SailPoint IdentityIQ

Version: 8.2.0.1000

File Access Manager v8.2 Service Pack 1 Deployment Guide

Copyright ©2019 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 ©**2019** 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
List of Tables ..... **Error! Bookmark not defined.**
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
Deploying Version 8.2 Service Pack 1 ..... ***5***
Pre-upgrade Steps 5
Service Pack Deployment 5
Post Upgrade Actions 7
Chapter 4: ***Important Information and Updates*** ***9***
Chapter 5: ***Troubleshooting*** ***10***
Chapter 6: ***List of Released E-Fixes*** ***13***
Service Pack 1 13

List of Figures

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

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.

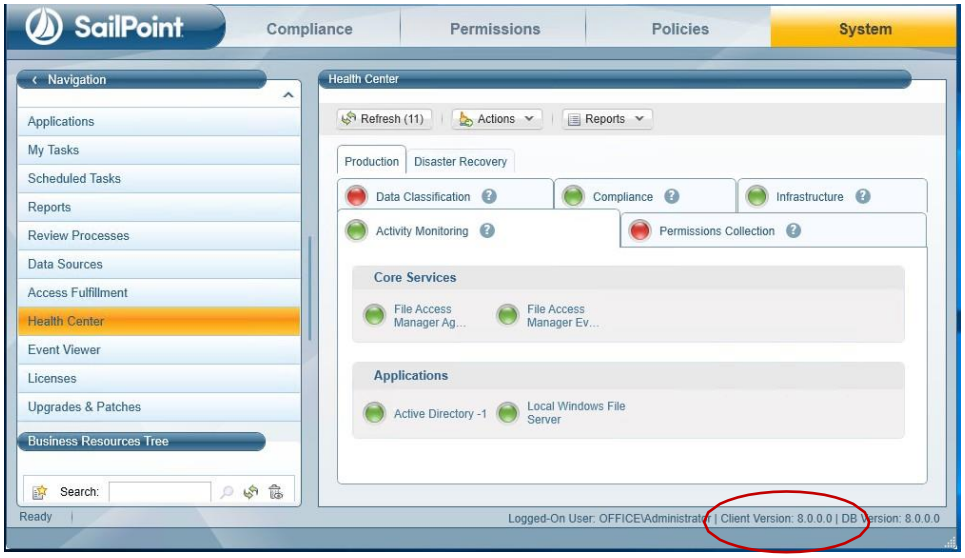


Figure 1 Application Monitors Screen

File Access Manager version numbers are represented by a four-section number, e.g., 8.2.0.1000.
The first two sections represent major releases. File Access Manager 8 GA release number is 8.0.0.0. whereas, File Access Manager 8.2 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 1 version number is 8.2.0.1000.
The Database version number will be updated with every service pack. For File Access Manager 8.2 Service Pack 1, the database version number is 8.2.0.1000.
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 1, the database version number is 8.2.0.1000.

Infrastructure components, such as Elasticsearch and RabbitMQ will retain the same version number, unless an update to the actual infrastructure components is applied, in which case their version number will be updated as well. 8.2 Service Pack 1 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	8.2.0.1000
File Access Manager Elasticsearch	5.1.1
File Access Manager RabbitMQ	3.7.4
File Access Manager API	8.2.0.1000
File Access Manager Web Client	8.2.0.1000
File Access Manager Administrative Client	8.2.0.1000
File Access Manager Data Classification	8.2.0.1000
File Access Manager Permission Collection	8.2.0.1000
File Access Manager Activity Analytics	8.2.0.1000
File Access Manager Agent Configuration Manager	8.2.0.1000
File Access Manager Collector Synchronizer	8.2.0.1000
File Access Manager Crowd Analyzer	8.2.0.1000
File Access Manager Event Manager	8.2.0.1000
File Access Manager Reporting Service	8.2.0.1000
File Access Manager Scheduled Task Handler	8.2.0.1000
File Access Manager User Interface	8.2.0.1000
File Access Manager Watchdog	8.2.0.1000
File Access Manager Workflow Service	8.2.0.1000
File Access Manager Activity Monitor Connectors	8.2.0.1000

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 SP1 the Backup folder would be {%FILE_ACCESS_MANAGER_HOME%}\Backup\8.2.0.1000

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 1

The deployment process consists of the following steps:

1. Downloading the Service Pack from this Compass Location
2. Read the Service Pack deployment guide thoroughly
3. Pre-deployment Steps
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

None for 8.2 SP1.

Service Pack Deployment

1. Extract the "File Access Manager v8.2.0.1000.zip" installation package.
2. Navigate to the "Service Pack 1" 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 1.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.

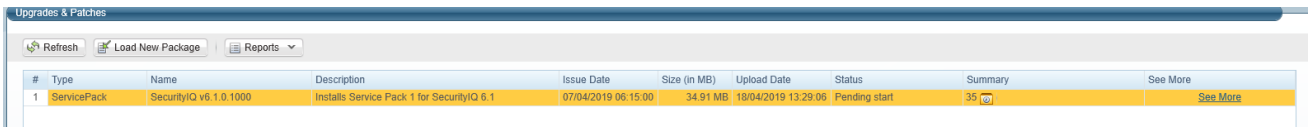


Figure 2: Upgrades & Patches table

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

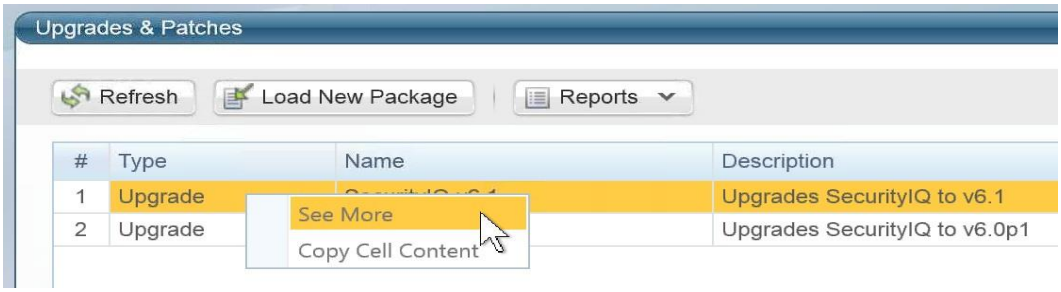
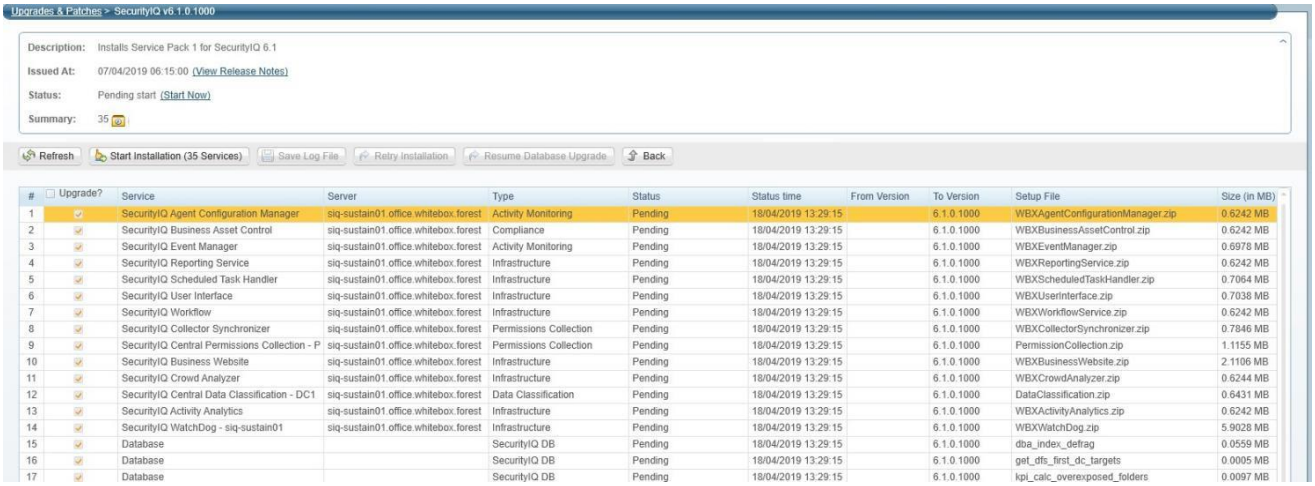


Figure 3: Expand Service Pack package - Details

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.



#	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.

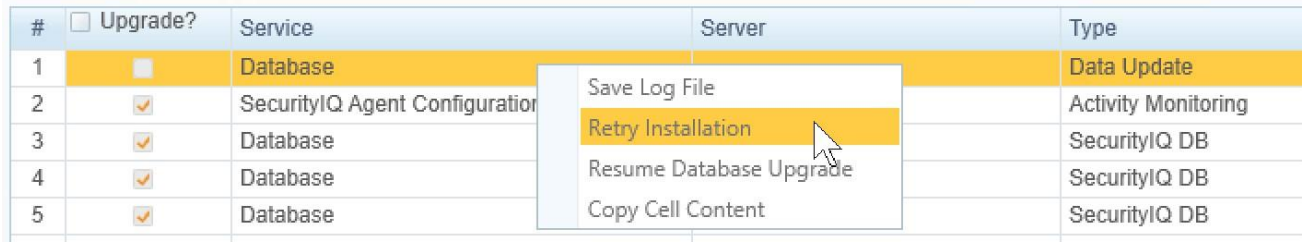


Figure 5: Retry installation line

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 from Activity Analytics and Event Manager service folders

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.

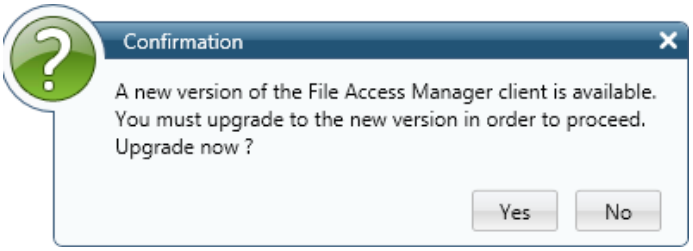


Figure 4: Message - Update File Access Manager Client

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 8.2.0.1000
The IdentityIQ File Access Manager Database version should be set to 8.2.0.1000

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

Chapter 4: Important Information and Updates

SIQETN-3024 – Allow Event Manager to Optionally Save to DB, Delete Event Backups

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"

The current behavior and default configuration (or if the values are missing from the Database) is True for both values. Events will be stored to elastic and backups of those events will also be saved to SQL. And when events are deleted, the corresponding SQL event backups will also be deleted.

If "Store event backups to SQL Server" is set to False, the event manager(s) will save events to Elastic only; backups to SQL will not be made.

If "Remove SQL backups on event deletion" is set to False, event deletion tasks will only delete events from Elastic; any existing SQL event backups will be retained. Any existing SQL event backups that are skipped from being deleted in this way will not be delete-able from FAM using deletion tasks, even if "Remove SQL backups on event deletion" is reset to True. When setting "Remove SQL backups on event deletion" to False, the user is responsible for the lifetime and ultimate deletion of those skipped events.

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.

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 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.