File Access Manager

Forensics

Version: 8.3 Revised: March 29, 2022

Contents

Forensics Introduction

The forensics' screens allow the administrators to view analysis screens of data collected by the File Access Manager services. The tables can be filtered to fit specific needs, and filters can be saved, and shared with others as well.

The File Access Manager website has the following forensics' screens:

- Activity forensics
- Permissions' forensics
- Identities' forensics
- Data Classification forensics

Forensic queries can be used to answer questions such as:

- Who has accessed files classified as Credit Cards?
- Who can access folders classified as SSN?
- Are there users without a password in the system, or users who haven't logged in for the past six months?

Forensics Types

There are four Forensic types:

- Permissions
- Identities
- Activity
- Data Classification

Using Permission Forensics

The Permission Forensics screen lets the user monitor and analyze the user and group permissions. On this screen you can create queries to analyze the permissions of specific groups of users, save and share queries for selecting users and groups, generate reports, run permission scans, and revoke explicit permissions of users.

This page supports reports and campaigns.

This component answers questions, such as:

- Which users have access to what resources?
- Which users have not used permissions granted to them?
- Which permissions were granted to each group?
- Which groups are not being used?

The table displays the permissions, according to the level of granularity selected in the filter.

When creating a filter, you can define the granularity of the report using the **View by** field, and can mark stale permissions on the table, according to the unused time selected.

> The query will retrieve the first 100,000 results. Narrow the search to obtain a better fit.

Reports

See Generating Reports

Filters

See Filters: Creating and Editing a Forensics Query

Viewing Permission Forensics

The Permission Forensics table displays the permissions retrieved by the query run.

The data displayed, by default, includes the following columns for each permission:

- What resource
    - Business resource full path
    - Application
- Who the user is
    - User name
    - User display name
    - Group name
    - User domain
    - Group domain
    - User entity type
    - Group entity type
- The permission type
    - Permission type
    - Classification Category
    - Is Inherited
    - Inherits Permissions
    - ACL Type Allowed?

To change the order of the columns, drag the column titles.

Additional columns available are:

Application group, Application type, Business Resource Logical Path, Business Resource Name, Business Resource Type, Creates Loop, Creation Timestamp, Cumulative Last Used, Department, Distinguished Name, Group Path, Is Effective, Is Owner Permission, Is Riskiest, Is, SID History, Last Login Date, Last Used Date, Loop Path, Password Never Expires, Password Not Required, Permission Type Description, User Disabled, User Email, User Locked

To select columns to display:

1. Click the Column chooser icon on the table header bar.
2. Select the columns to display from the drop down list.
    - Click **Show All** / **Show Less** to display a full list of columns / only the default columns in the column chooser. This does not change the selection of columns to display in the table.

- User the search field to narrow down the list of columns in the column chooser.
- Click **Reset Columns** to reset to the default selection and order of the columns in the table.

View by

You can change the granularity of the output by selecting the View By type. These options will determine whether to check a user's direct permissions , or permissions granted by groups the user belongs too, as described below:

- Groups & Users direct Permissions

This view displays direct Users' and Groups' permissions but does not display the Group members.

- Users direct & Group membership Permissions

This view displays user permissions based on direct permission, group membership, and nested group membership. This view doesn't list the users in the groups Everyone and Authenticated Users.

- Everyone Groups expanded, Users direct & Group membership Permissions

This view displays user permissions based on direct permission, group membership, and nested group membership, including listing the members of the Everyone and Authenticated Users groups.

> The default view is the Users and Groups view.

> In the permission forensic screen, the View By field can be changed after setting or restoring the filter

Mark Stale Permissions

Select the time period for stale permissions. The user permissions which were not in use for X time (configurable) will be marked in red.

Scope and Hierarchical Search

By default, when you select a business resource (BR) to scope its permissions, only the direct BR permissions (not the child BR permissions) displays.

Special Groups - Group Entity Type

When creating a filter, you can select the group entity type from the **Field** field.

In Windows-based environments, the user groups are *Everyone*, *Authenticated Users*, and *Domain Users*.

Everyone

Includes all users.

Authenticated Users

Includes all users without a guest.

Domain Users

Includes a group with all users in the domain. By default, any user created is a member of this group (but it is possible to remove that user).

Owner Permission Field

File Access Manager permissions forensics allows identification and tracking of Owner permissions in the AFM interface:

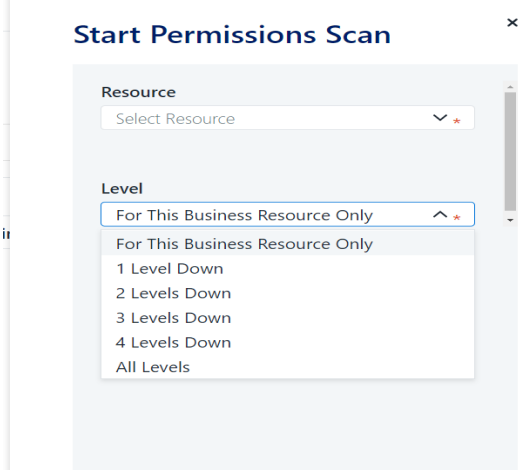
- A proprietary column, called “Is Owner Permission” indicates whether a given permission is an Owner permission.
- A proprietary query attribute is dedicated for filtering Owner permissions (allowing queries and/or reports listing the owners of resources).

Permission Scan for Business Resource

The Permission Scan collects the security information from the scanned BRs, and stores it in the File Access Manager database. This includes which users or groups have access to the BR, and whether the access is inherited. The permission scan stores access types such as read, write, full control, etc., depending on the application type.

When requesting a permission scan, you can set the resources to scan, and the number of levels below the requested BR to scan.

To perform a permission scan:



1. Open the Permission Forensics screen
   Forensics > Permissions
2. From the **Global Options** dropdown menu, select **Start Permission Scan.**
3. This will open the Permission Scan panelSelect the scan level:

- This Business Resource only
- This Business Resource and levels 'Level 1-4' and 'All Levels'

4. Click **Scan** to start the scan, or **Cancel** to return to the Permission Forensics screen.

DFS Support

- For DFS resources, the Permission Forensics table will show the physical, as well as the logical path of resources.

- You can create a filter for DFS resources by logical path only. To select a logical path, select **Resource** on the **Select Field** drop down menu, then navigate to the required path on the resource tree on the **Select Resource** dropdown menu. (See Searching for Resources Using a Resource Tree).

Removing Explicit Permissions Using the Permission Forensics Page

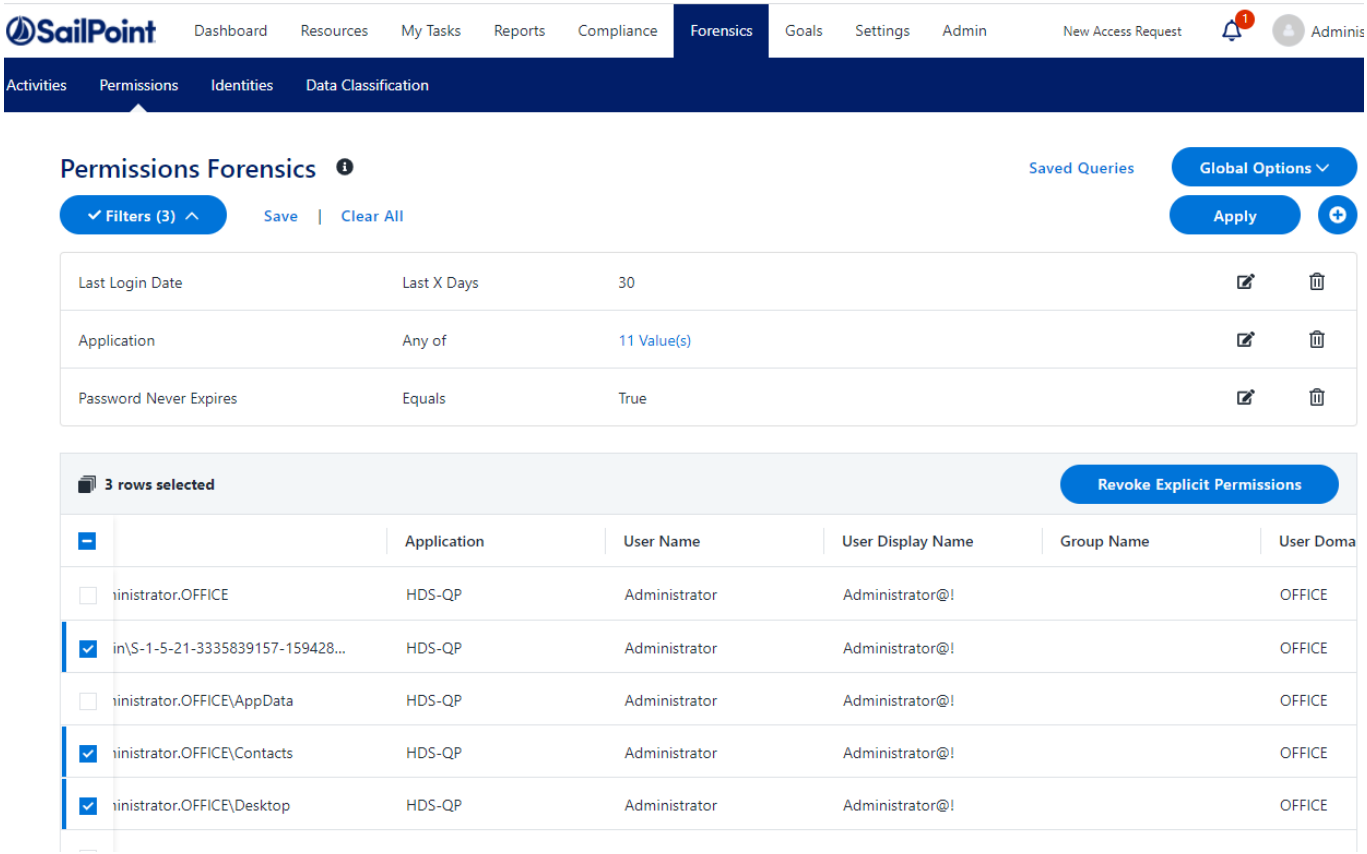
> This process will revoke explicit permissions from non-normalized resources that are configured for access fulfillment. Permissions that are inherited will not be removed.

1. Navigate to **Forensics > Permissions.**
2. Set a filter, as described in Filters: Creating and Editing a Forensics Query.
3. Click **Apply** to run the filter.
4. Set the View to **Groups and Users direct permissions**.
5. In the permission results, select the permission rows to remove, by clicking the checkbox on the row.

   Before selecting which permissions to remove, be sure that:

   - The Application in which the BR resides is configured to support Access Fulfillment for Direct Permission Removal. Configuration has additional information on how to configure removal of explicit permissions.
   - The permission is defined directly on the BR (the value in the **Is Inherited** column is “False”).
   - The selected permission is not a normalized group, created and managed by File Access Manager.

6. Click **Revoke Explicit Permissions**.

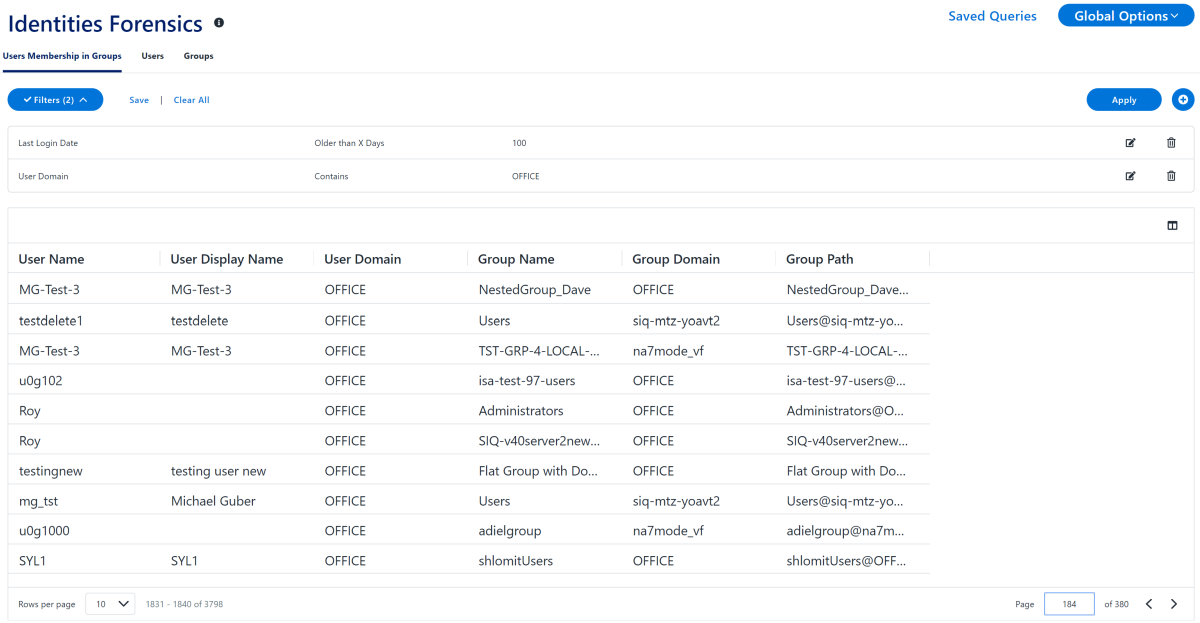


Identity Forensics

Navigate to **Forensics > Identities**.

The Identities Forensics screen displays users, groups and their relationship recorded by the system. Use filters to focus on specific data, The page supports reports and campaigns.

The displayed output is limited to the first 100,000 results.



Tabs

> Each tab has a separate filter and stored query list.

Select the tab to display different data about users, groups and their relationship.

Users' Membership in Groups

View of users and their group memberships;.

Users

This tab displays users and their attributes, defined in the identity store.

Groups

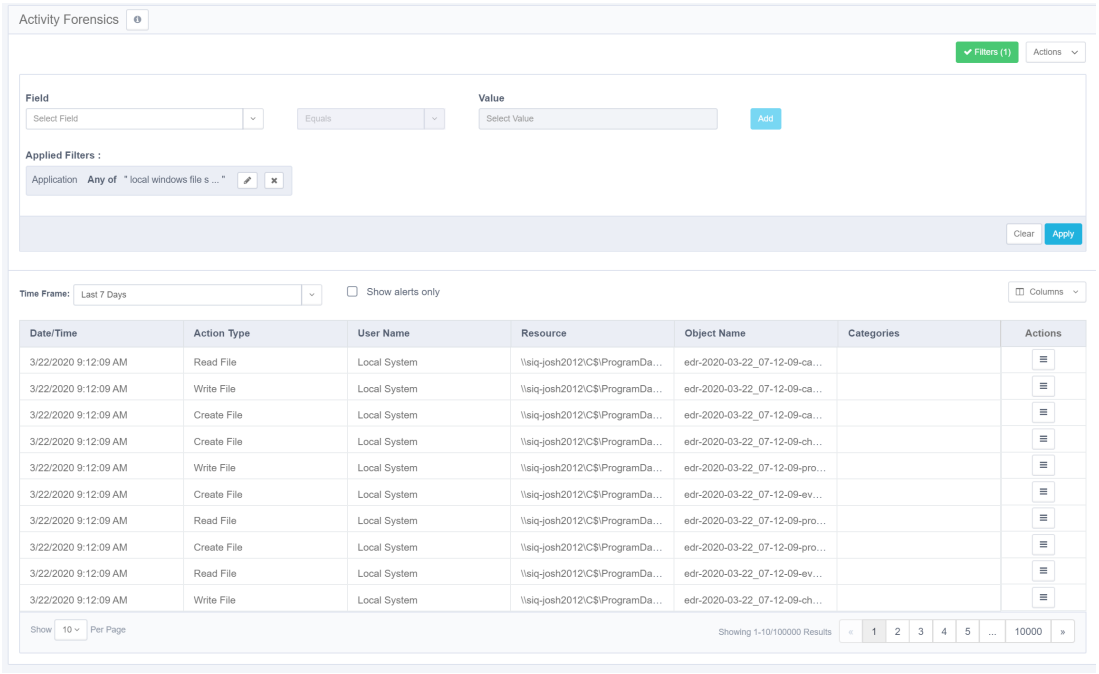
This tab displays groups and their attributes, defined in the identity store.:

Identity queries involve identity stores connected to File Access Manager, regardless of the permissions attached to these identities.

Activity Forensics

To locate the Activity Forensics page, navigate to **Forensics > Activity**.

The Activity Forensics page can be used to track user activities in various areas of interest. For example:

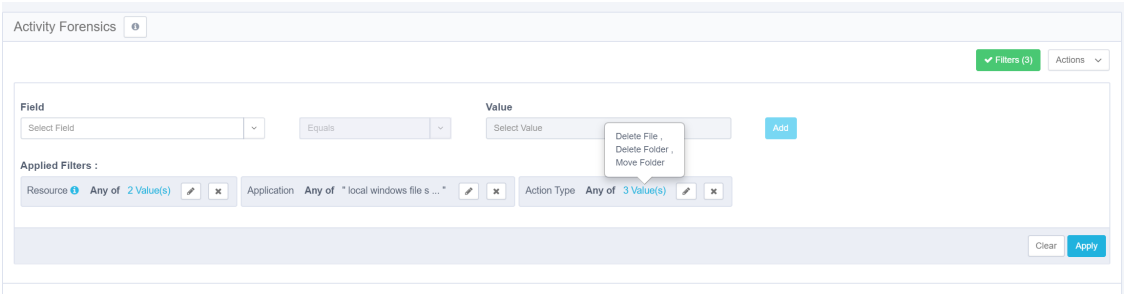


Filter

The activity forensics filter allows users to focus on set scenarios and areas of interest.

When you open the activity forensics page, it will load with the last query used.

The query is composed of one or more filters, combined with an **and** operator.



Creating a Query

1. Create a filter.
    a. Select a field from the field dropdown list.
    b. Select an operator
    c. Select or type in a value. For multiple values, start typing part of the value, and select items from the dropdown list by ticking the checkbox next to each item.
2. Click **Add** to add this filter to the query list
3. Repeat to add additional filter items to the query
4. Click **Apply** to run the query, and display the results

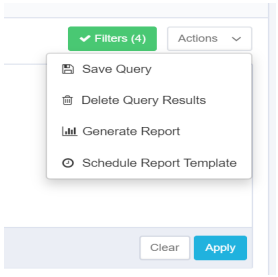
Common Activity Forensics filter fields

Action type	
Application	From the applications connected and monitored by File Access Manager
Application type	
Category	As assigned by the data classification module
Object name	
Resource	Specific folder or folders to monitor
User	

Storing and Sharing Queries

The 10 last queries are stored for reuse, with the query timestamp as the name.

You can store queries for later use, with a meaningful name, with the option of sharing them with other users.



:

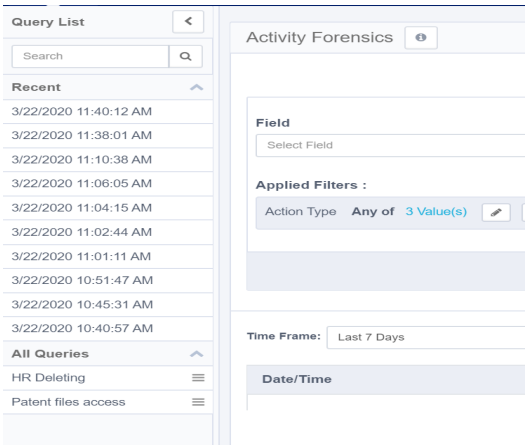
To store or share queries

1. Click the **Actions** dropdown menu on the top right corner.
2. Click **Save Query** to open the Save Query dialog box
3. Type in the query name, and , optionality, the name of a user(s) to share the query with.
    a. Start typing the user name. To add a user to the share list, click the **+** button.

Loading Stored Queries

To load a stored query, open the query list panel on the left side of the activity forensics page. You might have to click the restore button **>** , if this panel is minimized.

Click on a recent query, or a stored query to load the query, and apply it to the results.



Saving the Query to a Report

you can create a report out of an activity forensics query.

Select **Generate Report** from the **Activities** dropdown menu.

The report will be available in **Reports > My Reports**.

Creating a Scheduled Report from a Query

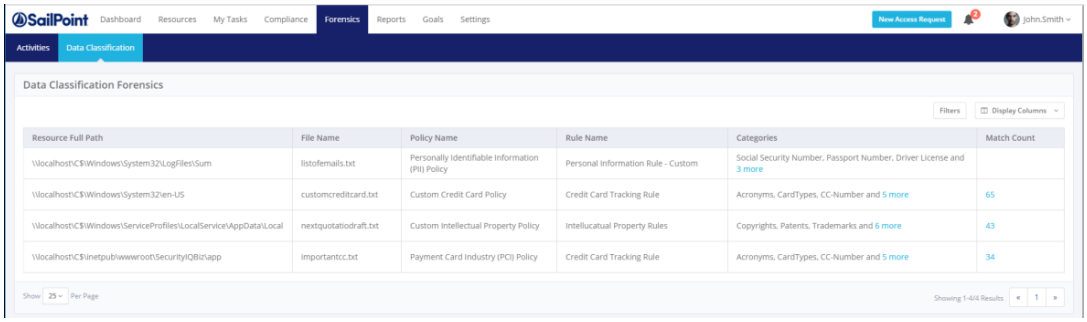
You can also create a repeated report from the query.

Select **Schedule ReportTemplate** from the **Activities** dropdown menu to open the Schedule Report Template panel.

Data Classification Forensics

The Data Classification Forensics screen can be found by navigating to **Forensics > Data Classification**. It displays data classification results, based on your active policies. Use filters to focus on specific data. You can sort the results by "Match Count". The returned records are limited to 10,000 results.

> The Data Classification Results table shows results of the data classification process running in File Access Manager, as well as any data classification results imported from an external source, using the Import Data Classification Results feature. This might lead to duplicate entries from the two sources.



Reports

Data Classification reports can be found in the report templates, using the *Classified Data* tag to locate relevant reports.

Using the Data Classification Forensics Table

Users can change one or more of the default columns by clicking on “Display Columns”, and selecting one or more columns from the dropdown menu.
Currently, all columns display, including the following:

Application

This column displays all the system applications.

Application Type

This column displays all the system application types.

Last Updated

This is the timestamp of the last classification process, in which the file was classified into the specified category.

Result Type

This is the source of the classification result (Content, Behavioral, or Imported Classification).

> The default column headings, from left to right, are: Resource Full Path, File Name, Policy Name, Rule Name, Categories, and Match Count. You can clear any selections made in the Policy, Rule, and Category search fields by clicking “Clear Selection” on the top right of each field

1. Select a result type from the Result Type dropdown menu.

All

All possible result types

Behavioral

Only results from behavioral rules

Composite Classification

Results from composite rules (Combining the results of several classifications)

Content

Only results from content rules

Imported

Normally, the administrative client imports the results from a Data Loss Prevention (DLP) product that has already scanned the results to control what data end users can transfer, so there is no need to rescan those results.

2. Type a number in both the Match Count (Bigger than) and the Match Count (Smaller than) fields to restrict the number of Regular Expression (Regex, the general standard for textual search) results.

> Users can see the resources according to the user scope they have.

A result record represents the classification of a certain file by file, rule and policy. A single file can be classified into multiple rules/policies, resulting in a separate record in the result for each file-to-rule-to-policy relation.

The result record consists of default columns, which can be changed, based on the users' requirements:

Resource Full Path

This is the full path of the resource in which the file resides.

File Name

This is the name of the classified file.

Policy Name

This is the name of the policy, by which the file is classified.

Rule Name

This is the name of the rule, by which the file is classified.

Category

This is the classification category name used by the rule.

Match Count

This is the maximum number of matches under any rules requirements contained in the file . This is not an aggregative figure, and does not sum up the number of matches in each of the rule requirements for the file. Instead, it represents the highest match count yielded by any of the rule requirements, and should be viewed as a sensitivity score attributed to the file, in accordance with the applicable policy rules.

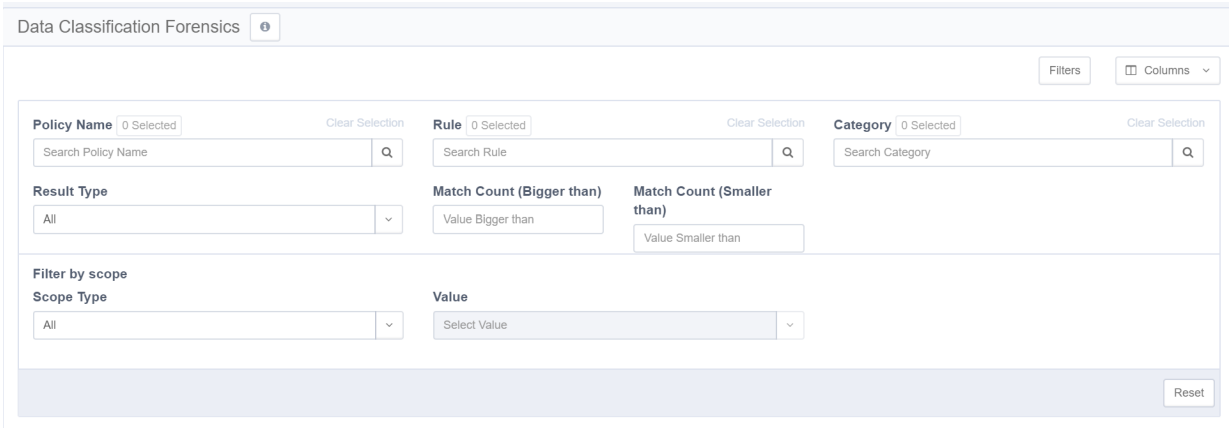
For example, if a policy rule contains two rule requirements – one matching credit card numbers with ten occurrences of credit card numbers within the same file, and another matching telephone numbers with eight occurrences of telephone numbers within the same file, the Match Count value of the file for that category (assigned by the rule) would be 10 (rather than 18, or 8), since it represents the maximum number of occurrences matching any of the rule requirements within that policy rule.
When the result displays a regular expression search, this field will be clickable and display the masked matches of the regular expression.

The query will retrieve the first 10,000 results. Narrow the search to obtain a better fit.

Filter

Complete the following steps to

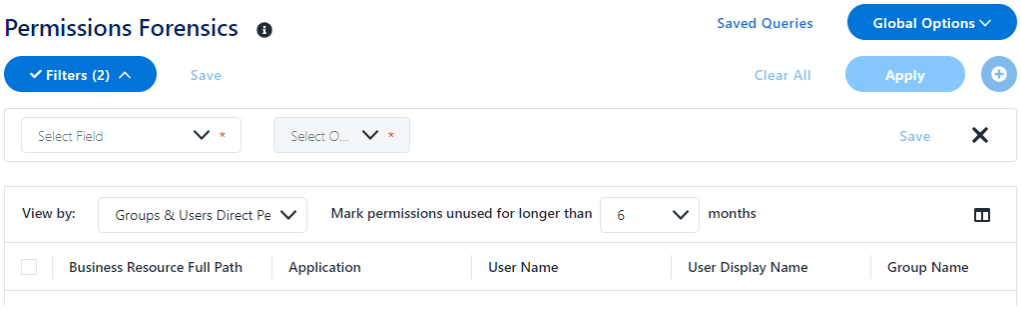
1. To filter data classification forensics:
    a. Click the “Filters” button at the top right of the screen.
    b. The filter screen displays.



The forensics results can be filtered by:

- Policy Name
- Category
- Rule Name
- Result Type (All, Content, Behavior, Imported)
- Match Count (Bigger than/Smaller than)
- Filter by Scope
    a. Select a scope type (Application type, Application, or Resource) from the Scope Type dropdown menu.
    b. Select a corresponding resource from the Resources dropdown menu.
    You can clear a selection from this dropdown menu by clicking “Clear Selection” on the top right of the menu.
    c. Click Reset at the bottom left of the filtering screen to apply all the selected filters.

Filters: Creating and Editing a Forensics Query



A query is a collection of one or more filters that let you select from a list of parameters to select user types, permissions, user scenarios or permission scenarios to analyze.

1. Click **Clear All** to clear the current filters, and clear the grid.
2. Click **+** to add a filter to the query.
3. Select a field to filter by from the **Select Field** dropdown menu, and the filter criteria, according to the filed type and parameters.
4. Click **Save** to add the filter line to the query, or Cancel to start over.
5. Add more filter lines by repeating these steps as required.

   For example:

   ```
   "Last login date older than 100 days
   and
   Password not required equals True”
   ```

6. Click **Apply** to run the query.

> For Permission Forensics, the data retrieved depend on the user scope of the user running the query. The data returned will only be within the applications and resources within each application to which the user running the query has access.

> A Query can be deleted only by the user who created it.

To search for resources using a resource tree

You can add resources for the filter by navigating down the resource tree and selecting the requested branch.

1. Open a new filter line
2. Select **Resource** from the **Select Field** drop down list
3. Open the **Select Resource** drop down menu to view the resource tree.

To save a query:

- Click **Save**. That will open a popup screen to enter the query name.
- Click **Save** or **Cancel** to continue.

To retrieve a saved query:

> If you select a saved query, the contents of your current query will be overwritten.

1. Click **Saved Queries**
2. Select a query from one of the saved query lists:
   - *Recent* – a list of your recently used queries. These queries are named and ordered by the timestamp.
   - *Saved* – a list of queries saved by the user.
   - *Shared* – a list of queries shared with the user.

   Clicking on a Query loads the filters and displayed columns for the Query. A Query object cannot be edited, and changes made after loading a Query do not impact the loaded Query object. However, these changes can be saved in a new Query.

To share a forensics query:

Sharing a query will make the query available in the quarry list of other users in this forensics screen.

1. Create a query as described above.
2. Click **Save**.
3. Type in a name for the query.
4. Type in the name or part of a name of the user to share the query with.
5. Select the user from the dropdown list.
6. Click **Save** to save the query to your list and the assigned user's query list.
7. The query will be stored in the other user's list under "**Shared**".

Generating Reports

To generate a report from the last run query:

1. Run a query as described above, or by selecting a saved query from the query list.
2. Select **Global Options > Generate Report**.
3. The report will be available in My Reports

To schedule and save a report template:

1. Run a query as described above, or by selecting a saved query from the query list.
2. Select **Global Options > Generate Report**.
3. Name the schedule, and fill in the scheduling parameters.