extracted the log4j.zip
5. Run the following command `.\ElasticSearchLog4J.ps1`

Please note if you have already applied this fix manually there is no need to run this script; however there is no negative effect if you choose to do so anyway.

Please note:

- Tool needs to be run on the server hosting the elastic search service.
- SAILPOINT_HOME environment variable needs to correctly set to the 'SailPoint' folder containing the 'elasticsearch-5.1.1' folder.

LiteDB Change Considerations (ONLY needed if upgrading from 8.2)

This section is only necessary if upgrading from 8.2 directly to 8.2 SP3. If you have already applied 8.2 SP1 or 8.2 SP2 this section can be skipped as these changes should have already been made.

Changes in Service Pack 1 required a change in LiteDB version. As Service Packs are cumulative these considerations should be taken into account if upgrading directly from 8.2.

In making this change any old LiteDB files become problematic when restarting a service. These files are located in the Activity Analytics and Event Manager services. More details are located in the Post Upgrade Actions section of this guide.

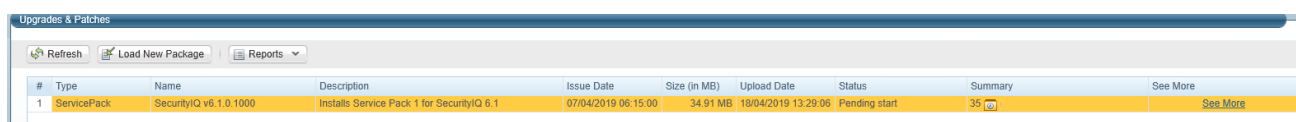
Post upgrade steps include deleting these old liteDB files which has the potential to include enriched events (activities) which have not yet been sent to Elasticsearch/SQL, which would incur potential event loss. These are *not* raw events which that can be resent through the Event Manager, but events which have already been processed. To have minimal impact, we recommend – in order:

- stopping all Activity Monitors services allowing the Event Manager(s) to finish processing events
 - To verify the Event Manager has finished processing events, locate the EventManager-Statistics.log (located in the SailPoint\Logs folder) and wait for the following queues to display 0.
 - Event Collector's events in memory waiting to be processed: 0
 - Elasticsearch Sending Queue contains 0 bulks (0 events)
 - (Optional if you store events to the DB) SQL Sending Queue contains 0 bulks (0 events)
- stopping the Event Manger service(s)
- deleting the .db files located in the Event Manager directory (note you may or may not have all files – you only need to delete what exists)
 - BulkWriter SQL_SqlData_Cache.db
 - BulkWriter Elastic_ElasticData_Cache.db
 - DCCache.db
- starting the Service Pack upgrade

As turning off the activity monitors will also incur not collecting events while service is stopped, we recommend running these steps in off-peak business hours to minimize losses.

Service Pack Deployment

1. Extract the “File Access Manager v8.2.0.4000.zip” installation package.
2. Navigate to the “Service Pack 4” folder.
3. Log into the IdentityIQ File Access Manager administrative client 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 v8.2 Service Pack 4.wbxml**” 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	19/04/2019 13:29:06	Pending start	35	See More

Figure 2: Upgrades & Patches table

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

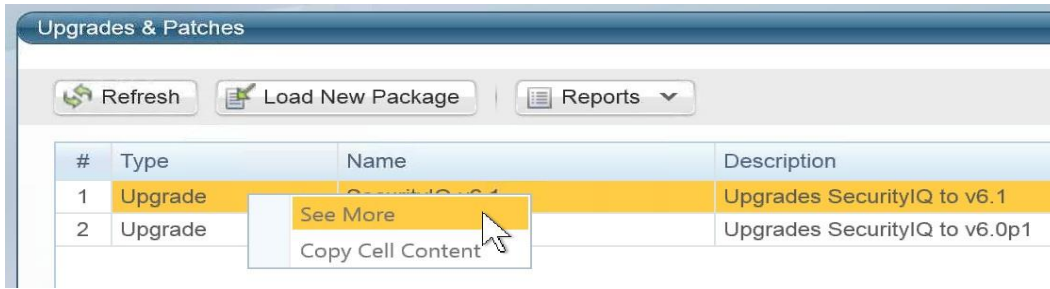


Figure 3: Expand Service Pack package - Details

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

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

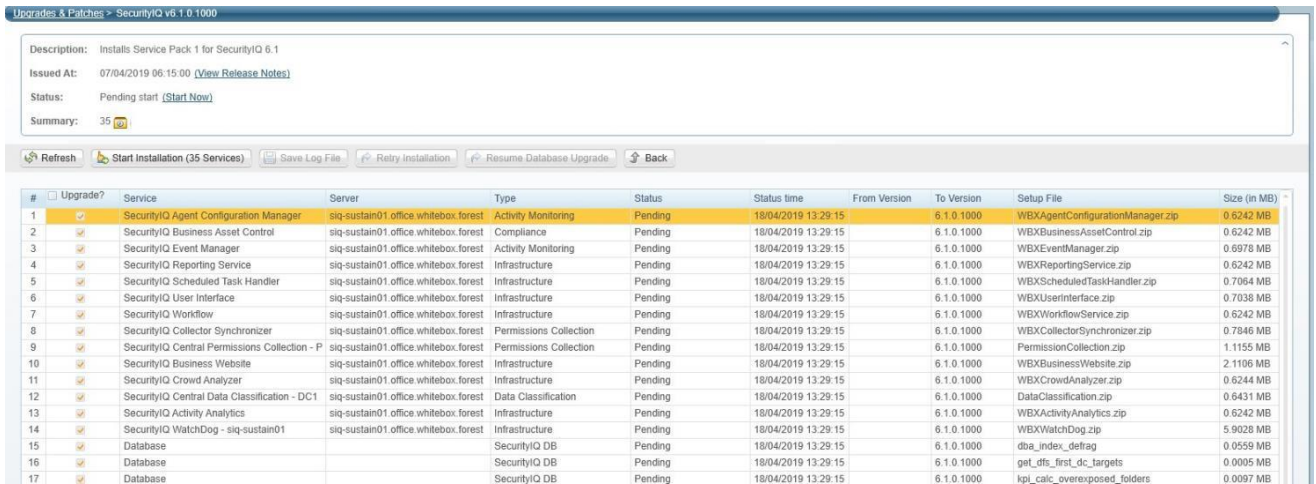


Figure 4: Review Service Pack package - Details

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

The Service Pack deployment process runs a series of prerequisites checks before the Database update begins. Then proceeds to perform the Database updates.

Following the Database updates, the first component to be updated will be the Watchdog Service, installed on the server hosting the User Interface core service.

Following that, all other components will be updated.

What if an update line fails?

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

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

#	<input type="checkbox"/> Upgrade?	Service	Server	Type
1	<input type="checkbox"/>	Database		Data Update
2	<input checked="" type="checkbox"/>	SecurityIQ Agent Configuration		Activity Monitoring
3	<input checked="" type="checkbox"/>	Database		SecurityIQ DB
4	<input checked="" type="checkbox"/>	Database		SecurityIQ DB
5	<input checked="" type="checkbox"/>	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

Delete *.db files (upgrade from 8.2 only)

If you have not yet deleted the .db files complete the following. If you already have, you can skip this section.

After the components have been upgraded for this service pack, perform the following steps for the Activity Analytics and each Event Manager service instance:

1. Stop the service.
2. Navigate to the service folder in a File Explorer window.
3. Sort the files by type until you can view all file types that end in **.db**.
4. Delete these files.
5. Restart the service.

IdentityIQ File Access Manager Client Upgrade

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

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

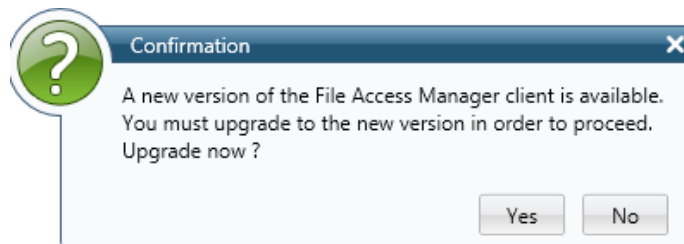


Figure 4: Message - Update File Access Manager Client



Validate the Service Pack update

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

The versions of the IdentityIQ File Access Manager components should be set to 8.2.0.4000

The IdentityIQ File Access Manager Database version should be set to 8.2.0.4000

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

Chapter 4: Important Information and Updates

SIQDEV-20473 – Website v1 JS XSS vulnerability fix

During internal testing, we've discovered a Cross-Site Scripting (XSS) vulnerability in the AngularJS component of our web application. This vulnerability can be leveraged by attackers to inject and execute HTML/JS code within the context of our web application, through certain fields. This issue is address in 8.3 SP3, 8.2 SP4 and all subsequent releases and services packs, including the upcoming 8.4.

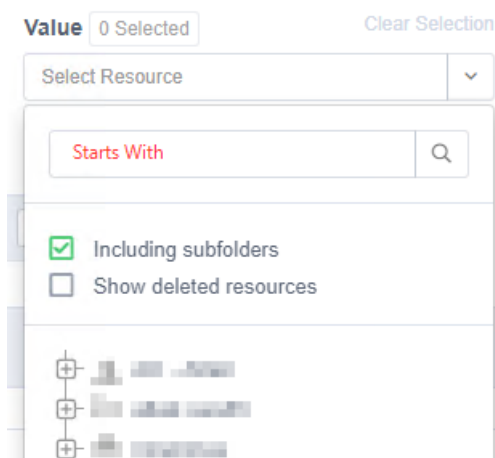
CVSS Vector scoring 6.0 (Medium)

SIQSUS-709 – Event Manager File Category Cache to use SQLite

The Event Manager now uses SQLite as the local cache replacing LiteDB. Enhancements to the design with respect to the synchronization of data to minimize event processing blockages and lower memory usage due to event queue backup as well as improving overall performance. See SQLite Event Manager File Category Cache – Performance Test Results documentation for more details located <https://community.sailpoint.com/t5/File-Access-Manager-Documents/SQLite-Event-Manager-File-Category-Cache-Performance-Test/ta-p/229048>.

SIQENT-3176 – Resource filter adjust to starts with instead of contains

To improve query response time performance without a significant increase in the size of the database, the resource field filter will now be limited to 'Starts With' searches.



SIQSUS-702 – SailPoint Rebranding



We have recently updated our branding which is now reflected in both the Admin Client and business website. Changes have not been made to other areas of the product (like reporting). This will be implemented with the next major release.

If, after the upgrade is complete, the updated branding is not displayed please clear your browser cache, relaunch the browser and sign back in - the new branding should now be visible.

SIQSUS-705 – Microsoft Changes to GCC URL Impact to O365 Applications

Starting Sept. 15th, 2022 Microsoft will restrict Government Community Cloud (GCC) accounts access to the Microsoft 365 Management Activity API endpoints through Enterprise Management API URL. For those account, Microsoft will enforce data collection using the Microsoft 365 Management Activity API through designated Government Community Cloud (GCC) URLs. You can find details regarding this change here: <https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-apis-overview> Also communicated in announcements MC221116, MC223431 & MC395212.

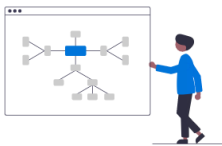
Please find more details here: [File Access Manager Blog: Update Notice for O365 Government Cloud Users](#)

There is now a new field for SharePoint Online and One Drive application configuration screens. This will allow you to select your plan type. On upgrade, it will default to Enterprise and will **not** delete any current authorization codes configured. If you have a GCC plan, you will need to edit your current application configuration to select the GCC from the Office365 Plan dropdown. Upon selecting the new plan type the codes will automatically be deleted which will allow for new codes to be entered.

If you are on an Enterprise plan reconfiguration of these applications is not necessary.

Connection Details - SharePoint Online

Enter the connection details. For further information refer to the connector installation guide or the application vendor.



Tenant Name
Enter a valid Tenant Name / Domain Name in order to display a link to the authorization code page

Tenant Name

Office365 Plan
Enterprise

SharePoint Online Authorization Code

SharePoint Online Admin Authorization Code

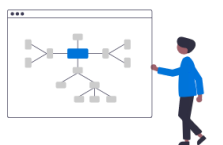
SharePoint Online My Authorization Code

Management Authorization Code

Analyze Permissions on Files

Connection Details - OneDrive for Business

Enter the connection details. For further information refer to the connector installation guide or the application vendor.



Tenant Domain Name
Enter a valid Tenant Name / Domain Name in order to display a link to the authorization code page

Office365 Plan
Enterprise

OneDrive Authorization Page
[Click this link to get the OneDrive Authorization Code](#)

OneDrive Authorization Code
Enter Authorization Code from the Authorization Page

O365 Management Authorization Page
[Click this link to get the O365 Management Authorization Code](#)

O365 Management Authorization Code
Enter Authorization Code from the Authorization Page

SIQETN-3104 – Implement Dynamic Memory Utilization for Data Classification

We have worked to improve how our data classification task runs. We now check and adjust memory usage while running to prevent out of memory exceptions. This optimization will override any manual configuration changes applied (such as changes to the `maxLuceneQueueSizeBytes`, `contentExtractionThreadsCount` set in the Data Classification Configuration and `Indexer_MaxThreads` located in the `DC_Parameters` table). These optimizations also include service level fault protection during text extraction.

Please note server resources may have high usage while data classification tasks are running.

SIQETN-3025 – Adjust Data Classification Forensics Report to Allow for more than 10K Results

Previously there was a hard coded limit of 10,000 results for Data Classification reports. This has been changed to match other reports which has the Excel limitation of 1 Million rows.

Please note this value was initially set to 10K to maintain performance; therefore if utilizing larger values please be aware the report may take significantly longer to generate based on the size of the report.

SIQETN-3075 – Deleted DEC Information in Forensic Search Parameters

Based on customer feedback, we adjusted forensics to no longer display deleted DEC information. However, we realize this may not be desired by all customers (as there may be a need to search older activities with this information). Therefore we added a configuration key to revert if desired.

To revert, update `<add key="includeDeletedTriggers" value="False" />` in the `<appSettings>` section of the `SiqApi.dll.config` file

By default this is set to “True” (to no display deleted application parameters)

SIQETN-3080 – IdentityIQ DEC Timeout

Timeout for IIQ DEC was too long blocking events while waiting for a response. This timeout was reduced and made configurable. A new key "IIQTimeoutSeconds" was added to the Event Manager configuration to allow for further adjustment if needed. The values unit of measure is in seconds.

Update `<add key="IIQTimeoutSeconds" value="{as desired}" />` to the file `EventManagerServiceHost.dll.config` in the `<appSettings>` section.

SIQETN-2976 – Adjusting Custom Fulfillment to Allow Cloud Based Apps

Allow cloud applications to use custom fulfillment.

Impersonation will be enabled by default for custom fulfillment. To control whether impersonation is used when running custom fulfillment scripts, add the following key to the file `CollectorSynchronizerServiceHost.dll.config` in the `<appSettings>` section with the appropriate value:

`<add key="shouldImpersonate" value="true" />`

SIQETN-3026 – Overhaul of Data Classification Policy Corrections

1. Spelling/verbiage use of terms based completely on WHO ICD-10 policy. Refer to [ICD-10 Version:2019](#)
2. Based on ICD-S+T split, if user has created user-defined ICD-T policy, customer will need to rename/delete in favor of new OOTB ICD-T policy.

SIQETN-3076 –Data Classification Policy Updates

EU Phone Number policy rule has been split into separate rules per country for GDPR policy so it will be possible to disable specific country phone number rules.

SIQETN-3055 – Support Proxy Server

Support environment variables `ALL_PROXY` to configure proxy address, and `NO_PROXY` to configure address and domains to exclude from being proxied (comma-separated list).

SIQETN-3006 – Server installer requires default web site in IIS

Allow IIS site to override from "Default Web Site" during server installation.

Follow the instructions in the contained README in the service pack sub-folder "SIQETN-3006".

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  Tools  Internet Information Service (IIS) manager).
6. Select the Application Pools node.
7. Verify that the IdentityIqFamV1_ApplicationPool, IdentityIqFamV2_ApplicationPool and SiqApi_ApplicationPool are missing from the Application Pools node.
8. Create the new application pools, (naming them IdentityIqFamV1_ApplicationPool, IdentityIqFamV2_ApplicationPool and SiqApi_ApplicationPool), with the following parameters: .Net CLR Version: .Net CLR Version v4.0.30319 Managed pipeline mode: Integrated
9. Check the “**Start application pool immediately**” checkbox.
10. For each application pool, navigate to Advance Settings (Right-click  **Advanced Settings**)
11. Under Process Model, set the “**Identity**” parameter to **LocalSystem**.
12. Under Recycling set the “**Regular Time Interval (minutes)**” to **720**.
13. From the Site panel (on the left), navigate to **IdentityIQFAM**, and click on it.
14. Click “**Basic Settings**” on the right. If this option is not available, right click **IdentityIQFAM** (on the left) and select “Convert to Application”.
15. On the newly opened screen, click **Select**, select the IdentityIqFamV1_ApplicationPool you created earlier, and click **OK** twice.
16. Double click “**Authentication**”.
17. Enable “Windows Authentication” and disable all other authentication methods.
18. Repeat Steps 11-15 for the SiqApi site and SiqApi_ApplicationPool.
19. Reset the IIS using the iisreset command.

Business Website

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

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

Suggested solution:

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

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 4

SIQETN-3068 – Unable to delete campaigns referencing deleted applications

Corrected inability to delete or modify campaigns configured with a 'by application' permission filter after the application reference is deleted.

SIQETN-3155 – Netapp Failure Enumerating shares

For Netapps with hundreds of top level shares, corrected failure in ability to enumerate through those shares.

SIQETN-3156 – Primary Key Constraint in Database Cleanup task

Corrected uniqueness in index defrag stored procedure

SIQETN-3160 – KPI Resource calculation Error

Corrected issue of not being able to convert data type

SIQETN-3167 – Adjust media type return for integration between IIQ and FAM mismatched versions

Adjusted media type return to allow for integration of FAM and IIQ regardless of the version each product is on.

SIQETN-3168 – Primary Key Constraint error in Event Manager Bulk Writer

Corrected primary key constraint issue in Event Manager

SIQETN-3169 – Data Classification task Hanging if OCR enabled

Corrected when for certain image files when OCR scope is enabled the data classification task would hang.

SIQETN-3176 – Adjust Resource filter query from contains to starts with

See Chapter 4: Important Information and Updates

SIQETN-3179 – Box fails Retry on Throttling Error during Permission Collection



Corrected to properly retry if we receive throttling error during Box Permission Collection

SIQETN-3180 – Password ReEncryption Task Can Fail If IC configured by properties

Corrected constant key Trusted Domains

SIQETN-3181 – newtonsoft.json referencing incorrect version

Corrected newtonsoft.json version

SIQETN-3182 – EMC Isilon AM High Memory Usage

Corrected potential for High Memory usage for Isilon Activity Monitoring

SIQETN-3186 – DR services not activating after Production shutdown

Handle PROD server not reachable via discovery method. Change ES URL reference.

SIQETN-3189 – Improve Efficiency of Dashboard Widget Calc task

Adjusted stored procedure to improve efficiency while running

SIQETN-3191 – EXO AM not switching to individual mailbox queries

Corrected internal recovery mechanism was inadvertently disabled when app-only authentication was introduced

SIQETN-3193 – Improve Efficiency of Dashboard Widget Calc task (#2)

Adjusted stored procedure to improve efficiency while running

SIQSUS-709 – EM File Category Replication Store to use SQLite

See Chapter 4: Important Information and Updates

SIQDEV-20473 – Website v1 JS XSS vulnerability fix

See Chapter 4: Important Information and Updates

Service Pack 3

SIQETN-2996 – Activity Reporting in Resource Screen is Inaccurate for SPO

Corrected activity count for Resource and Activity Forensic screen for SharePoint Online.

SIQETN-3009 – Resource Tree Returns Resources with similar names

Adjusted filter to only display relevant information

SIQETN-3040 – Default SMTP SPO template does not pickup all template variables

Corrected to properly include variables in SMTP response

SIQETN-3105 – Normalization Failing on Large Groups

Added refresh cache to allow for groups larger than 1500 members

SIQETN-3109 – Adjust Box Crawl to Pick Up Unique Permissions

Box permission collection relies on data cached from crawl. Always run crawl task before permission collection for best results.

Made following changes to Box Crawl:

- fix bug relating to partial "calculation of resources' size" regardless of setting
- fix bug relating to setting: Analyze "shared link" permissions on files. It could interfere with analyzing folders.
- fix bug relating to setting: Analyze "collaborators" permissions on files. It could interfere with analyzing folders.

SIQETN-3117 – Permissions Marked Stale

Fixed forensics permissions view by "group & user direct permissions" option to align unused calculation with other view by options.

SIQETN-3127 – Policy Object For ABA Routing misspelled

Corrected spelling

SIQETN-3128 – DC Failing from Duplicate Resource

Addressed duplicate resources by using distinction upon fetching

SIQETN-3129 – Deleted BRs displaying in Resource / Data screen

Add where clause to remove delete users from being displayed

SIQETN-3134 – Activity resource name incorrect for Active Directory

Corrected name of resource in resource screens for Active Directory

SIQETN-3140 – Syslog sending emplate with Alert

Corrected to no longer include template when sending syslog alerts.

SIQETN-3141 – Response save is not updating syslog messaging

Updated response cache to check for message or severity changes.

SIQETN-3141 – reportStatistics can cause crawl crash with unhandled exception

Added try-catch to prevent service crash

SIQETN-3145 – Unused permission logic error

Correct logic error in Forensic page for unused permission calculation

SIQETN-3149 – Users with Special Characters Fail Normalization

Escape characters residing in groups

SIQETN-3150 – ResourceTypes endpoint missing scim part of Route

Corrected api path to include necessary path part

SIQETN-3151 – OCR Matches Do Not Return with Protected Extraction Enables

Corrected so OCR will trigger when Protected Extraction is enabled

SIQETN-3152 – Null Reference Exception in DEBUG

Allowed owner value to be null

SIQETN-3153 – Missing DC Categories in Events

Properly deserialize property from LiteDB

SIQETN-3154 – Retrieve data from DB for campaign report

Added missing report columns back to campaign report

SIQETN-3163 – Missing DC Category Under certain conditions

Corrected missing categories for mixed case files.

Service Pack 2

SIQDEV-17271 – Loading Failed in User Permission Paths

Fixed loading failed error for User Permission Paths.

SIQETN-2752 – Crawler Duplicate Key Errors

Crawl would fail when encountering duplicate resources, adjusted for better handling of duplicates.

SIQETN-2791 – Unexpected characters in user input field cause 500 Error

Corrected the double quote meta-character causing internal server errors when present in the Forensic search filter

SIQETN-2959 – Alert Email Not Sent to Data Owner

Corrected alert emails to be properly sent to designated data owners.

SIQETN-3025 – Adjust DC Forensic Report to Allow for more than 10K Results

Expanded Data Classification reporting to generate with over 10K results.

SIQETN-3042 – Data Owner Unable to Revoke Access when using DFS Solution

Enabled approval bypass for DFS Owner.

SIQETN-3053 – Sandbox Text Extraction Process

Implemented service level fault protection during text extraction.

SIQETN-3075 – Forensic Search Parameters Not Deleted with Associated Application

Fixed no longer displaying deleted DEC information after DEC has been deleted. See Chapter 4: Important Information and Updates for more information

SIQETN-3080 – IIQ DEC Timeout Too Long

Adjusted timeout in IIQ DEC to avoid event blockage. See Chapter 4: Important Information and Updates for more information

SIQETN-3084 – Support NoLanguage mode when querying EXCH On prem

Exchange changed its PowerShell connection from FullLanguage to NoLanguage mode which resulted in issues when connecting with the current Exchange Activity Monitor. Fixed connection.

SIQETN-3085 – EM DC Results Sync Fixes and Enhancements

Performance enhancements related to data classification results synchronization and improved logging.

SIQETN-3087 – IIQ Unable to Correlate classifications from FAM Classification Task

Added back Uniquelntentifier field and adjusted naming conventions to be consistent between versions.

SIQETN-3089 – Exception crashes service

In rare cases, exception can be thrown during Permission Collection causing task to fail and service to crash. Ensured crash would not occur if exception was hit.

SIQETN-3091 – TimeStamp can causes Box Activity Monitoring To Stop Receiving Activity

Events stream cursor would not advance if chunk of results had same time stamp. Made changes to use different position variable.

SIQETN-3092 – Database deadlock Error Fails Permission Collection

Deadlock during a stored procedure in permission collection would cause permission collection task to fail. Changed to wrap in lock.

SIQETN-3093 – Dox DC authorize token not refreshing

Fixed Box data classification authorization errors that may occur when initial authorization token expires

SIQETN-3096 – Exch On Prem Crawl Not Recovering After Error for Statistics

Some PowerShell sessions were not recovering after folder statistics call. Changed to more resilient calls.

SIQETN-3099 – NetApp AM in StandBy When Using HA

Adjusted HA Netapp Activity Monitors to always be in a wake state enforcing Active/Active vs Active/Passive mode.

SIQETN-3103 – Behavioral Data Classification performance

Improved behavioral data classification task performance

SIQETN-3104 – Implement Dynamic Memory Utilization for Data Classification

See Chapter 4: Important Information and Updates

SIQETN-3112 – ‘index.htm’ should be changed to ‘#’ in website URL

Corrected url

SIQETN-3113 – Deleted User can be selected as Data Owners

Deleted users appear in the Data Owner selection, and these deleted users can be assigned/saved as data owners. Corrected to not display deleted users.

SIQETN-3114 – Password is not Masked in AUDIT_LOG table

Changes in 8.2 displayed certain plaintext passwords in audit log table (only visible directly in database, not visible anywhere else in FAM). Updated APIs to hide in body parameter stored in database and delete any existing plaintext password.

SIQETN-3115 – View Missing Columns

Forensics page failing to load when querying DFS resource, fixed view.

SIQETN-3116 – GRPC Server-side components have default limit

Adjusted GRPC communication to no longer have size limit.

SIQETN-3121 – DB Script Needs to be compatible with SQL Server 2012

Changes made to SQL script for SIQETN-2752 needed to be adjusted to also be compatible with SQL Server 2012

SIQETN-3122 – Lock update_ra_roles_br_permissions while inserting

Add locking to not allow querying existing roles and inserting new roles.

Service Pack 1

SIQETN-2754 – Box Activity Monitoring Improved De-Duplication Mechanism

Box Activity Monitoring would display duplicate activity, improved to remove duplicates before reporting.

SIQETN-2885 – Box Activity Monitoring API Call Improvements

Enhancement to code that queries for new Box Events to use a single reader thread and using API cursors where possible so that API calls are more efficient, less likely to be throttled by Box and more reliable.

SIQETN-2952 – Discard rules improperly read regex from database

Fix case where regular expression pipe character is converted to comma in browser.

SIQETN-2958 – Error while Revoking Direct Permission on a DFS resource

Fix bug preventing revocation of permission on a DFS resource.

SIQETN-2964 – Requesting access same as a colleague for a DFS Resource

DFS access request fix same as colleague not displaying any users.

SIQETN-2976 – Adjusting Custom Fulfillment to Allow Cloud Based Apps

Allow cloud applications to use custom fulfillment.

SIQETN- 2985 – Access request approvals to DFS data owners not sent

Add support for DFS data owner approval for access requests.

SIQETN-2978– SharePoint Online Memory Optimization

Optimizations to SharePoint Online caching, client connectivity, and object usage during a Permission Collection task to reduce overall memory usage.

SIQETN- 2988 – SPO Campaigns return no records when using an identities filter based on local groups

Campaigns using a filter on 'group entity type' with a value of 'local group' will now return results.

SIQETN-2991 – Azure Identity Collection Failure When Duplicate User Parsed

Fix bug where duplicate user is not detected during Azure identity collection.

SIQETN- 2993 – SharePoint On-Prem/Online Crawl Performance is Slow When Scope is Restricted

Improve performance during Sharepoint crawl tasks when crawl scope inclusions, exclusions, or scope regex is defined.

SIQETN-3082– Crawler Inclusion/Exclusion Scope Fix from Web UI

Fix path separator issue for SharePoint Online type paths when set in Web UI interface.

SIQETN-2995 – Duplicate File Property Name Causes Data Classification To Fail to Process File

Fix bug where duplicate file meta-data key causes indexing error.

SIQETN- 2997 – Box Crawler fails due to non-escaped character single quote

Sanitize Box cached data when saving to DB during crawl.

SIQETN- 3001 – Active Directory Activity Monitor Slow Performance When Processing Well Known SIDs

Cache failed SID lookups when processing AD events to improve performance.

SIQETN-3006 – Server installer requires default web site in IIS

Allow IIS site to override from "Default Web Site" during server installation.

SIQETN-3010 – Search User Exit and Syslog Response types

Fix bug where User Exit and Syslog response types are not searchable when defining Discard or Alert Rules.

SIQETN- 3013 – Event Manager reduce locking while syncing data

Optimize event manager data synchronization.

SIQETN- 3014 –API Paths Missing SCIM part of route

Fix bug where SCIM part of API path was missing for FAM API endpoints.

SIQETN-3016 – Reports Task Hangs in 'Reports Pending Send'

Fix report generation hanging in 'Reports Pending Send' status.

SIQETN-3018 – Dashboard KPI resources calculation widgets failed

Added IS NOT NULL statement to filter out NULL role_bam_ids.

SIQETN-3019 – Box Identity Collector Not Utilizing Latest Token

Ensure up-to-date access token is used for all Box API calls when synchronizing identities.

SIQETN-3024 – Allow for Event Manager to Optionally Save to DB

This enhancement supports the ability to turn off/on whether SQL event backups are made, and also whether they are cleaned up during event deletion.

Two new system configuration options are now supported in the DB table system_configuration_value: "Store event backups to SQL Server" and "Remove SQL backups on event deletion"

SIQETN-3025 – Adjust DC Forensic Report to Allow for more than 10K Results

Data Classification Reports now support over 10K results. The configuration value supporting this limit is now "Maximum Forensics Reports Page Results" in the system_configuration_table.

SIQETN-3026 – Overhaul of Data Classification Policy Corrections

Updates to ICD policies: Spelling/verbiage use of terms based completely on WHO ICD-10 policy. Refer to [ICD-10 Version:2019](#). Based on ICD-S+T split, if user has created user-defined ICD-T policy, customer will need to rename/delete in favor of new OOTB ICD-T policy.

SIQETN-3076 –Data Classification Policy Updates

EU Phone Number policy rule has been split into separate rules per country for GDPR policy so it will be possible to disable specific country phone number rules. Also includes fix for Canadian SIN policy object and enhancement for Financial IBAN rule.

SIQETN-3032 – Data Classification Import Result Fails When Task Scheduler on DEBUG

Bug fixes for Data Classification import.

SIQETN-3034 – Loading Failed Permission Forensics when Unable to Find BR ID

Fix bug where non-existent business resource lookup causes error in browser.

SIQETN-3035 Allow only the 'wbxadmin' to login to the website in SAML

When configured for SAML authentication, allow special WBXAdmin user to login through website.

SIQETN-3036 – Active Directory Identity Collection can fail if domain connectivity is unstable

Surround Identity Collection Active Directory queries with a retry mechanism.

SIQETN-3041 – Slow Performance Calling SCIM API DataClassificationResults

Optimize the SQL query for data classification results when using SCIM API.

SIQETN-3044 – Box Does Not Check Retry-After when Throttled/Box Scaling Limit Reached

Added waits if received 429 or 503 responses prior to and after calls to Box. Also handle Box internal scaling limit error response so that first 3000 groups are returned.

SIQETN-3050 – Exchange Online activity case insensitive app name comparison

Fix error when processing activity caused by FAM Exchange Online Azure authentication application where tenant name case does not match event case.

SIQETN-3055 – Support Proxy Server

Support environment variables ALL_PROXY to configure proxy address, and NO_PROXY to configure address and domains to exclude from being proxied (comma-separated list).

SIQETN-3058 – Skip bad Data Classification batches in Event Manager when syncing

Fix for event manager to support data classification results of any size.

SIQETN-3072 – SharePoint Online API Query Limit

Fix to support SharePoint Online API change

SIQETN-3073 – Warn log level

Fix when setting NLog log level to WARN.

SIQETN-3079 – Fix IsAdOnlyDataOwner calculation on login

Fix bug where SQL is incorrectly generated, causing delay during login.

Additional logging in SiqApi service when logging in fails for a user

Additional logging to assist in diagnosing problems during Web UI login.