SailPoint IdentityIQ

Version: 8.4.0.1000

File Access Manager v8.4 Service Pack 1 Deployment Guide

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.

“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 8.4 Service Pack 1 .... ***5***

Pre-upgrade Steps 5

Service Pack Deployment 5

Post Upgrade Actions 7

Chapter 4: Important Information and Updates ***8***

Chapter 5: Troubleshooting ***10***

Chapter 6: List of Released E-Fixes ***14***

Service Pack 1 14

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

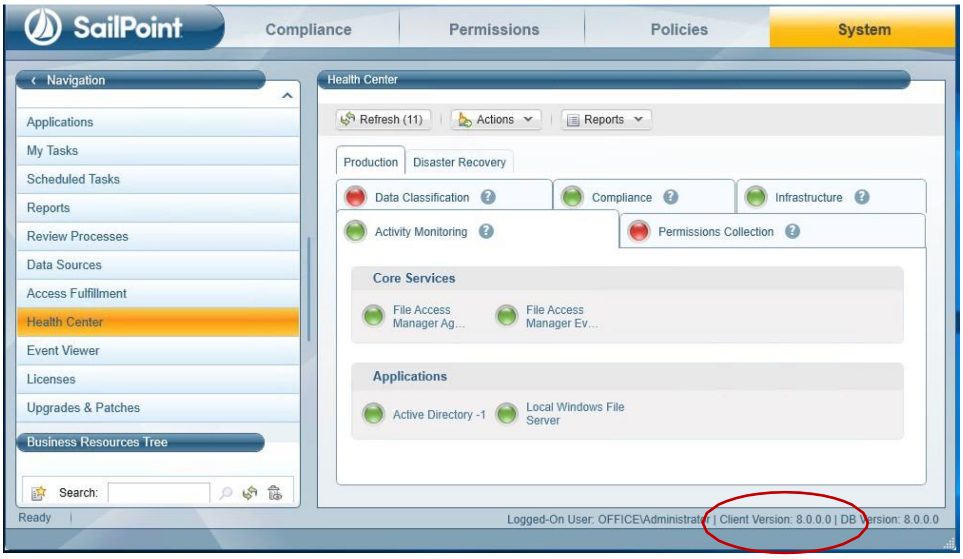
Starting from version 6.1, SecurityIQ (FAM) Service Packs deployment is done automatically. Service Packs are deployed by the File Access Manager update deployment mechanism. By simply uploading a Service Package through the Administrative Client, and pressing a button to initiate the deployment, the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



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., 8.4.0.1000.
The first two sections represent major releases. File Access Manager 8 GA release number is 8.0.0.0. whereas File Access Manager 8.4 release will be represented by the number 8.4.0.0.
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 8.4 Service Pack 1 version number is 8.4.0.1000.
The Database version number will be updated with every service pack. For File Access Manager 8.4 Service Pack 1, the database version number is 8.4.0.1000.
The Client version number will be updated if the service pack includes changes to the Administrative Client. For File Access Manager 8.4 Service Pack 1, the Client version number is 8.4.0.1000.

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. 8.4 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	8.4.0.1000
File Access Manager Elasticsearch	8.2.2
File Access Manager RabbitMQ	3.9.14
File Access Manager SCIM API	8.4.0.1000
File Access Manager REST API	8.4.0.0
File Access Manager Business Website	8.4.0.1000
File Access Manager Administrative Client	8.4.0.1000
File Access Manager Data Classification	8.4.0.1000
File Access Manager Permission Collection	8.4.0.1000
File Access Manager Activity Analytics	8.4.0.1000
File Access Manager Agent Configuration Manager	8.4.0.1000
File Access Manager Collector Synchronizer	8.4.0.1000
File Access Manager Crowd Analyzer	8.4.0.0
File Access Manager Event Manager	8.4.0.0
File Access Manager Reporting Service	8.4.0.1000
File Access Manager Scheduled Task Handler	8.4.0.1000
File Access Manager User Interface	8.4.0.1000
File Access Manager Watchdog	8.4.0.0
File Access Manager Workflow Service	8.4.0.0
File Access Manager Activity Monitor	8.4.0.0

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\8.4.0.1000} (*the contents of the folder will be related to the pre-upgraded version*).

Chapter 2: Support Matrix

Table 3 IdentityIQ File Access Manager Server Support Details

System	Supported Versions
IdentityIQ File Access Manager Servers	Windows 2016/2019/2022
Workstation	Windows 8 and above
Browser	Edge, Firefox, Chrome, Safari
Database	MS SQL Server 2014/2016/2017/2019/2022

Chapter 3: Deploying Version 8.4 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

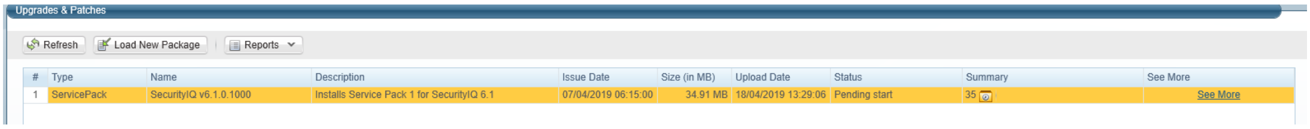
Pre-upgrade Steps

Install EXO PowerShell module.

For those who use Exchange Online Connector please follow the installation prerequisites section: **Chapter 4, SIQSUS-881 – Modernize EXO Connectivity v3.0.**

Service Pack Deployment

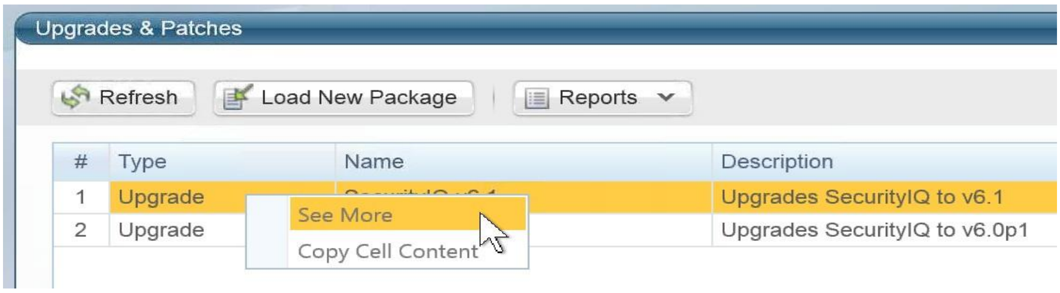
- Extract the “File Access Manager v8.4.0.1000.zip” installation package.
- Navigate to the “Service Pack 1” folder.
- Log into the IdentityIQ File Access Manager administrative client Client
- Click **System** >> **Upgrades & Patches** >> **Load New Package**
  This will open the **Load Package** dialog.
- Press **Browse** and load the file “**File Access Manager v8.4 Service Pack 1.wbxpkg**” from the Service Pack folder.
- Press **Upload Package**.
  The system will upload and validate the file. This might take a few minutes.
- Once it is validated, press **Save**. This will add the upgrade package to the upgrades page.



#	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

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

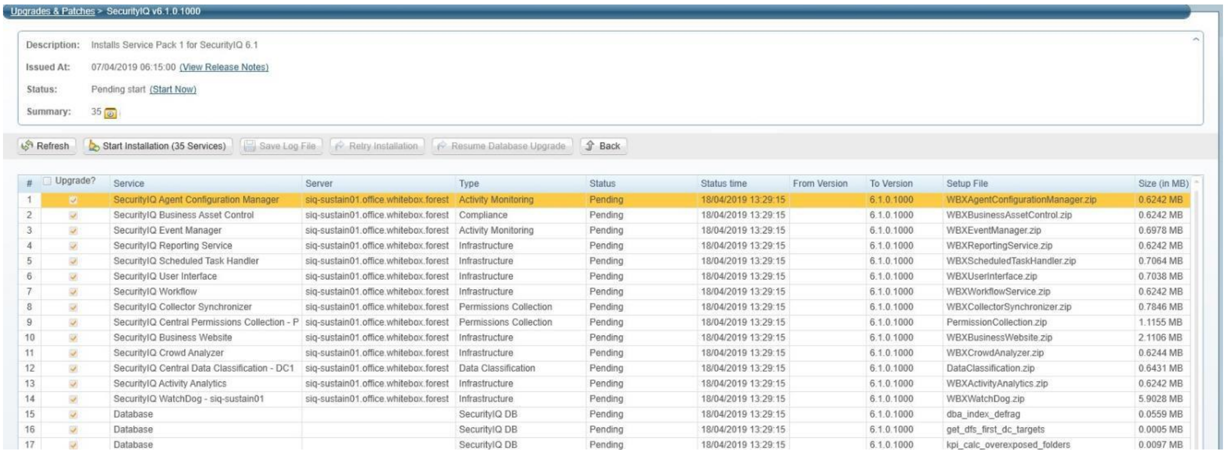


#	Type	Name	Description
1	Upgrade		Upgrades SecurityIQ to v6.1
2	Upgrade		Upgrades SecurityIQ to v6.0p1

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
Refresh
Start Installation (35 Services)
Save Log File
Retry Installation
Resume Database Upgrade
Back

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

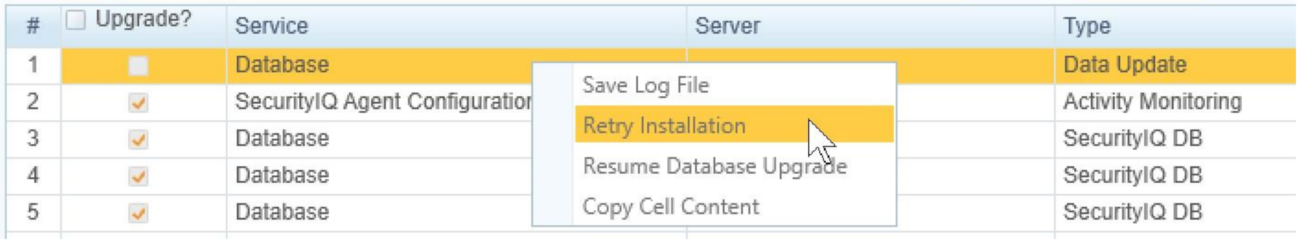
- Click **Start Installation** and **Confirm** to start the installation process.

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

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

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

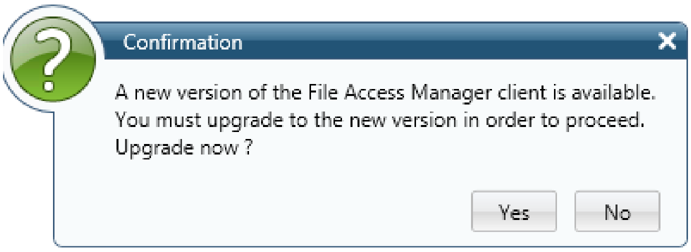
Note: See *Chapter 5: Troubleshooting* **for further suggestions and information.**

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 8.4.0.1000
The IdentityIQ File Access Manager Database version should be set to 8.4.0.1000

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

Optional: Uninstall .Net Core 3.1

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

Navigate to the Control Panel > Programs > Uninstall a program

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

Chapter 4: Important Information and Updates

SIQSUS-881 – Modernize EXO Connectivity v3.0

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

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

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

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

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

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

New Module Installation Prerequisite:

The new module will need to be manually installed by the customer on any machines running Exchange Online tasks: Activity Monitoring and the Permission Collection engine. The command to installs the latest version of the module and should be run from an elevated administrator PowerShell prompt:

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

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

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

```
Get-InstalledModule
```

Optimized Get-EXO* Cmdlets

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

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

Mailbox Folder Statistics Collection Now Opt-In To Address Performance

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

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

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

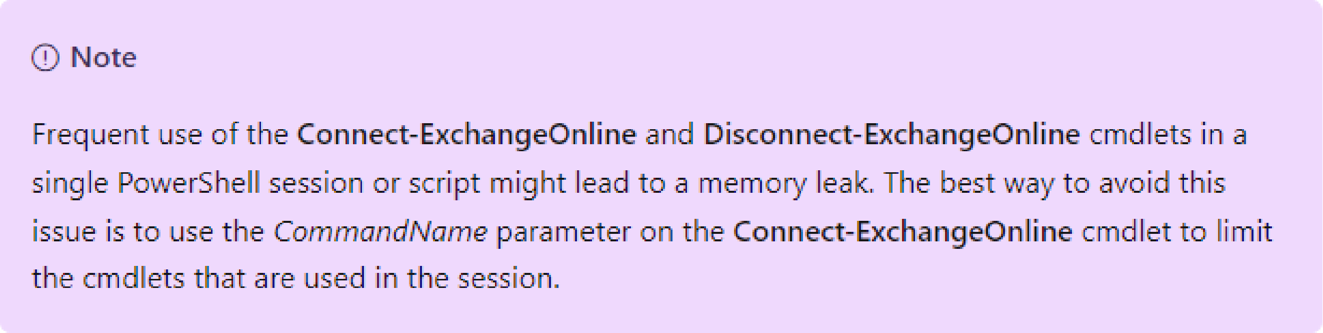
Exclude Internal Folders "SubstrateHolds" and "DiscoveryHolds"

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

Memory Usage

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

There is a note about it on the [Microsoft EXO module about page](#):



ⓘ Note

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

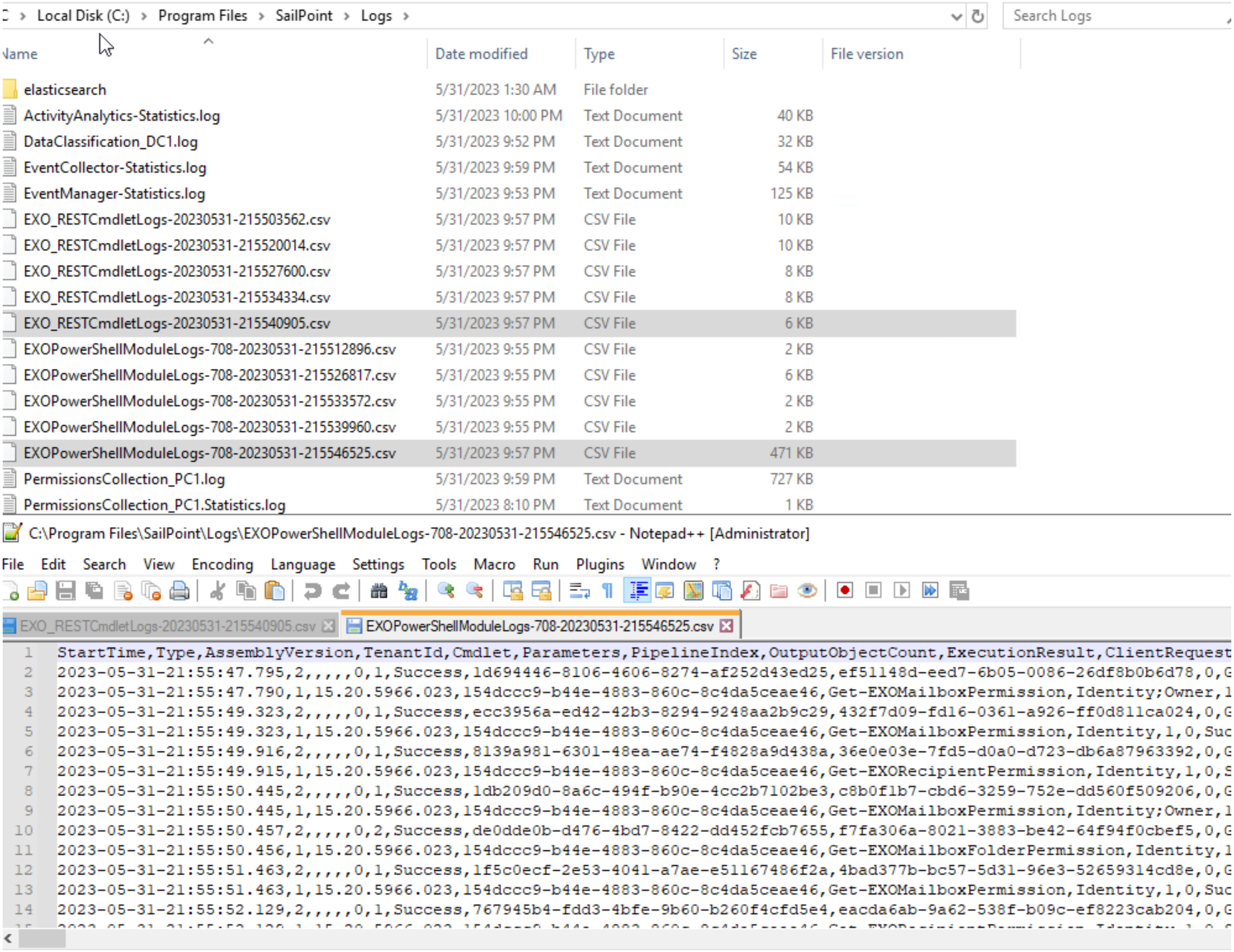
We are using the CommandName parameter to import any needed REST cmdlets to reduce memory usage. When this is corrected by Microsoft, we will include Microsoft updates/recommendations into the upcoming Service Pack.

Overall Performance

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

Logging and Configuration

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



Name	Date modified	Type	Size	File version
elasticsearch	5/31/2023 1:30 AM	File folder		
ActivityAnalytics-Statistics.log	5/31/2023 10:00 PM	Text Document	40 KB	
DataClassification_DC1.log	5/31/2023 9:52 PM	Text Document	32 KB	
EventCollector-Statistics.log	5/31/2023 9:59 PM	Text Document	54 KB	
EventManager-Statistics.log	5/31/2023 9:53 PM	Text Document	125 KB	
EXO_RESTCmdletLogs-20230531-215503562.csv	5/31/2023 9:57 PM	CSV File	10 KB	
EXO_RESTCmdletLogs-20230531-215520014.csv	5/31/2023 9:57 PM	CSV File	10 KB	
EXO_RESTCmdletLogs-20230531-215527600.csv	5/31/2023 9:57 PM	CSV File	8 KB	
EXO_RESTCmdletLogs-20230531-215534334.csv	5/31/2023 9:57 PM	CSV File	8 KB	
EXO_RESTCmdletLogs-20230531-215540905.csv	5/31/2023 9:57 PM	CSV File	6 KB	
EXOPowerShellModuleLogs-708-20230531-215512896.csv	5/31/2023 9:55 PM	CSV File	2 KB	
EXOPowerShellModuleLogs-708-20230531-215526817.csv	5/31/2023 9:55 PM	CSV File	6 KB	
EXOPowerShellModuleLogs-708-20230531-215533572.csv	5/31/2023 9:55 PM	CSV File	2 KB	
EXOPowerShellModuleLogs-708-20230531-215539960.csv	5/31/2023 9:55 PM	CSV File	2 KB	
EXOPowerShellModuleLogs-708-20230531-215546525.csv	5/31/2023 9:57 PM	CSV File	471 KB	
PermissionsCollection_PC1.log	5/31/2023 9:59 PM	Text Document	727 KB	
PermissionsCollection_PC1.Statistics.log	5/31/2023 8:10 PM	Text Document	1 KB	

C:\Program Files\SailPoint\Logs\EXOPowerShellModuleLogs-708-20230531-215546525.csv - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
EXO_RESTCmdletLogs-20230531-215540905.csv
EXOPowerShellModuleLogs-708-20230531-215546525.csv

```
StartTime,Type,AssemblyVersion,TenantId,Cmdlet,Parameters,PipelineIndex,OutputObjectCount,ExecutionResult,ClientRequest
2023-05-31-21:55:47.795,2,,,,,0,1,Success,1d694446-8106-4606-8274-af252d43ed25,ef51148d-eed7-6b05-0086-26df8b0b6d78,0,G
2023-05-31-21:55:47.790,1,15.20.5966.023,154dccc9-b44e-4883-860c-8c4da5ceae46,Get-EXOMailboxPermission,Identity;Owner,1
2023-05-31-21:55:49.323,2,,,,,0,1,Success,ecc3956a-ed42-42b3-8294-9248aa2b9c29,432f7d09-fd16-0361-a926-ff0d811ca024,0,G
2023-05-31-21:55:49.323,1,15.20.5966.023,154dccc9-b44e-4883-860c-8c4da5ceae46,Get-EXOMailboxPermission,Identity,1,0,Suc
2023-05-31-21:55:49.916,2,,,,,0,1,Success,8139a981-6301-48ea-ae74-f4828a9d438a,36e0e03e-7fd5-d0a0-d723-db6a87963392,0,G
2023-05-31-21:55:49.915,1,15.20.5966.023,154dccc9-b44e-4883-860c-8c4da5ceae46,Get-EXORecipientPermission,Identity,1,0,S
2023-05-31-21:55:50.445,2,,,,,0,1,Success,1db209d0-8a6c-494f-b90e-4cc2b7102be3,c8b0f1b7-cbd6-3259-752e-dd560f509206,0,G
2023-05-31-21:55:50.445,1,15.20.5966.023,154dccc9-b44e-4883-860c-8c4da5ceae46,Get-EXOMailboxPermission,Identity;Owner,1
2023-05-31-21:55:50.457,2,,,,,0,2,Success,de0dde0b-d476-4bd7-8422-dd452fcb7655,f7fa306a-8021-3883-be42-64f94f0cbef5,0,G
2023-05-31-21:55:50.456,1,15.20.5966.023,154dccc9-b44e-4883-860c-8c4da5ceae46,Get-EXOMailboxFolderPermission,Identity,1
2023-05-31-21:55:51.463,2,,,,,0,1,Success,1f5c0ecf-2e53-4041-a7ae-e51167486f2a,4bad377b-bc57-5d31-96e3-52659314cd8e,0,G
2023-05-31-21:55:51.463,1,15.20.5966.023,154dccc9-b44e-4883-860c-8c4da5ceae46,Get-EXOMailboxPermission,Identity,1,0,Suc
2023-05-31-21:55:52.129,2,,,,,0,1,Success,767945b4-fdd3-4bfe-9b60-b260f4cfd5e4,eacda6ab-9a62-538f-b09c-ef8223cab204,0,G
```

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

References:

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

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

Permission Forensics Call

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

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

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

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

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

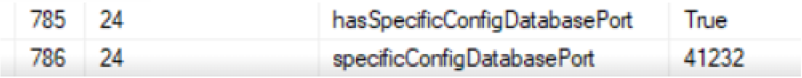
These changes will allow for custom port use for the SharePoint Content databases.

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

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

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

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



785	24	hasSpecificConfigDatabasePort	True
786	24	specificConfigDatabasePort	41232

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

SIQSUS-850 – Migration to Microsoft Graph API

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

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

Necessary steps:

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

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

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

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

Considerations:

A list of resources that are accessed by File Access Manager using the REST graph API include:

https://graph.windows.net/{tenant_domain_name}/tenantDetails
https://graph.windows.net/{tenant_domain_name}/users
https://graph.windows.net/{tenant_domain_name}/users/{user_id}
https://graph.windows.net/{tenant_domain_name}/groups/{group_id}
https://graph.windows.net/{tenant_domain_name}/directoryRoles
https://graph.windows.net/{tenant_domain_name}/directoryRoles/{role_id}

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

Chapter 5: Troubleshooting

Upgrade Package Loading Fails

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

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

Suggested solution:

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

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

NHibernate configuration

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

Suggested solution:

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

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

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

   a. Make sure the SecurityIQ Home environment variable is set to the correct location
   b. Ensure that the folder named “External Tools”, containing the “makecert.exe” executable, or copy that folder from the Core Services server (the server hosting the User Interface service), and place it in the SecurityIQ Home directory
   c. Ensure that the folder named “ServerInstaller” exists in the “%SECURITYIQ_HOME%\File Access Manager” path, and within that folder you can locate the “Tools” directory or copy it from the Core Services server.
   d. Navigate to the “DBResetPassword” folder
   e. In a Command Line window (cmd) from the “DBResetPassword” directory path, run the following command:

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

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

Business Website

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

Suggested solution:

1. Navigate to the wwwroot folder on the server hosting the Website at C:\inetpub\wwwroot).
2. Verify that the IdentityIQFAM and SiqApi folders are in the wwwroot folder.
3. If these folders are in the wwwroot folder, but there are still problems with the Business Website, contact support.
4. If these folders are **not** in the wwwroot folder, perform the following steps:
5. Open the Internet Information Service (IIS) manager (Server Manager 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.

Improper upgrade path

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

Steps to "rollback" the failed installation.

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

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

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

After the DB has been cleaned up and reloading the Client the 8.3 SP5 wbxpkg will no longer be listed in the 'Upgrades & Patches' screen. This allows for following a valid upgrade path to 8.3.0.000 and then retry SP5, Once FAM has been upgraded to at least 8.3.0.0000 there should be no issue reloading the SP5 wbxpkg and successfully completing the installation.

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

SIQSUS-706 – Clarify Design & Implement/Make changes around Group Permission Staleness

This issue will update permission forensics to use business resource's last used if available otherwise current behavior will remain unchanged.

SIQSUS-881 – Modernize EXO Connectivity v3.0

Use latest EXO V3 module and Get-EXO* optimized cmdlets where possible so that RPS (remote power shell) can be disabled for tenants.

SIQSUS-850 – Adjustment from MS Announcement to Deprecate Graph Azure AD API

Corrected reauthenticate Azure AD token process so Azure Synchronize IC Task won't fail.

SIQETN-3038 – Add In 'Empty' & 'Not Empty' operators for Category Filter in Forensics searches

'Empty' & 'Not Empty' operators for Category Filter in Forensics searches added.

SIQETN-3040 – Default SMTP SharePoint Online - Single Activity template does not pick up all template variables

Changed several potential versions of Share Point Online to SharePointOnline in the SMTP response body via database script, user story.

SIQETN-3185 – Null Reference Exception in Activity Reporting Due to duplicate event IDs

Allow Null values, and add logging to understand further why Event has Null data.

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

Increase SCIM API's permission query's index limit to ten million. Additional restructuring was done to improve performance. Two additional indexes have been introduced to improve query plans.

SIQETN-3197 – website dashboard - threshold alert widget - ElasticSearch query timing out.

Improves performance of “threshold alerts” website dashboard.

SIQETN-3201 – SharePoint on-premise data classification failure to connect to HTTPS URL

Added support for SharePoint on-premise HTTPS endpoints during data classification.

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

Added enhancement to allow for custom port use as well for the content databases.

SIQETN-3205 – lock update_ra_users_br_permissions while inserting

Improved duplicate user handling during permission collection.

SIQETN-3206 – Composite Rule Policies Overrides one another so only one is tagged on qualifying resource

Added extra validations so now Composite Rules Policies are all now tagged accordingly within Forensics > Data Classifications menu.

SIQETN-3207 – Duplicates Not handled properly in gDrive crawl

Perform cleaned up for all duplicates vs in batches.

SIQETN-3208 – Dashboard Widget Calculation performance improvement

Performance improvement of 2 stored procedures that handle DFS within Dashboard calculation task.

SIQETN-3211 – Alerts to data owners not triggered off events on SPO when set through Resources->Alerts screen

Updated relevant tables with correct SPO events.

SIQETN-3212 – Some alerts to data owners not triggered off events on NetApp when set through Resources->Alerts screen

Updated relevant table with correct NetApp events and operators..

SIQETN-3213 – Token Refresh Server Resiliency Enhancement

Tokens refresh every 10 minutes before they are set to expire. If within this 10 minute window will keep trying to refresh every 1 minute until the token has completely expired.

SIQETN-3214 – Query Injection Provides Ability To Manipulate Database Queries

The vulnerable query was updated and validated along with the HTTP error message details.

SIQETN-3216 – Responses with Incorrect or Missing Content-type

Correct content-type on all response specified.

SIQETN-3217 – Impersonation of users on the FAM WEBUI does not change user accounts during impersonation

Addressed failure of impersonation.

SIQETN-3218 – FAM.SCIM self referencing loop

Resolved "self referencing loop detected" exception in FAM SCIM API.

SIQETN-3221 – AWS S3 Connector Incorrectly Pages Results Causing Crawl Failure

Implemented proper paging for all AWS queries that return List responses with Marker or NextToken property.

SIQETN-3222 – Rename Resource Alerts 'File or Folder is modified' to ''File is modified'

Updated to ‘File is modified’ and remove ‘Folder’.

SIQETN-3223 – Correct continuous append

string builder is cleared and re-initialized with a new insert statement before appending next batch of row data.

SIQETN-3224 – Identity collector failure during delete

Allow identity collectors with mapped data sources to be deleted.

SIQETN-3225 – Some alerts to data owners not triggered off events in several endpoints when set through Resources->Alerts screen

Updated policy_business_rule_type_wpc_field table with correct operators.

SIQETN-3226 – Typo in User Group Memberships report

Both reports updated with the correct wording.

SIQETN-3227 – SPO ans OneDrive not showing all resource info in alert email

Added missing fields + hyperlink to resource.

SIQETN-3228 – OneDrive Drive Verification Fails Crawl During Root Collection When Using skipOneDriveExistenceVerification

Code updated to avoid issues when using skipOneDriveExistenceVerification flag.

SIQETN-3230 – Content Type displaying Incorrectly for SharePoint On Prem

Fix code that the engine will distribute the content type map to crawler.
Fix UI to show each content type total size when mouse hover on them.

SIQETN-3233 – wbxadmin login failed with impersonation bug fix

Addressed failure of impersonation.