SecurityIQ v6.0 Service Pack 3

SecurityIQ Version: 6.0.0.3000

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.

Table of Contents

List of Tables

Table of Revisions

Ver. #	Description	Author	Date
6.0	Final Version	Hanan Levy	13 Jul 2018
6.0SP2	Update	Colin Wyatt	1 Nov 2018
6.0SP3	Update	Ivan Pointer	1 Feb 2019

1. PLANNING YOUR SERVICE PACK DEPLOYMENT

1.1. What is a Service Pack?

SecurityIQ 6.0 release introduced the concepts of Service Packs.

Service Packs are cumulative packages containing all released E-Fixes to date, since the last Major or Patch release.

Service Packs allows customer 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 SecurityIQ components for which bug fixes or performance enhancements were issued, while the rest of the system remains untouched.

1.2. Service Packs Deployment Process

In SecurityIQ 6.0 Service Packs deployment is performed by running the SIQServicePackInstaller tool, provided as part of the Service Pack, and located in the SIQServicePackInstaller folder. The tool will update most services, the websites, and the client. The remaining components must be updated manually. Components that must be updated manually include: Database scripts, Activity Monitor services, Elasticsearch, RabbitMQ, the SecurityIQ Server Installation, and the Collector Manager. If there are updates for these components, they will be included in the Service Pack in folders with the component's name. Only if such updates exist they should be applied manually, otherwise, no action is required. All other SecurityIQ services, including all core services, Data Classification Engines and Collectors, and Permission Collection Engines and Collectors will be updated by the SIQServicePackInstaller.

The SIQServicePackInstaller tool must be launched on each server containing SecurityIQ components the needs to be updated including all machines on which the Administrative Client is installed.
You do not need to run the tool on servers hosting ***only*** manually updated components, i.e., the Database Server, Application Monitors, Elasticsearch, and Rabbit MQ.

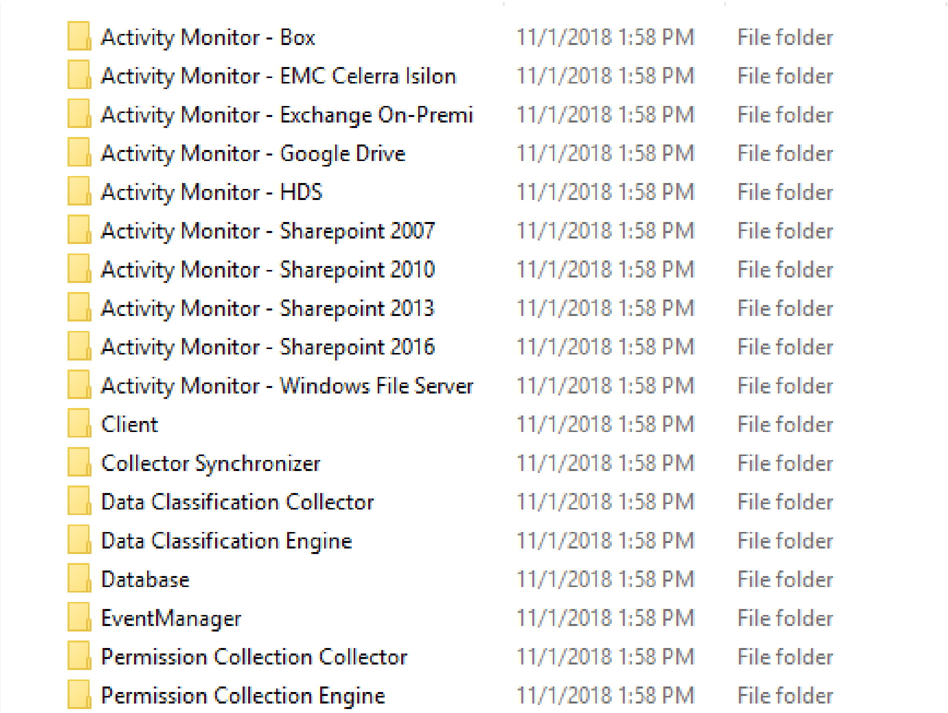
The SIQServicePackInstaller tool launches a dialog which allows the user to select the location of the Service Pack folder and then apply the service pack. The tool will make a backup of the destination component's folder with the suffix "_BAK-<TIMESTAMP>" alongside the original folder. If any problems occur during the service pack installation, these backup folders can be used to restore the original files. Messages will be displayed in the tool showing informational progress messages, as well as any warnings or errors. Warning and error messages will be highlighted orange and red. An output log file will also be created in the same directory as the SIQServicePackInstaller.exe tool.

Starting from the SecurityIQ 6.1, Service Packs deployment would be done automatically. Using the new Upgrade Mechanism, Service Pack packages would be uploaded to SecurityIQ by the administrator and will automatically deploy themselves updating all relevant services and components. This mechanism will have built-in backup and rollback procedures, to revert any changes in case of any issues encountered during the deployment process. In case of any issues or errors with the automated deployment, fixes can be deployed manually.

1.2.1. Service Pack Structure

Each Service Pack contains a zip file, with the Service Pack number and version number (see below).

The Service Pack zip file contains a folder for each updated component. Components may include the SecurityIQ core services (e.g. UserInterface, Reporting, Workflow, etc.), installers, multiple-installed services such as Permission Collection and Data Classification Engines and Collectors, or Application Monitors, and infrastructure components such as Database (SQLServer scripts), Elasticsearch, and RabbitMQ.



Activity Monitor - Box	11/1/2018 1:58 PM	File folder
Activity Monitor - EMC Celerra Isilon	11/1/2018 1:58 PM	File folder
Activity Monitor - Exchange On-Premi	11/1/2018 1:58 PM	File folder
Activity Monitor - Google Drive	11/1/2018 1:58 PM	File folder
Activity Monitor - HDS	11/1/2018 1:58 PM	File folder
Activity Monitor - Sharepoint 2007	11/1/2018 1:58 PM	File folder
Activity Monitor - Sharepoint 2010	11/1/2018 1:58 PM	File folder
Activity Monitor - Sharepoint 2013	11/1/2018 1:58 PM	File folder
Activity Monitor - Sharepoint 2016	11/1/2018 1:58 PM	File folder
Activity Monitor - Windows File Server	11/1/2018 1:58 PM	File folder
Client	11/1/2018 1:58 PM	File folder
Collector Synchronizer	11/1/2018 1:58 PM	File folder
Data Classification Collector	11/1/2018 1:58 PM	File folder
Data Classification Engine	11/1/2018 1:58 PM	File folder
Database	11/1/2018 1:58 PM	File folder
EventManager	11/1/2018 1:58 PM	File folder
Permission Collection Collector	11/1/2018 1:58 PM	File folder
Permission Collection Engine	11/1/2018 1:58 PM	File folder

1.2.1.1. Service Packs Database Updates

Service Packs may include changes that need to be executed in the SQLServer database, such as DML scripts that modify content, or DDL scripts that modify the structure of database components such as tables, views and stored procedures.

Unless otherwise specified Database changes must ***always*** be executed as the first step of the Service Pack deployment.

Updating from a clean 6.0 GA Release to the latest Service Pack

Under the folder "Database", the file SINGLE_SCRIPT.sql contains all the scripts combined into one script that can be run once (This script is the sequential combination of all the files in the sub-folder "individual scripts").

Updating from Service Pack 2 (and above) to the latest Service Pack

The folder "Database" will also include differential Database Update Scripts, that contains all database changes made between the different Service Packs. Thus if you're deploying Service Pack 3 on an environment that was already updated with Service Pack 2, the script named SP2_to_SP3.sql will include all database changes that need to be applied to roll the database forward to Service Pack 3.
If this is the case on your environment, only the differential script, and not the full one, should be executed.

Database Scripts should be executed on the SecurityIQ database and schema.

Important!

Any object should be backed up before being altered. Please see section 1.2.1.3 Backup Measures below – for possible backup methods.

1.2.1.2. Service Packs Deliverables Updates

As part of the Service Pack deployment, certain deliverables will be replaced with new ones containing the fixed and / or improved code and functionality. Most commonly, those deliverables would be in the form of Dynamic-link libraries (in-short, Dll's), and executables. In addition, some changes may involve changing auxiliary files such as configuration files (e.g. app.config and web.config files).

Important!

Before performing ANY change to the SecurityIQ deliverables, the original files **MUST** be safely backed-up and stored.

Having the original deliverable readily available, will allow you a quick and easy roll-back path. 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.

(for backup measures see section 1.2.1.3 Backup Measures below).

The process of *manually* replacing deliverables is the following:

1. Stop or close the relevant component or service – make sure that the component's or service's executable is indeed down and does not appear in the Windows Task Manager before moving on to the next step.
In case the Service Pack involves updating the SecurityIQ Website, IIS should be stopped.

2. Identify the files to be replaced.

3. Backup the original files to a safe location (see section 1.2.1.3 Backup Measures).

4. Replace the original files with the files provided in the Service Pack for that component.

5. Perform any additional changes, to auxiliary files or other, as specify in the Service Pack instructions.

6. Start the component or service (including IIS if applicable).

As a verification step, check the logs after starting the component or service, to ensure the clean startup and execution of the component.

1.2.1.3. Backup Measures

Deliverables Backups

As backup measures we STRONGLY recommend that you create a copy of the files that are about to be replaced or modified, in a different location, that is not affected by the changes, and arrange the folder structures in an organized, coherent way, that will allow you to identify which files belong to which component.

Copying the original folders to a safe, and preferably backed-up, location is ideal.

A minimal measure would be copying the original files to another folder on the same server.

Website Deliverables Backups

When backing up Website components (on the IIS servers), the backup folders should not be placed within the IIS root directory.

Database Backups

As a rule, we recommend that regular backups will be performed on the SecurityIQ 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 would 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.

In the case of data changes, we recommend that a copy of the table be made before changing any data.

1.2.1.4. End-point related \ multiply-installed Services

Some of the SecurityIQ components can be installed multiple times. Such is the case with Permission Collection and Data Classification Engines and Collectors, for instance. If a service pack contains an E-Fix for such a component, for example, a Permission Collection Engine, this fix should be applied on all instances of that component, unless otherwise specified.

End-Point Related Components

Occasionally, a Service Pack would include E-Fixes targeted for a specific end-point. For example, a Service Pack can contain an E-Fix specifically for the NetApp Permission Collection collector, or Activity Monitor. In these cases, the E-Fix should be deployed only if it applies to an end-point on your environment. To use the same example, if you do not have NetApp end-points configured, there's no need to deploy E-Fixes relating to that specific end-point.

If, however, a Service Pack contains both generally applicable E-Fixes, and end-point specific E-Fixes, and both apply to your configuration, both types of E-Fixes should be deployed.

End-Point Specific updates must be applied manually.

1.3. Version Numbers

SecurityIQ version numbers are represented by a four-section number, e.g., 5.1.1000.0.

The first two sections represent major releases. SecurityIQ 6 GA release number is 6.0.0.0. whereas, SecurityIQ 5.1 release is represented by the number 5.1.0.0.

The next section represents Patch Releases, e.g., SecurityIQ 5.1P1 version number is 5.1.1000.0.

Service Pack updates are reflected in the last section, and so SecurityIQ 6.0 Service Pack 3 version number is 6.0.0.3000.

The Database version number will be updated with every service pack. For SecurityIQ 6.0 Service Pack 3, the database version number is 6.0.0.3000.

The Client version number will be updated if the service pack includes changes to the Administrative Client. For SecurityIQ 6.0 Service Pack 3, the database version number is 6.0.0.3000.

Infrastructure components, such as Elasticsearch and RabbitMQ will retain the same version number, unless and update to the actual infrastructure components is applied, in which case their version number will be updated as well.

1.3.1. Versions included in this release:

Table 2 Lists SecurityIQ Service Pack Components Versions.

Table 1. SecurityIQ Components Version Details

Component	Version
SecurityIQ Database	6.0.0.3000
SecurityIQ Elasticsearch	6.0.0.0000
SecurityIQ RabbitMQ	6.0.0.0000
SecurityIQ API	6.0.0.3000
SecurityIQ Web Client	6.0.0.3000
SecurityIQ Administrative Client	6.0.0.3000

2. SUPPORT MATRIX

Table 2 lists SecurityIQ server support details.

Table 2. SecurityIQ Server Support Details

System	Supported Versions
SecurityIQ Servers	Windows 2012R2/2016 64bit
Workstations	Windows 7 and above
Browsers	IE 11, Edge, Firefox, Chrome, Safari
Databases	MS SQL Server 2012/2014/2016 64bit

3. 6.0 Service Pack 3 Deployment

3.1. Pre-deployment Steps

Before the performing any changes, perform the following steps:

1. Back up the SecurityIQ database before starting the Service Pack deployment.
2. Before replacing any deliverables, ensure that you have created a copy of the original deliverables.

3.2. Deployment Steps

1. First, manually run the database scripts associated with the service pack, found in the “Database” folder. You have a few options:
    a. If you are updating from a base install (i.e. 6.0 GA), you can run “SINGLE_SCRIPT.sql” to bring your database all the way up to the latest service pack.
    b. If you are applying a service pack to an earlier service pack, such as upgrading to SP3 from SP2, you will find a script named “SP2_to_SP3.sql”, to advance forward.
    c. You can also apply the scripts individually (keeping in mind, the order of the scripts), which are found in the “individual scripts” directory.
2. Run the SIQServicePackInstaller.exe tool to automatically apply the service pack files to services (excluding Activity Monitors), websites, and the Client, on all machines with SecurityIQ installed.
3. In case of any issues or errors with the automated deployment, fixes can be deployed manually.
4. Manual Replacement Process for deliverables not applied with SIQServicePackInstaller:
    a. Identify the component / service that is being updated.
    b. Ensure that no task that relates to that service / component is currently running. If there are running tasks, either let those tasks finish, or stop the tasks through the Administrative Client.
    c. Stop the component / service to be updated. Make sure that the executable of that component / service is completely down and does not appear in the Windows Task Manager.
    d. Identify the deliverables to be replaced and create backup copies of these deliverables. Follow the instructions in the Backup Measures (1.2.1.3) section.
    e. Replace the deliverables with the new deliverables supplied by the Service Pack package.
    f. Perform any additional steps instructed by the Service Pack deployment instructions (if applicable).
    g. Start the component / service after the updates have been applied and ensure the successful startup and availability of that component.
    h. Check the logs for any errors and / or warning after the component / service has been started.

3.3. Special Cases

Special Cases are Updates (E-Fixes and Enhancements) that are not automatically deployed by the Service Pack. If needed, these updates need to be deployed manually.

The deliverables for the “Special Cases” updates are located under the “Special Cases” folder in the Service Pack, each in its own individual folder, bearing the identifier and the name of the update. Follow the instructions below to deploy the updates.

3.3.1. SIQETN-2157 – Server Installer E-Fix

SIQETN-2157 is an E-Fix provided for the SecurityIQ Server Installer and relates to the installation of the RabbitMQ component.

If you have already successfully installed SecurityIQ and the RabbitMQ component, this E-Fix should not be applied.

If you have not yet installed SecurityIQ, or the RabbitMQ, we recommend that you will apply this E-Fix.

To apply the fix:

1. Install the SecurityIQ Server Installer

2. Make sure RabbitMQ and Erlang are not installed on the system.
For that, the following conditions must be met:

  2.1. The RabbitMQ service is uninstalled, and its installation folder is completely deleted.

  2.2. Erlang is uninstalled, and its installation folder is completely deleted.

  2.3. Any environment variable starting with ERLANG or RABBIT is deleted.

  2.4. The file called .erlang.cookie is deleted (Under %USERPROFILE% of the user who installed RabbitMQ).

  Note: You might have a problem deleting the folders.
  If that's the case, either restart the server and try again, or download Process Explorer and kill the process called epmd.exe
  (it usually doesn't appear in the Windows Task Manager).

3. Apply the fix by doing the following under the Server Installer's folder:

  3.1. Backup and replace SecurityIQServerInstaller.exe.

  3.2. Under Resources, backup and delete rabbitmq.conf, and place rabbitmq.config in its stead.

  3.3. Under Resources, backup and replace the archive called rabbitmq-server-windows-3.7.4.zip.

4. Perform the SecurityIQ and RabbitMQ installation.

Note: You might run into a plugin related issue when you try installing again.
If that's the case, go back to step 2 again and try installing a second time.

3.3.2. SIQETN-2265 – Server Installer and Collector Manager

As part of the SIQETN-2265 fix, some updates need to be applied to the SecurityIQ Server Installer and the SecurityIQ Collector Manager. The files that need to be updated are located in the Service Pack folder, under the Server Installer and Collector Manager folders respectively.

To Apply changes to the Server Installer:

1. On each server containing SecurityIQ services (with the exception of Agents and Collectors), identify the Server Installer folder, located under the SecurityIQ Home Directory
2. Backup the content of the Server Installer folder to a different location
3. Copy the files included in the Service Pack, under the Server Installer folder, use them to replace the files in the Server Installer folder on the server.

To Apply changes to the Collector Manager:

The Collector Manager is a utility deigned for the installation and configuration of Activity Monitor services, and Collectors for the Permission Collection and Data Classification Engines. As such it is not being deployed in itself. It is sufficient to update the libraries on a single centralized location containing the Collector Manager, and there no need to update any servers. The Collector Manager is part of the SecurityIQ 6.0 release installation package, located under \v6.0 Full Installers\Agents.

1. Locate you copy of the SecuirtyIQ 6.0 installers
2. Backup the content of the Agent folder to a different location
3. Replace the files under the Collector Manager folder, with the files contained in the Service Pack, under the Collector Manager.

3.3.3. SIQETN-2343 – Website Dashboard, Database and KPI Improvements

Enhancement SIQETN-2343 introduce important performance enhancement to the KPI Dashboard, to address some performance issue reported by several customers.
The following changes are included in this enhancement:
1. Resource Dashboard is removed from the Business Website
2. Data Owner Dashboard now retrieves KPI information from the pre-calculated KPI Data, calculated by the Dashboard Widgets Calculation Scheduled Task, that runs nightly.
3. Improved Database Statistics calculation algorithm included in the DB Cleanup Task.
4. Improved Website single-session requests concurrency – concurrent request no longer blocking each other on long-running requests.
5. DFS Resources are temporarily exempted from the Data Owners Dashboard. DFS Data Owners resource will be re-added to the Data Owners Dashboard in another enhancement to be released shortly. Tracking Item Enhancement - SIQETN-2364.

Since we did not want to make unnecessary changes to environments who do not experience the same performance issue, this enhancement is not automatically deployed, and need to be deployed manually.

To Apply this enhancement:

1. Back up the SiqApi and SecurityIQBiz folders
   (located either under %SystemDrive%\inetpub\wwwroot or %SECURITYIQ_HOME% on the server hosting the SeucirtyIQ Website)
2. Backup the Stored Procedure whiteops.dba_index_defrag in the SecurityIQ database
3. The folders with the same names as the ones mentioned above (SecurityIQBiz and SiqApi) contain some files to replace with respect to their corresponding hierarchies. Replace those files where they appear in the folder structure. Some of the files might not have duplicates in their folders, but that's expected.
4. Run the script located under the sql folder on the SecurityIQ database.
5. Run iisreset on the server hosting the SeucirtyIQ Website.
   Service Pack E-Fixes

3.3.4. List of E-fixes

Service Pack 1

1. **SIQETN-2114** – Adding local time for email alerts from activity monitoring
2. **SIQETN-2117** - Role Path does not show in the User Membership in Groups results in Admin Client
3. **SIQETN-2119** - Resources created by Activity Monitoring, may be created with wrong hierarchy or appear as roots

4. **SIQETN-2120** – “NOT” operators aren't filtering on WPC fields in the Activity Forensics page (Not Contains, Not starts with, etc.)
5. **SIQETN-2122** – Old / Irrelevant Permissions are not being properly deleted
6. **SIQETN-2129** - Resources created with plain drive letters (colon-suffixed drives, e.g. C:\)
7. **SIQETN-2131** - NetApp mount points are not being crawled
8. **SIQETN-2135** - Exchange activity not getting AD enriched
9. **SIQETN-2136** - Reports generation fails occasionally
10. **SIQETN-2139** - Hierarchical queries are limited to 100 recursive loops
11. **SIQETN-2152** - Permission Collection and Data Classification services taking too long to start can timeout and stop
12. **SIQETN-2153** - SharePoint IIS logs defined to be written under an explicit local path in a multi-server farm aren't collected in Automatic mode
13. **SIQETN-2128 -** Group Membership information for an activity is not being enriched, if the group name contains specials character (e.g. brackets)
14. **SIQETN-2174** - Cannot set data owners to a DFS resources containing special characters
15. **SIQETN-2177** - Reports Creation Date field in the SecurityIQ website displays "Invalid Date" or an incorrect date
16. **SIQETN-2178** - RabbitMQ Crawler Engine fails near completion when running over 3 hours
17. **SIQETN-2157** - RabbitMQ fails to start when installed on a path with spaces which is not on the system drive

Service Pack 2

18. **SIQETN-2206** - Excel data classification does not extract number fields
19. **SIQDEV-4850 -** No permissions displayed for folder after PC task
20. **SIQETN-2203 -** EMC Isilon Activity Monitor: Short path expansion(path with tilde) can cause delays in event reader thread
21. **SIQETN-2225 -** Elasticsearch Reindex Events task fails on JSON parsing error
22. **SIQETN-2111 -** Box - No Events received
23. **SIQETN-2197 -** Slow service startup can cause windows service start failure
24. **SIQETN-2231 -** Unable to normalize folder because error finding domainData in cache by DomainName
25. **SIQETN-2232 -** Events stuck in the Event Collector queue because of Classification replication across DFS link targets
26. **SIQETN-2234 -** Data Classification Rule Using "Contains None of" Works as "Contains Any/All of"
27. **SIQETN-2235 -** Automatic Access Fulfillment task not being created for revocation of user membership in groups
28. **SIQETN-2236 -** WCF services fail to start on Operation Timeout error
29. **SIQETN-2048 -** Some group (role) nesting relationships can cause timeout exceptions

30. **SIQETN-2243 -** Data Classification: DB Delete fails with conflicted REFERENCE constraint when re-indexing
31. **SIQETN-2188 -** Collector Manager - Installation fails when service account password contains double quotes
32. **SIQETN-2249 -** SharePoint IIS logs can't be read when a non-log / badly formatted file exists in the log folder
33. **SIQETN-2122 -** Permissions which are no longer relevant are not properly deleted
34. **SIQETN-2073 -** Campaign report performance
35. **SIQETN-2247 -** Google Drive events can't be parsed, ArgumentOutOfRangeException
36. **SIQETN-2257 -** Security Update for the "getConfigFields" function
37. **SIQETN-2258 -** Default Password for admin client AD authenticated users
38. **SIQETN-2263 -** Uploading a malformed upgrade package could cause a malicious file to be extract to the user interface server local drive
39. **SIQETN-2254 -** Restricting communications to TLS 1.2 prevents RabbitMQ communications
40. **SIQETN-2198 -** Data Owner and Resource Dashboards Loading Failed
41. **SIQETN-2264 -** Remove decryptString method from User Interface API
42. **SIQETN-2265 -** User Interface Security Updates
43. **SIQETN-2259 -** Permission Collection likely to timeout with long running Identity Sync
44. **SIQETN-2260 -** Google Driver Permission Collection with Collector fails to collect permissions if crawler has not been run while Collector service has been running
45. **SIQETN-2268 -** Wrong Max Recursion syntax on Permission Collection on a specific BR
46. **SIQETN-2269 -** Permission queries for DFS Applications can cause high CPU usage
47. **SIQETN-2248 -** Crawler exclusion regex doesn't prevent the Crawler from trying to access site collections
48. **SIQETN-2237 -** Data Classification Performance Enhancements - Post 6.0 release

Service Pack 3

49. **SIQETN-2209** – Data Classification Results do not include all DFS resources when filtering by DFS app or app type
50. **SIQETN-2273** – NetApp CIFS 7-Mode + Tunneling - Permission Collection doesn't work
51. **SIQETN-2294** – Business Website fails to load (timeout) - due to long running query for Data Owners resources.
52. **SIQETN-2296** – Poor Performance in delete activities and cleanup task
53. **SIQETN-2297** – Exchange Online crawler unable to retrieve mailboxes
54. **SIQETN-2298** – Sensitive Account Exclusions causes erroneous "must_not" ES clause (missing comma)
55. **SIQETN-2322** – Permission Collection fails for NetApp C-mode with Load Sharing Mirror Volumes
56. **SIQETN-2336** – New Access Requests - Always shows DFS as requestable
57. **SIQETN-2338** – New Access Request - Application has defunct access request template after template deletion
58. **SIQETN-2343** – Website Dashboard, Database and KPI Improvements
59. **SIQETN-2344** – Data Classification Services (Engine or Collectors) crash with Access Violation exception
60. **SIQETN-2359** -Data Classification Keyword policy objects contain empty values and colons
61. **SIQETN-2342 -** Sharepoint Online Permission Collection - ignore site collection exclusions

3.3.5. E-Fixes Detailed Description

Service Pack 1

3.3.5.1. SIQETN-2114

Add local time for email alerts from activity monitoring

When sending an email alert based on activity monitoring, the time of the event is displayed in UTC. Adding Local Time to email alert signifying the local time zone.

3.3.5.2. SIQETN-2117

Role Path does not show in the User Membership in Groups results in Admin Client

When running an Identity query on User Membership in Groups,

The Role Path / Group Path field, indicating the role hierarchy that relates the user to a group, is not being populated.

3.3.5.3. SIQETN-2119

Resources created by Activity Monitoring, may be created with wrong hierarchies or appear as roots

Activity Monitoring may generate Business Resources if a captured activity event does not have a corresponding BR. In some case, these BRs are created with the wrong hierarchy.

This mostly occur in Windows Cluster fileserver Applications, but has the potential to affect other agents.

3.3.5.4. SIQETN-2120

Not operators aren't working for WPC fields in Activity Forensics page on the Web UI (Not Contains, Not starts with, etc.)

When creating a filter on the Activity Forensics screen with one of the NOT operator (Not in, Not contains, Not equals, etc.) on one of the WPC fields, the filter does take effect and results are not filtered.

3.3.5.5. SIQETN-2122

Old / Irrelevant Permissions are not being properly deleted by the Permission Collection task

As part of the Permissions Collection process permissions that are no longer relevant are removed from the database. Some permissions were missed by that process, resulting in an accumulation of redundant permissions and unwanted DB growth.

3.3.5.6. SIQETN-2129

Resources are created with plain drive letters

When performing activities on cluster nodes from a remote computer (e.g. \\server-fs\share\...), resource will occasionally get created with a physical path and so new cluster share node will be created in the form of colon suffixed drive letters (e.g., "F:\").

3.3.5.7. SIQETN-2132

NetApp mount points are not being crawled

NetApp mount points, as opposed to shares, are being excluded / ignored during the crawl process.

3.3.5.8. SIQETN-2135

Exchange activity not getting AD enriched

When the activity domain property returned by the identity object in exchange is not set to a NETBIOS name, the referenced domain is not fetch and the activity is not being enriched.

3.3.5.9. SIQETN-2136

SIQETN-2136 - Reports generation fails occasionally reporting index out of range exceptions in the log.

3.3.5.10.SIQETN-2139

SIQETN-2139 - Hierarchical queries are limited to 100 recursive loops

By default, SQLServer hierarchical queries are limited to 100 nested levels. If the nesting degree in a query exceeds 100 levels, the query fails. This may affect permission, role data queries and reports, among others.

3.3.5.11.SIQETN-2152

SIQETN-2152 - Permission Collection and Data Classification services taking too long to start can timeout and stop

Permission Collection and Data Classification Engine and Collector services, may take too long to start and load, due to various reasons. In some cases, they may exceed the service startup timeout period, and fail to start.

3.3.5.12.SIQETN-2153

SIQETN-2153 - SharePoint IIS logs defined to be written under an explicit local path in a multi-server farm aren't collected in Automatic mode

For SharePoint events, IIS logs are used to get view events. Those logs default to a path under %SystemDrive%. When working in Automatic mode with a multi-server farm, this path is retrieved and %SystemDrive% is replaced by a UNC to the server's administrative share representing the system drive. If the logs are set to an explicit local drive (i.e. C: or D, the path is not parsed to a UNC, which means the logs remain unreachable.

3.3.5.13. SIQETN-2128

SIQETN-2128 - Group Membership information for an activity is not being enriched, if the group name contains specials character (e.g. brackets)

3.3.5.14.SIQETN-2174

SIQETN-2174 - Cannot set data owners to a DFS resources containing special characters

Setting a data owner to a DFS business resource, whose name contains special characters (e.g. underscore ("_")) fails. Though it appears to be working it does not take hold and does not appear after restarting the client and in the web UI.

3.3.5.15.SIQETN-2177

SIQETN-2177 - Reports Creation Date field in the SecurityIQ website displays "Invalid Date" or an incorrect date

When opening the SecurityIQ Website and navigating to Reports → My Reports, the Reports table displays reports with "Invalid Date" (or some incorrect date) as their Creation Date field.

This is caused by different language cultures interpreting the date string coming back from the server wrong.

3.3.5.16.SIQETN-2178

SIQETN-2178 - RabbitMQ Crawler Engine fails near completion when running over 3 hours

In environments with RabbitMQ installed, crawler tasks that run for more than three hours may fail, due to defunct queue channels.

3.3.5.17.SIQETN-2157

SIQETN-2157 - RabbitMQ fails to start when installed on a path with spaces which is not on the system drive

When installing SecurityIQ services to a path with spaces on a drive other than the system drive (e.g. E:\Program Files\SailPoint), RabbitMQ fails to start properly, which causes it to rollback the installation. This is a defect in either RabbitMQ or Erlang (which RabbitMQ uses as a framework).

Service Pack 2

3.3.5.18.SIQETN-2206

SIQETN-2206 - Excel data classification does not extract number fields

Extracting contact from Excel files ignore date and number fields
After applying the fix, the documentExtractorOptions app.config key needs to be uncommented, and its value should be EXCELMODE=CSV

3.3.5.19.SIQDEV-4850

SIQDEV-4850 - No permissions displayed for folder after PC task

Permission Collection tasks creates empty ACL sets in the DB

3.3.5.20.SIQETN-2203

SIQETN-2203 - EMC Isilon Activity Monitor: Short path expansion(path with tilde) can cause delays in event reader thread

Isilon BAM running out of memory due to events were backing up due to the event activity path containing a tilde(~), which results in an attempt to resolve the path to it's long name, assuming it could be a legacy 8.3 folder path. 3-minute delays for each resolution were observed although wasn't necessary

3.3.5.21. SIQETN-2225

SIQETN-2225 - Elasticsearch Reindex Events task fails on JSON parsing

When running the Elasticsearch ReIndex Events task, the task throws JSON parsing errors, which causes the task to fail. This may be caused by some event information the contain unescaped or un-pars-able data

3.3.5.22.SIQETN-2111

SIQETN-2111 - Box - No Events received

No Events received in Box application

3.3.5.23.SIQETN-2197

SIQETN-2197 - Slow service startup cause windows service start failure

Slowness in this initialization from slow network, or during machine startup when many services are starting at the same time, etc. may cause the service to be forcefully stopped by the windows service controller. Windows expects control to be returned relatively quickly when initializing and starting a service instance

3.3.5.24.SIQETN-2231

SIQETN-2231 - Unable to normalize folder because error finding domainData in cache by DomainName

Error in CollectorSynchronizer during access fulfillment where it is unable to find the active directory domain data based on the created connection pools

3.3.5.25.SIQETN-2232

SIQETN-2232 - Events stuck in the Event Collector queue because of Classification replication across DFS link targets

If a DFS application exists, events for resources that are DFS link targets get Classifications from the resource as well as other targets of the same link. This mechanism copies the classifications between different targets of the same link when a relevant event arrives, and caches the results, but the act of retrieving the link targets requires DB access, which can slow the process down considerably. This mechanism is now retired

3.3.5.26.SIQETN-2234

SIQETN-2234 - Data Classification Rule Using "Contains None of" Works as "Contains Any/All of"

Data Classification Rule Using "Contains None of" Works as "Contains Any/All of" due to an operator mismatch

3.3.5.27.SIQETN-2235

SIQETN-2235 - Automatic Access Fulfillment task not being created for revocation of user membership in groups

Access Certification campaign on user membership in groups is not generating an automatic fulfillment task, even though campaign is set with auto fulfill and the IC enables fulfillment

3.3.5.28.SIQETN-2236

SIQETN-2236 - WCF services fail to start on Operation Timeout error

Starting a WCF service (discovered on a PC Enginer) fails on startup, with an Operation Timeout error - trying to connect to the WCF Server endpoint

3.3.5.29.SIQETN-2048

SIQETN- Some group (role) nesting relationships can cause timeouts

Starting a WCF service (discovered on a PC Enginer) fails on startup, with an Operation Timeout error - trying to connect to the WCF Server endpoint

3.3.5.30.SIQETN-2243

SIQETN-2243 - Data Classification: DB Delete fails with conflicted REFERENCE constraint when re-indexing

Re-running the data classification job that should re-index, then delete results that are no longer needed (excluded). It still fails with a Reference Constraint (FK) error

3.3.5.31.SIQETN-2188

SIQETN-2188 - Collector Manager - Installation fails when service account password contains double quotes

When trying to install an agent which requires a service account, entering a password which contains double quotes (") results in failure.

Errors vary from none at all to seemingly permission related. Switching the log level to DEBUG can help identify this bug by looking for the first instance of "addInstance, Result code" (without quotes) and seeing things like 1639 - Invalid command line argument, or any other error which looks like bad arguments were provided

3.3.5.32.SIQETN-2249

SIQETN-2249 - SharePoint IIS logs can't be read when a non-log / badly formatted file exists in the log folder

To get View events for SharePoint applications, the BAM has to read the IIS logs on the SharePoint farm servers. If a new file appears in the IIS log folder, which is either not a log file or can't be read for fields, it effectively stops the log reading process until both of the following conditions happen in order:

1. A new proper log file appears in the folder.
2. The BAM service is restarted

3.3.5.33.SIQETN-2122

SIQETN-2122 - Permissions no longer relevant are not properly deleted

Part of the Permissions Collection process is removing permissions which are no longer relevant from the database. This part at times may miss permissions, resulting in an accumulation of redundant permissions and unwanted DB growth

3.3.5.34.SIQETN-2122

SIQETN-2122 - Permissions no longer relevant are not properly deleted

Part of the Permissions Collection process is removing permissions which are no longer relevant from the database. This part at times may miss permissions, resulting in an accumulation of redundant permissions and unwanted DB growth

3.3.5.35.SIQETN-2073

SIQETN-2073 - Campaign report performance enhancements

3.3.5.36. SIQETN-2247

SIQETN-2247 - Google Drive events can't be parsed, resulting in an ArgumentOutOfRangeException

When User1 in Google Drive shares content with User2, User2 is able to see that content in their Shared With Me screen. User2 can choose to map the content to their own drive, but they can also choose not to, in which case the content will still be available through the Shared With Me screen. In this case, the path to the content through User2 would not have a true root folder as a parent. When User2 performs an action on User1's content, one of the fields SIQ tries to populate is User2's access path to the content, but since there's no root folder in the path when looking through User2, the path is not properly parsed and is left blank. This causes an ArgumentOutOfRangeException when trying to access this path

3.3.5.37.SIQETN-2257

SIQETN-2257 - Security Update for the "getConfigFields" function

Method signature should receive config field type identifier

3.3.5.38.SIQETN-2258

SIQETN-2258 - Default Password for admin client AD authenticated users

Default password may be used under certain conditions on Admin Client login screen

3.3.5.39.SIQETN-2263

SIQETN-2263 - Uploading a malformed upgrade package could cause a malicious file to be extract to the user interface server local drive

Uploading a malformed upgrade package which contains unique characters in the file path causes the user interface to extract the file into a specific folder, and the file is not deleted after the package was discovered as malformed

3.3.5.40.SIQETN-2254

SIQETN-2254 - Restricting communications to TLS 1.2 prevents RabbitMQ

When restricting communications to TLS 1.2 on Windows, Engines and Collectors for both PC and DC can't communicate with RabbitMQ

3.3.5.41.SIQETN-2198

SIQETN-2198 - Data Owner and Resource Dashboards Loading Failed

Data Owner and Resource Dashboard load time is exceedingly long and eventually times out which causes the dashboard page load to fail

3.3.5.42.SIQETN-2264

SIQETN-2264 - Remove decryptString method from User Interface API

Data Owner and Resource Dashboard load time is exceedingly long and eventually times out which causes the dashboard page load to fail

3.3.5.43.SIQETN-2265

SIQETN-2265 - User Interface Security Updates

Security enhancements for the User Interface service

3.3.5.44.SIQETN-2259

SIQETN-2259 - Permission Collection times out with long running Identity Sync

The RoleAnalyticsEngine creates and monitors the identity sync task, but it uses a hard-coded 10-minute timeout, which is too low and unnecessary

3.3.5.45.SIQETN-2260

SIQETN-2260 - Google Driver Permission Collection with Collector fails to collect

The GoogleDriveInterface creds may require a certificate, but during a Permission Collection task, the GoogleDriveRACollector never sets the static ServiceAccountCertificate property

3.3.5.46.SIQETN-2268

SIQETN-2268 - Wrong Max Recursion syntax on Permission Collection on a specific BR

Running a permission collection on a specific BR fails with wrong syntax on MaX Recursion clause

3.3.5.47.SIQETN-2269

SIQETN-2269 - Permission queries for DFS Applications can cause high CPU usage

Running permission queries on the Admin Client or permission reports can cause the DB server to load the CPU, causing slowdowns and hangs for everything trying to talk to the DB

3.3.5.48.SIQETN-2248

SIQETN-2248 - Crawler exclusion regex doesn't prevent the Crawler from trying to access site collections

The Crawler exclusion regex is used after fetching the Application's root resources to filter out resources we don't want to crawl. In SharePoint's case, we try to access each root site collection we find to collect information for later stages, but some of this information is gathered from the content databases, to which the Crawler would be denied access if not permitted. This won't fail the Crawl task, but problematic as the Crawler attempts to access those site collections if they are excluded.

3.3.5.49.SIQETN-2265

SIQETN-2237 - Data Classification Performance Enhancements - Post 6.0 release

3.3.5.50.SIQETN-2209

Data Classification Results do not include all DFS resources when filtering by DFS app or app type

A bug was found in the optimized stored procedure _get_classification_results_by_filter_dfs_ when filtering by DFS app type or DFS app in the forensics data class page, only 1 link hierarchy of results is fetched.

3.3.5.51.SIQETN-2273

NetApp CIFS 7-Mode + Tunneling - Permission Collection doesn't work

NetApp PC can now deal with the 7-mode + tunneling scenario after accounting for a null member.

3.3.5.52.SIQETN-2294

Business Website fails to load (timeout) - due to long running .getOwnedResources

The issue was caused by an inefficient fetch of the data owner's resources in order to determine whether or not the user is a data owner.

The fix involved running optimized queries to determine that, instead of fetching on the resources and parsing through them.

3.3.5.53.SIQETN-2296

Poor Performance in delete activities and cleanup task

Performance fix for deletion of events. An updated approach to deleting events to improve performance.

3.3.5.54.SIQETN-2297

Exchange Online crawler unable to retrieve mailboxes

After successful queries of all mailboxes, subsequent crawlers fail with following error:

System.Management.Automation.CmdletInvocationException: No valid sessions were specified. Ensure you provide valid sessions that are in the Opened state and are available to run commands.

3.3.5.55.SIQETN-2298

Sensitive Account Exclusions causes erroneous "must_not" ES clause

When a behavior rule, and a sensitive account exclusion are defined, the elasticsearch query that is generated includes a "must_not" clause, that is missing a preceding comma.

3.3.5.56.SIQETN-2322

Permission Collection fails for NetApp C-mode with Load Sharing Mirror Volumes

When trying to run a Permission Collection task on a NetApp Vserver which makes use of Load Sharing Mirror Volumes, the Qtree fetch fails with a duplicate key in the dictionary. This is because the qtree is basically duplicated across multiple physical nodes and has the exact same path.

A Load Sharing Mirror Volume is a volume in a NetApp storage cluster which mirrors another volume for load-balancing purposes. They are read-only and are recommended as a best practice for root volumes.

3.3.5.57.SIQETN-2336

New Access Requests - Always shows DFS as requestable

DFS always is displayed as requestable resource, even if the only Access Request Template defined does not include DFS.

3.3.5.58.SIQETN-2338

New Access Request - Application has defunct access request template after template deletion

When an application is added to the system after an Access Request Template has been defined, then application added to the template: When the template is deleted, the application is not updated.

(in table bam, the column access_request_template_id is still set to the deleted template)

This causes the application to be listed as requestable in the SIQ website.

3.3.5.59.SIQETN-2343

Website Dashboard, Database and KPI Improvements

Performance enhancements to the KPI Dashboards. Enhancements include:
Resource Dashboard is removed from the Business Website

Data Owner Dashboard now retrieves KPI information from the pre-calculated KPI Data, calculated by the Dashboard Widgets Calculation Scheduled Task, that runs nightly.

Improved Database Statistics calculation algorithm included in the DB Cleanup Task.

Improved Website single-session requests concurrency – concurrent request no longer blocking each other on long-running requests.

3.3.5.60. SIQETN-2344

Data Classification Services (Engine or Collectors) crash with Access Violation exception

Data Classification services that use the Hyland libraries to read file content - crash with Access Violation errors in what seems to be a random manner.

The issue is caused by a bug in the Hyland libraries that causes them an Access Violation exception, which causes their component to crash and crash our services.

3.3.5.61.SIQETN-2359

Data Classification Keyword policy objects contain empty values and colons (:)

Some Data Classification Policy Object include empty values and colons which may cause parsing errors.

3.3.5.62.SIQETN-2342

Sharepoint Online Permission Collection - ignore site collection exclusions

When trying to gather permissions and local users and groups, the PC engine lists all site collections and ignores site collections excluded by regex..