File Access Manager

User Guide

Version: 8.2 Revised: July 19, 2021

Contents

Contents ..... **iii**

Introduction **1**

The File Access Manager Web Interface 1

Data Owner Dashboards 1

File Access Manager Website User Types 1

Plain users 1

Auditor 1

Data Owners 2

Compliance Managers 2

Administrators 2

Users 2

Accessing the User Screens 3

Web Interface **4**

Navigation 4

Interface Languages 5

Navigating the Data Grid 6

Time and date format 6

Notifications 6

Dashboard **8**

Administrator Tab 8

Data Owner Tab 16

My Tasks **20**

Access Certification 20

Access Certification Task Details 22

Detailed Task Screen 22

Bulk Actions 24

Filters 24

View Graph 25

Access Request 27
Access Request Task Details 28
Owners' Election 29
Owners Election Task Details 29
Data Owners Election 29
Elected Data Owner Review 32
My Requests 33
My Requests Task Details 34
Reports **36**
Editing Scheduled Reports in the Administrative Client 36
Report Templates 36
Manage Report Tags 36
Report Mechanism 39
Report Operations 39
Report Editing 39
Report Actions 41
Compliance **42**
Access Certification 42
Access Certification Flow: How to Create And Run a Campaign 42
Campaign Management 43
Create a Campaign 47
General Details: 48
Filter Selection: 49
Review Process: 50
Fulfillment Process 52
Display Columns 54
Campaign Invitation 54
Reminder Emails 55
Access Certification – Create Campaign - Save 56

Campaign Templates 57
Create an Access Certification campaign based upon an existing Access Certification template 61
Alert Rules 63
Managing Alert Rules 63
Scope 64
Filters 65
Response 65
Resource-based Alert Rules 66
Troubleshooting Activities 66
Application 67
Activity Monitor Log 67
Event Manager 67
Events Backup 67
Threshold Alert Rules 69
Architecture and Flow 69
Limitations 69
Create/Edit a Threshold Alert Rule 69
Forensics 70
Filters: Creating and Editing a Forensics Query 70
Generating Reports 72
Permission Forensics 72
Viewing Permission Forensics 73
Scope and Hierarchical Search 74
Special Groups - Group Entity Type 74
Owner Permission Field 75
Viewing Identity Forensics Results 77
Tabs 78
Activity Forensics 78
Filter 79

Data Classification Forensics 81
Reports 82
Using the Data Classification Forensics Table 82
Filter 83
Goals 85
Running Goals 85
Completed Goals 89
Show Status 90
Resources Tab 92
The Election Tab 93
Creating Goals 94
New Access Request Wizard 100
Administrative Groups 101
Shares & Folders 104
SharePoint Resources 106
File Servers Tab 106
SharePoint Tab 107
Exchange Tab 107
Active Directory Tab 107
Other Applications Tab 107

Introduction

The File Access Manager Web Interface

The IdentityIQ File Access Manager is in process of migrating all functionality from the admin client to the IdentityIQ File Access Manager website.

The opening screen, for most users, is the data owner dashboard, which gives an overall view of the applications being monitored.

Data Owner Dashboards

Data owner dashboards are a collection of informational screens for business data owners. Data owners use their dashboards to answer the following questions:

- Who accesses data?
- Who has access to what data, and what actions can they perform on it?
- What sensitive data types reside within thse data?
- Who are the top active users of the data?
- What data / permissions are stale?
- In addition, data owners can:
    - Define which actions will trigger a notification to the data owner
    - Receive reports based on those notifications.

File Access Manager Website User Types

IdentityIQ File Access Manager is preconfigured with the following capabilities that can access the Web Interface. Additional capabilities can be created , according to the rights the different users require, with the assistance of SailPoint Professional Services or Partners.

Plain users

- The first screen that plain users see is My Tasks.
- Users can access the My Tasks and Reports tabs.
- Users handle ad hoc tasks, including:
- Reviewing Access Certification Campaigns and Access Requests
- Asking for permissions through the Access Request Wizard
- Viewing reports

Auditor

- The auditor capability is intended for users who perform internal audits, and assist in external audits, on user access information within the organization.

- See and manage all reports
- See and run the forensic screens

> This capability does not by default have permission to delete reports.

Data Owners

- The first screen that data owners see is **Dashboard**.
- Data owners can access the tabs **Dashboard**, **Resources**, **My Tasks**, **Reports**, and **Forensics**.
- Data owners handle ad hoc tasks but are also responsible for the data involved in those tasks. The Resources view displays problems to data owners for them to correct.

Compliance Managers

- The first screen that campaign managers see is **My Tasks**.
- Campaign Managers can access the tabs **My Tasks**, **Reports**, **Compliance**, **Forensics**, and **Settings**.
- Campaign managers handle the same ad hoc tasks as users.

Administrators

- The first screen that administrators see is Dashboard.
- Administrative users can access all screens.
- Administrators have the full scope meaning that they have access to all data.
- Administrators access everything that Data Owners access, including general settings, configurations, and the definition and management of crowd sourcing elections and goals.

Users

- -

Capability Screens	Administrator	Compliance Manager	Data Owner	Auditor
Dashboard	✓		✓a	
Resource	✓		✓	
My Tasks	✓	✓	✓	✓
Reports	✓	✓	✓	✓
Compliance	✓	✓ b		
Forensics	✓	✓ c	✓	✓
Goals	✓			
Settings	✓	✓d		

a. Data Owners see a limited version of the dashboards that is relevant to the capability

b. The Compliance Manager cannot access the **Alert Rules** under the **compliance** menu

c. Compliance Managers have access to the Data Classification Forensics page only.

d. Compliance Managers' access to the Settings screen is limited to the Access Certification Message Template

For a full description of the permissions set per capability, see the **web_permission** table in the File Access Managerdatabase.

The capabilities in your system can be modified, and new capabilities added by the administrators and implementation teams, and might differ from the table above.

Accessing the User Screens

Access is determined by the following:

- Rights the user has. These determine what the user can do in the web client, mostly in terms of screens the user can access and actions the user can perform on each screen. The users' rights are determined by the capabilities the user is associated with.
- Scope assigned to the user. Some screens on the IdentityIQ File Access Manager website have built in filters of content, according to the user scope, that determine what resources the user can see and act on.
    - Data Owner dashboard
    - Resources
    - Forensics
    - Reports and report templates

The user scope and user capabilities can be set by the IdentityIQ File Access Manager administrator.

Web Interface

This chapter describes the IdentityIQ File Access Manager websiteIdentityIQ File Access Manager website, together with its capabilities and main navigation procedures.

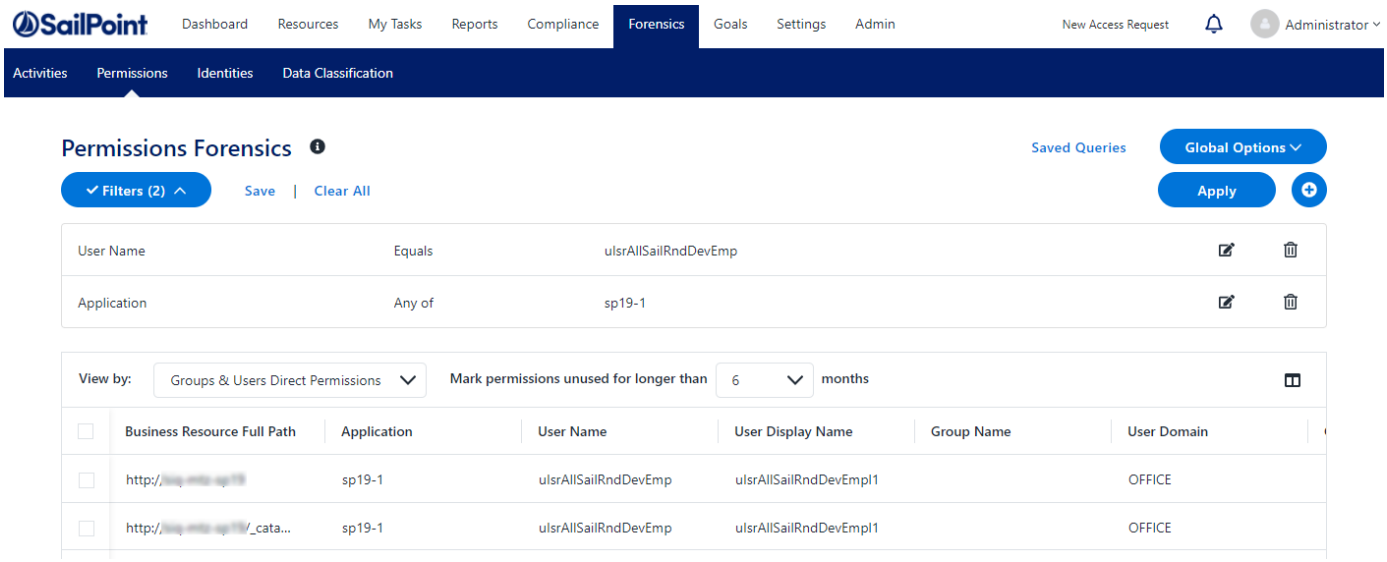
Navigation

This section describes the main user interface areas, as well as their content and purpose.

> If you click the “I” on any screen, a tool tip with a description of the screen is displayed.

The top left of the main screen features tabs for each of the primary tabs in the IdentityIQ File Access Manager website system, including the following:

- Dashboard
- Resources
- My Tasks
- Reports
- Compliance
- Forensics
- Goals
- Settings
- Admin



The top right portion of the main screen remains the same for all Navigation screens. It features (from left to right) a tab for a New Access Request (if enabled) and a menu with the user name and photo.

The main screen includes the following sections:

- New Access Request – Used to open the Access Request wizard (common to all screens (Dashboard, My Tasks, Resources, Settings, and Reports)
- Notifications – listing outstanding reports and requests
- User Name Tab
    - Change the interface language
    - About - File Access Manager and SailPoint copyright and patent information.

Interface Languages

The IdentityIQ File Access Manager website supports interfaces in the following languages :

Chinese (Simplified)	German
Chinese (Traditional)	Hebrew
Danish	Italian
Dutch	Japanese
English	Portuguese (Brazil)
French (France)	Spanish
French (Canadian)	Swedish

To change the interface language:

1. Click the arrow next to the user name on the top corner of the screen and select “Language”.
2. This will open the language selection screen (see image below). Select a language, and then click Save. The language will remain set until the next time you change the language.

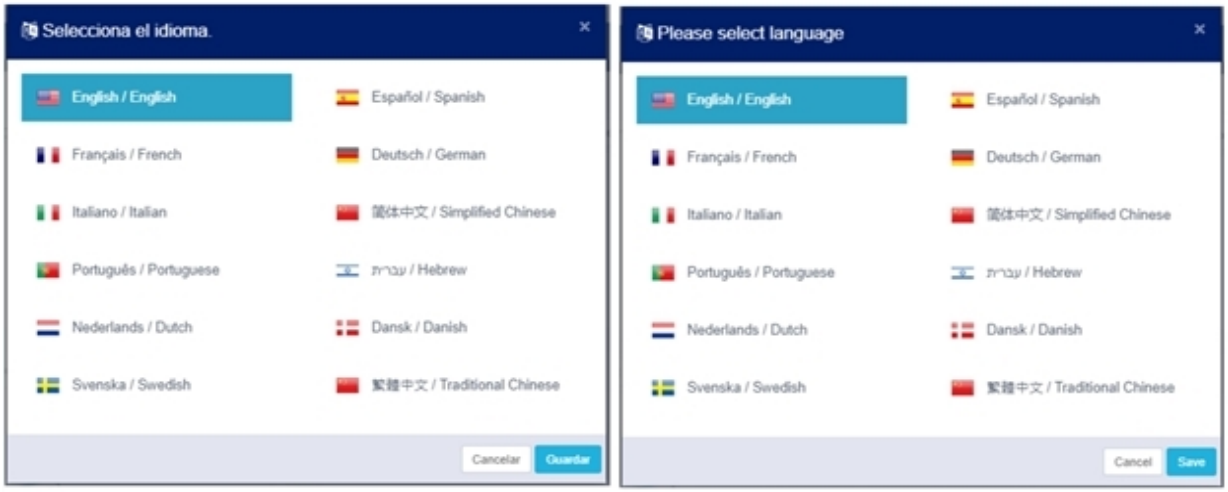
    In case the current language is not set to a language you understand:

    The language selection menu is the only option under the user name menu. This menu will be positioned in the top right, or top left corner of the screen, depending on the current language direction.

3. On the language selection panel, the “Save” button is the button in light blue, the “Cancel” button the one in white. (Note: There might have been a few languages added since the screenshot taken below).

    The Web Localization chapter of the IdentityIQ File Access Manager Administrator Guide describes

how to define additional languages.



Navigating the Data Grid

To navigate within a page:

- To see more results per page (the default is 10), select the dropdown menu on the left side of the screen to choose 10, 25, 50, or 100 results per page.
- To navigate from the current page to the previous page, click **<<** at the bottom right of the page.
- To navigate from the current page to the next page, click **>** at the bottom right of the page.

Time and date format

The time and date format are taken from the browser setting, according to the language/locale.

For example, using a language setting of English(US), will result in a date and time format of:

MM/DD/YYYY H:MM (AM/PM)

This setting is used, regardless of the language setting selected in the IdentityIQ File Access Manager website.

Notifications

All users can see notifications of the success or failure of various operations on any system task and from all screens.

The notifications icon is a dark gray bell that displays in the notification panel at the top right of each screen. The number next to the bell icon indicates the number of notifications for which the user has not yet viewed. (In this context, “viewed” means that the user has not yet clicked on the notification link.)

Open the notification window to clear the notification counter. If there are no notifications, the bell icon displays without a notification counter.

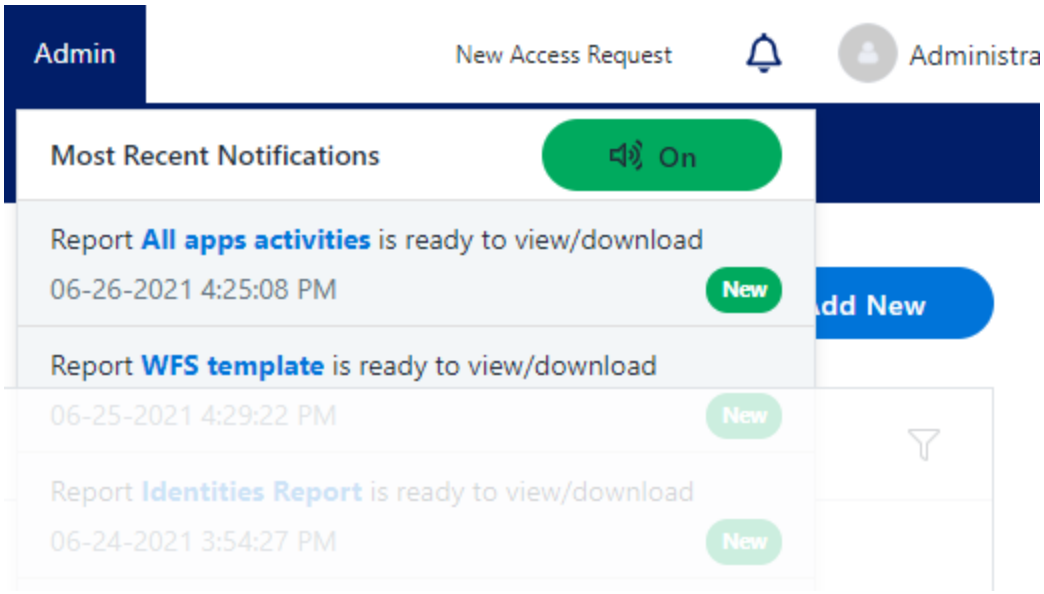
Notification Panel

To view new notifications:

1. Click the gray bell icon in the notification panel.
2. A list of the last ten notifications displays, with the most recent notification at the top of the list.

> New notifications also display the word “New” in white letters on a green background. This no longer displays after the user clicks on the notification.

3. Click the link (if the link displays, since not all notifications have links) in a selected notification.
4. The link redirects the user to the object of the notification (for example, a report or a campaign).



Dashboard

Traditionally, IT personnel or security personnel have determined which individuals can access specific operations on specific resources. However, since these personnel are not always directly involved with those resources on a daily basis, they often rely on other personnel to determine who should have access to specific resources.

Users who understand the ramifications of data falling into the wrong hands are the best candidates to be data owners of specific resources.

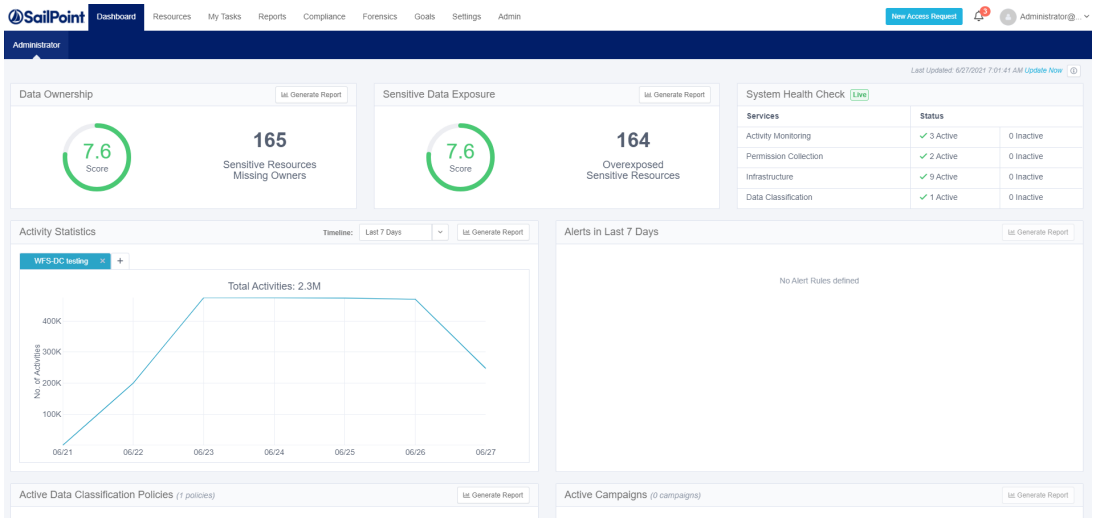
The IdentityIQ File Access Manager Dashboard provides a bird's eye view of data vulnerabilities, so that data administrators and data owners can determine what actions to take to safeguard resources, and to prevent data from further exposure.

The Dashboard has an Administrator tab (with information specific to administrators) and a Data Owner tab (with information specific to data owners).

Administrator Tab

The Administrator tab of the Dashboard consists of the following widgets:

- Data Ownership
- Sensitive Data Exposure
- System Health Check
- Activity Statistics
- Alerts in Last 7 Days
- Active Data Classification Policies
- Active Campaigns
- Top Sensitive Resources by Activity
- Top Users with Pending Tasks



The administrator dashboard features a graphic overview to assist in monitoring the system. Its widgets show various system statistics for detailed analysis, including reports and drill-downs to forensics screens. You can update the widgets on the Administrator Dashboard either automatically (continuously or once a day, depending on the widget) or manually (when a user clicks the Update Now link).

When the Update Now task finishes, the system generates a Notification and displays it as a new unread notification that refreshes the Dashboard.

1. Click **Update Now** to update all widgets in the Administrator tab.
   A task starts to update tables with information (in the background) for widgets, either automatically (daily) or manually.
2. Click the bell icon to open the Most Recent notifications.
   The Last Updated date to the left of the Update Now button changes accordingly.

The following subsections describe each of the Administrator Dashboard sections in detail.

Data Ownership

The Data Ownership widget displays the number of resources with classified data that are missing an assigned data owner (who must review and approve the access of users to resources). This widget displays the compliance score of each resource and is updated once a day (by default). Click **Update Now** to refresh the data.

The main portions of the Data Ownership widget are:

Generate Report

Click **Generate Report** in the widget to generate a report with a detailed list of resources. The system sends a notification (in the bell icon) when the report is ready, and you can access the report by navigating to **Reports > My Reports**.

Score

The score consists of a number and an associated color, as follows:

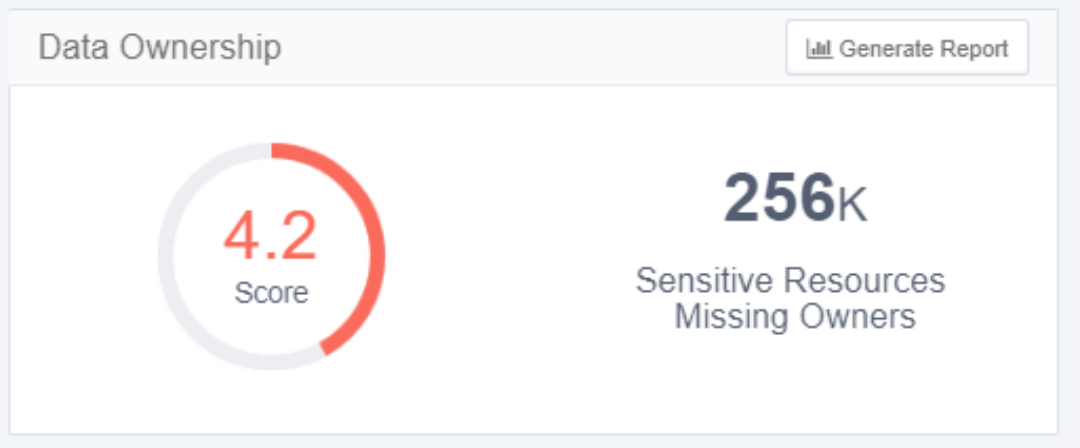
- A score of 0 to 5 displays in red, and indicates a high risk
- A score of 5.1 to 7.5 displays in yellow, and indicates a medium risk
- A score of 7.6 to 10 displays in green, and indicates a low risk

Counter

The counter displays the number of sensitive resources missing owners.

- If the number of resources is one thousand or more, it is expressed in K (for example, 10,000 displays as 10K).
- If the number of resources is one million or more, it is expressed in M (for example, 10,000,000 displays as

10M).



Sensitive Data Exposure

The Sensitive Data Exposure widget displays the number of resources (considered overexposed) with classified data that allow access to a large group of users. This widget (updated daily by default) also displays each resource's compliance score.

To configure a resource as overexposed, navigate to **Settings > General > Overexposed** Resources, where you can view the current definition of overexposed resources and redefine overexposed resources, if required.

The main portions of the Sensitive Data Exposure widget are the same as the main portions of the Data Ownership widget, described in "Administrator Tab" on page Administrator Tab.

This widget displays the exposure of sensitive data, and is updated once a day (by default). Click **Update Now** to refresh the data.

System Health Check

The System Health Check widget (which is live, and updated continuously) displays the status of system services. This widget displays a list of active and inactive services (by service and status), some of which may be restarted.

The widget displays services by category, and the status indicates the total number of active and inactive services, wherein an inactive service is one with a problem.

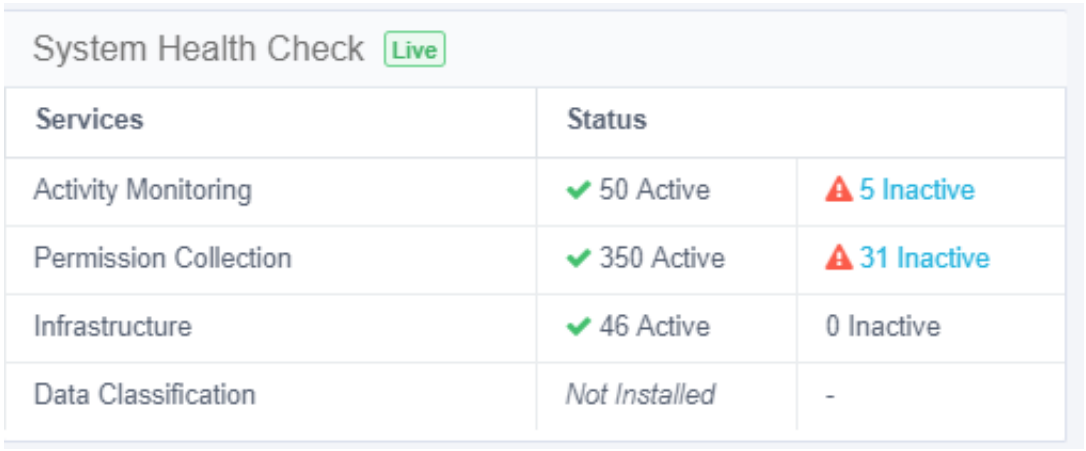
This widget is updated continuously.

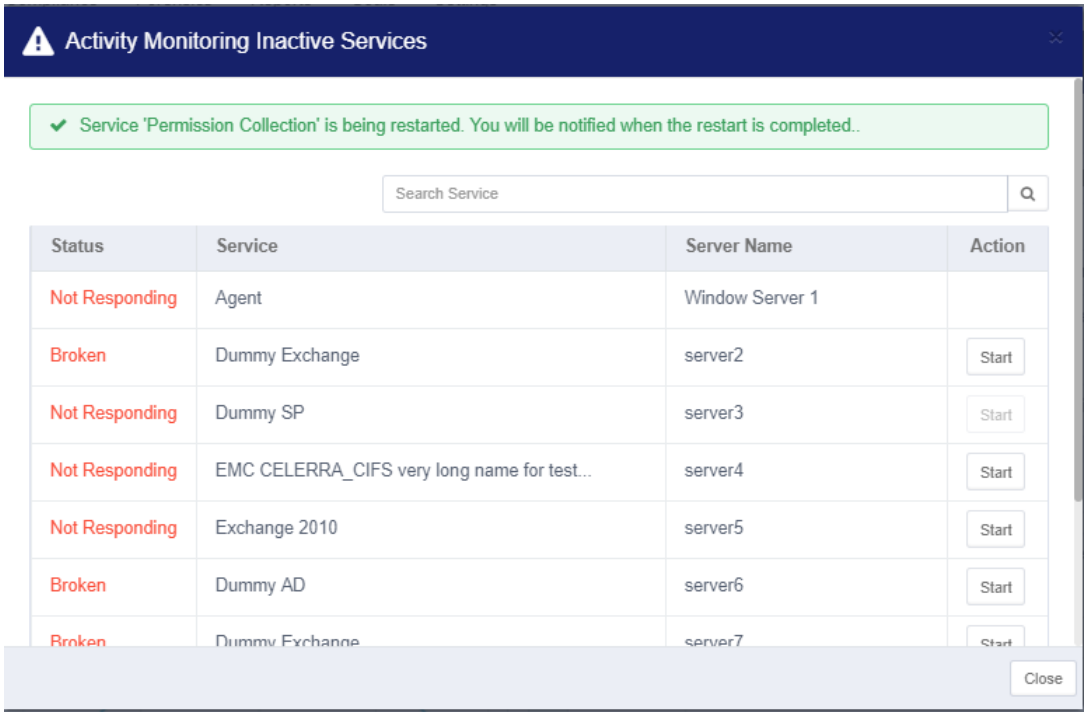
To view a screen with a list of all inactive services and the reasons they are inactive, Click a blue Inactive link. An Inactive Services screen displays a table with the following columns:

- Status (Not Responding, Broken)
- Service (service name)
- Server Name (name of the server on which the service resides)
- Action (Start [Enabled], Start [Disabled], and empty (no screen action).

Click **Start** in a row on the table to start the service in that row.

Click **Close** to close the Activity Monitoring Inactive Services screen.





Activity Statistics

The Activity Statistics widget displays a trend graph of activities per application, with each tab representing a different application. Select the applications to monitor by adding tabs (by clicking on the "**+**" to the right of the tabs), or by removing tabs (by clicking on the "**x**" in the tab). The maximum number of tabs is five.

The main portions of the Activities Statistics widget are:

Timeline drop-down menu

(Last 24 Hours, Last 72 Hours, Last 7 Days, and Last 30 Days)

Generate Report tab

"Administrator Tab" on page Administrator Tab describes this tab.

Activity Statistics graph

- Hover the mouse over any point on the graph to display a tool tip with information on the number of activities on a given date and time.
- Click the graph to drill down to the activity forensics screen with a list of activities per resource. (You can also access this screen by navigating to **Resources > Activities**.)

Click anywhere on the graph to display the associated activities in the forensics activities screen.

This widget is updated online. Reload the page to refresh the data.

Alerts in Last 7 Days

The Alerts in Last 7 Days widget displays the number of alerts created within the last seven days, particularly the five access rules with the most alerts (those with the top five access rules).

The main portions of the Alerts in Last 7 Days widget are:

Generate Report tab

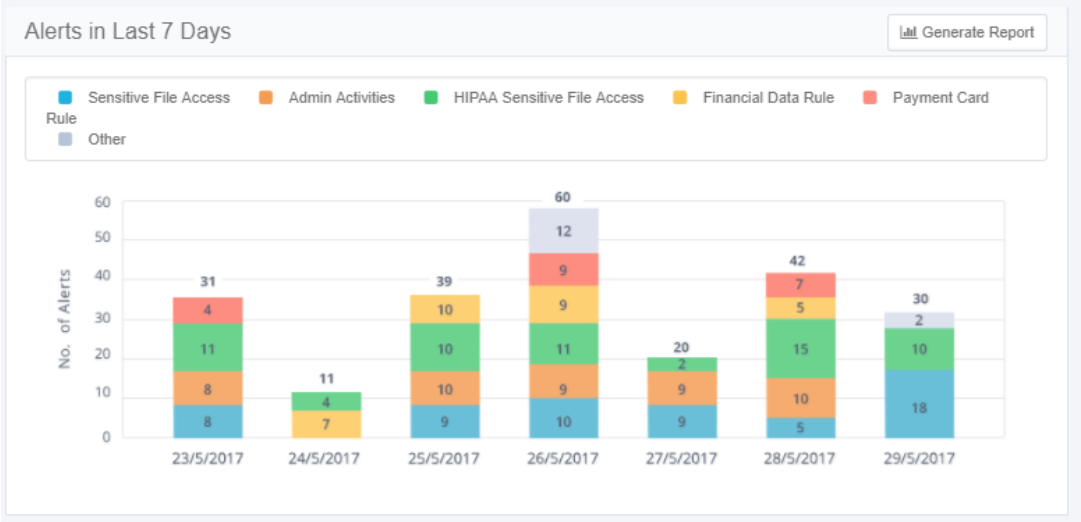
Section "Administrator Tab" describes this tab.

Alerts in Last 7 Days graph

Hover the mouse over any portion of a bar graph to display a tool tip with information on the number of alerts of a specific type, the alert date, and the group for whom the alert was issued.

Click a bar on the graph to display the list of classified resources in the selected application.

This widget is updated online. Reload the page to refresh the data.



Active Data Classification Policies

The Active Data Classification Policies widget displays the active data classification policies in a separate graph for each policy. Each graph displays the five applications with the most policy-classified resources.

The main portions of the Activities Statistics widget are:

Number of Policies

The number is in parentheses after the widget name. Only one policy bar graph displays at a time. Click the arrows to the right or left of the graph to display graphs for other policies.

Generate Report

Section "Administrator Tab" describes this tab.

- Active Data Classification Policy graph
- This graph shows the number of resources for each of the five top applications for a given policy.

Click a bar on the graph to display the list of classified resources in the selected application.

This widget is updated once a day (default). Click **Update Now** to refresh the data.

Active Campaigns

The Active Campaigns widget displays a graph showing the progress of active campaigns, with a separate screen for each campaign.

The main portions of the Active Campaigns widget are:

Number of Active/In Progress Campaigns

The number is in parentheses after the widget name. Only one campaign circle graph displays at a time. Click the arrows to the right (to display the next graph) or left (to display the previous graph) of the graph to display the graphs of other campaigns.

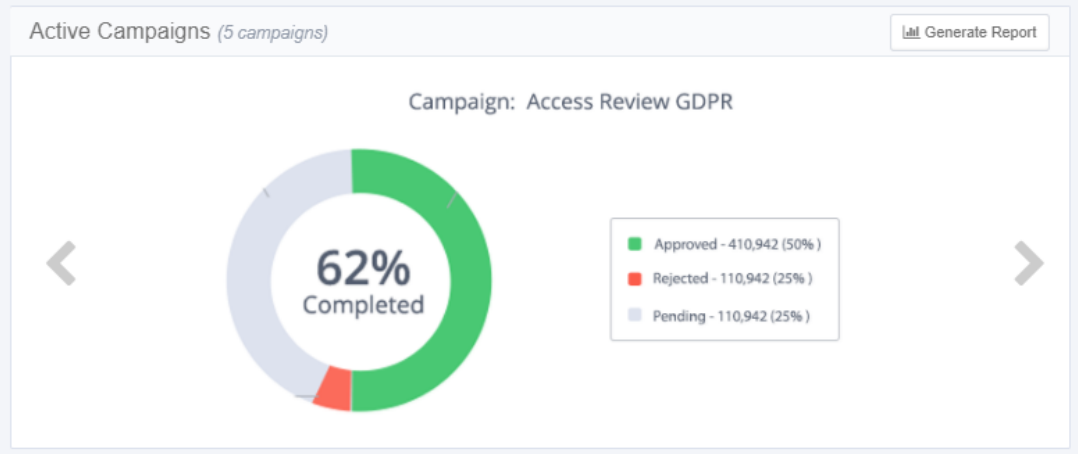
Generate Report

Section "Administrator Tab" describes this tab.

- Active Campaign graph
- This circle graph shows the percentage of records for each active campaign, as well as the campaign status (approved is green, rejected is red, and pending is gray).

Click a bar in the graph to drill down to a screen with a list of pending records per reviewer in a selected campaign. (You can also display this screen by navigating to **Compliance > Access Certification**.)

This widget is updated once a day (default). Click "Update Now" to refresh the data.

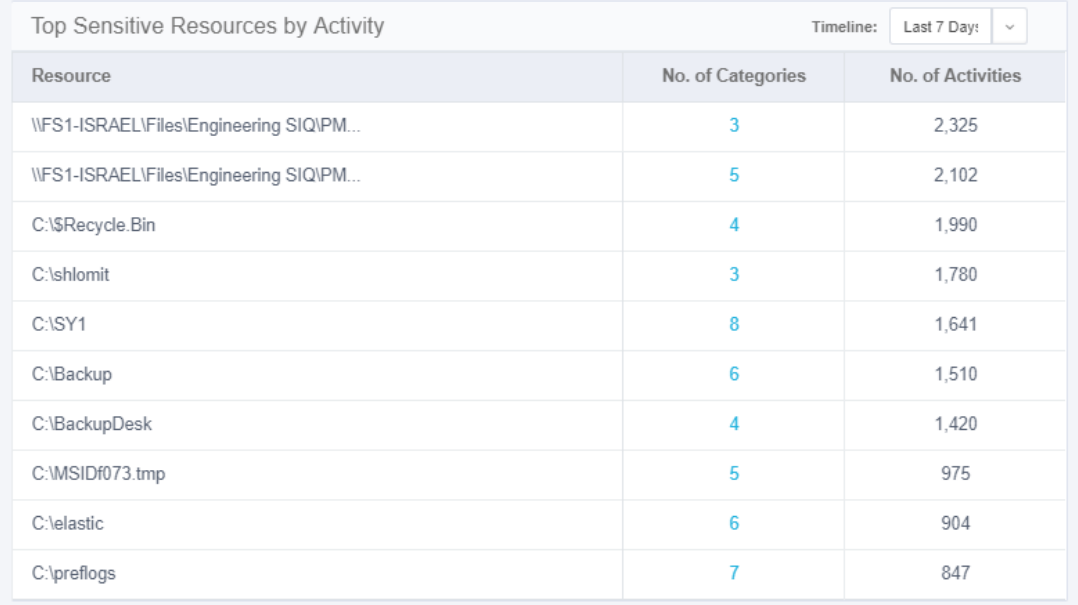


Top Sensitive Resources by Activity

The Top Sensitive Resources widget displays a table of the sensitive resources with classified data, with the most activities within a selected time frame. The table includes columns for the number of categories and number of activities for each resource listed.

Click the mouse on the number of categories in a resource to display the names of the categories.

This widget is updated online. Reload the page to refresh the data.



Resource	No. of Categories	No. of Activities
\\FS1-ISRAEL\Files\Engineering SIQ\PM...	3	2,325
\\FS1-ISRAEL\Files\Engineering SIQ\PM...	5	2,102
C:\$Recycle.Bin	4	1,990
C:\shlomit	3	1,780
C:\SY1	8	1,641
C:\Backup	6	1,510
C:\BackupDesk	4	1,420
C:\MSIDf073.tmp	5	975
C:\elastic	6	904
C:\preflogs	7	847

Top Users with Pending Tasks

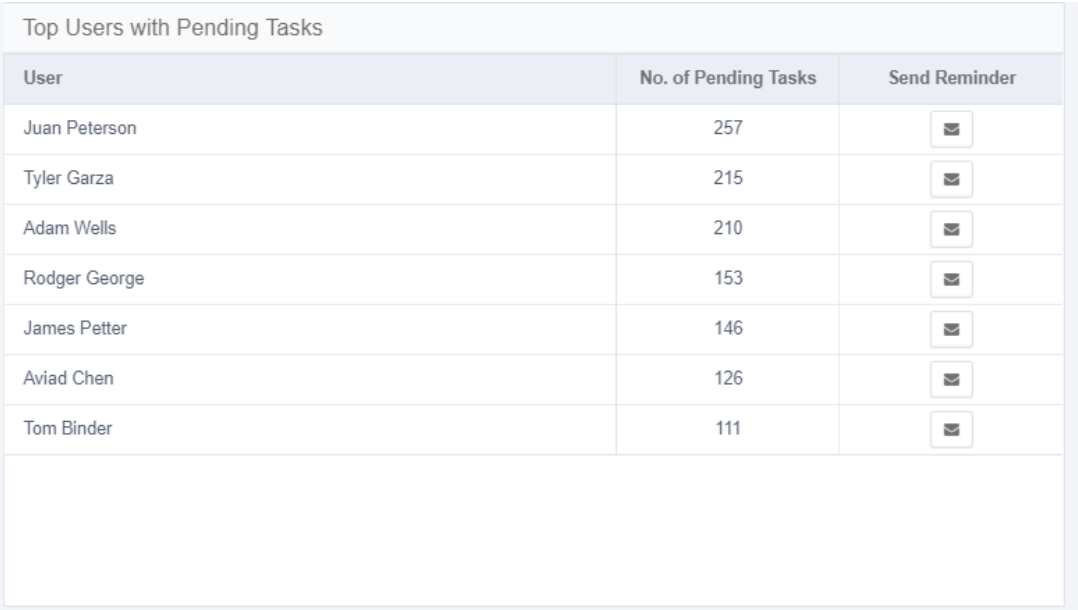
The Top Users with Pending Tasks widget displays a table of IdentityIQ File Access Manager users with the most pending tasks. Examples of tasks are access certifications and access requests.

The table includes columns for the name of the user, the number of the user's pending tasks, and a button to send a reminder to the user

Click the Send Reminder icon in the row of the user to send the user a reminder of the tasks still pending.

The following alert displays: "Email reminder to [User FullName] is being sent. Notification will be provided upon completion."

This widget is updated once a day (default). Click "Update Now" to refresh the data.

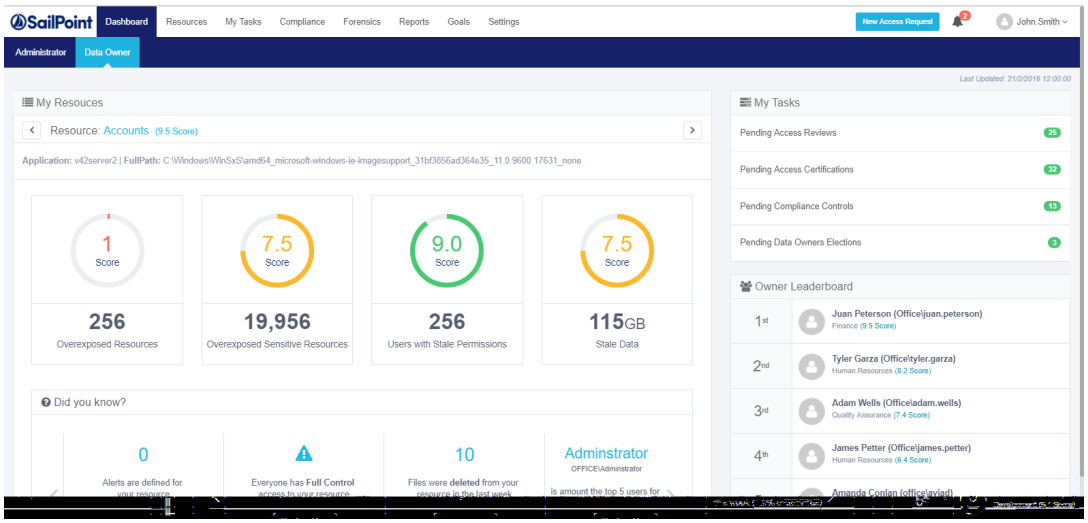


User	No. of Pending Tasks	Send Reminder
Juan Peterson	257	
Tyler Garza	215	
Adam Wells	210	
Rodger George	153	
James Petter	146	
Aviad Chen	126	
Tom Binder	111	

Data Owner Tab

The Data Owner tab of the Dashboard in the Web user interface consists of the following sections:

- My Resources
- Did You Know?
- My Tasks
- Owner Leaderboard

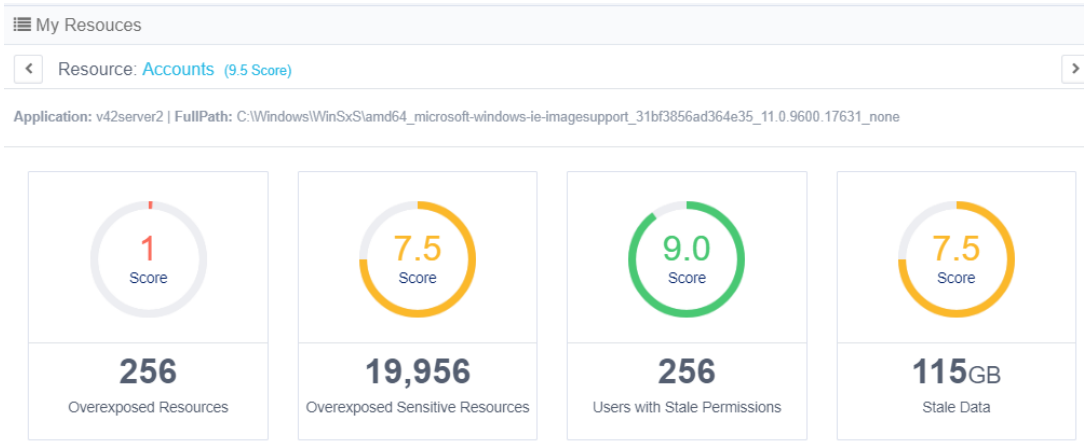


The following subsections describe each of the Data Owner Dashboard sections in detail.

My Resources

The My Resources section is located at the top of the main Dashboard display. The displayed information changes, depending upon the logged-in user's owned resources.

The number in parentheses after the name of the resource is the average score of all the KPIs (Key Performance Indicators). The name of the application and its full path are beneath the Resource name.



The KPIs (Key Performance Indicators) change, based on the resource selected.

Each of the KPIs lists the number of indicators and their weighted scores (from 1-10), are also displayed in a color-coded circle graph.

The KPIs are:

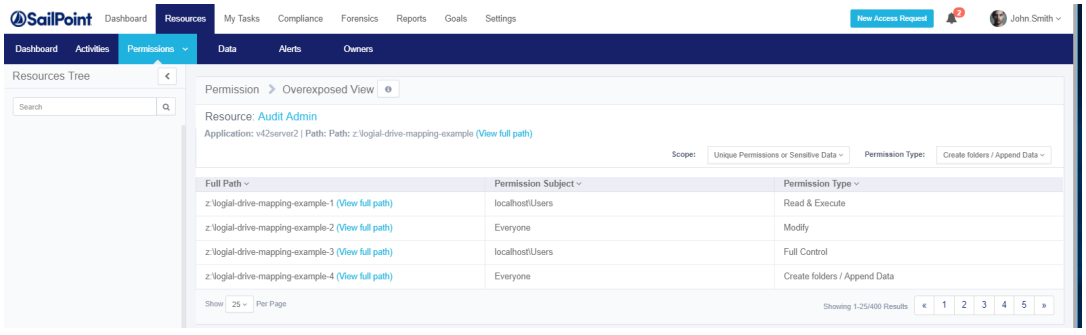
- Overexposed Resources
- Overexposed Sensitive Resources
- Users with Stale Permissions (permissions older than 12 months)
- Stale Data (data older than 12 months, expressed in number of megabytes or gigabytes)
- The color-coded scores are:
- **Red** (0-5)
- **Yellow** (5-7.5)
- **Green** (7.5-10)

To see the details of a specific KPI with the applicable filters, scope, and permission type:

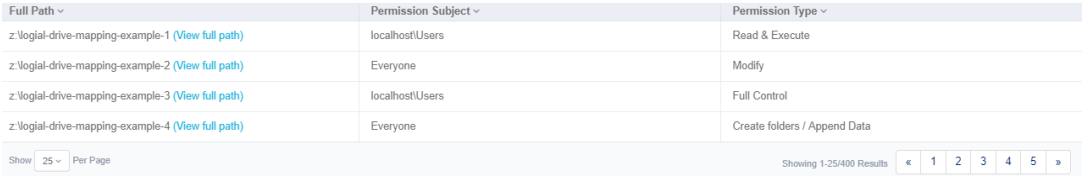
Navigate to **Resources > Path** (for example, C:) **>KPI**

OR

Select a specific KPI in the Dashboard view



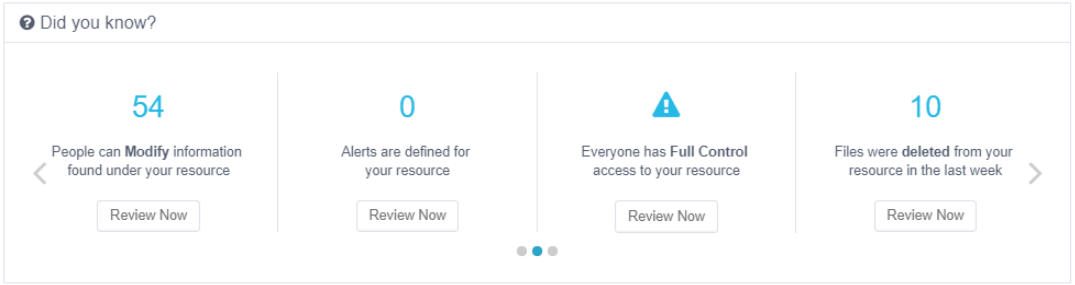
Select a KPI to see details, with the relevant filters, scope, and permission type.



Click the Dashboard tab to return to the Dashboard view.

Did You Know?

The “Did you Know?” area of the Dashboard contains useful information about an owned resource. Such information includes statistics, resource information of logged in users, and warnings. Information may include identification of users who can access resources with specific permission types or the number of users that used a specific resource within a defined period. This information is updated for each logged-in user.



To navigate the Did You Know carousel:

1. Click the **>** to the right (or the < to the left) of the displayed entries.
2. Click a specific Did You Know? item to review it.
3. Use touch selection and navigation (left or right) when viewing Did You Know? information on a tablet.

The carousel displays four items at a time, and automatically moves to the next four items every 5 seconds. The progress dots at the bottom of the Did You Know section indicate how many total pieces of information (in groups of four) are available. For example, if the Did You Know section displays five dots, there are twenty total pieces of information.

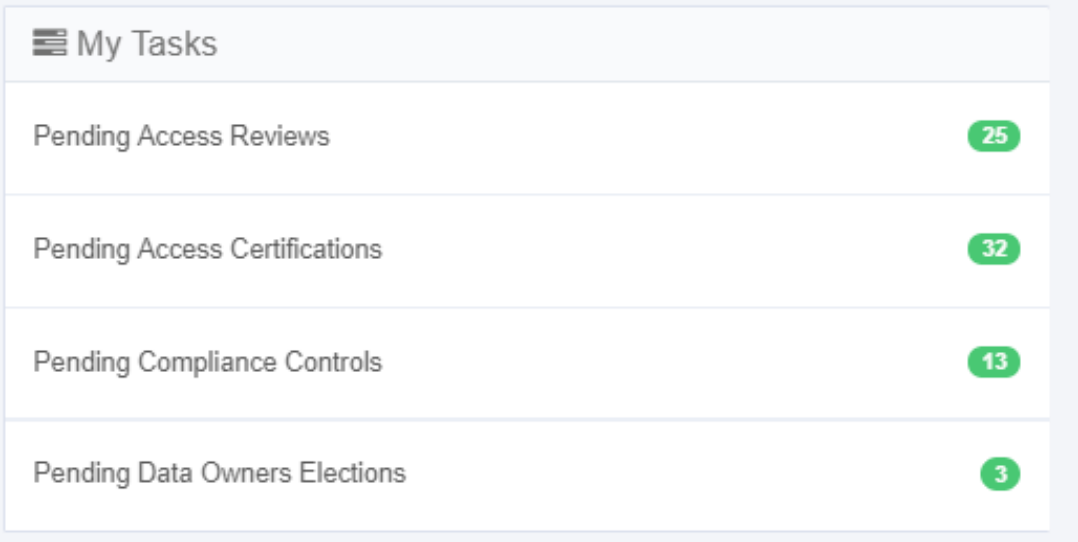
Click **Review Now** to display the details of any item of information in Did You Know.

My Tasks

The My Tasks section, at the top right of the Dashboard display, lists the number of pending items in the following categories:

- Access Certifications
- Access Requests
- Owners Election

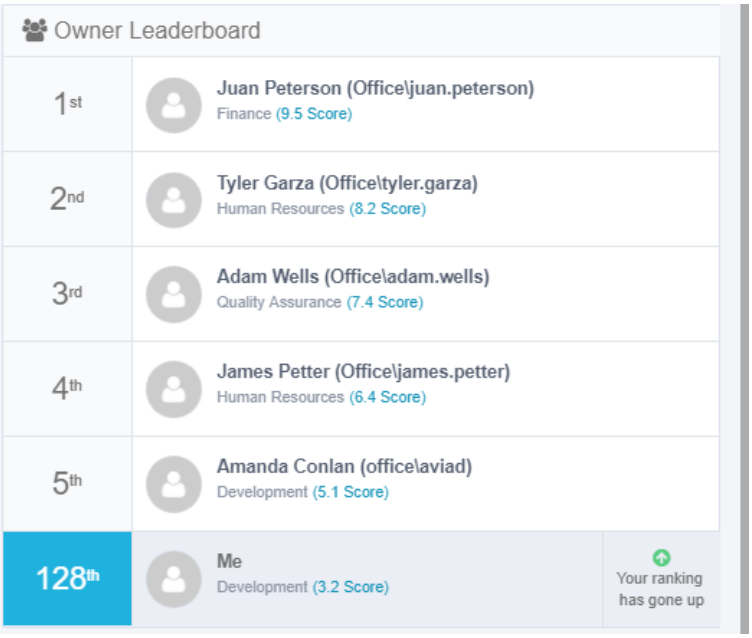
> It is possible to navigate directly to the My Tasks view for a task by selecting that task.



Owner Leaderboard

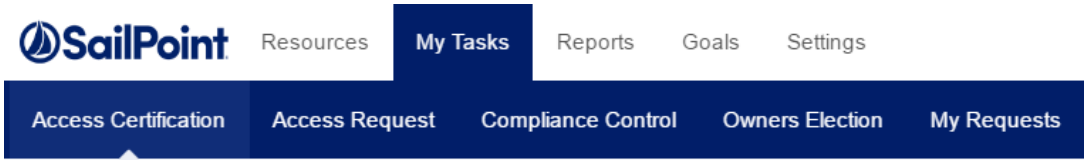
The owner Leaderboard section of the Dashboard displays information about the data owners with the highest-ranking score per owned resource.

Owner Leaderboard scores are ranked only for data owners, displaying the identities and scores of the top five data owners and the score of the logged in user (displayed as “Me”). The “Me” entry indicates whether the user’s rank has increased (a green arrow pointing up) or has decreased (a red arrow pointing down).



My Tasks

The tasks in My Tasks include approval tasks and user requests.

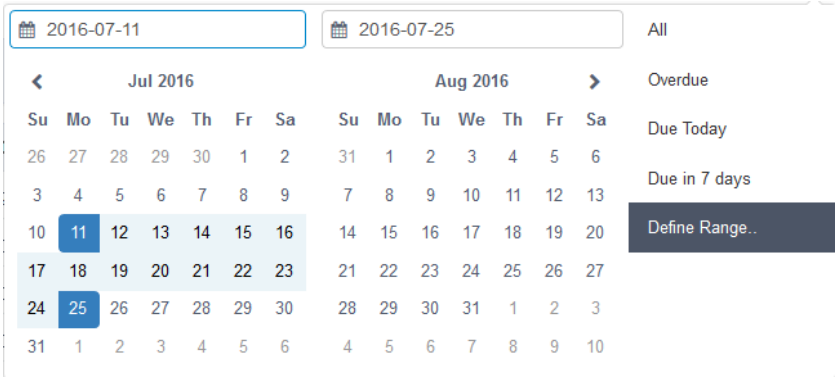


Access Certification

To filter campaigns displayed by default, perform the following steps:

1. Click the Access Certification tab.
2. Click **Filters** at the top right of the displayed list.
3. Select one of the following options from the Applications dropdown menu:
   - All
   - [Name of Relevant Application]
4. Select one of the following options from the Current Status dropdown menu:
   - All
   - In Process
   - Closed
5. Select one of the following options from the Due Date dropdown menu:
   - All
   - Overdue
   - Due Today
   - Due in 7 Days
   - Define Range …
     If you select “Define Range …”, a two-month calendar view displays, as shown in the figure below.
     a. Select a start date.
     b. Select an end date.

        The selected date range displays in the Due Date dropdown box.



Two-Month Calendar View for Define Range…

6. Select the **Reset** button below the dropdown menus, on the far right of the screen, to reset all the filters.

> Once you have selected the Applications, Current Status, and Due Date filters, the word “Filters” in the Filters button changes from gray lettering on a white background to white lettering on a green background.

The filtered Access Certification tasks display in a table below the dropdown menus, with the following columns:

Due Date

In mmddyyyy format – Displays Expired (in red), Expires soon (in yellow), or is empty

Name

The name of the campaign

Application

The application related to the campaign

Current Status

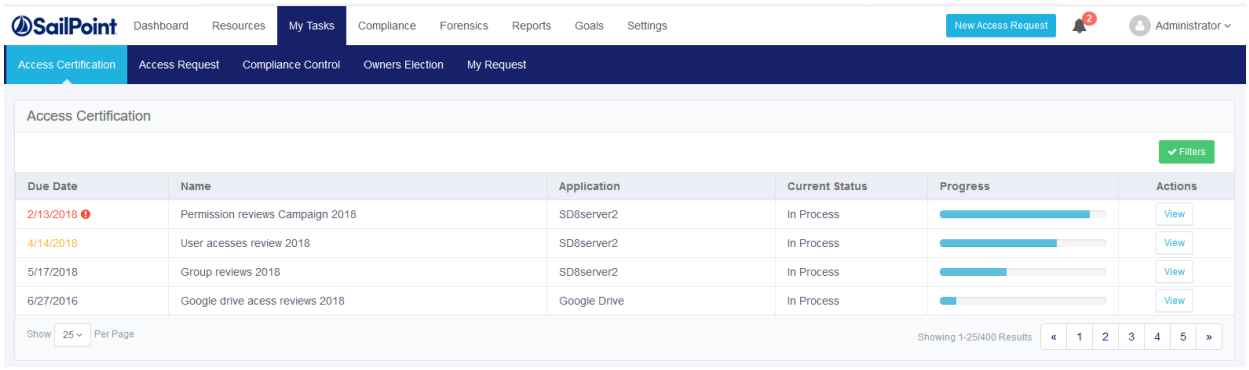
The current status of the campaign

Progress

A progress bar, showing the relative progress made in the campaign

Actions

Selection of the **View** button in the same row as a given campaign to display the access certification details.



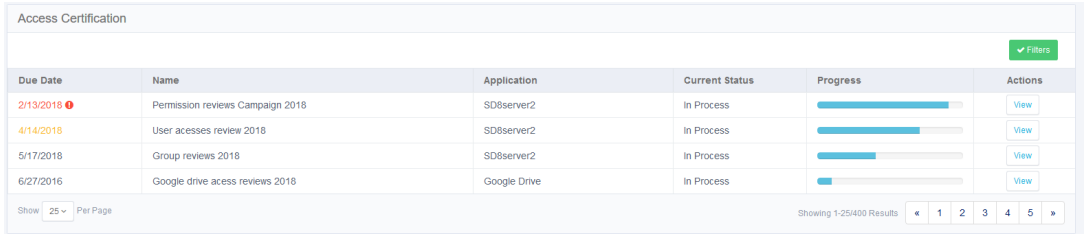
Access Certification Filter Screen

Access Certification Task Details

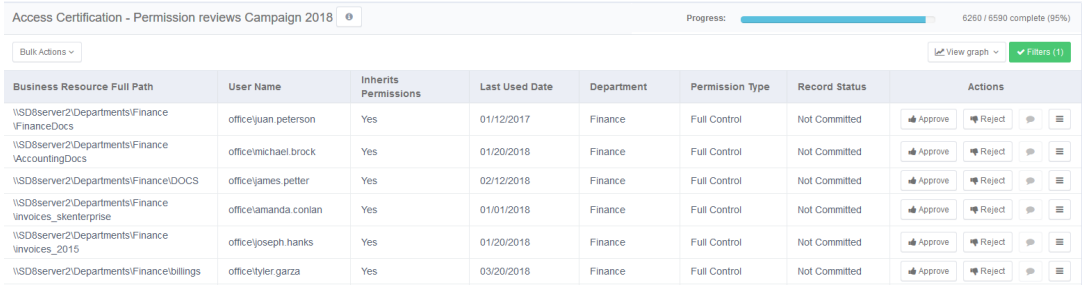
Administrators execute campaigns that generate access certification tasks for the campaigns' reviewers. This window gives a business user an easy and intuitive way to approve/reject hundreds of thousands of permissions in the selected campaign, and features advanced filtering capabilities and representation of the permissions, based on grouping criteria, in chart form.

To view access certification details for a selected task, click **View** under the Actions column of the task to be viewed.

The Access Certification detailed task screen shows permissions for the business data owner to review. This screen is similar to the task screens for Access Request . The displayed columns vary, based upon the administrator's selections. An administrator can set other columns in an Object's template in the Administrative Client.



A detailed task screen of the selected task displays.



Detailed Task Screen

If a campaign has instructions, the left side of the Access Certification detailed task screen first row displays the name of the campaign and a link to display the campaign's instructions.

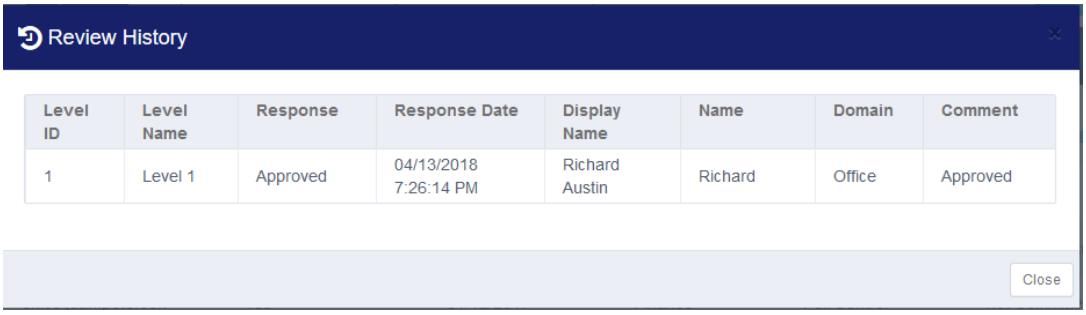
The right side of the first row contains a progress bar that displays how far this task as progressed.

The columns in the main Access Certification detailed task screen are dynamic.

The Actions column options are: Approve, Reject, Comment, and Select.
The Select options are: Review History and User's Permission Paths.

> Sort a column in alphabetical or numerical order by selecting any of the column headings.

When you click Review History, the Review History box displays.



The Review History columns include:

- Level ID
- Level Name
- Response
- Response Date
- Display Name
- Name
- Domain
- Comment

> If no history is available, the window displays the following text: "There is no Review History to show". All a reviewer's selections (approve, reject, comment, history) display the next time the reviewer checks My Tasks.

When you select User's Permission Paths, the permission paths display.

- When finished filtering, click **Approve** to approve the filters, or **Reject** to reject the filters.
- Click **Commit** to save changes or **Close** to close without saving changes.

To navigate within the Detailed Task List:

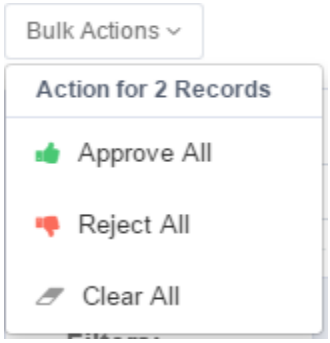
The bottom of the Detailed Task screen displays the previous (Prev) or next (Next) screen, and the number of the total number of screens displayed (for example, 1/2 indicates that the first of two screens displays).

- To see more results per page (the default is 10), select the dropdown menu on the left side of the screen to choose 10, 25, 50, or 100 results per page.
- To navigate from the current page to the previous page, click **Prev** or **<** at the bottom right of the page.
- To navigate from the current page to the next page, click **Next** or **>** at the bottom right of the page.

Bulk Actions

To execute bulk actions on all permissions in a current filter, perform the following steps:

1. Click **Bulk Actions**. A dropdown menu displays, showing the number of records in the filter results, with the following options:
    - Approve All – Changes all Pending Decision status rows in the current filter results to Pending Commit status
    - Reject All – Changes all Pending Decision status rows in the current filter results to Pending Commit status
    - Clear All – Changes all Pending Decision status rows in the current filter from Pending Commit status to Pending Decision status. You cannot revert committed rows.



2. Click **Yes** to clear all records, or click **No** to return to the previous screen.

Filters

Click **Filters** at the far right to filter table rows, based on displayed fields, operators, and values, as follows:

Fields

This includes all the column headings listed above.

The static fields that do not display in the table columns are: 1. Record Action – options are Approved\Rejected. and 2. Record Status – options are “Pending decision”, “Pending Commit”, “Committed” and “Not Committed”

Operators

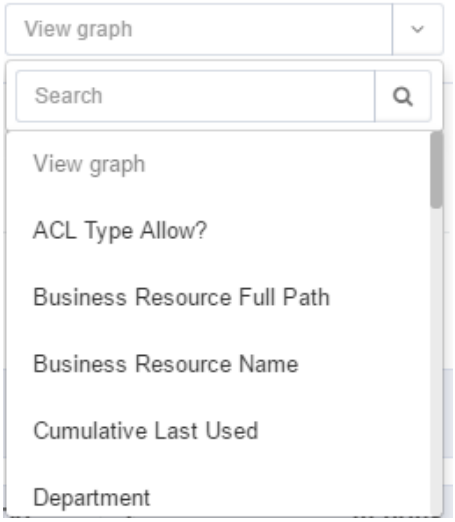
- Contains – free text
- Equals – auto-completes the value (the only choice for the static fields listed above)
- Starts with – free text

- Empty – no value
- Value – Values based upon the operator selected

View Graph

To the right of the Bulk Actions dropdown menu is a View Graph dropdown menu that provides various selections of graph views.

Graphs are a convenient way to view the results of filtering, and are available from the dropdown menu, immediately to the right of **Bulk Actions**. The graph groups filtered results per the selected field in the menu. There are as many chart views as there are fields.

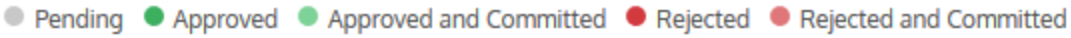


To view filters as a graph, perform the following steps:

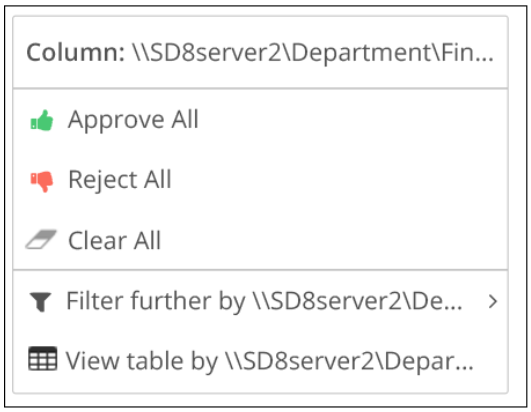
1. Click the **View Graphs** dropdown menu, and select a chart view. A bar chart view displays, with different colored columns and a key to the chart.

In Access Certification Task Details67, **Department** was selected as the chart view and separate bar charts display for Dept1, Dept2, and Null (No department).

Access Certification Task Details68 shows a magnified view of the chart key for the chart in Access Certification Task Details67, in which different colors are used for tasks that are Pending (gray), Approved (dark green), Approved and Committed (light green), Rejected (dark red), and Rejected and Committed (light red).



2. Click a chart column.
   A pop up screen displays an entire column (with the number of items in parentheses) or a portion of the column (with the number of items in parentheses).
3. Click Pending for Action.
   A dialog displays with the following options:
   - Approve All
   - Reject All
   - Clear All
4. Click Approve All, Reject All, or Clear All. A Question Dialog displays, asking for confirmation, and providing space for a free text comment (only for Approve All or Reject All).
5. Click **Yes** to confirm, or click **No** to return to the previous screen.
6. Alternatively, click **Entire Column**.
   A dialog displays with the following options:
   - Approve All
   - Reject All
   - Clear All
   - Filter further by (filtered item) – Displays additional selected filtering
   - View table by (filtered item) – Displays the table with the applied filters



7. Select Chart Filtered by (filtered item).
   A dialog displays with field options for chart groups.
8. Click a field for chart groups.

After selecting a field, the chart displays, grouped by the new field and filtered by the selected value (in this case, Dept2). This is not a bulk action.

Access Request

To filter Access Request tasks displayed by default, perform the following steps:

1. Click the Access Request tab.
2. Select one of the following options from the Type dropdown menu:
   - All
   - Request
   - Revoke
3. Select one of the following options from the Status dropdown menu:
   - All
   - Pending Creation
   - Pending Review
   - Pending Fulfillment
   - Closed
4. Select one of the following options from the Applications dropdown menu:
   - All
   - [Name of Relevant Application]
5. Select one of the following options from the Origin dropdown menu:
   - All
   - Self-Request
   - [Campaigns that generated access requests]
6. Select one of the following options from the Due Date dropdown menu:
   - All
   - Overdue
   - Due Today
   - Due in 7 days
   - No Due Date
   - Define Range …
     If you select “Define Range…”, a two-month calendar view displays, as shown in Access Certification.

- Select a start date.
- Select an end date.

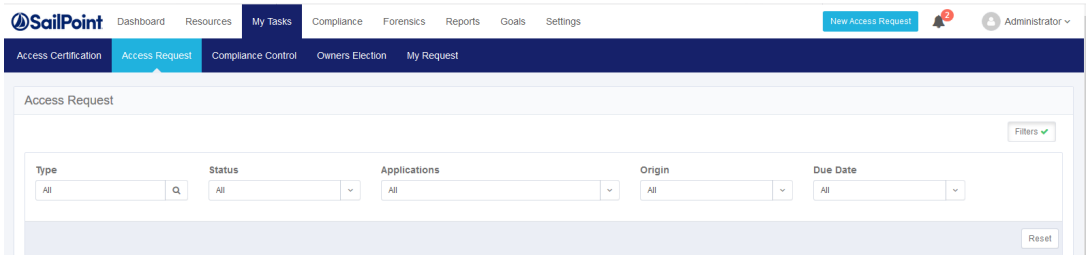
The selected date range displays in the Due Date dropdown box.

7. Select the **Reset** button below the dropdown menus, on the far right of the screen, to reset all the filters.

Once you have selected the Applications, Status, and Due Date filters, the word “Filters” in the Filters button changes from gray lettering on a white background to white lettering on a green background.

The filtered Access Request tasks display in a table below the dropdown menus, with the following columns:

- Due Date – Displays Expired (in red), Expires soon (in yellow), or is empty
- Request ID – A unique, system-provided ID for each access request
- Request Type – The access request type (for example, Request or Revoke)
- Requester – The entity issuing the given access request
- Application – The application related to the access request (if there is one)
- Origin – The origin of the access request (for example, Self-Request or a campaign that generated an access request)
- Request Date – The date on which the access request was issued, in mm/dd/yyyy format
- Current Status – The current status selected from the Current Status dropdown menu
- Progress – A progress bar, showing the relative progress made in the access request process
- Actions – Click the **View** button in the same row as a given access request to display the details of that access certification.



Access Request Task Details

All users can generate Access Requests, using the New Access Request wizard in the IdentityIQ File Access Manager website. Reviewers can also generate Access Requests to reject Permissions in a campaign.

If access is to be revoked, this can be considered a “Revoke” type of Access Request.

To view access request details for a selected task, perform the steps indicated in “Access Certification Task Details” above.

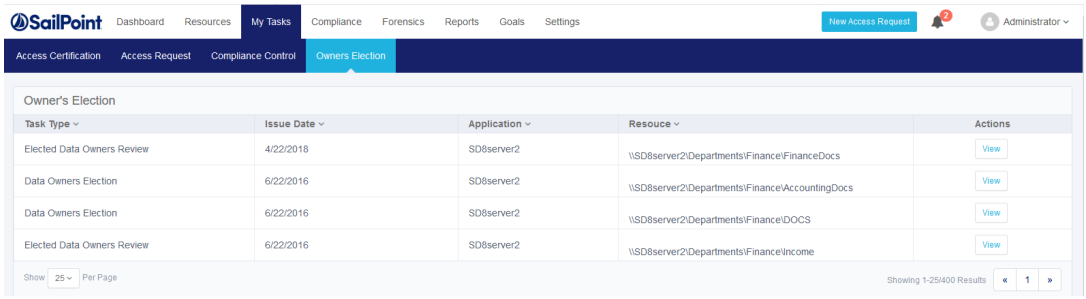
The Access Request detailed task screen shows permissions to review. This screen is similar for Access Certification, and Access Request. Every screen features the # column and the Actions column. Other columns vary, based upon the administrator’s selections.

Owners' Election

To view Owners Election tasks displayed by default, click the Owners Election tab.

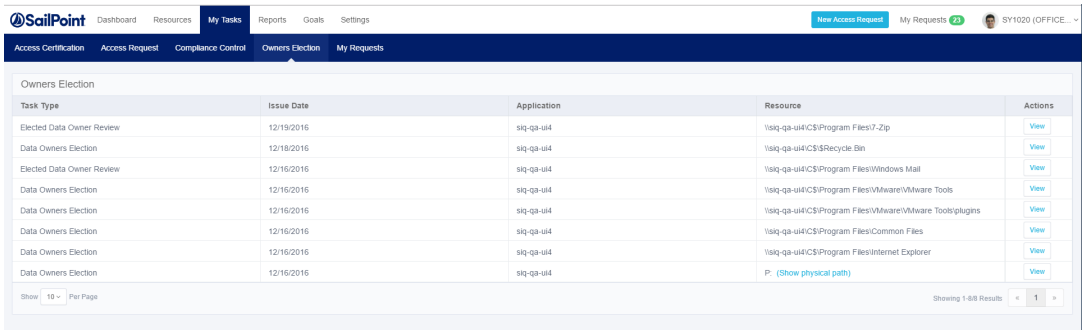
The Owners Election tasks display in a table with the following columns:

- Task Type – Displays the task type (for example, Elected Date Owner Review or Data Owners Election)
- Issue Date – The date of the election or review, in mm/dd/yyyy format
- Application – The application of the resource for which a data owner was elected
- Resource – The resource for which a data owner was elected
- Actions – Click the **View** button in the same row as a given access certification to display the details of that access certification.



Owners Election Task Details

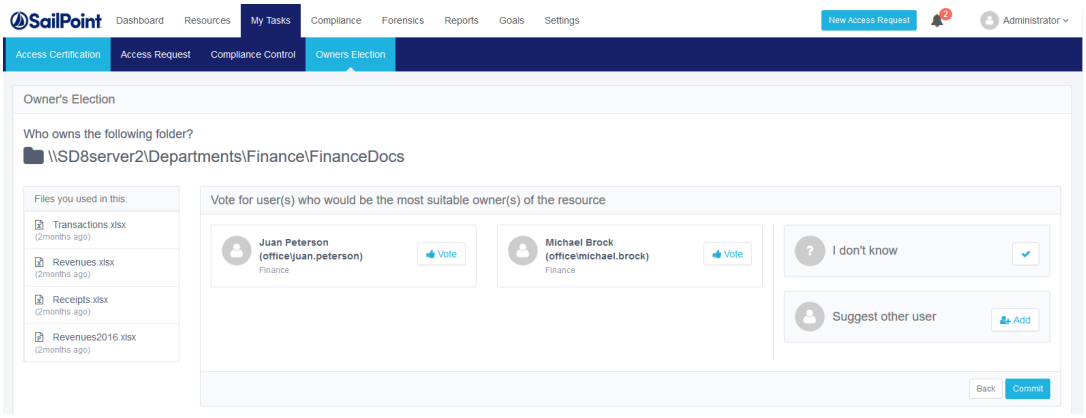
After an administrator has executed one or more goals, those goals will be displayed in the main screen of **My Tasks > Owners' Election** for the user to act.



Data Owners Election

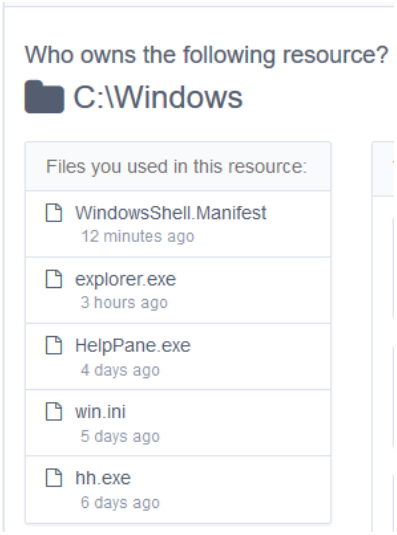
Navigate to **My Tasks > Owners' Election**.

Click the **View** button under Actions on the far right of one of the "Data Owners Election" task types to display the "Who owns the following resource?" screen for that task.



The resource name displays at the top left of the screen. In “Who owns the following resource?” Screen, the resource is **C:\Windows**.

Under the resource is a list of files that the logged-in user used and an indication of how long ago each file was used.



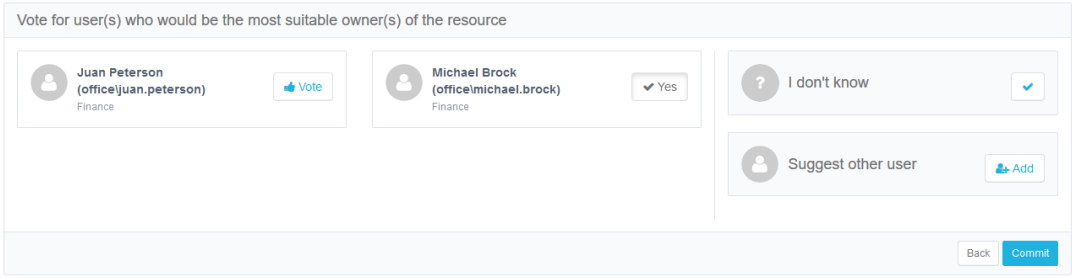
To vote for a probable data owner:

1. Click the Vote button to vote for one or more of the displayed probable data owners.
   The probable data owner’s status changes from a blue thumbs-up with “Approve” on a white background to a white check mark with “Yes” on a green background.
2. Click **Yes** again (which is a toggle switch between “Vote” and “Yes”) to withdraw your vote.
3. Click **Add** to the right of *Suggest other user* to select a prospective data owner whose name is not already displayed.

4. The *Please choose a user* search box displays.
5. Type the account name, or the first few characters of the name, in the search box.
   A list of accounts displays below the search box, with an indication of the number of results (a maximum of 50 results) displayed.
6. Select a user's name.
7. Click **Add**.
   The user's name displays, with a green "Yes" button and a blue x to the right of the user's name. If you click the x, it removes the suggested candidate data owner.

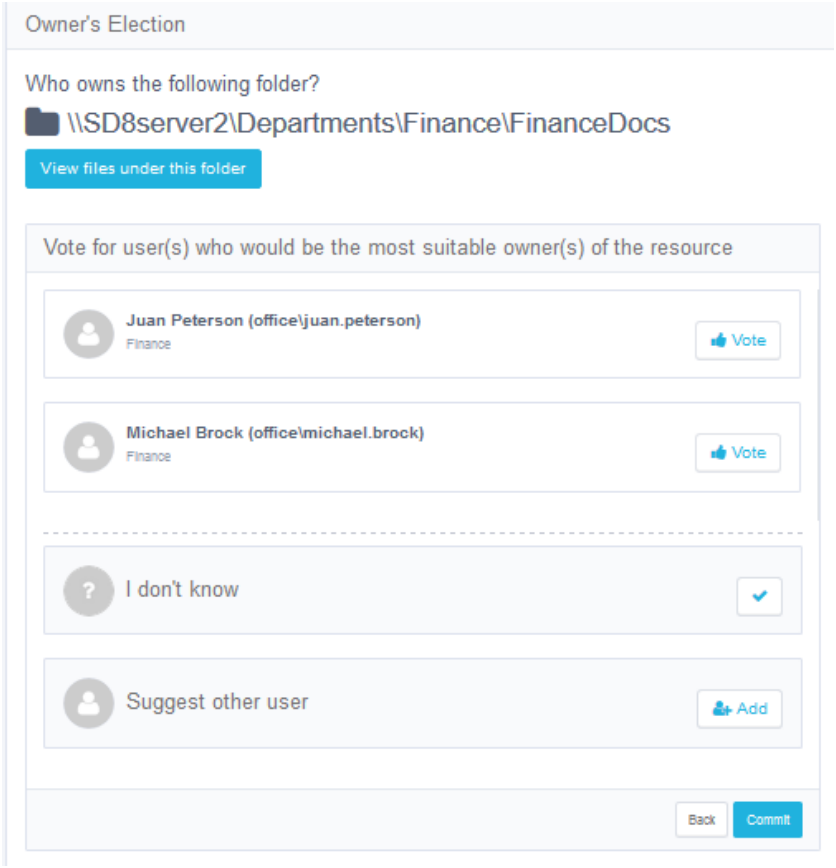
> After you have selected a name for the "Other" probable data owner, a new "Other" probable data owner displays, as shown in New "Other" Suitable Data Owner (Michael). You can vote for up to two "Other" data owner candidates.

> If you attempt to vote for more than two "Other" data owner candidates, the following error message displays: "You cannot add more than two other users."



8. Click **I Don't Know** if you do not know for whom to vote.
   Selecting "I Don't Know" cancels all the votes.
9. Click **Commit** in the *Who owns the following folder* screen to complete the election process. Otherwise, click **Discard** in that screen to discard the voting results. The Commit choice is not available until you have voted for at least one candidate.
10. If you click **Discard**, a Question dialog displays, asking whether you want to discard all actions taken. click **Yes** to discard all the actions or click **No** to return to the "*Who owns the following folder?*" page.

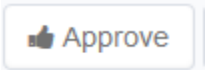
> If a smaller screen is used, the display adjusts responsively to accommodate the information differently, as shown in the figure below. You can view the files used by selecting “Files you used in this resource”.



Elected Data Owner Review

To review the results from the Data Owners Election, and to make a final decision for a probable data owner:

1. Navigate to **My Tasks > Owners’ Election**.
   The Elected Data Owner Review task displays.
2. Click **View** under Actions to the far right of “Elected Data Owner Review” task type.

   The “Review Owners’ Election” screen displays. The left and middle portions of the screen display the names of the first and second place candidates (as well as the third and fourth place candidates, depending upon the system settings) and the percentage of eligible voters who completed voting for those candidates. The right portion of the screen displays the names of the runner-up candidates.
3. Click 

under the name of an elected owner to approve of that elected owner.

4. Click 

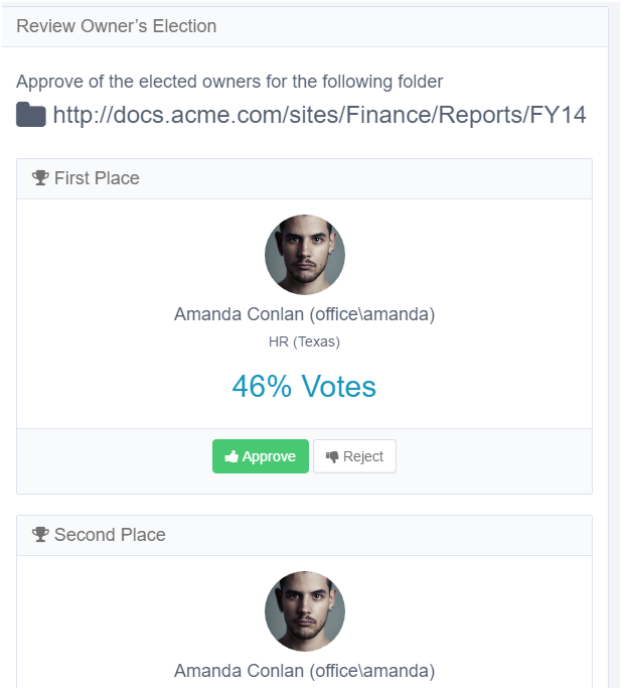
under the name of an elected owner to disapprove of that elected owner.

   > Since each approval or disapproval is independent of the others, it is possible to approve or disapprove of some or all the elected owners, and it is possible to click Approve or Reject under the same candidate if you change your mind.

5. Click **Commit**.

   > It is not possible to click Commit until you have approved or rejected all the candidates (not the runners-up).

If a smaller screen is used, the display adjusts responsively to accommodate the information differently.



My Requests

My Requests displays a list of requests pending review. A user can filter the list based on …

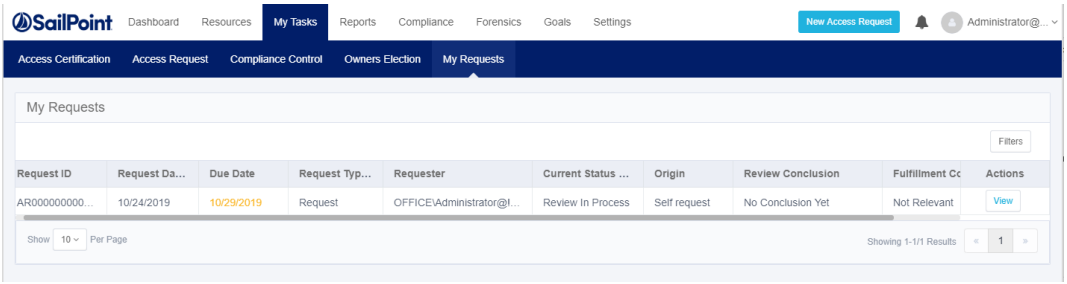
To filter My Requests tasks displayed by default, perform the following steps:

1. Click the My Requests tab.
2. Select one of the options from the Request Type dropdown menu.
3. Select one of the options from the Status dropdown menu.
4. Select one of the options from the Review Conclusion dropdown menu.
5. Select one of the options from the Fulfillment Conclusion dropdown menu.

6. Select one of the options from the Request Date dropdown menu.
   If you select “Define Range …”, a two-month calendar view displays, as shown in Access Certification58.
   - Select a start date.
   - Select an end date.
7. The selected date range displays in the Due Date dropdown box.
8. Click the **Reset** button below the dropdown menus, on the far right of the screen, to reset all the filters.

   > After you have selected the Applications, Status, and Due Date filters, the word “Filters” in the Filters button changes from gray lettering on a white background to white lettering on a green background.

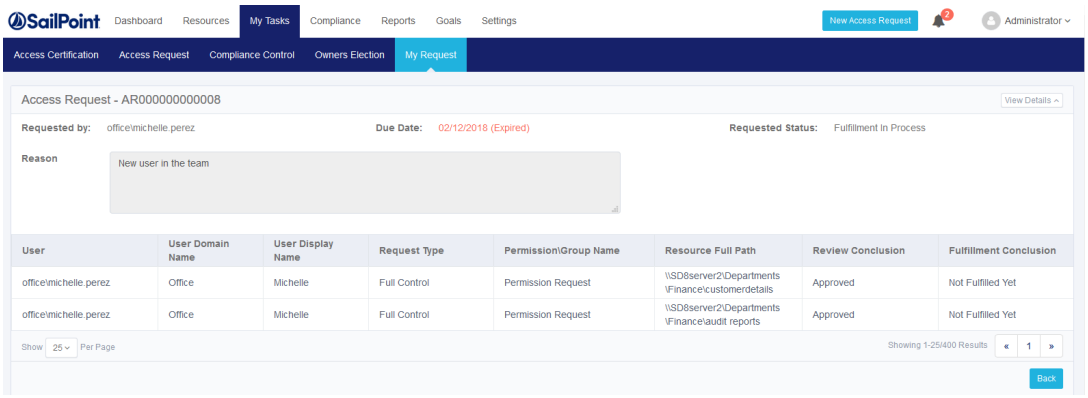
9. The filtered My Requests tasks display in a table below the dropdown menus.



My Requests Task Details

To view request details for a selected task, perform the following steps:

1. Click **View** under the Actions column of the task to be viewed.
2. The “My Requests” view screen displays.



My Requests ViewThe first line contains the name of the access request (granting or revoking a request or a group of requests) on the left, and a View Details button on the right.

1. Click **View Details** to view the details of the access request.

The second line lists the following information from left to right:

- Requested by – The user requesting the access request
- Due Date – The date the request was initiated

- Current Status – The status of the request, for example, “Review in Process”

The third line lists the reason(s) for the request.

The details of the request are in a table under the third line, with the following columns:

- User
- User Domain Name
- User Display Name
- Request Type
- Permission/Group Name
- Resource Full Path
- Review Conclusion
- Fulfillment Conclusion

> The following entities may view an access request:
> The user who submitted the request
> The user for whom access was requested.

Reports

IdentityIQ File Access Manager provides advanced report generation capabilities. Reports can be generated using report templates in the IdentityIQ File Access Manager website, or initiating reports off tablesin the IdentityIQ File Access Manager Administrative Client.

Regardless of where reports are generated, all reports can be retrieved in the IdentityIQ File Access Manager website.

Editing Scheduled Reports in the Administrative Client

Scheduled reports that are created in the Administrative Client can be edited in the Reports table.

The following fields can be modified:

Name

Description

Viewable by

Scheduling

Available to users who have the permission `Report Templates Administrator`

Sharing

Available to users who have the permission `Report Templates Administrator`

Displayed column

Available on certain types of reports

Reports make processed data available to the appropriate data owners.

Report Templates

Report templates are templates for built-in reports, based on the user who accesses them. For example, administrators and users who have the permission Report Templates Administrator see all report templates, while data owners see only templates that are shared with data owners, and other users (non-administrators and non-data owners) do not see any report templates.

Web Client

Navigate to the *Reports* > *Report Templates* screen on the IdentityIQ File Access Manager website to use IdentityIQ File Access Manager's built-in report templates for standard and customized reports.

Manage Report Tags

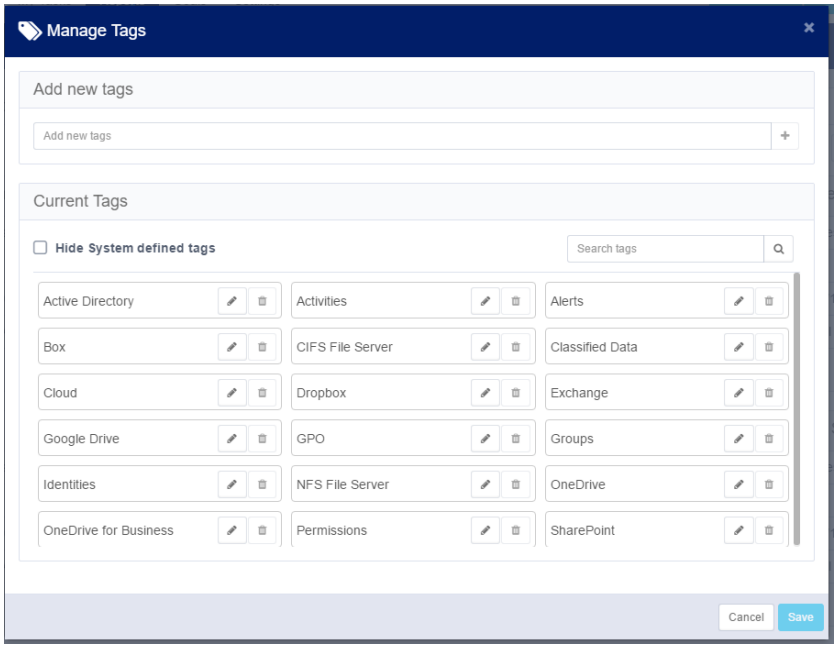
You can assign one or more tags per report to help find them later.

Managing Tags

This option is available by default to the Administrator capability only.

System tags cannot be deleted. The Delete option - a trashcan icon - is disabled for system tags.

1. Click **Manage Tags** to change or delete report tags.
   The Tag Management screen displays.
2. Available options are:
   - Hide system-defined tags (by checking the check box)
   - Search for tags
   - Edit tags
   - Add customized tags
3. Click the **Edit** option (a pencil icon) next to a non-system tag to edit that tag. It is not possible to use a name that already exists or to have a blank tag.
4. Click **Save** to the right of the edited tag to save it.
5. Click **Save** at the bottom of the Manage Tags screen to save all changes.



Filter Reports by Tags

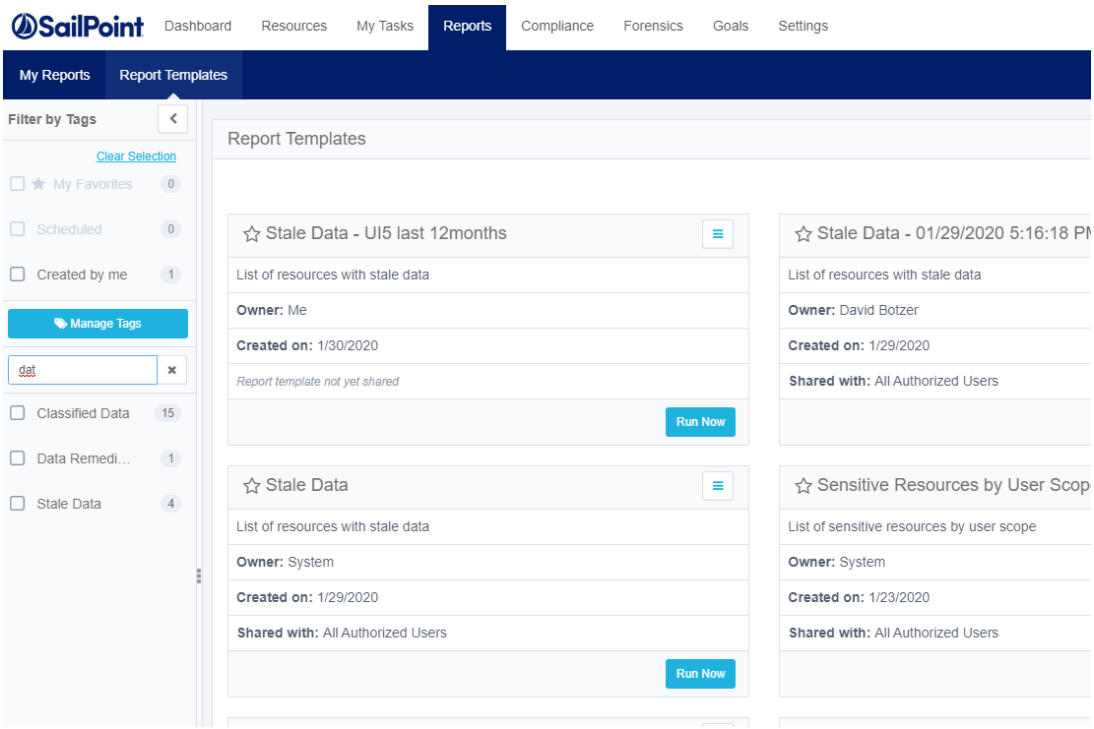
The Filter by Tags panel on the left can be used to filter out relevant report templates:

Search field:

1. Type in the report tag. Available tags will be filtered out as you type.
2. Select one of the available tags to filter the report templates displayed.

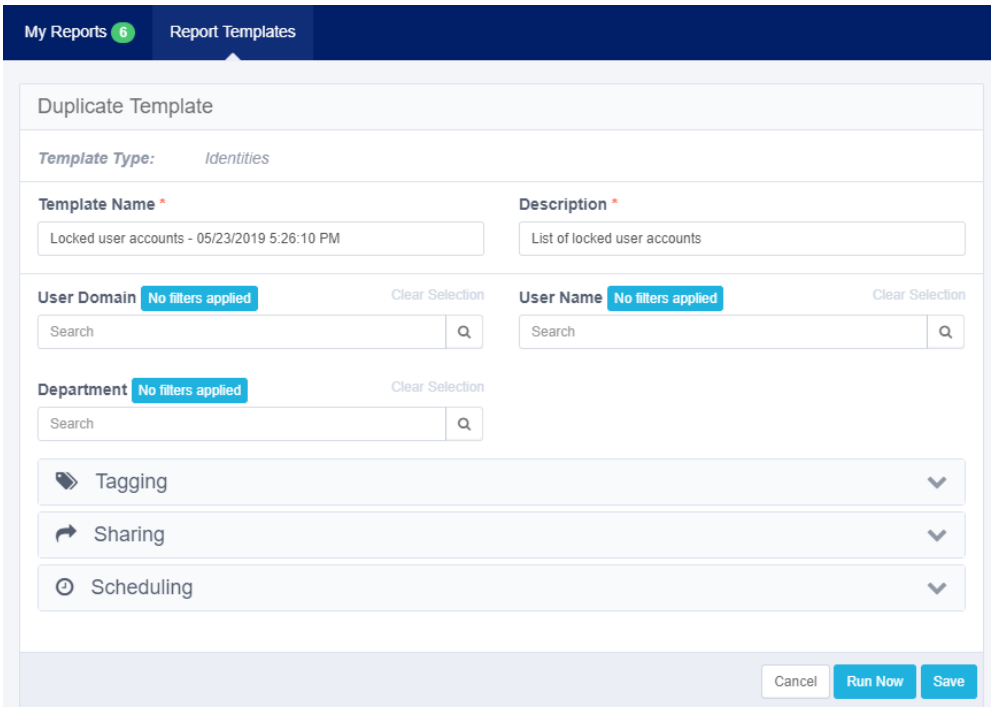
Created by me

Select this checkbox to filter out your own report templates



Run a report or create a scheduled report

1. To run the report with settings other than the default parameters, select **Duplicate** from the template menu. *The Duplicate Template panel opens.*
2. Set the desired report parameters, scheduling times, and other setup fields.
3. Click **Run Now** to run the report now.
4. Click **Save** to save the template for future use of this template.



Report Mechanism

IdentityIQ File Access Manager sends reports to the recipients defined in the **Viewable by** section of the report.

The system sends an email with a link to the report only to recipients with permission to download the report. If a recipient forwards that link to a user without permission to download a report, the recipient will not be able to download the report.

Report Operations

To open the report management screen:

Navigate to **Reports**.

- Double click on a report to display report details. The Report Details window will display under the Reports window.
- Click **Refresh** to refresh the Reports list.
- Click **Delete** to delete a selected report

> This option is available only to users with the *System>Reports>Delete* permission .

Report Editing

The following fields are available to edit a customized report:

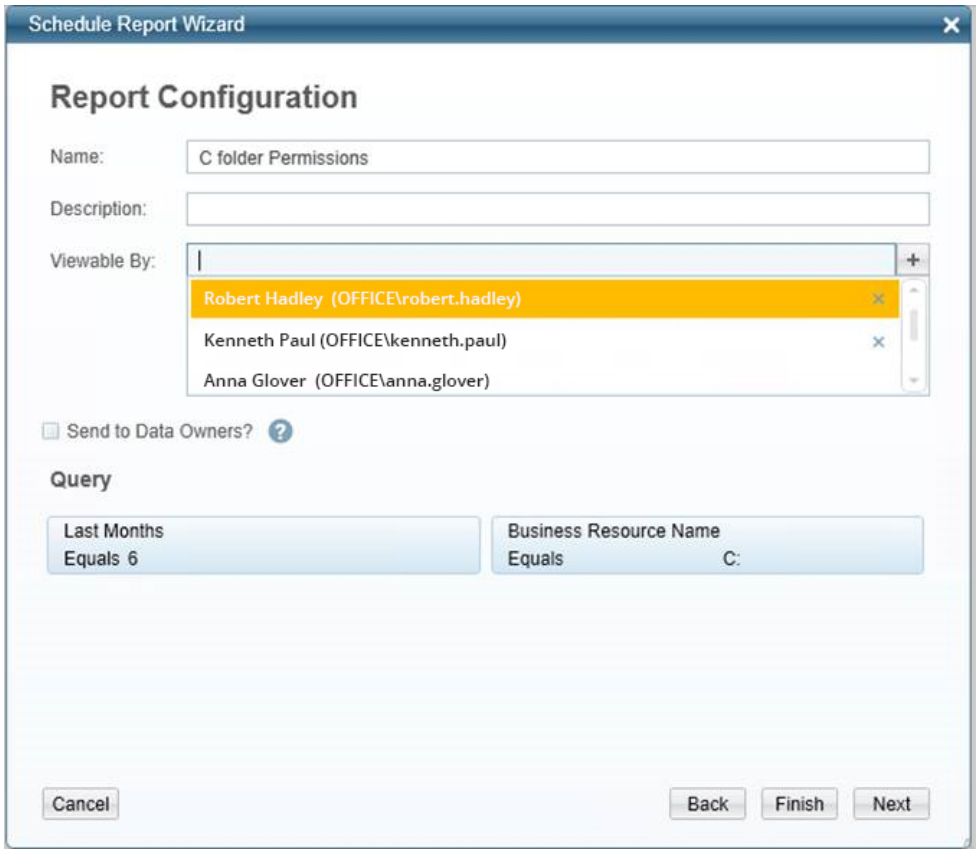
- Custom fields to display (where supported)
- Recipients list
- Name

- Description
- Scheduling

> It is not possible to change the query filter of a saved customized report.

To edit report parameters:

1. Navigate to Reports
2. Select a scheduled report from the list to edit
3. Click **Edit**.
   The **Welcome to the Schedule Report Wizard** Screen displays.
4. Click **Next** on the *Schedule Report Wizard Welcome* page.
5. The **Report Configuration** screen of the Schedule Report Wizard already displays the name in the **Name** field.



6. Type a description in the **Description** field.
7. Double click in the **Viewable By** field to view a list of users who can view the report.
8. Click on a user's name and click the **+** sign.
9. The user's name appears in the box under the **Viewable By** field.
10. Check the **Send to Data Owners** check box to send the report to data owners.

11. Relevant queries appear in the **Query** section of the **Report Configuration** screen.
12. Click **Finish** to send the configuration to the system without configuring a report schedule.
13. If you click **Finish**, the following Confirmation popup displays: “You are creating a report without a scheduler. Do you wish to continue?”
14. Click **Yes** to save the report without configuring a report schedule, or **No** to return to the **Report Configuration** screen.
15. If you click **Yes**, and the following Warning popup displays: “This action can only run by a File Access Manager user that is associated with a user from the authentication store. The action will not be executed”. This means that you logged into the client with a local File Access Manager user, rather than with an Active Directory user from the Authentication Store. Only Active Directory users can create reports, since File Access Manager needs the email address of the user and the user’s identity to generate the report.
16. Otherwise:
17. Click **Next**.
18. The Report Configuration screen displays.
19. Check the **Create a Schedule** check box to create a schedule, or click **Finish** to send the report configuration to the system without a schedule.
20. If you click **Finish**, the following Confirmation popup displays: “You are creating a report without a scheduler. Do you wish to continue?”
21. Click **Yes** to send the configuration to the system without configuring a report schedule, or **No** to return to the **Report Configuration** screen.
22. If you click **Yes**, the following Warning popup displays: “This action can only run by a File Access Manager user that is associated with a user from the authentication store. The action will not be executed.”

Report Actions

> It is not possible to delete a scheduled report.

- (Right click) **Run Now** – Run the report and send it to all recipients.
- (Right click) **Run now and send only to me** – Run the report and send it to the current user who is active in the IdentityIQ File Access Manager Administrative Client.

Compliance

Campaigns are procedures that complete access certification, and begin with the creation of a Campaign Template. The Campaign Template defines the campaign activities. Identities and Permissions Forensics or Access Certification can also create campaigns.

Access Certification

Create campaigns to certify permissions or identities.

Campaigns are created from campaign templates. You can have recurring or scheduled campaigns to check access certifications regularly.

You can use existing campaign templates, create a template from an existing one, or create a new campaign template.

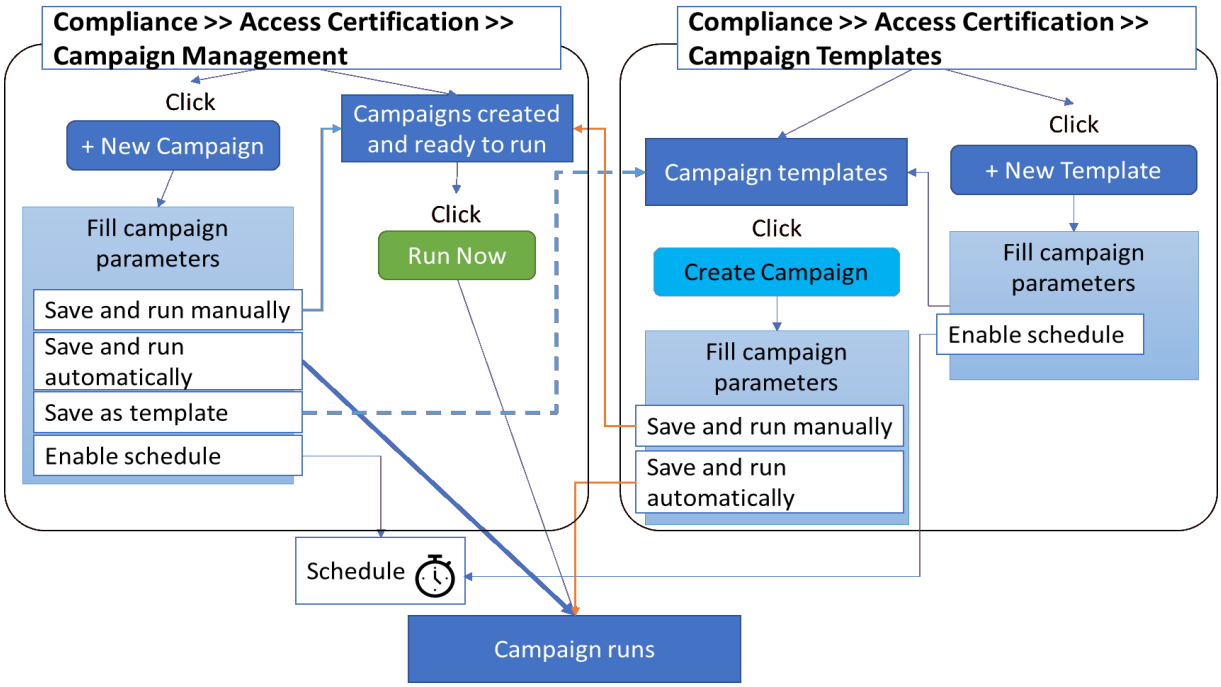
Access Certification includes the following steps (in order):

1. Determine the identities/permissions to be certified.
2. Determine the review process to use.
3. Create an Access Certification Campaign.

Access Certification Flow: How to Create And Run a Campaign

Campaigns have the following stages:

- *Campaign template* - Basic parameters from which you can create a campaign
- **Campaign Created and ready to run** - Campaigns waiting to be run
- **Campaign In progress** (see a full list of campaign statuses in the section below) - Campaigns in various stages of being run



You can run a campaign by any of the following methods:

Compliance > Access Certification > Campaign Management

- Select a prepared campaign, and click **Run Now**.
- Click **+New Campaign**, create a campaign and run it. You can also save the created campaign as a template for later, or schedule it.

Compliance > Access Certification > Campaign Templates

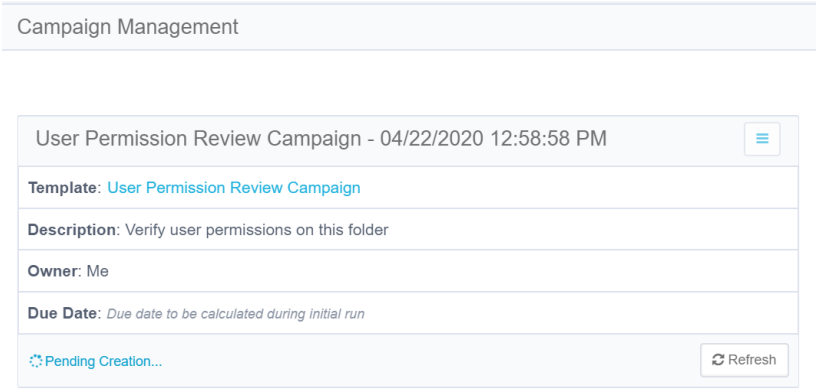
- Click **+ New Template**, fill the parameters, then basically you're at the next stage.
- Select a template, and click **Create Campaign**. Fill in the parameters, then either press run now, or schedule.

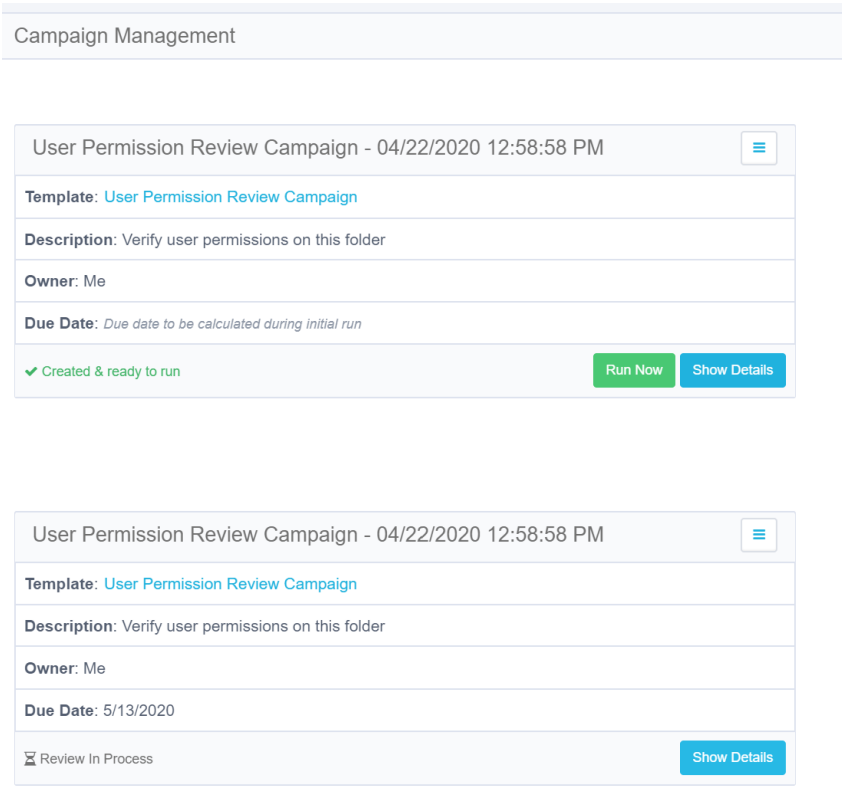
Campaign Management

Navigate to: **Compliance > Access Certification > Campaign Management** .

Valid campaign statuses are:

- Completed
- Created
- Creation Failed
- Deletion Failed
- In Progress
- Pending Completion
- Pending Creation
- Pending Deletion
- Pending Re-initialization
- Pending Review in Progress



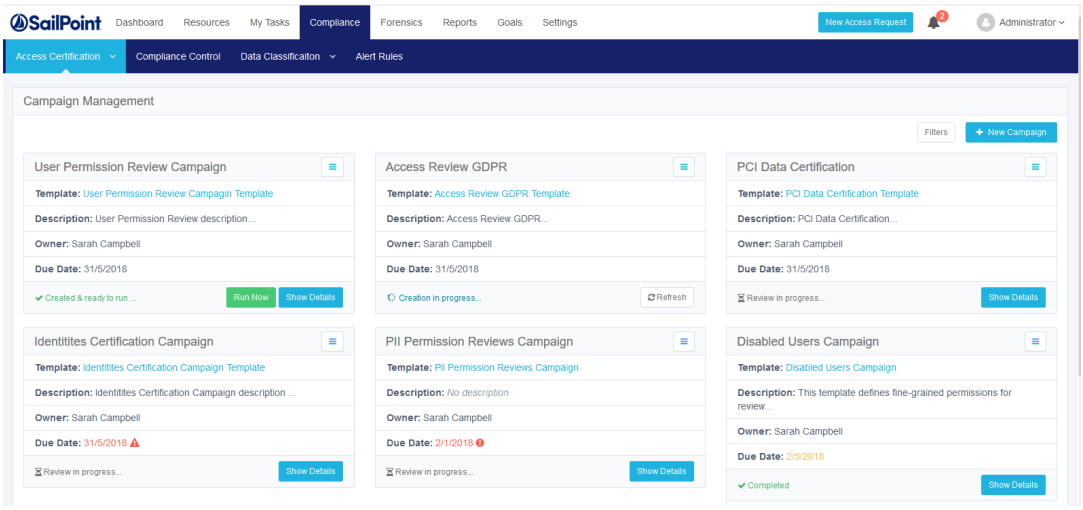


To manage existing campaigns, perform the following steps:

Navigate to **Compliance > Access Certification > Campaign Management**.

The Campaign Management screen displays.

The campaigns display from left to right, sorted chronologically, by date of campaign creation.



Each displayed campaign lists the following information:

Template

The template name displays as a link, which the user can click to edit the template. Any changes that the user makes to the template will only affect future campaigns. If the campaign was created without a template, “No Template” will display (but not as a link).

Description

The template description displays.

Owner

The template owner displays.

Due Date

The due date displays. If the status is “Creation in Progress” or “Created & ready to run”, then “Due date to be calculated during initial run” displays.

When the campaign status is “Review in Progress”, the due date is yellow from 0-7 days before the date, or red if the due date has passed.

Refresh

This button refreshes the current campaign status, and is located on the bottom left of the displayed campaign.

Run Now

This button only displays for a campaign whose status is *Created & ready to run*.
When you click this tab, it creates a task that:

- Runs the campaign
- Sets a campaign due date
- Sets the campaign reviewers
- Sends email notification to the reviewers, requesting them to approve or reject suggested user accesses.

The menu button, on the top right of each campaign display, contains various options, depending upon the campaign status.

Options include:

Edit

Edit the campaign.

Save as Template

Save the campaign as a template.

Refresh

Refresh the user’s view of the campaign status.

Reinitialize

Create a task that reinitializes the campaign.

Delete

Delete the campaign.

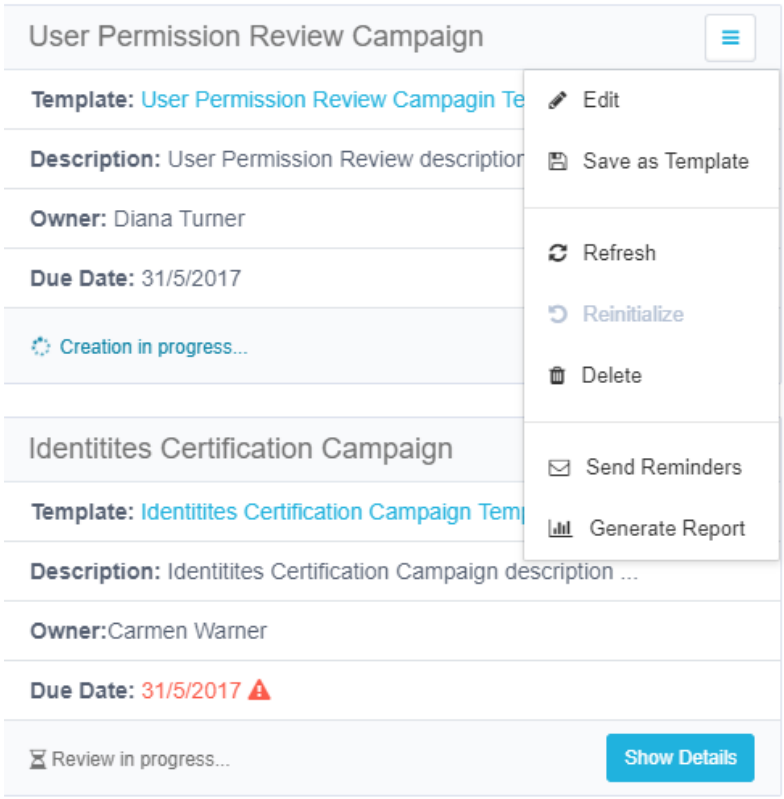
Send Reminders

Send reminder emails to reviewers to complete the campaign.

Generate Report

After you click this option, you can view the generated reports by navigating to **Reports > My Reports**.

> This report contains a detailed list of all records, including their process levels and a summary of their statuses.



Filter the campaigns:

1. Click **Filters**.
2. Under Filters, type or select the relevant data in the following fields to narrow your search of campaigns:

   Campaign Name

   Type the campaign name, or the first few characters of the campaign name, and then click the Search button next to that field.

   Owner

   Type the owner (user) name, or the first few characters of the name, and then click the Search button next to that field.

Status

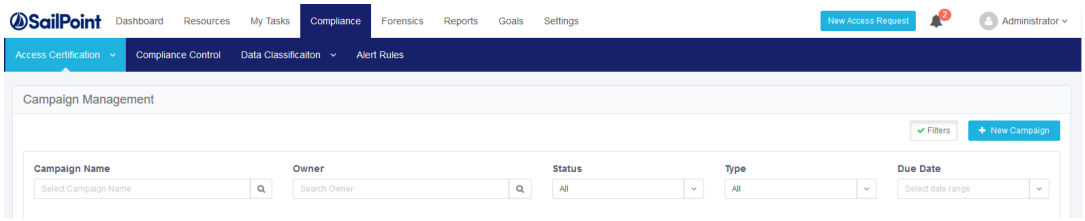
Select a valid status from the drop-down menu (See full list above).

Type

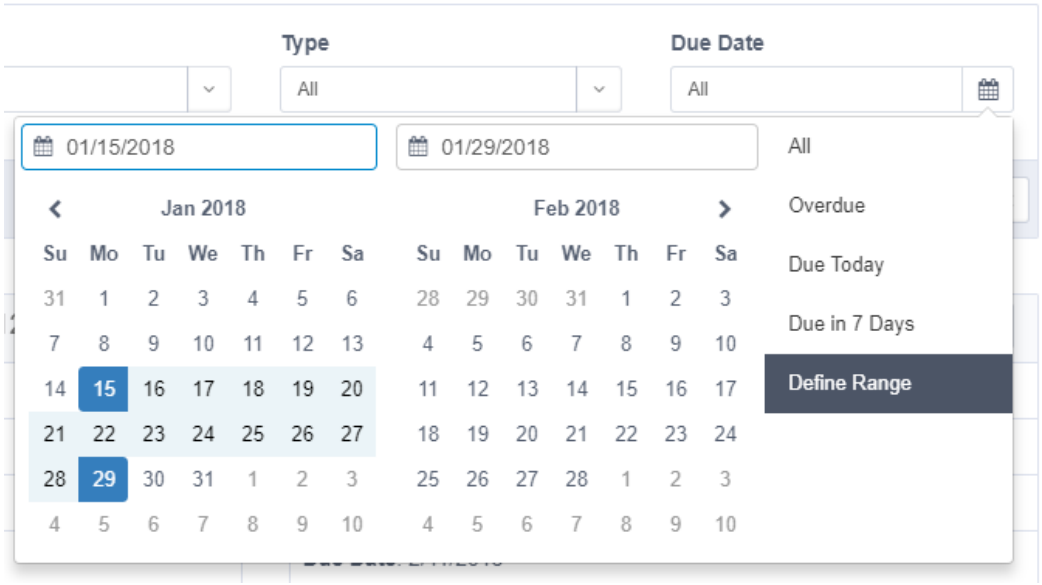
Select “All”, “Permissions”, or “Identities” from the drop-down menu.

Due Date

Select **All**, **Overdue**, **Due Today**, **Due in 7 Days**, or **Define Range** from the drop-down menu.



If you select **Define Range** from the drop-down menu, a calendar displays for you to select a date range.



Create a Campaign

Compliance managers and administrators - or anyone with the proper access rights - can create an access certification campaign, with or without an access certification template.

You can create a one-off campaign, store the campaign definitions as a template to be reused in future, or create a recurring or scheduled campaign.

To create an Access Certification campaign without an Access Certification template:

1. Navigate to **Compliance > Access Certification > Campaign Management**.
2. Press **+ New Campaign**

The Create Campaign screen displays, and includes the following steps :

1. General Details
2. Filter Selection
3. Review Process
4. Summary
5. Save

> Fields marked with an asterisk are mandatory

General Details:

In **General Details**, type or select the relevant data in the following fields:

Name

Enter the name of the campaign. This is a mandatory field.

Description

Enter a description of the campaign.

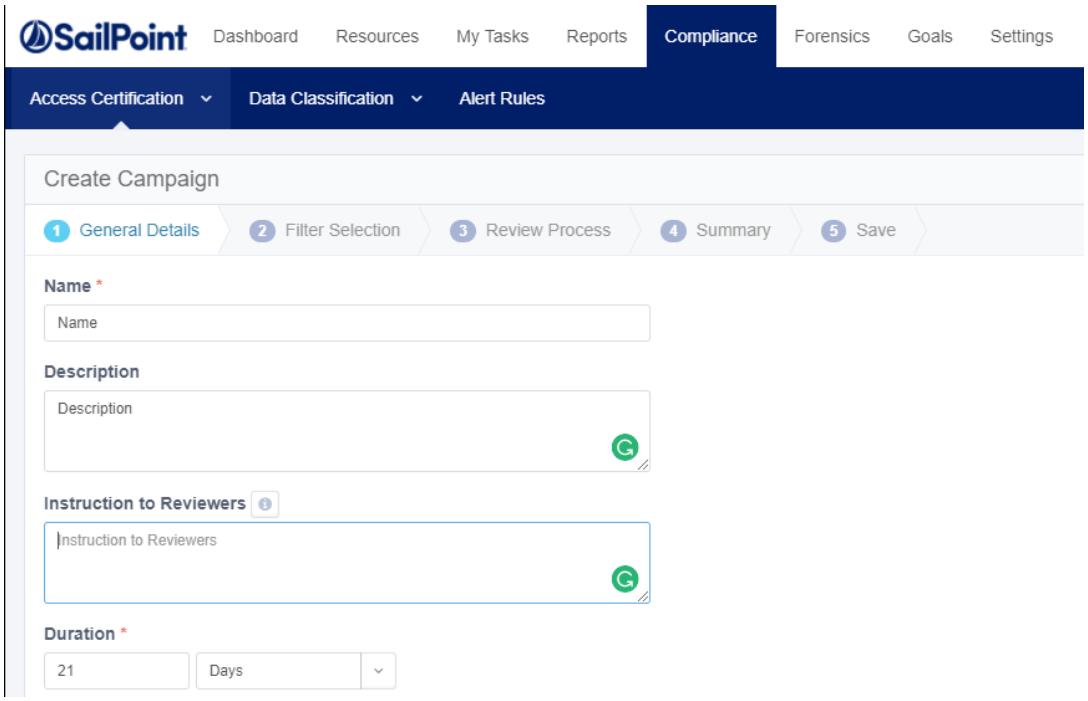
Instruction to Reviewers

This instruction text will display to the reviewer in the approval screen. It can also be used in the campaign mail templates.

Duration

Select **Days**, **Weeks**, or **Months** from the drop-down menu, and type in the relevant number of days, weeks, or months. This is a mandatory field.

The system sets the due date of a campaign, based upon the campaign duration. The due date is the recommended end date of a campaign, although the campaign does not end automatically on that date.



Click the information icon (letter “i” after the name of a field) under any of the Access Certification campaign steps listed above to view a more detailed explanation of that field.

Filter Selection:

1. Click **Next.**
2. The **Filter Selection** tab is highlighted and the tab fields display.
3. In **Filter Selection**, type or select the relevant data in the following fields:

Filter Type

Select a filter type (All, Permissions, or Identities) from the drop-down list.

You can update the filter selection in the Administrative Client (if you have permission to do so), and then click the Refresh button.

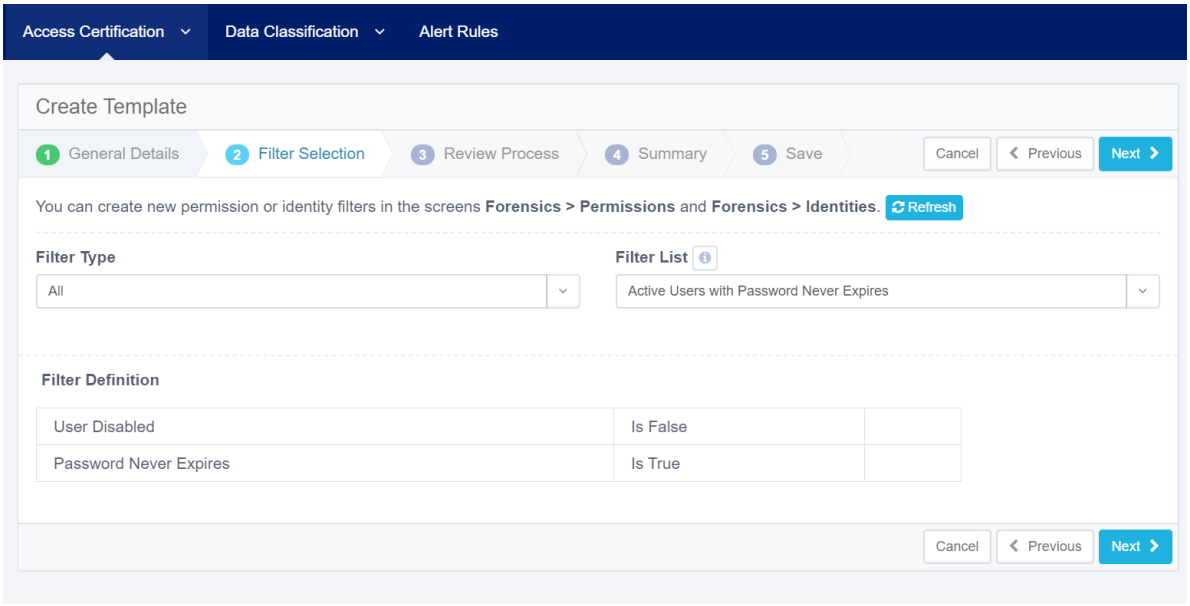
Filter List

Select a filter from the drop-down list.

Some of the filters are predefined, out-of-the-box Permissions and Identities filters.

Filter Definition

The displayed filter definition is based on the Administrative Client definitions.



If there are several items included in the definition, click the number of items to display the items.

Review Process:

1. Click **Next.**

   The **Review Process** tab is highlighted and the tab fields display.

   The predefined review process sources are “By Data Owner” or “By Selected Reviewer(s)”. If you select “By Data Owner”, the review process is only available for Permission type filters.

2. In **Review Process**, type or select the relevant data in the following fields:

   Source

Select a source (All, Predefined, or Custom) from the drop-down list.

Review Process

Select a review process from the drop-down list. (The processes available depend upon the Source you selected.)

You can update the review process list in the Administrative Client (if you have permission to do so), and then click the Refresh button.

Type of Account

Select either **User Account** or **Group Account** from the drop-down list.

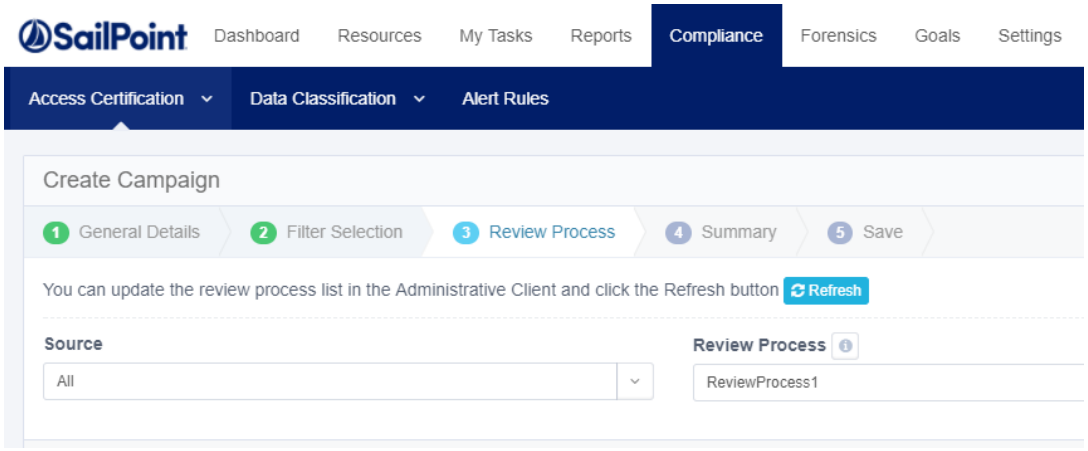
This option is only displayed if you chose the **By Data Owner** review process or the **By Selected Reviewer(s)** review process.

Default Reviewer(s)

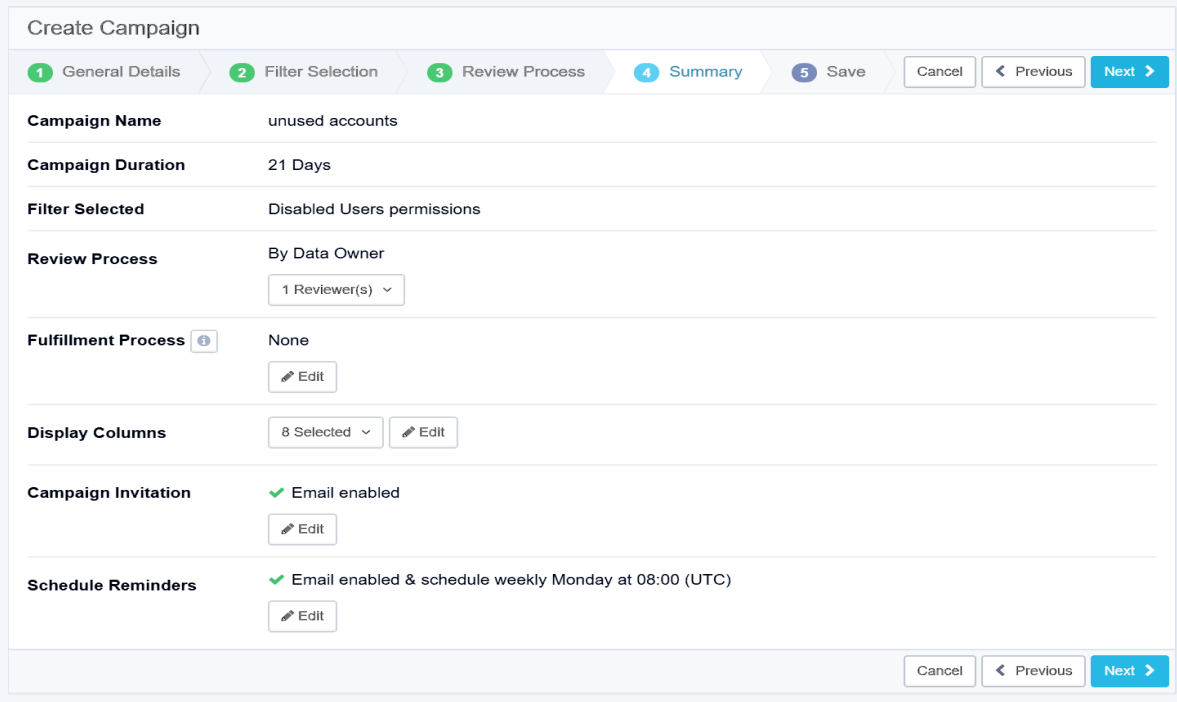
This option is only displayed for the **By Data Owner** predefined review process, since default reviewers are the reviewers when no data owner was found.
This is a mandatory field.

Selected Reviewer(s)

This option is only displayed for the **By Selected Reviewer(s)** predefined review process to set a static list of reviewers. You can choose multiple users or groups.
This is a mandatory field.



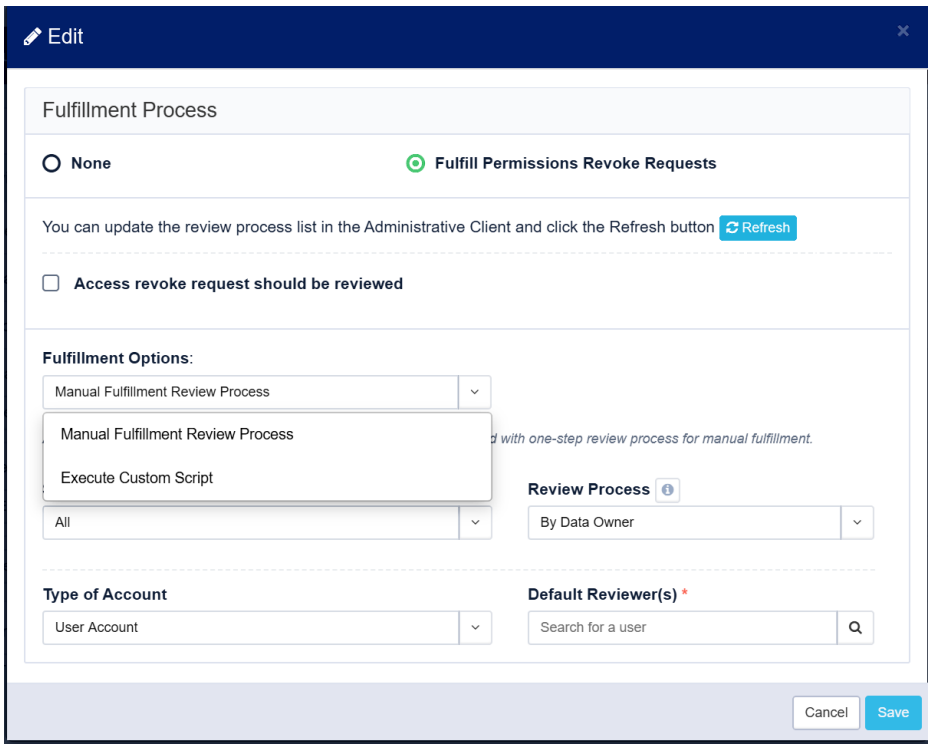
3. Click **Next**.
The **Summary** tab opens, showing a summary of the campaign. In this screen, you can view and edit the review parameters before saving and / or running the review.



Fulfillment Process

The following is available only for a predefined review process. Click the drop-down list to display the selected reviewer(s).

1. Click the **Edit** button to open the *Fulfillment Process* tab.



None

No fulfillment process

Fulfill Permissions Revoke Requests

Perform revoke requests that arise from this access campaign

Clicking this option will open the fulfillment option panel

Access revoke request should be viewed

To review the access revoke request, check the checkbox. An access revoke request is created at the end of the campaign if any records were rejected. This request contains all the permissions that the campaign reviewers revoked.

Fulfillment options

The fulfillment process could be either manual, where a user removes the users' access, or automaticaly, by a script provided by the users.

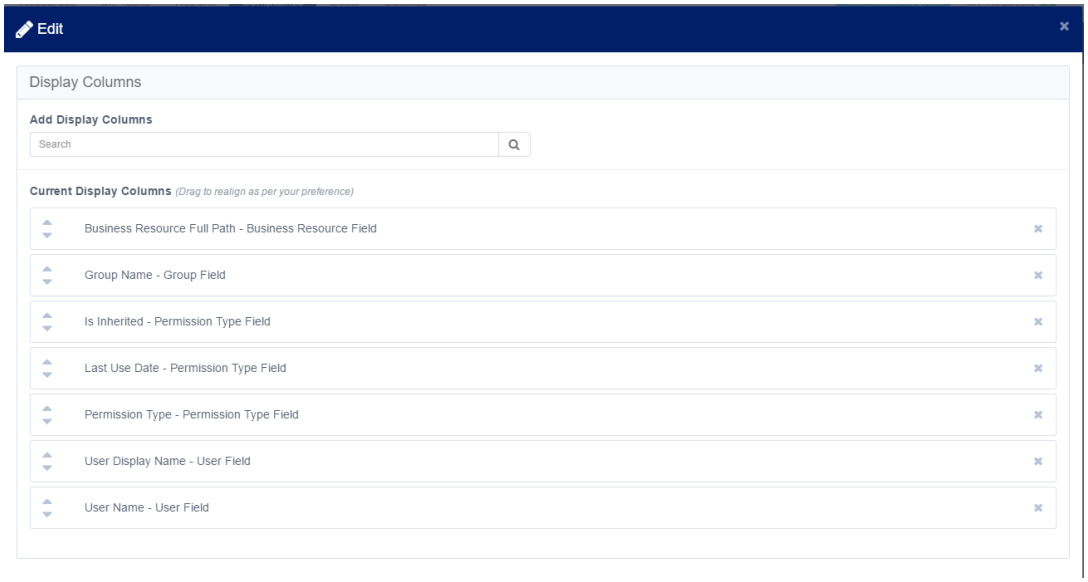
Manual Fulfillment Review Process – If an access request involves non-managed resources and identifies, a one-step review process is assigned to be fulfilled manually. The user responsible for the fulfillment will receive a fulfillment task.

Execute custom script - Automatic fulfillment using a customer supplied script from the Collector Synchronizer Service folder. The script handles the fulfillment of the revoke requests. This process works on unmanaged BRs only.

Display Columns

Click the drop-down list to display the selected columns. Click the **Edit** button to edit this selection. The columns available are based on the filter selected in Step 2. Therefore, if the filter has changed, the columns will also change accordingly.

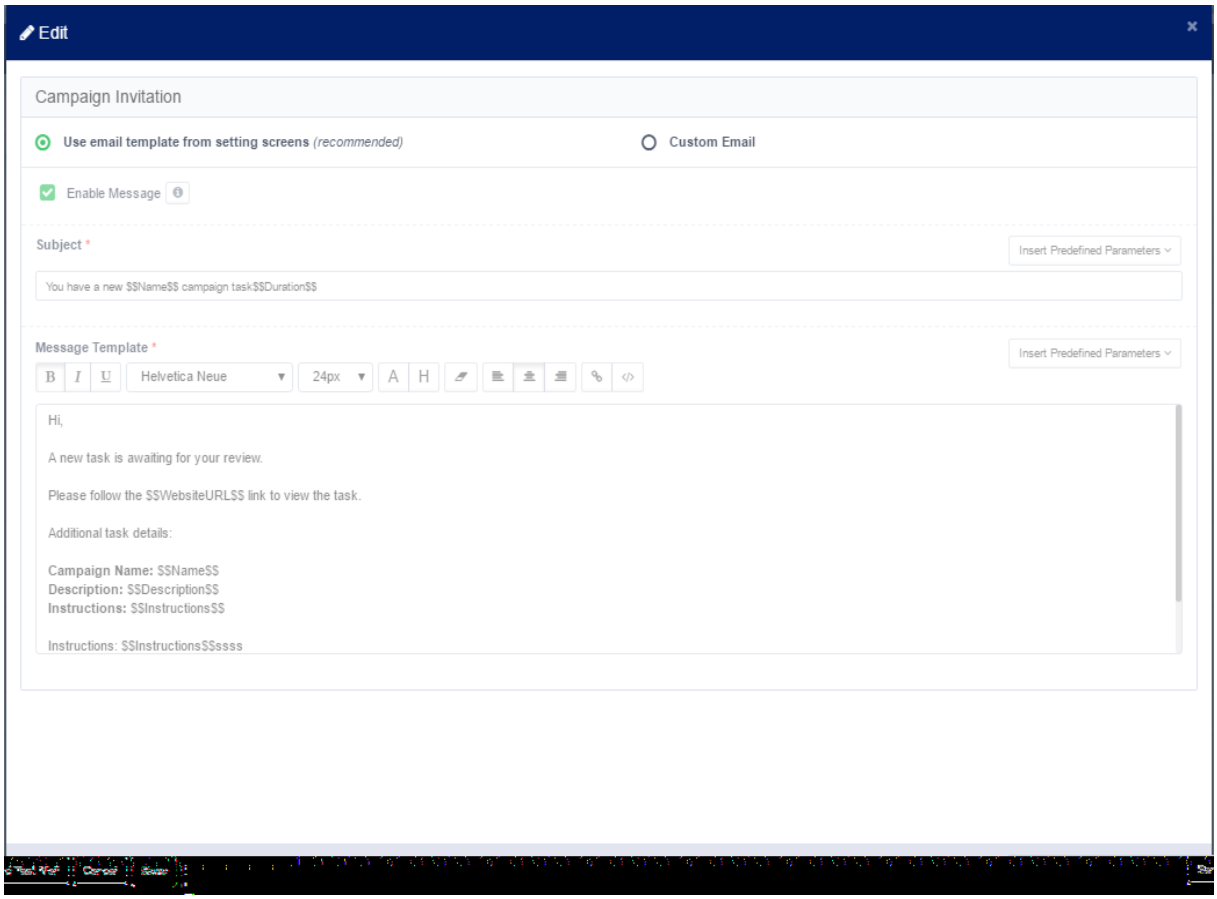
- To add columns in the Edit screen, type free text in the *Add Display Columns* field.
- To delete items in the Edit screen, click the “x” to the right of the name of a display column in the fields under *Current Display Columns*.
- To change the order of items in a column, drag and drop the items to the desired location in the column.



Campaign Invitation

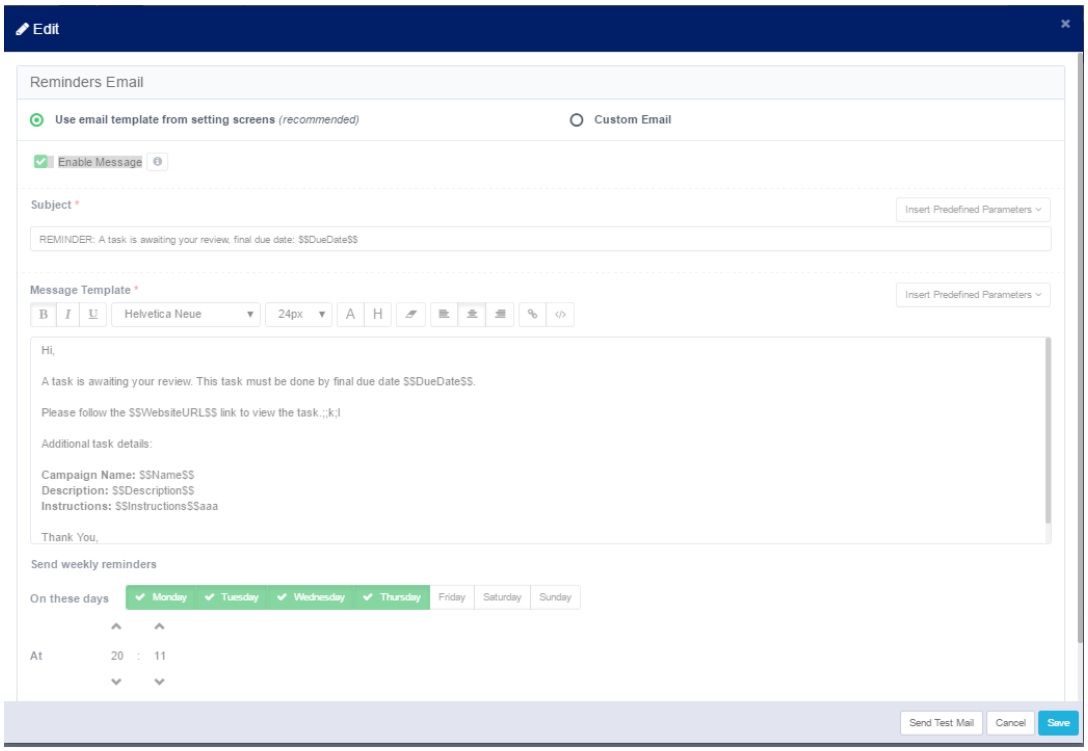
Click the Edit button to edit this selection.

In the Edit screen, click **Use email template from setting screens (recommended)** or **Custom Email** (to create an email that differs from the default email).

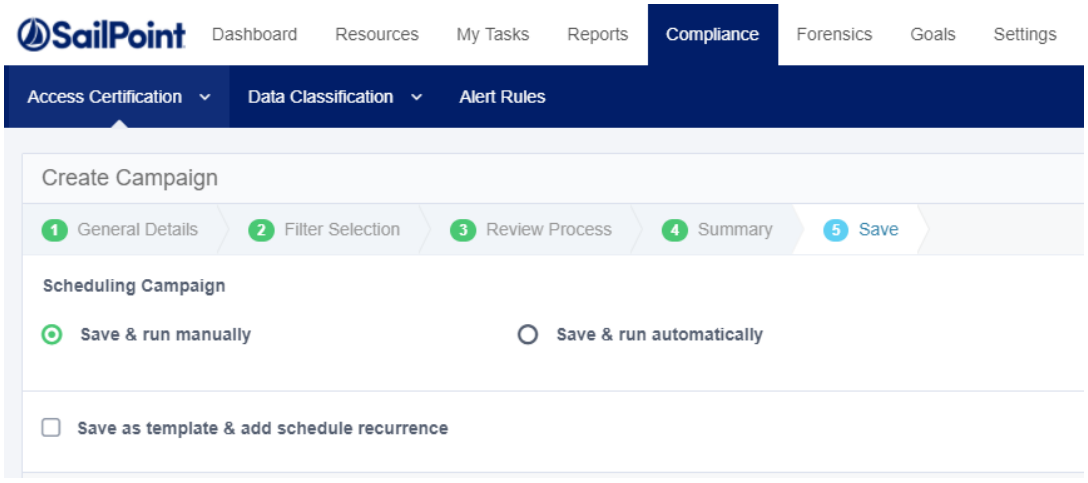


Reminder Emails

1. Click the **Edit** button to edit this selection.
2. In the Edit screen, click **Use email template from setting screens (recommended)** or Custom Email (to create an email that differs from the default email).
3. You must select the days and the time of day to send weekly reminders.



4. **Save:**When you have completed all edits, click **Next**. The **Save** tab is highlighted and the tab fields display.



Access Certification – Create Campaign - Save

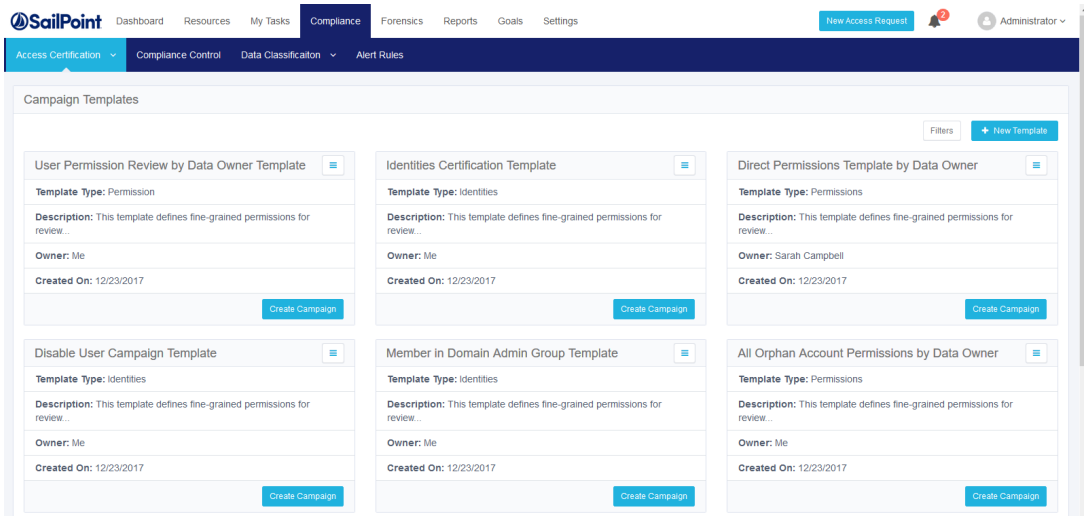
1. Click one of the following options under *Scheduling Campaign*:
   - **Save & run manually** to run the campaign when you choose after the campaign has been created and is ready to run, or
   - **Save & run automatically** to run the campaign after it has been created and is ready to run.
2. If desired, check the **Save as template & add schedule recurrence** checkbox.

> You may create a campaign template with or without a scheduler. Also, you may either run the template-created campaign automatically after creating the template, or you may run it manually in the future.

3. Click **Save**.
   *An Information pop-up window displays to indicate that the campaign has been saved successfully, and a task is created to create the campaign, itself. A **Campaign Management** link displays to redirect you to a screen to view the campaign. Alternatively, you can view the campaign by navigating to **Compliance > Access Certification > Campaign Management**.*
4. Click **Close**.

Campaign Templates

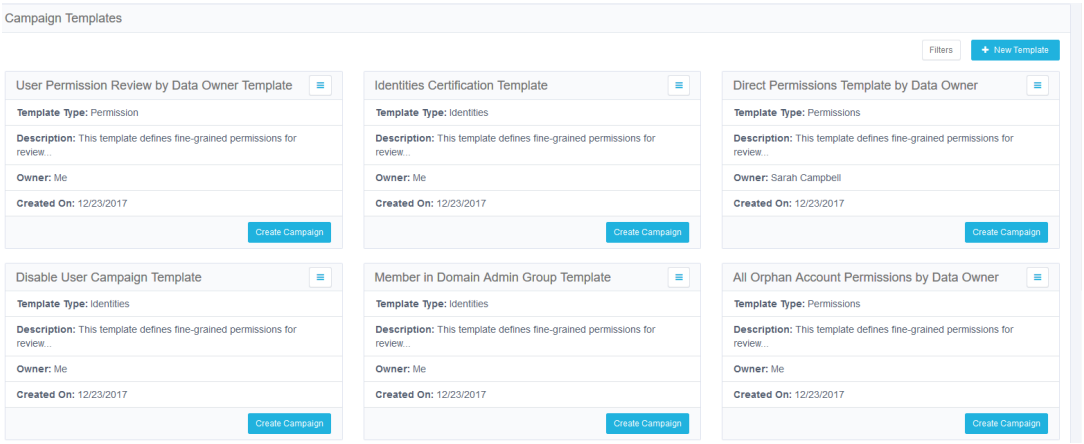
If you created campaigns using a template, and you want to delete that template, you can only do so after first deleting the campaigns from which it was created. If you attempt to delete the template, a notification will display the campaigns on which the template was based, and will request that you delete the campaigns before you delete the template.



Compliance managers and administrators can select one of the following actions to manage campaign templates:

- Create a new template
- Edit an existing template
- Duplicate an existing template
- Delete an existing template
- Create a campaign, based on an existing template

The templates display from left to right, row by row, sorted chronologically (by date of template creation).



You can filter the display of current templates to find the templates more quickly.

To filter the available campaign templates:

1. Click the **Filters** button.
2. Under **Filters**, type or select the relevant data in the following fields to narrow your search of campaign templates:

   Template Name

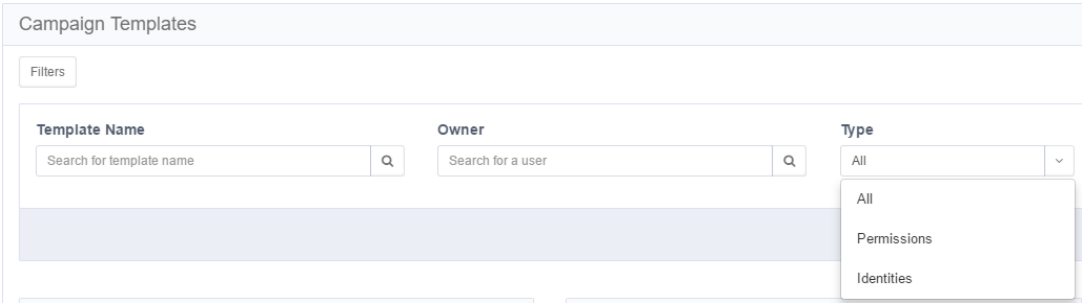
   Type the template name, or the first few characters of the template name, and then click the Search button next to that field.

   Owner

   Type the owner (user) name, or the first few characters of the name, and then click the Search button next to that field.

   Type

   Select **All**, **Permissions**, or **Identities** from the drop-down menu.



Create a New Access Certification Template

1. Navigate to **Compliance > Access Certification > Campaign Templates**.
2. Click **+New Template**.
   The Create Template screen displays, and includes the same steps in the same order as the Create Campaign steps:

a. General Details – This step has the same fields as the Create Campaign step, except that the name field is for a template (not a campaign), and the description field is for a template (not a campaign).

b. Filter Selection – This step has the same fields as the Create Campaign step.

c. Review Process – This step has the same fields as the Create Campaign step.

d. Summary – This step has the same fields as the Create Campaign step.

e. Save – The Save fields displayed in the “Create Template” process differ from the Save fields displayed in the “Create Campaign” process.

3. Follow the process steps described in creating a campaign, from **General Details** to **Save**.
4. When you reach the **Save** step, the **Save** tab is highlighted and the tab fields display.
5. You may save the template with or without a schedule.
6. Save the new template without a schedule by leaving the “Enable Schedule” checkbox unchecked, or
7. Save the new template with a schedule by checking the “Enable Schedule” checkbox, and then type or select the relevant data in the following fields:

   - Frequency Type – Select “Monthly” or “Yearly” from the drop-down menu.
   - Starts On – Click the calendar icon to the right of this field and select a start date from the calendar that displays.
   - Ends On – Click either the “Never” or the “On” radio button.
     To make the selection available indefinitely, click “Never”, and the end date selection will not be enabled.
     To make the selection available for a set period, click “On”, then click the calendar icon to the right of this field, and select an end date from the calendar that displays.
   - Interval Of – Type the number of months or years (depending upon the “Frequency Type” selection) to indicate how often to schedule the template.
   - The new campaign will be created from the “Starts on” date to the “Ends on” date, based on the selected frequency and interval in months or years.
   - Summary – This field summarizes the selections made in the previous fields (for example, “every 2 months on [start date] until [end date]).
   - Time – Use the up and down arrows to select a schedule time, based on the 24-hour clock (for example, 1:05 p.m. displays as 13:05).

8. Run the campaign manually (not on a set schedule) by leaving the “Campaign will run automatically on the set schedule” checkbox unchecked, or
9. Run the campaign automatically on the set schedule by checking the “Campaign will run automatically on the set schedule” checkbox.

   > All campaigns created from this template and set to run automatically will continue to run until they are reset manually.

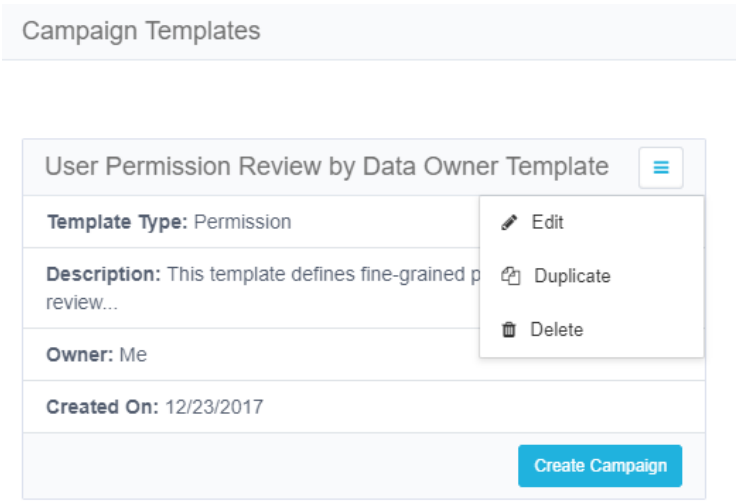
10. Click **Save**.

An Information pop-up window displays to indicate that the template has been saved successfully, and a task is created to create the template.
A "Template Management" link displays to redirect you to the Campaign Templates screen to view the template.
Alternatively, view the campaign by navigating to **Compliance > Access Certification > Campaign Management**.

11. Edit the template to make changes to an existing template.
12. Duplicate the template to make a new template based on an existing template (with some changes, if needed).

Edit an existing Access Certification template

1. Navigate to **Compliance > Access Certification > Campaign Templates**.
2. Select a template from the displayed templates.
3. Click the menu button on the top right of the selected template.
   *The **Edit**, **Duplicate**, and **Delete** options display.*



4. Click **Edit**.
   The Edit Template screen displays, and includes the same steps in the same order as in the Create Template screen:
   a. General Details
   1. Filter Selection
   2. Review Process
   3. Summary
   4. Save
5. Review each step and make any relevant changes.
6. Click Save to save the changes.
   An information pop-up window displays to indicate that the template has been saved successfully.
7. Click **Close**.

Duplicate an existing Access Certification template

1. Navigate to **Compliance > Access Certification > Campaign Templates**.
2. Select a template from the displayed templates.
3. Click the menu button on the top right of the selected template.
   The Edit, Duplicate, and Delete options display.
4. Click Duplicate.
   The Duplicate Template screen displays, and includes the same steps (in order) as the Edit Template screen.
5. Review each step and make any relevant changes.
6. Click **Next** to proceed to the next step.
7. Click **Previous** to return to the previous step.
   An Information pop-up window displays to indicate that the template has been saved successfully.
8. Click **Close**.

The duplicated template will be the newest template in the Campaign Templates display, and will have the same name as the original template, with *Copy of* before the name.

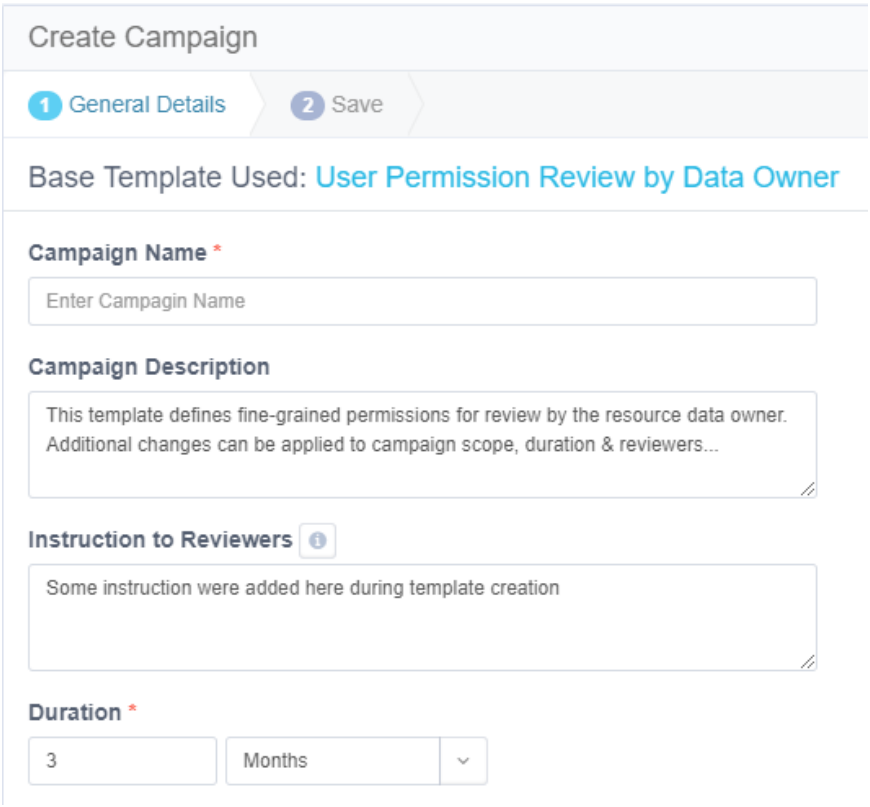
> If you no longer need a template, you can delete it, but it is not possible to recover a template that has been deleted.

Delete an existing Access Certification template

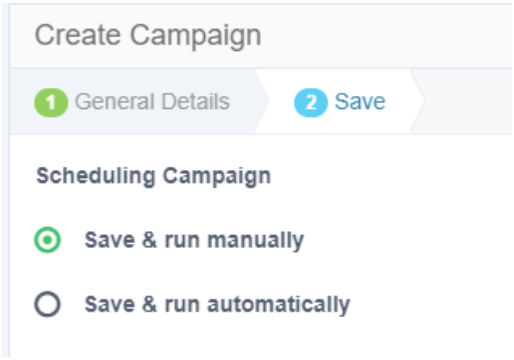
1. Navigate to **Compliance > Access Certification > Campaign Templates**.
2. Select a template from the displayed templates.
3. Click the menu button on the top right of the selected template.
   The Edit, Duplicate, and Delete options display.
4. Click **Delete**.
   A question pop-up window displays, asking if you are sure you want to delete the template.
5. Click **Yes** to delete the template, or click **No** to retain the template.

Create an Access Certification campaign based upon an existing Access Certification template

1. Navigate to **Compliance >** *Access Certification > Campaign Templates*.
2. Select a template from the displayed templates.
3. Click the Create Campaign button on the bottom left of the selected template.
   The Create Campaign screen displays, with the General Details step displayed automatically.



4. In the**General Details** tab, type or select the relevant data in the following fields:
   - Campaign Name – Enter the name of the campaign. This is a mandatory field.
   - Campaign Description – Enter a description of the campaign.
   - Instruction to Reviewers – This instruction text displays to the reviewer in the approval screen. It can also be used in the campaign mail templates.
   - Duration – Select “Days”, “Weeks”, or “Months” from the drop-down menu, and type in the relevant number of days, weeks, or months. This is a mandatory field.
     The system sets the due date of a campaign, based upon the campaign duration. The due date is the date on which it is recommended that a campaign should end, but the campaign does not end automatically on that date.
5. Click **Next**.
   *The **Save** step displays.*



6. Under Scheduling Campaign, select one of the following options:
    - Save & run manually – This option saves the campaign for you to run manually in the future.
    - Save & run automatically – This option saves the campaign, and runs it automatically when the template was set to run (in the Create Template or Edit Template steps).
7. Click **Save**.
   An Information pop-up window displays to indicate that the campaign has been saved successfully, and a task is created to create the campaign, itself. A "Campaign Management" link displays to redirect you to a screen to view the campaign. Alternatively, you can view the campaign by navigating to ***Compliance [[[Undefined variable FileAccessManager.SP_Menu_Separator]]] Access Certification [[[Undefined variable FileAccessManager.SP_Menu_Separator]]] Campaign Management****.*

Alert Rules

Alert Rules define activity-based criteria for generating system alerts, including notifications and customized responses, such as email, SysLog, or UserExit.

Compliance > Alert Rules – Defining alert rules

Examples of alert rules:

- A file under \\FileStorageApplication\HR is deleted by a user who is not a member of the HR department.
- A specific user reads more than 1000 files in one minute (considered a suspicious activity, regardless of whether the user or malware initiated the activity).

To view existing alert rules:

1. Navigate to **Compliance > Alert Rules**.
   All alerts, including alerts in the Resources section, display in this screen.
2. Click **Include Resource-based Rules** to view alerts from Resources.
3. You can filter the screen by:
    - Rule Name
    - Status - Activate or deactivate an alert rule from the main screen – there is no need to access the rule.....

Managing Alert Rules

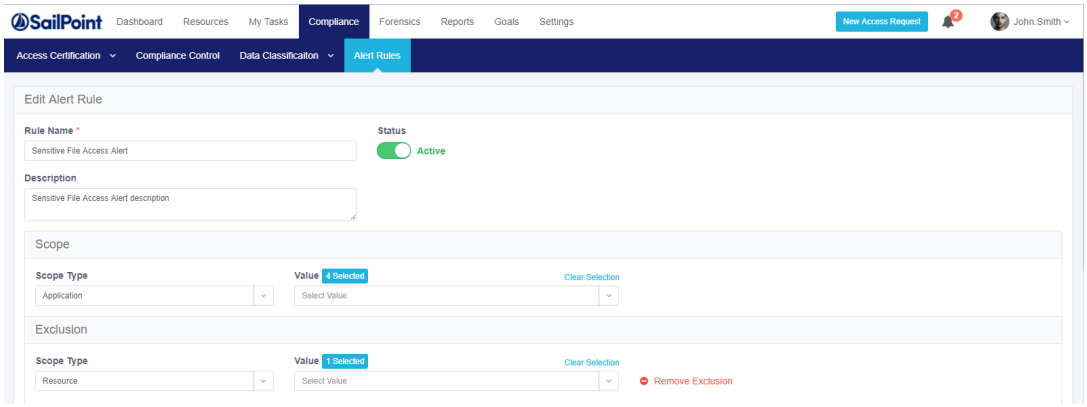
To access the alert rules, Navigate to **Compliance > Alert Rules**.

To open an alert rule for edit, double click the alert rule to edit.

To edit an alert rule:

1. Make changes to the relevant parameters of the General, Scope, Filters, Triggers, and Response sections of the Rule Criteria section, as appropriate.

> An Administrator can define and customize response options in the administrative client.



To duplicate an alert rule:

1. Click **Duplicate** from *Actions* in the alert rule to be edited.
2. The Duplicate Alert Rule screen displays, with all the definitions of the duplicated rule already filled in.
3. Make any required modifications.

> Duplicate a discard rule to create a new rule with definitions that resemble those of an existing discard rule.

To delete an alert rule:

1. Click **Delete** from *Actions* in the alert rule to be deleted.
2. A delete confirmation question displays.

Scope

Use Scope to select a relevant running target.

- Scope inclusion enables users to specify application type, application, or specific business resource to run an alert rule.
- Scope exclusion allows users to avoid running a rule on an irrelevant application type, application, or specific business resource.
- If the same resource is selected for both inclusion and exclusion, the resource will be excluded since exclusions always overrule inclusions.
- Resource scope selection allows users to select or unselect a subfolder to run a rule by checking the “Including subfolders” checkbox:

For example, if the business resource “Sensitive folder” has a sub-folder, called “Non sensitive folder” if the user deselects the “Including subfolders” checkbox, the rule will only run on the main resource, which is “Sensitive folder”.

Filters

If an application has a Data Enrichment Collector (DEC), the attributes of that DEC also display. However, you select more than one application from same application type, and the applications share the same DEC, only the DEC attributes common to all of the applications’ DECs display. If there are no DECs in common, only attributes relevant to the application type of the selected applications display.

Filter criteria allows users to specify suspicious behavior, based on the selected filter criteria parameters.

The available filter criteria attributes depend on the scope selected.

If you did not select a scope, or if you select an application type, or if you select applications from a different application type, only the following default attributes are available:

- Action Type
- Category
- Domain
- Event Date
- Event Time
- Path
- User Name

However, if you select a specific application type or a single application, or if you select multiple applications from a single application type, only the attributes relevant to the selected application type display.

Users can use queries saved in **Forensics > Activities** queries by clicking on **Load Query**, to display a list of all saved queries.

When the query is loaded, all the information in the Rule Criteria section (Scope and Filters) is overridden by the loaded query filters. If a query cannot be loaded, an error message displays.

The following queries are not available:

- Queries on alerts (since only existing queries on activities can be loaded)
- Mismatched queries
- Queries involving users from more than one domain

Response

The Response section allows users to define a response for an alert.

For example, when a new permission is added to a sensitive resource, all the Data Owners of that resource can receive an email, notifying them that a new permission was added.

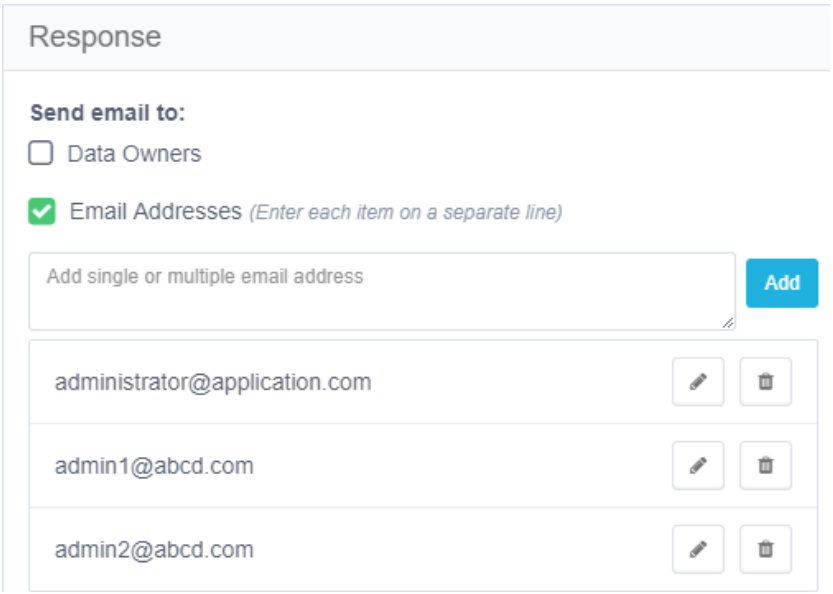
A Response may be one of the following:

- Email to specific email addresses, and/or to the Data Owners who own the resource.

  > Currently, the Data Owners option is available for Single Activity Alerts, but not for Threshold Alerts.

- Syslog
- User Exit

1. A Response object is created / edited in the IdentityIQ File Access Manager Administrative Client.



2. Click **Advanced Settings** to select additional option responses.

> Use the IdentityIQ File Access Manager Administrative Client to define and customize response options.

> File Access Manager Alert Response is an automatic default, since it retains the alert in the database. A user cannot opt out of the File Access Manager Alert Response.

Resource-based Alert Rules

Data Owners can activate Resource-Based Alert Rules (out-of-the-box alert rules) in the **Resource > Alerts** screen.

Administrators can navigate to **Compliance > Alert Rules** to perform the following operations on Resource-Based rules that were created by Data Owners:

- View the rule
- Change the rule's name/description
- Change the rule's status (active/inactive)
- Delete the rule

Troubleshooting Activities

The best way to troubleshoot activities is to follow their activity trail.

Use a specific Collector Installation and Configuration Guide to troubleshoot a specific monitoring issue for that Activity Monitor.

The lists below are suggestions of what to look for in the various services.

Application

- All prerequisites were completed successfully.
- Activities are generated when relevant. For example, check that relevant activities are generated in the Event Log in Active Directory or that they are included in the Exchange Audit log.

Activity Monitor Log

- The log has errors.
- Events were received (by viewing the Monitor Statistics file).
- Events were monitored, but not sent (by checking the monitoring mode – full, semi, and discard) .

Event Manager

- New events were entered (by viewing Event Collector statistics) and then moved to the memory queue.
- Events were saved in the Event Manager (one Connector at a time, or through a dedicated Event Manager).
- The Event Manager log has errors.

Events Backup

IdentityIQ File Access Manager includes a backup mechanism for events streaming into the Event Manager. Incoming events are serialized to disk as compressed bulk events.

- This backup mechanism allows for re-streaming the backed-up event bulks into the event manager in case of a failure in the events processing flow.
- A separate file is created daily, containing the bulk events received that day.

The behavior of the Events Backup mechanism is defined by several parameters under the <appSettings> tag in the Event Manager's app.config files:

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

<add key="WaitForBackupSeconds" value="5"/>

<add key="BackupEventsDir" value="EventsBackup"/>

<add key="RestoreBackedupEvents" value="false"/>

<add key="BackupRetentionDays" value="7"/>

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

Parameter	Type	Description	Default
BackupEvents	True/ False	Enables / Disabled the Events Backup mechanism	True
WaitForBackupSeconds	Number	Number of seconds the Event Managers service waits for the backup process to finish serializing in-memory events, on service shutdown, before it terminates the process	5 (seconds)
BackupEventsDir	Text	Directory path for the event backup files	EventsBackup in the service home dir
RestoreBackedupEvents	True/False	Activates backed up events restore on service startup	False
BackupRetentionDays	Number	Number of days to retain events backup files, before backup files are deleted.	7 (days)
CleanOldBackups	True/False	Enables/Disables automatic cleanup of expired backup files (older than *BackupRetentionDays*)	True

To Enable Events Backup

- Set the *BackupEvents* to **True** (default). This will cause the Backup mechanism to start.
- The *BackupEventsDir* by default will be set to EventsBackup in the service's home directory. This folder will be created by the service if it is not already there. If you wish events to be backed up to another location, change the *BackupEventsDir* parameter accordingly before the service is started, or restart it after the change. Make sure the drive containing the backup folder has enough space. (Space requirements depend on events traffic).
- Make sure the *RestoreBackedupEvents* parameter is set to false – if you don't wish to restore existing backups.
- Ensure all other parameters suit your needs, or configure accordingly.

To Restore events from previous backup

- Set the *RestoreBackedupEvents* to True before you start the service, or restart it after the change.
- Once the service is running with *RestoreBackedupEvents* set to True, it will attempt to restore all backup files, and will stream all backed up events, back to the Event Manager, to be processed and stored in File Access Manager.
- If you do not wish to restore all the backup files, but only specific files (days), you should copy the unnecessary files to another location.
- In case restoring the events fails, a new file contained the un-restored events will be created, with the *.recreated* suffix, indicating this file contains events that failed to be restored, and will not be re-attempted.

To Retain backups for specific dates or longer periods:

- Either disable the automatic cleanup of backup files, by setting the *CleanOldBackups* parameter to **True**, or modify the *BackupRetentionDays* parameter to suit the retention policy you wish to configure.
- When modifying app.config parameters, changes will take place only the next time the service is started, as app.config parameters are read on service startup.

Threshold Alert Rules

Architecture and Flow

The Activity Analytics service is responsible for the threshold calculation and issuing threshold-based alerts.

Activities are evaluated against threshold alert rules by the Event Manager during the processing of the activities, and if they match, they are marked as candidates for a threshold calculation.

The Activity Analytics queries the Elasticsearch every defined interval to bring activities candidate for threshold alerts. It then aggregates the activities and when the threshold is met, issues an alert and a response according to the definition in the threshold alert rule.

Limitations

Activities received more than 15 minutes after the Activity time (as the result of a temporary disconnection between the Activity Monitoring and the Event Manager) will be kept in the Database with the original Activity time, but will not be included in the Threshold Alert Rules calculation. However, if an Alert has already been created, the Activities that originated in the Alert timeframe, but were received after the 15-minute time window, will be updated in the relevant existing Alert record. (As a result, the total number of Activities in the existing Alert record will increase.)

The 15-minute time window helps limit the memory required for the Threshold Alert Rules calculation.

Please review the Compass forum for best practices. If required, the PS team can change the time window in the Database.

If Windows activities have more than one shared path, the system will send duplicate activities for a threshold alert calculation. For example, if Folder1 can be accessed by \\MyServer\Folder1 and by \\MyServer\C$\Main\Folder1, each activity performed in Folder1 will appear twice in the Database, each time, with a different shared path.

To prevent duplicate activities from being calculated in the total number of activities required to create a threshold alert, select “Windows” as the application type in the scope, and set the following filter in the **Alert Rule > Rule Criteria Filter** section:
Attribute = Original Access Path (OAP)
Operator = Empty

All duplicated Activities have the OAP field as part of the original path. Adding this filter causes the Threshold Alert Rule to ignore all duplicated Activities and to calculate only the original Activity.

Create/Edit a Threshold Alert Rule

See for information on creating a Threshold Alert rule.

Only administrators (not data owners) can view threshold alerts in Activity Forensics or in Reports.

Forensics

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

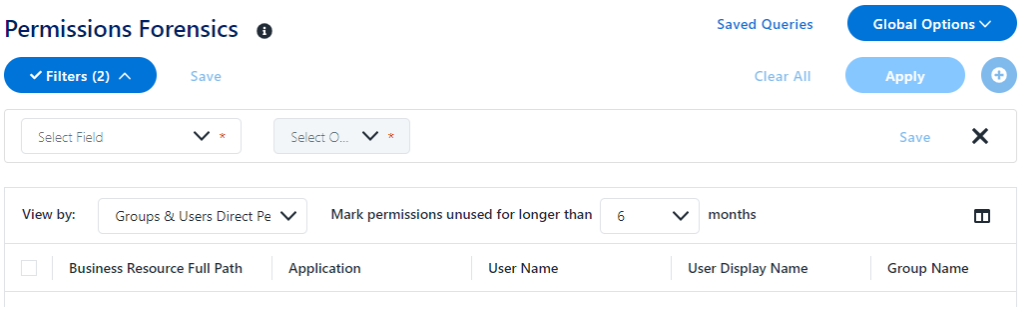
The IdentityIQ File Access Manager website has the following forensics' screens:

- 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?

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.

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:

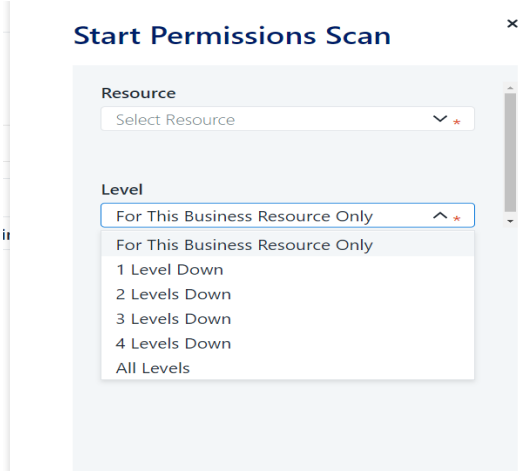
- A proprietary column, called “Is Owner Permission” indicates whether a given permission is an Owner permission.
- A proprietary query attribute is dedicated for filtering Owner permissions (allowing queries and/or reports listing the owners of resources).

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

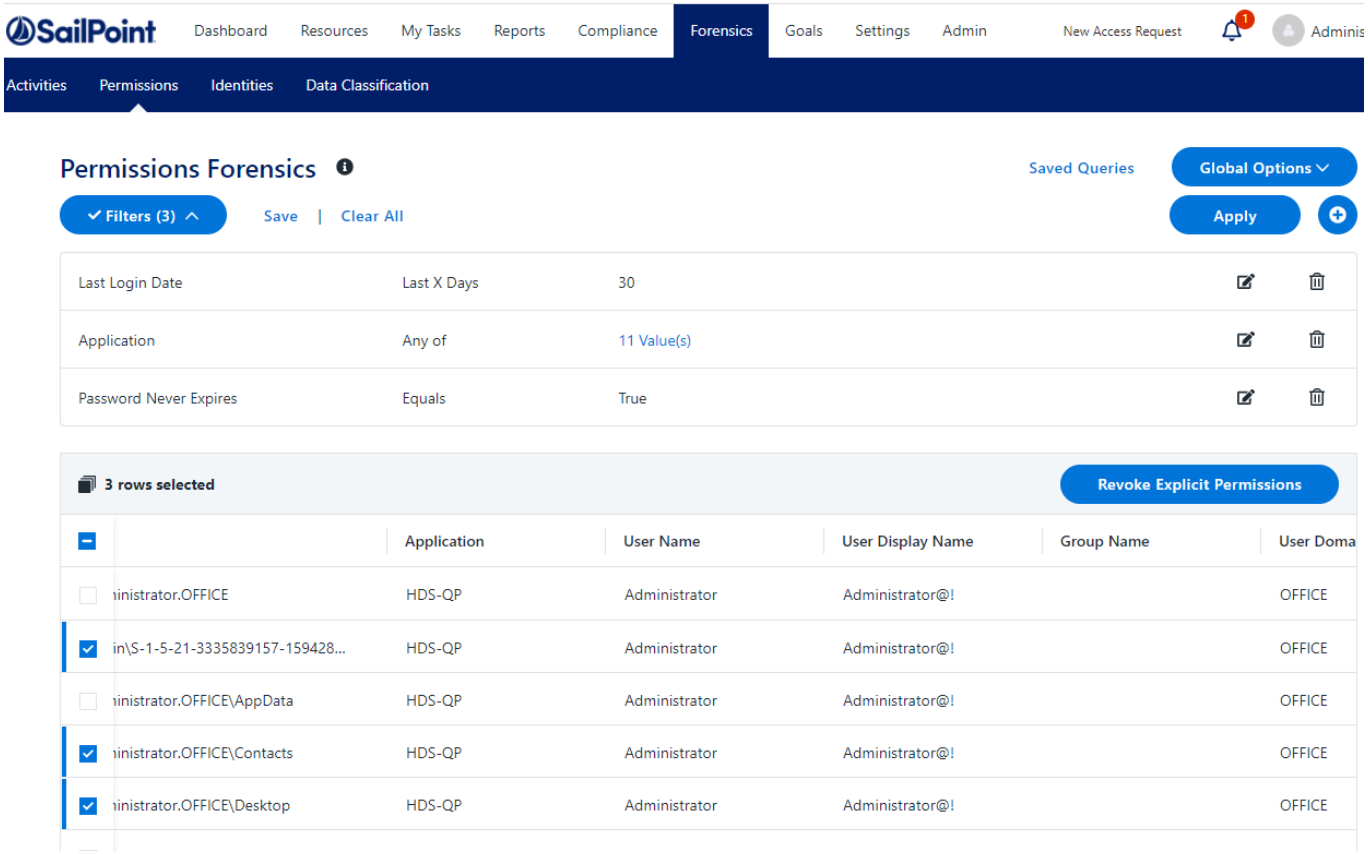
> This process will revoke explicit permissions from non-normalized resources that are configured for access fulfillment. Permissions that are inherited will not be removed.

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**.

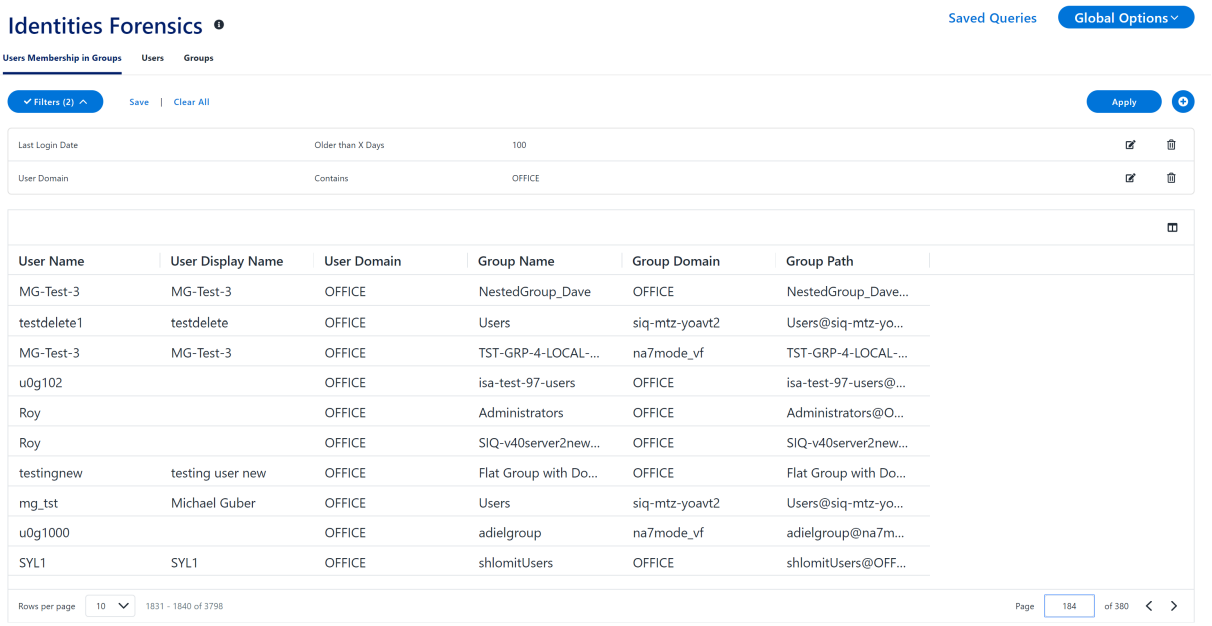


Viewing Identity Forensics Results

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.

limited to 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

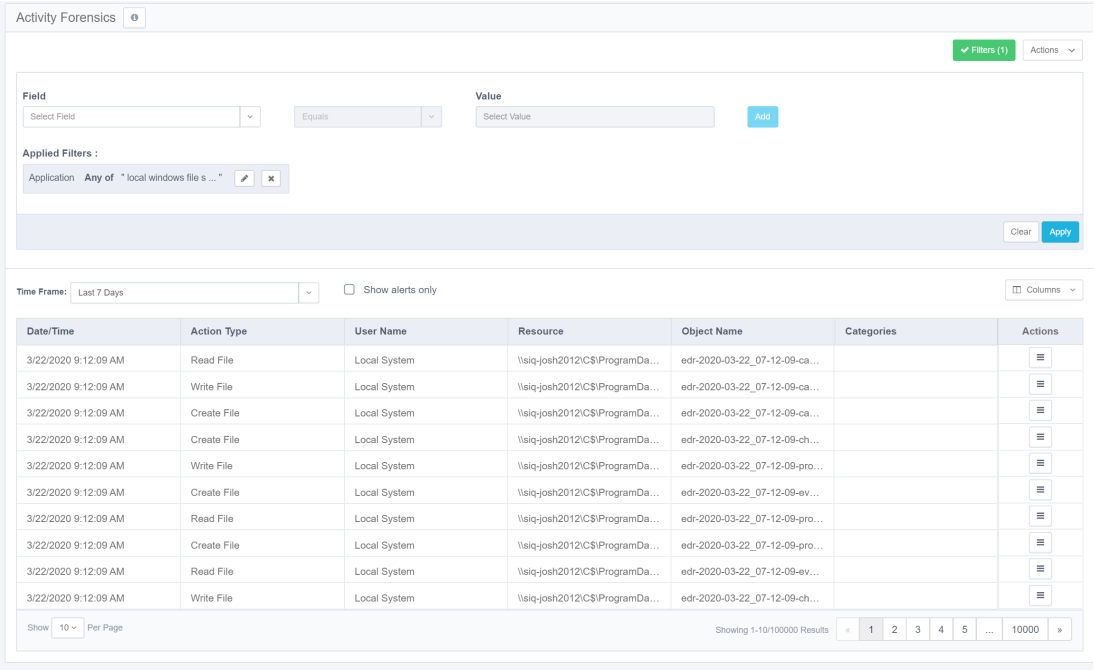
This tab displays groups and their attributes, defined in the identity store.:

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:

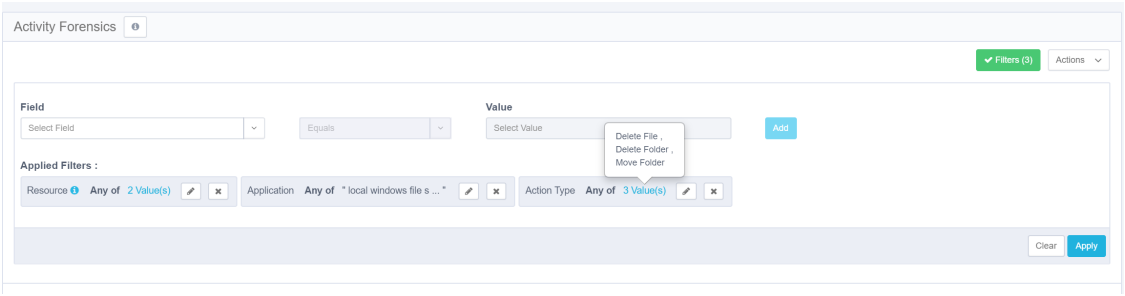


Filter

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 drop-down 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

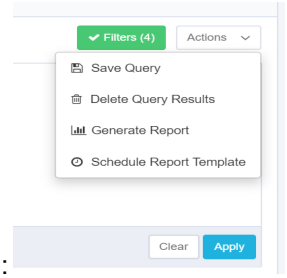
Common Activity Forensics filter fields

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.



:

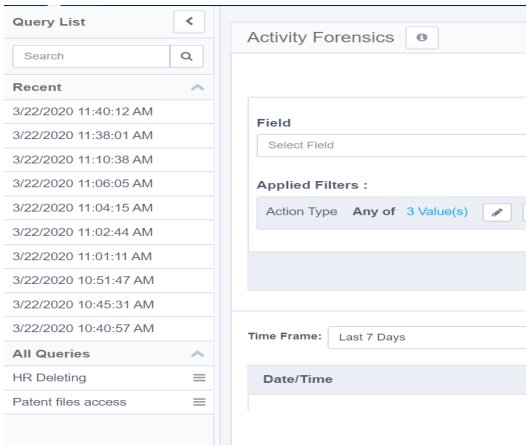
To store or share queries

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

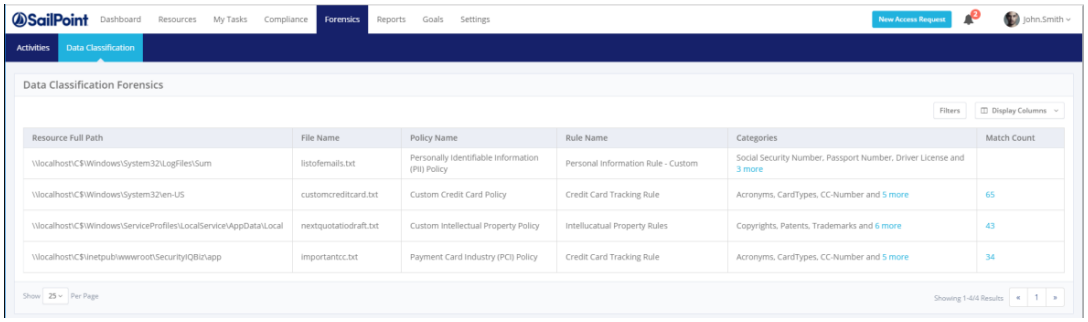
You can also create a repeated report from the query.

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 IdentityIQ 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.

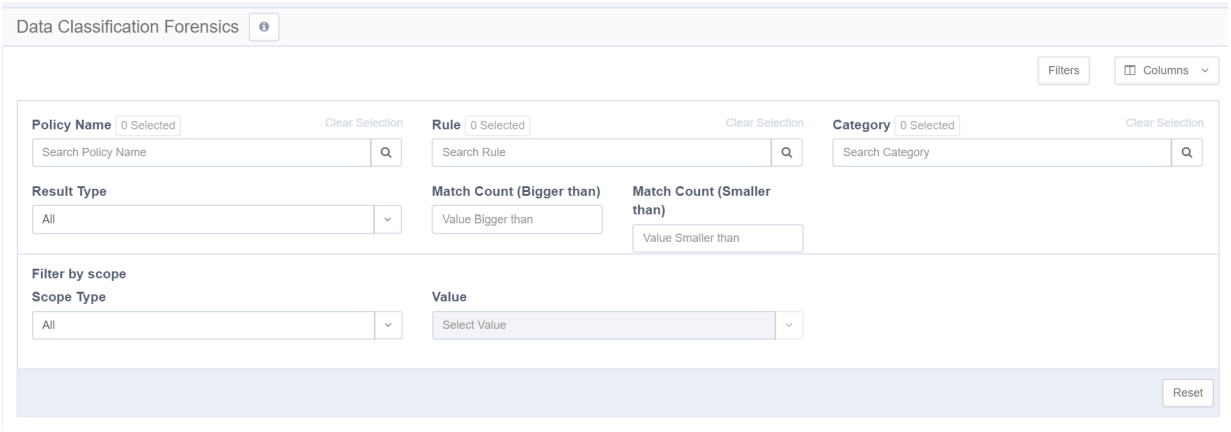
For example, if a policy rule contains two rule requirements – one matching credit card numbers with ten occurrences of credit card numbers within the same file, and another matching telephone numbers with eight occurrences of telephone numbers within the same file, the Match Count value of the file 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.

Goals

Currently, the only goal available is the Data Owner's Election. Data Owners are responsible for protecting the data within a specific resource. Administrators use the Goals process so that those who are the most knowledgeable regarding the use of a specific resource can elect (via a crowd sourcing process) the most suitable data owners for a specific resource.

> The right to view the Goals tab is assigned by default only to the administrator capability.

A *running goal* refers to each determination of a data owner of a resource in a crowd sourcing process, while a *goal* refers to a collection of all the determinations of data owners of resources in a crowd sourcing process. Therefore, a *goal* is a collection of *activities*.

For example, if the goal is to determine the identity of the data owners for five business resources in a file server application, that goal consists of five running goals – one for each resource.

The goal lifecycle stages are:

Goal creation

First, an administrator creates goal activities, specifying the goal type, application, scope, and settings.

Goal is Pending for Execution

After goal creation, but before the system sends emails to participants, an administrator checks the goal status, including the goal participants selected, and the data owner candidates selected, to validate successful goal creation.

Election

After goal execution, participants (who were decided upon in the creation process) vote for data owners.

Appointment

Reviewers review the selected data owners (unless the administrator choses the automatic selection of data owners(.

Completed

A goal is completed when all the goal activities have been completed (for example, all data owners have been assigned).

Running Goals

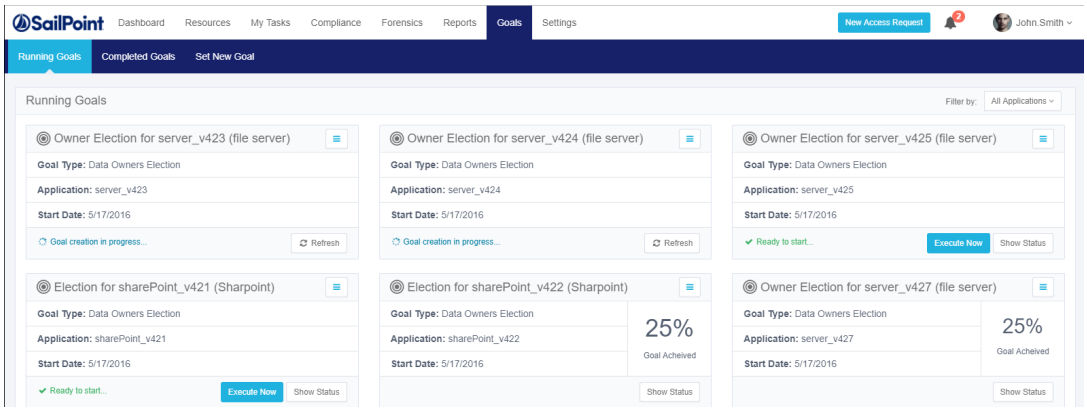
A running goal is a goal in process, in which no owner has yet been assigned to the goal resource. Any number of running goals may be displayed at any given time.

Administrators can manage goals more efficiently by viewing the status of the goals before executing them.

To view goal status details, perform the following steps:

1. Web Client Navigate to **Goals > Running Goals**.

The Running Goals screen displays.



Important general notifications display immediately under the “Running Goals” title. Examples of notifications include any goals that have been deleted or that have been reinitialized and are ready to start.

All goals display:

- Goal Type
- Application
- Start Date

If a goal is being created, “Goal creation in progress…” displays in blue at the bottom left of the goal display.

2. Click **Refresh** in any goal being created to refresh the goal creation progress status.

If a goal has been created, and is ready to start, “Ready to start…” displays in green at the bottom left of the goal display.

3. Click **Execute Now** to start the goal

Execution of the goal begins.

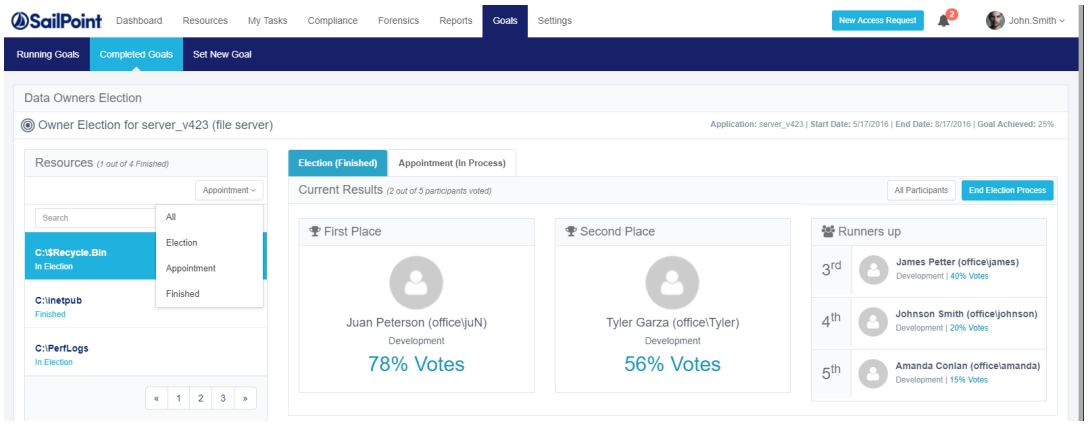
4. Click **Show Status** to show the goal status.

If a goal has already been started, the percentage of the goal achieved displays.

5. Click **Show Status** to show the goal status.

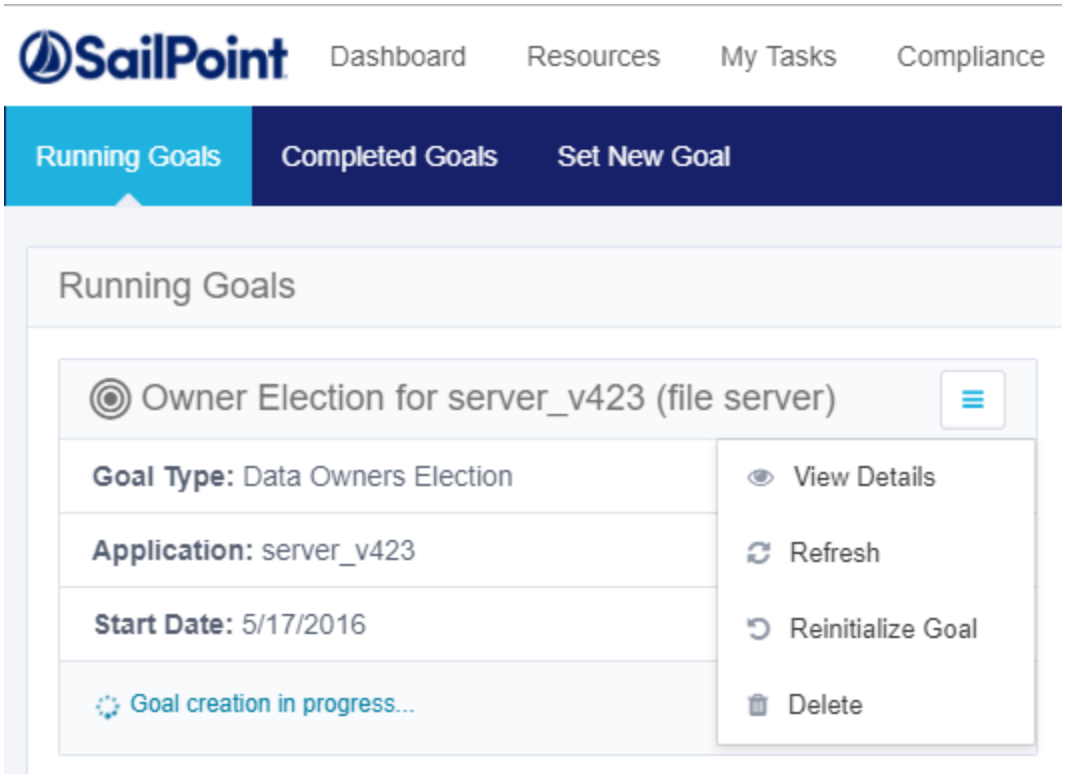
> Whether you click Goal Status in a goal that is ready to start (or in a goal that has already started) the status of the running goals displays, based on one of the following filtered statuses (the default being “All”):

- All – Displays all the resources in this goal
- Election – Displays resources in the Election state (pending completion of voting)
- Appointment – Displays resources in the Appointment state (pending review)
- Finished – Displays all the resources for which the Election and Appointment processes have been completed.



If no candidates were selected as data owners for a given resource, the message “There were no eligible candidates for the selected resource” displays to the right of the list of resource statuses.

6. Click the menu button on the right top of the Running Goals window to display a dropdown menu of status activities.



The Running Goals status actions include:

- View Details – Displays all goal details
- Refresh – Updates goal status
- Reinitialize – Starts the goal creation process from the beginning. The status will be “Ready for Execution” and

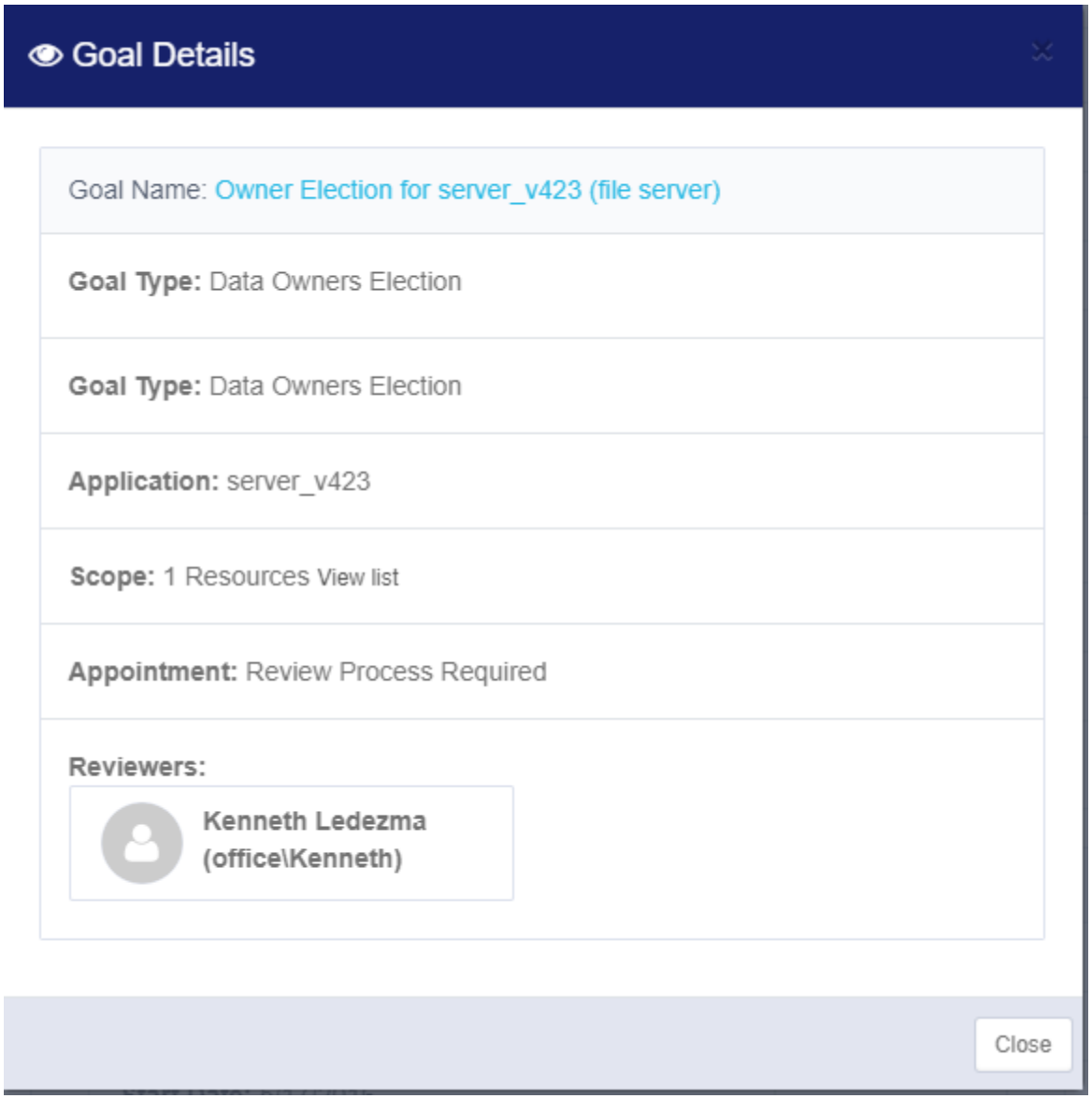
the system will delete all votes. This action cannot be undone.

- Delete – Deletes the goal

When you click Reinitialize, a Question dialog displays, asking if you are sure you want to reinitialize the goal. Click Yes to reinitialize, or No to return to the Running Goals screen.

- Delete – Deletes the goal. This action cannot be undone.

When you click Delete, a Question dialog displays, asking you to confirm deletion of the goal. Click Yes to delete, or No to return to the Running Goals screen.



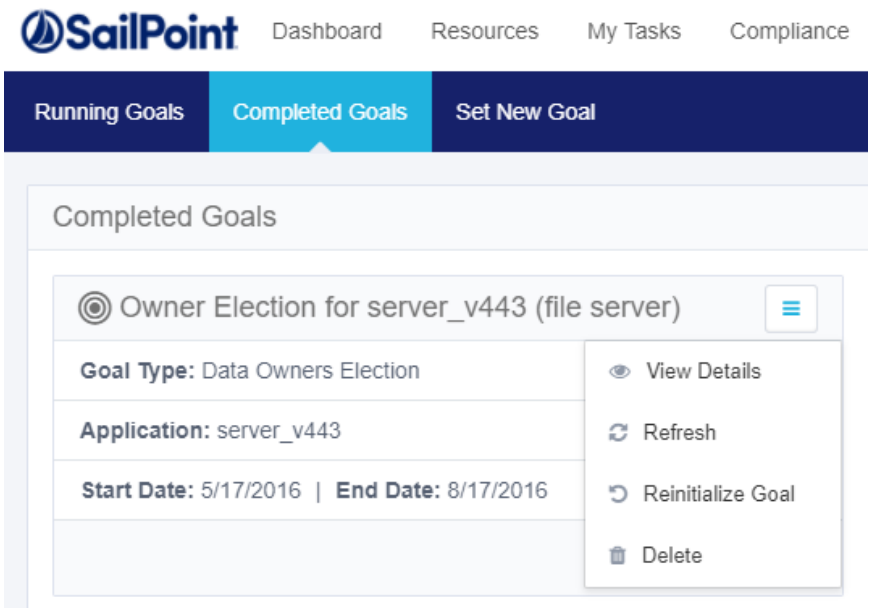
Completed Goals

A completed goal is a goal to which an owner has been assigned to the goal resource.

The Completed Goals tab displays a summary of the completed goals displays, including the following information:

- Goal Type
- Application
- Start Date
- End Date
- Percentage of Goal Completed

Click the menu button on the right top of the Completed Goals window to display a dropdown menu of status activities.



The Completed Goals status actions include:

View Details

Displays all the goal details.

Refresh

Updates the screen display.

Reinitialize Goal

Starts the goal creation process from the beginning. The status will be “Ready for Execution” and the system will delete all votes. This action cannot be undone.

When you click Reinitialize, a Question dialog displays, asking if you are sure you want to reinitialize the goal, and reminding you that proceeding will result in the permanent loss of all the data for that goal. Click Yes to reinitialize, or No to return to the Running Goals screen.

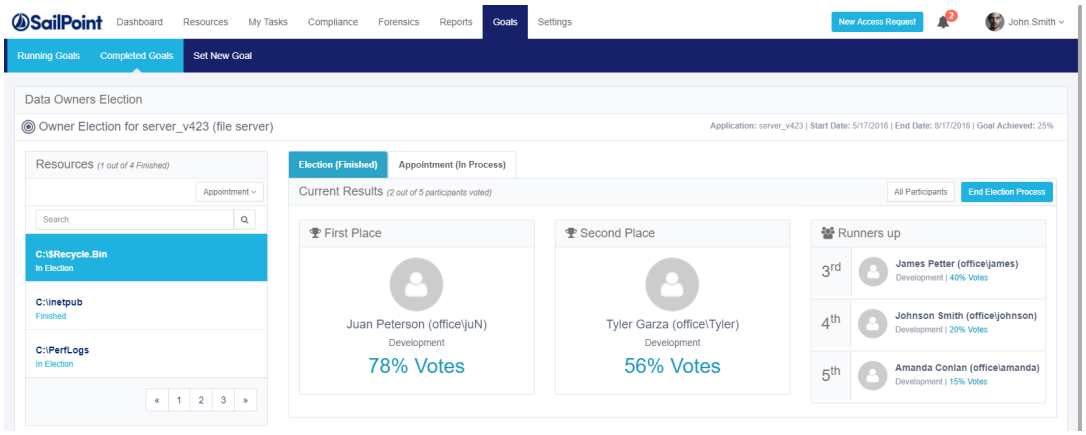
Delete

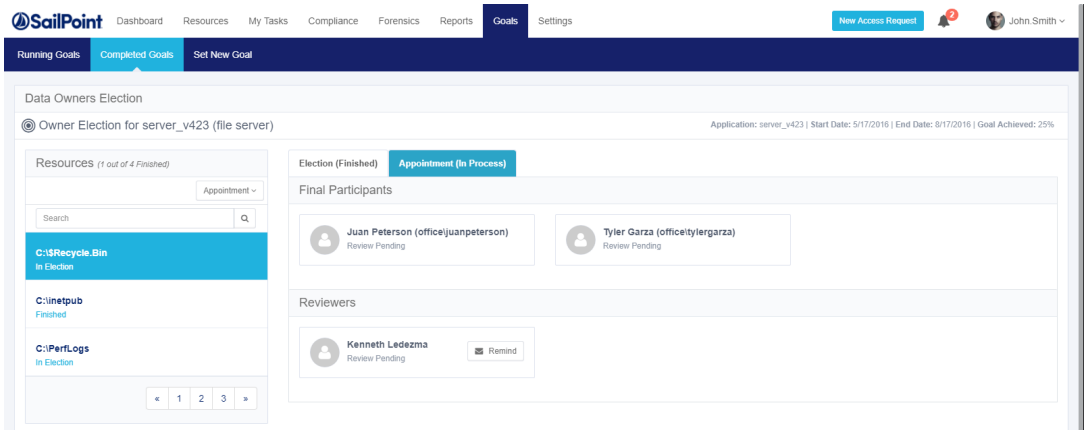
Deletes the goal. This action cannot be undone.

When you click Delete, a Question dialog displays, asking if you are sure you want to delete the goal. Click Yes to delete, or No to return to the Running Goals screen.

Show Status

Click **Show Status** at the bottom right of the Completed Goals box.





There are two final candidates pending the review of one reviewer. After a user (for whom a review process was required) has voted, the system will add a review task to the reviewer's task list.

> One user can be both a final candidate and a reviewer.

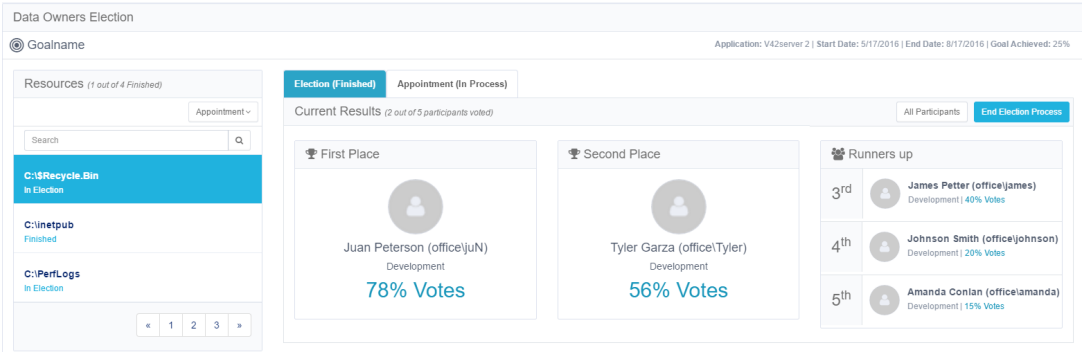
If a goal is ready for execution, you can view the status of that goal before executing it, by clicking the **Show Status** button (to the right of the "Execute Now" button at the bottom right of each goal marked "Ready for Execution".)

> If goal creation is in progress, the Execute Now and Show Status buttons are not available. The only available button is Refresh.

To view status details for a newly created goal:

Click **Show Status**. The Data Owners Election displays.

Resources Tab



The Resources section of the Show Status screen displays how many of the total activities (resources) for the displayed goal have been finished.

In the Status dropdown menu under Resources, the following options are available:

All

Displays all the resources in this goal

Election

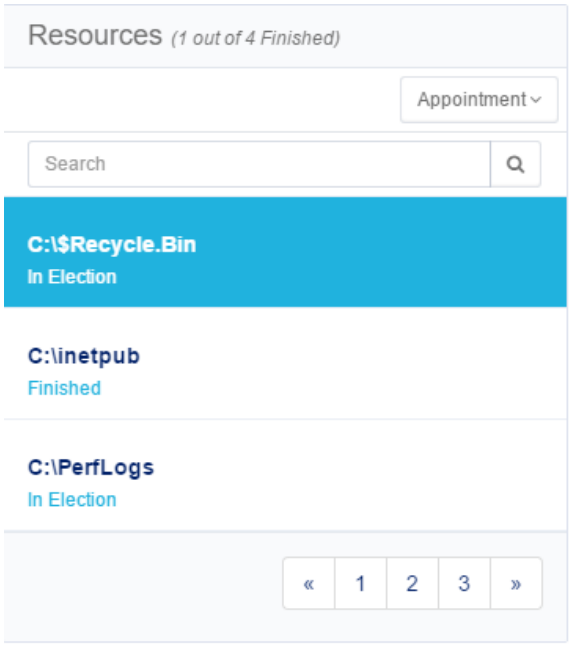
Displays activities in the Election state (pending completion of voting)

Appointment

Displays resources in the Appointment state (pending review)

Finished

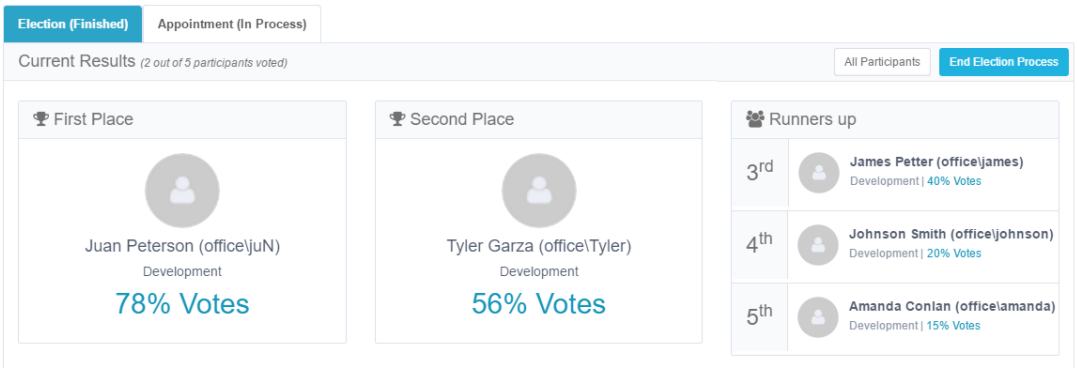
Displays all the resources for which the Election and Appointment processes have been completed.



The bottom right of the Resources section displays the previous (Prev) or next (Next) screen, and the number of the total number of screens displayed (for example, 1/2 indicates that the first of two screens displays).

The Election Tab

The Election section of the Show Status screen displays the “Current Results”, which is the number of participants (out of the total number of participants) who have voted. Up to five data owner candidates may be displayed, with their names, place, and percentage of votes received. However, the first and second place data owner candidates are given prominence.



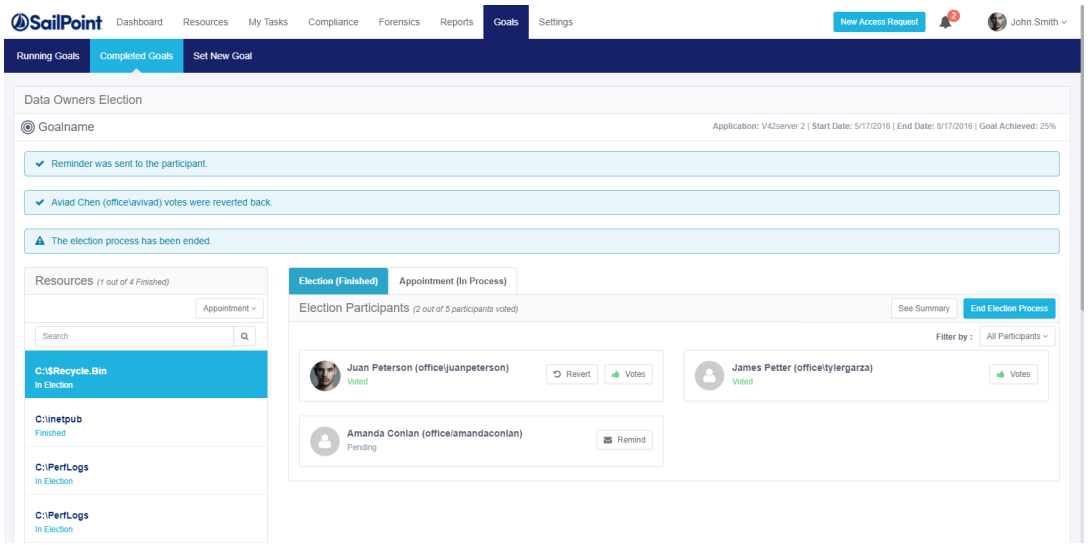
Click **All Participants** at the top right of the Election Participants section.

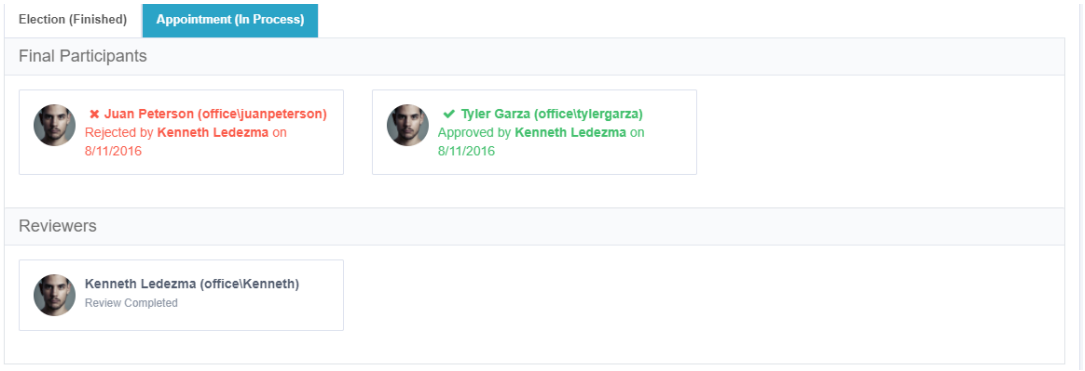
A summary of the election participants displays.

The viewing options are:

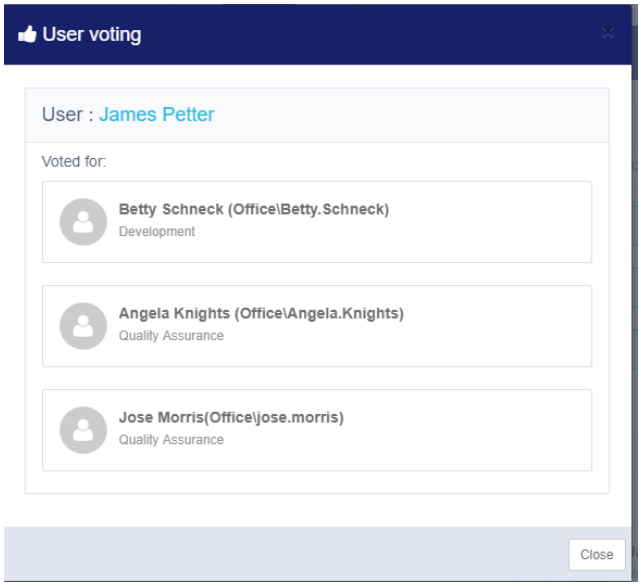
- All Participants
- Voted – The number of all participants who have already voted.
- Pending – The number of all participants whose vote is still pending.

> Navigation in the All Participants view of Election section of the Show Status screen is the same as in the Resources section of the Show Status screen.





- Click **Remind** next to a user who has not yet voted to remind that user to vote.
- Click **Votes** next to a user who has voted to see a list of the people for whom that user voted.



- Click **See Summary** in the top right of the Election section to return to the Summary view.
- Click **End Election Process** in the top right of the Election section to end the election process even if it does not include 100% of the votes.

A Question dialog displays, asking whether you want to end the election process.

Click **Yes** to end the election process or **No** to return to the previous screen.

Creating Goals

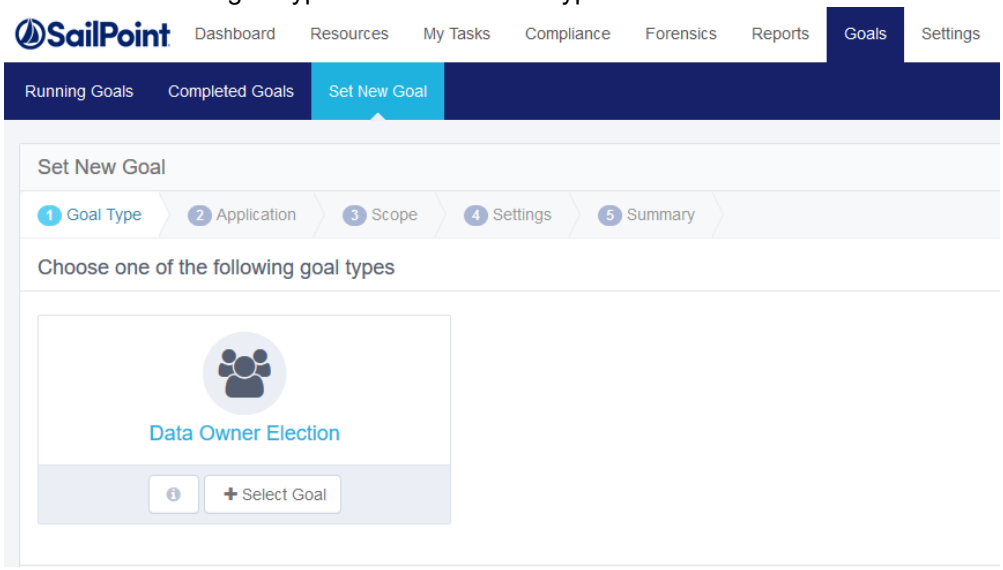
The Set New Goal process consists of the following steps:

- Goal Type
- Application
- Scope

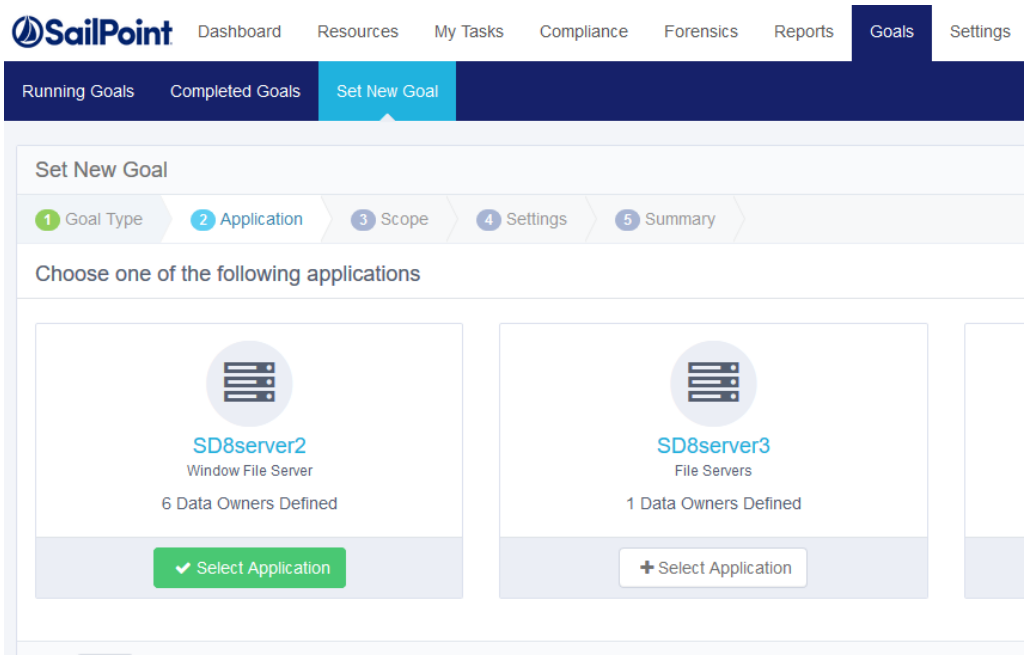
- Settings
- Summary

To set a new goal:

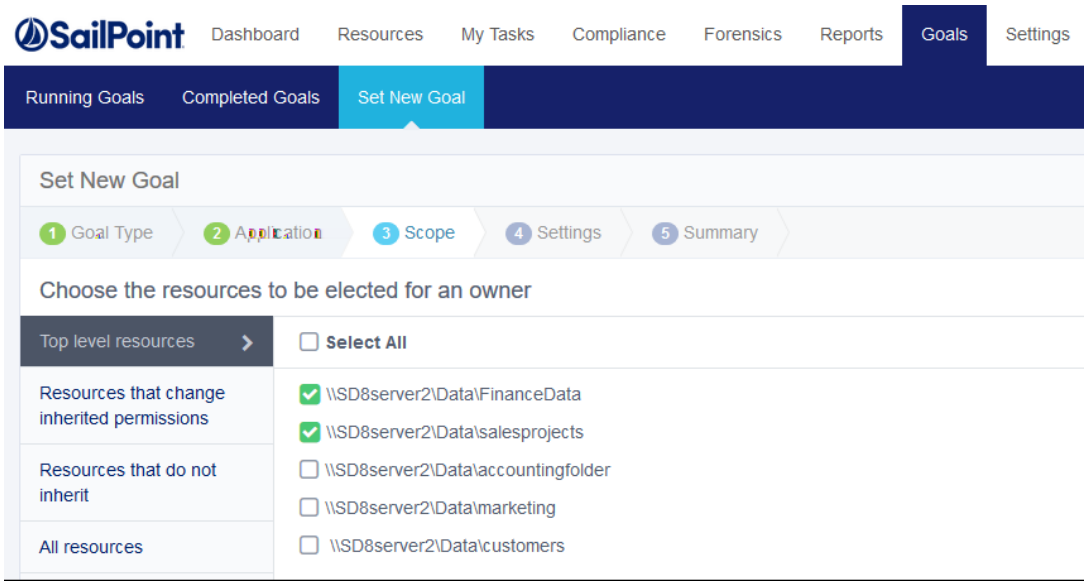
1. Navigate to **Goals > Set New Goal**.
2. Select the relevant goal type from the available types.



3. Click **Next** to select the Application .



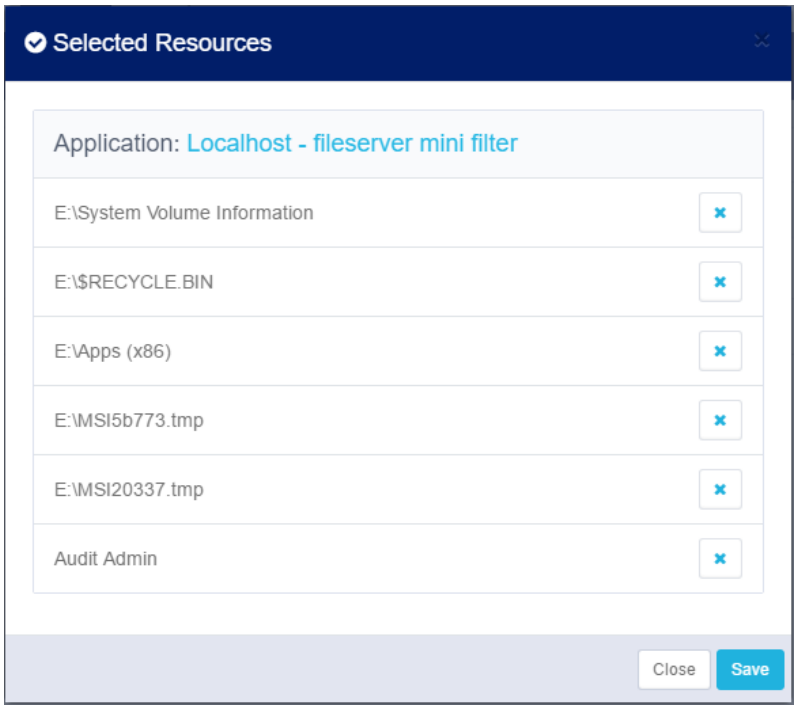
4. Select one of the applications displayed. The resources for this goal will be from the selected application.
5. Click **Next** to set the scope.



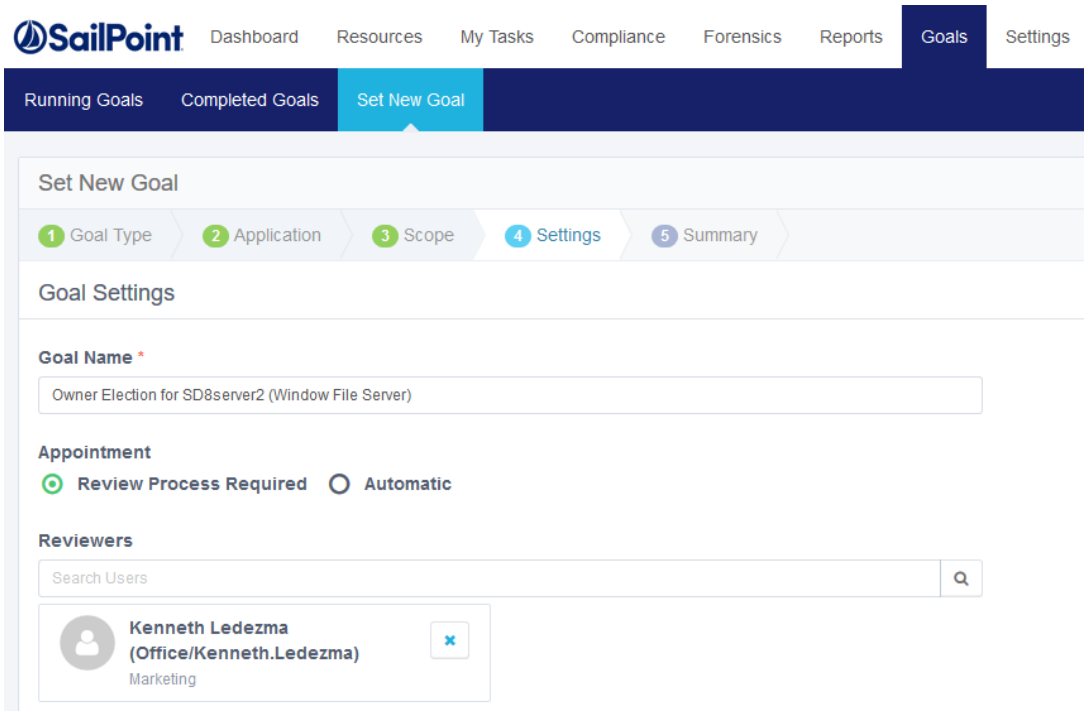
6. Select resources (one or more) from any of the categories, including:
   - Top level resources – Resources for a specific application from the top level of the resource tree
   - Resources that change inherited permissions – Resources that inherit permissions, with permissions added to those inherited permissions
   - Resources that do not inherit – Resources that break an inheritance
   - All resources – Resources from the entire resource tree
7. Check the check box next one or more resources to select that resource, then click **Add** under the resource list to add the resource as a new activity in the current goal.

   Check the **Select All** check box to select all the resources listed under each category.

   The number of resources selected displays in parentheses in “Resources Added”, and the added resources are unchecked in the original resource list.
8. Click **Resources Added** to display a list of Selected Resources.
9. Click the blue **X** to the right of any selected resource in the list of resources to deselect that resource.
10. Click **Save** to save the revised selection of resources.



11. Click **Next** to open the Settings screen.



12. In the **Goal Name** text box, type an appropriate name for the goal.
13. There are two methods of finalizing data owners:

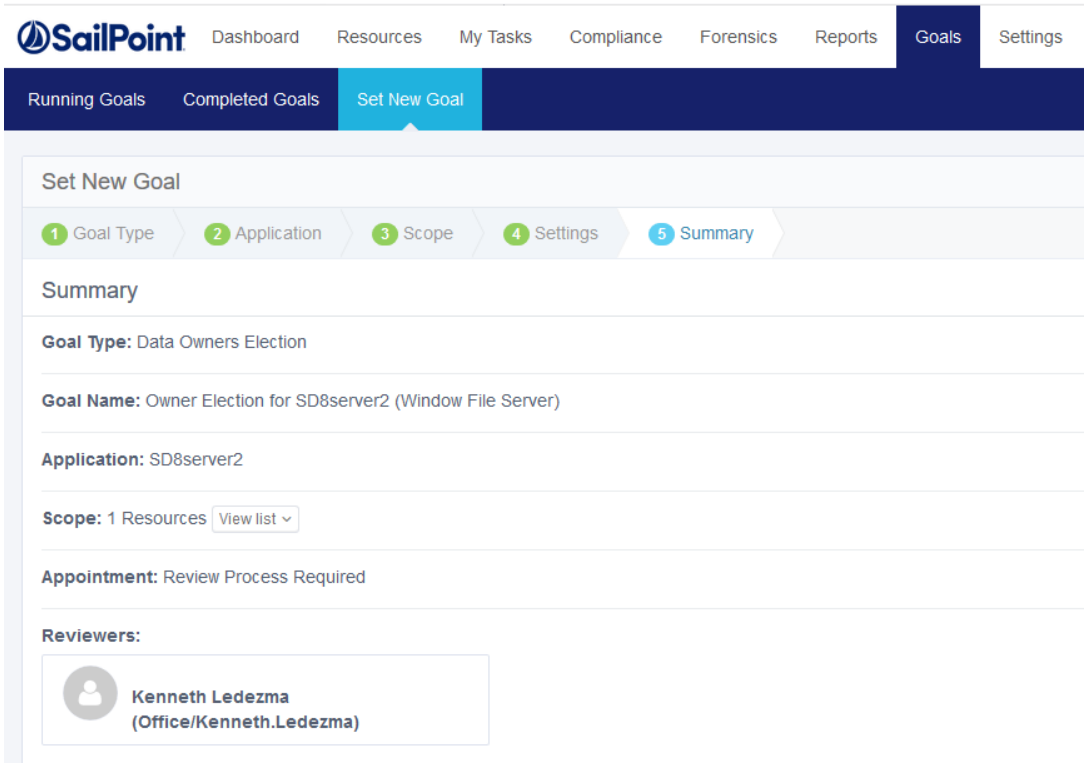
    Review Process Required

A reviewer has to either approve or reject the selected data owners who were voted for, before their final appointment.

Automatic

Appoint selected data owners without a review based on the votes of the participants

14. If you select “Review Process Required”:
    a. Select a reviewer by starting to type in the **Reviewers** text box.
    b. Select the blue x to the right of any selected reviewer in the reviewer list to deselect a reviewer.
15. Click **Next** to open the Summary screen.



The goal **Summary** screen lists the following information:

Goal Type

The goal type, for example, Data Owners Election

Goal Name

The name selected for the goal

Application

The application for which a data owner is to be selected

Scope

Number of resources

Appointment Method

Either “Review Process Required” or “Automatic”

Reviewers

Names of reviewers if the appointment method is “Review Process Required”

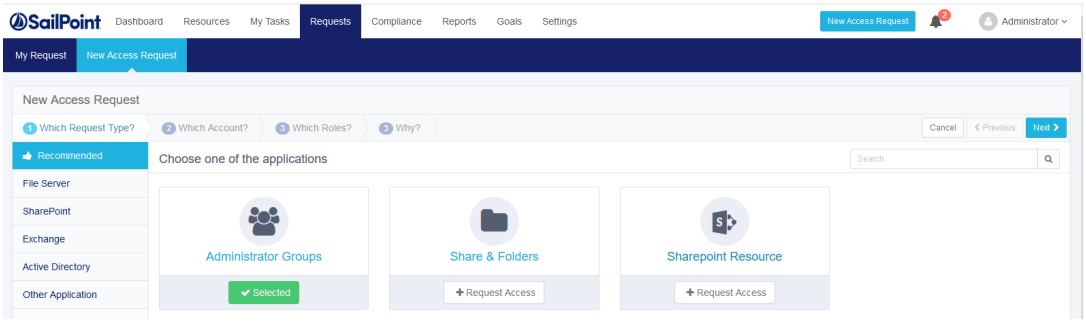
Click “View List” in Scope to view the selected resources.

16. Click **Create Goal** at the bottom right of the *Summary* screen.
17. A Success dialog displays, indicating that the goal was created successfully, and requesting that you execute the goal in “Running Goals”.
18. Click **OK**.

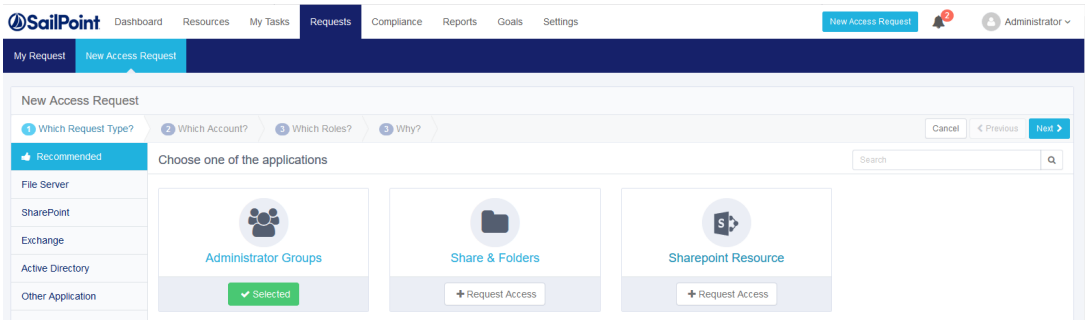
New Access Request Wizard

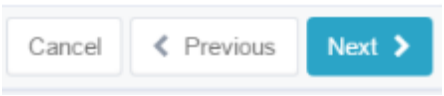
The New Access Request Wizard assists users in submitting new access requests, either for resource permissions, group memberships, or both.

Access the New Access Request Wizard by selecting New Access Request at the top right of the main window.



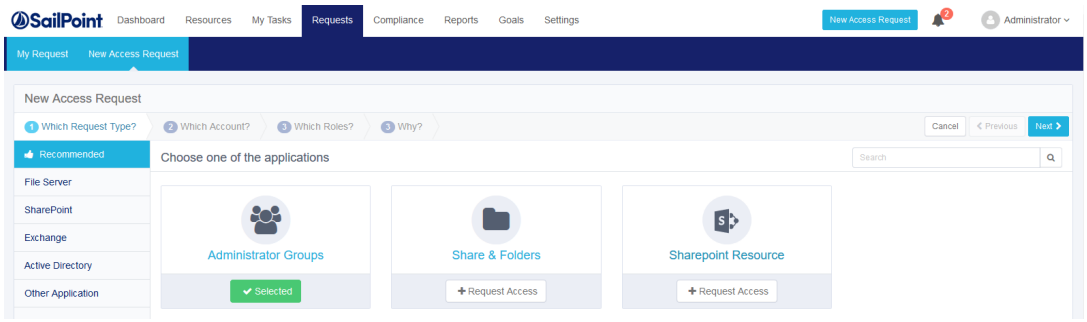
At any step (after the first step) of the New Access Request Wizard, you can return to the previous step by selecting **Previous** or you can cancel the wizard by selecting Cancel (both on the bottom right of the New Access Request window).



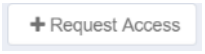


To run the New Access Request Wizard, perform the following steps:

1. Click **New Access Request**.
2. The **Which Request Type?** window displays.
3. Select Recommended from the list under “Which Request Type” (the default choice).
4. Click one of the request types: Administrative Groups (group membership), Shares & Folders (resource permissions), or SharePoint Resources (SharePoint resources permissions).

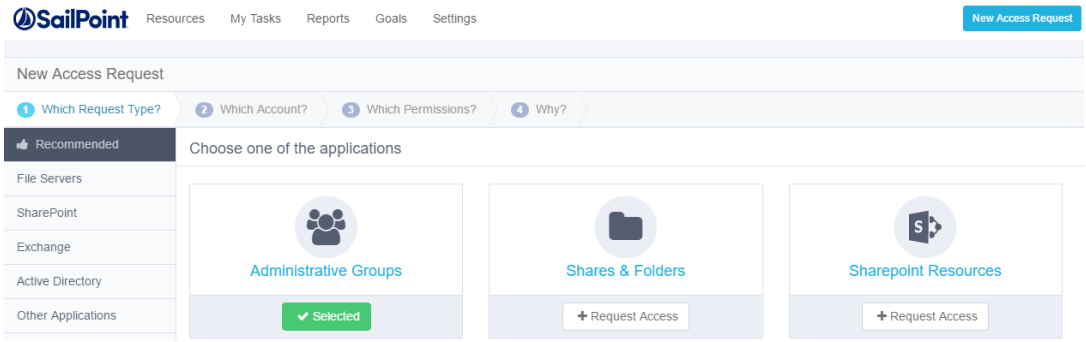


Administrative Groups

1. Click **+Request Access** under **Administrative Groups**. The button changes from 

(gray letters on a white background) to 

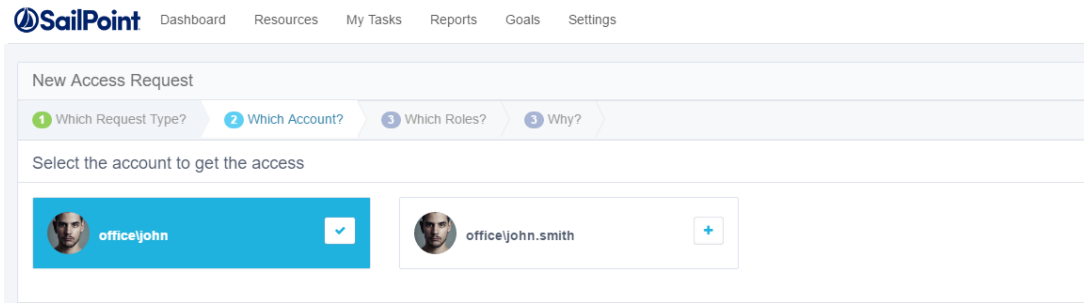
(white letters on a green background) to indicate that this access requested is now selected.



2. Click **Next** at the bottom right of the screen.

> At the bottom right of each screen, click:
> Cancel to cancel all your selections on this screen, or
> Previous, to return to the previous screen or
> Click one of the path milestones at the top of the screen, immediately under “New Access Request”, or
> Next to proceed to the next screen

3. The **Which Account?** window displays.



> If the logged-in user is associated with more than one account the wizard displays those accounts in the “Which Account? window. The logged-in user will be associated with more than one account if the administrator configured the “Unique User Account Mapping” in the Identity Collector configuration in the administrative client. If there is only one account, the wizard skips the Which Account? step, and displays the Which Groups? step.

4. Select the account to access by clicking the + sign to the right of the name of the account.
5. The plus sign next to the selected account changes to a check mark, and the account changes from gray letters on a white background to white letters on a blue background.

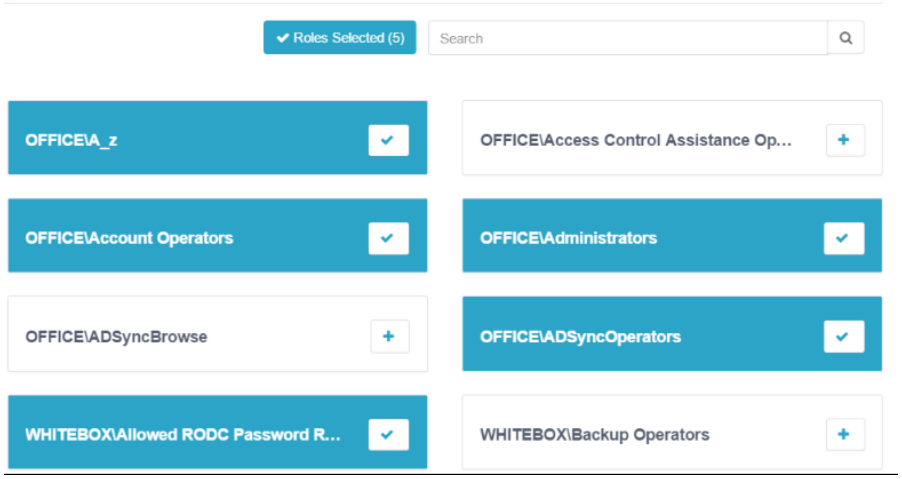
> Deselect accounts by unchecking the check mark next to the selected account.

The selected account name displays after the word “Selected” at the top of the window.

6. Click **Next**.
7. The **Which Groups?** window displays, with the top 50 results of available groups. These groups are all from the Authentication Store, which is the main domain, containing all users and groups.

> You can also search for a group by typing the name of the group in the Search box at the top of the list of available groups.

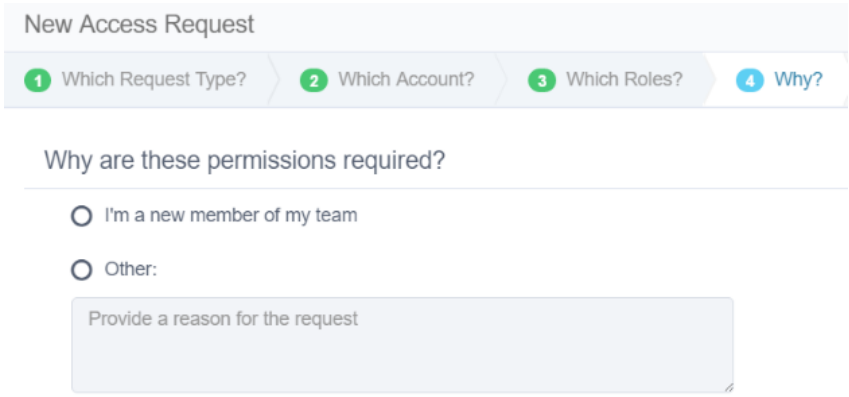
8. Select the groups by clicking the **+** sign next to the name of each group to be selected.
9. The plus sign next to the selected groups changes to a check mark, and the number of selected groups displays in the Groups Selected box, to the left of the Search box.



> Deselect groups by unchecking the check mark next to the selected groups.

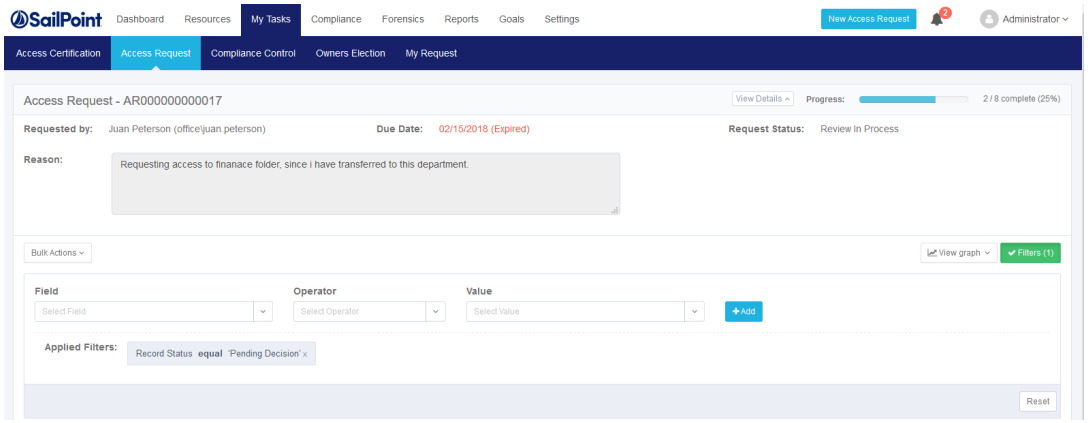
10. The selected group names display after the word “Selected” at the top of the window.

11. Click **Next**.
    *The **Why?** window displays.*



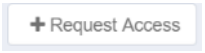
12. Click **I'm a new member of my team** or **Other**.
    If you click "Other" provide a reason for the request in the box below "Other".
13. Click **Finish** at the bottom right of the window.
    If the access request process succeeds, an Information dialog displays, noting that "Your request was successfully submitted".
14. Click **OK**.
    The "My Requests" button shows the updated total number of requests.

15. Click **View** on the right side of each request to view the details of that request.



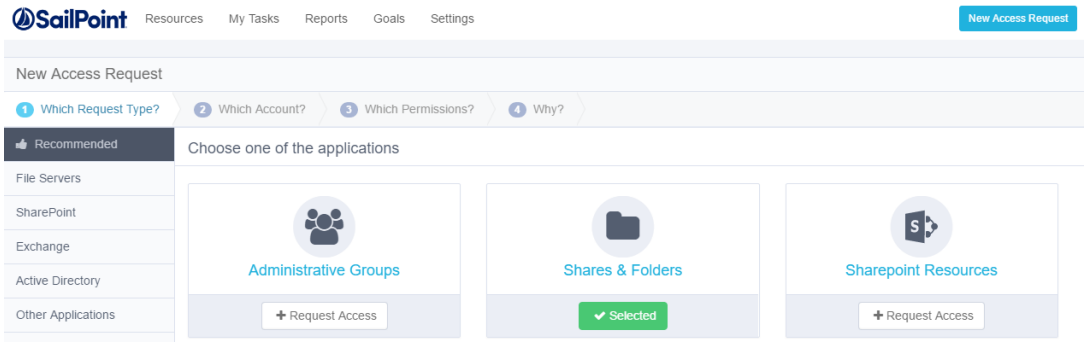
> The IdentityIQ File Access Manager Administrator Guide provides additional information the section Permissions / Access Requests.

Shares & Folders

1. Click **+Request Access** under **Shares & Folders**. The button changes from 

(gray letters on a white background) to 

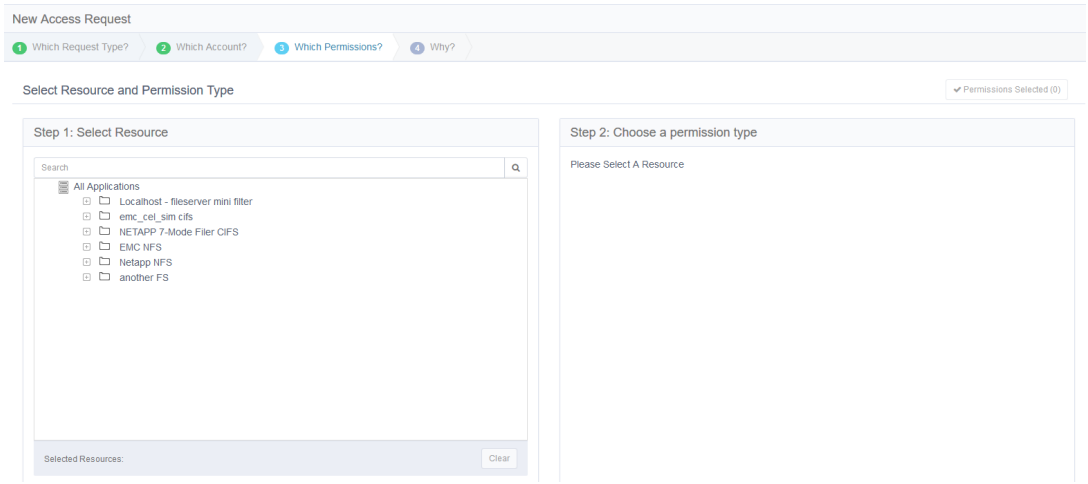
(white letters on a green background) to indicate that this access requested is now selected.



2. Follow Steps 2-5 in *Administrative Groups* .

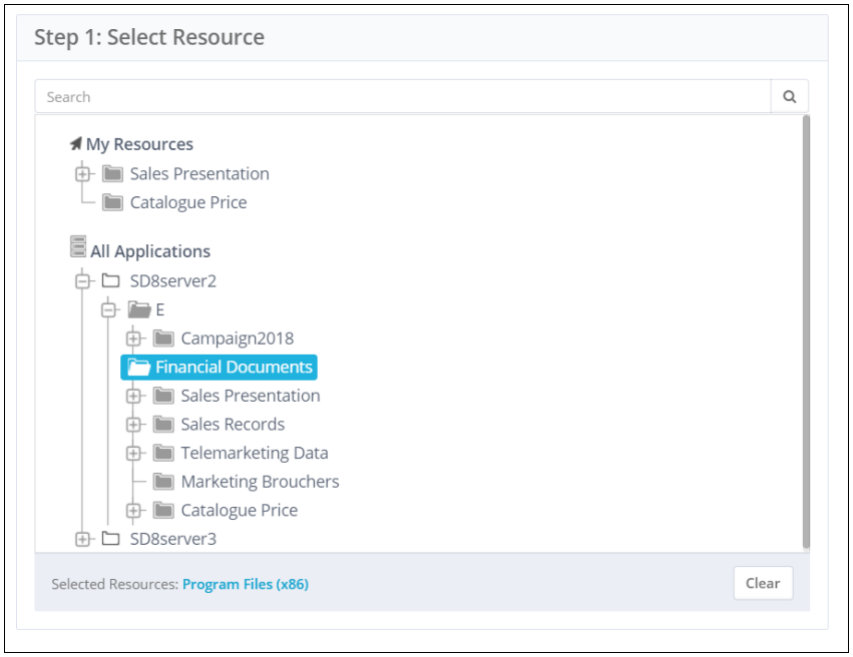
> If there is only one account, the wizard will skip the Which Account? step, and will display the Which Permissions? step.

3. Click **Next**.
The **Which Permissions?** window displays.

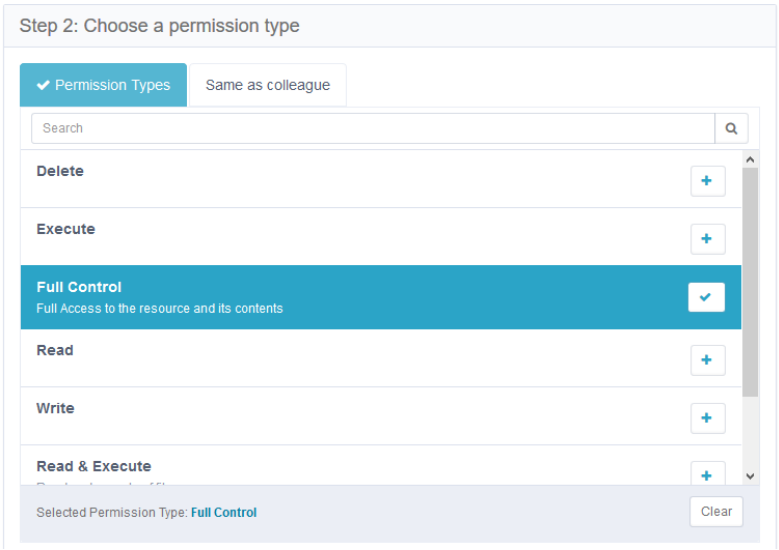


4. From **Step 1: Select Resource**, select a resource or type the name of the resource in the search box above the list of resources.

> Click **Clear** at the bottom right of the Step 1 window to clear the selection and select another resource.

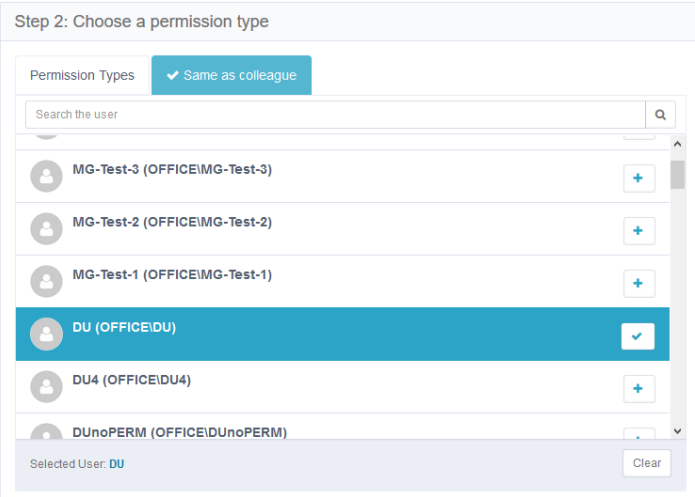


5. From **Step 2: Choose a permission type**, select a permission type or select the same permissions as those of a colleague (another user).
6. If you select **Permission Types**, select one of the available types.



7. If you click **Same as colleague**, either select one of the users (only if that user has relevant permissions) in the list or type the name of a user in the search box above the list of users.

> Click **Clear** at the bottom right of the Step 2 window to clear the selection and select another user.

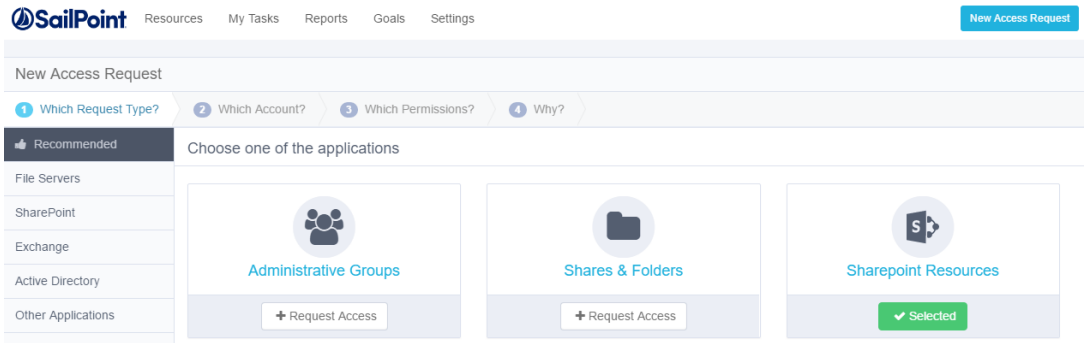


> At the bottom right of each screen, click:
> Cancel to cancel all your selections on this screen, or
> Previous, to return to the previous screen or
> Click one of the path milestones at the top of the screen, immediately under “New Access Request”, or
> Add Another Permission to add an additional permission, or
> Next to proceed to the next screen

1. Follow Steps 8-13 in “**Administrative Groups**” .

SharePoint Resources

1. Click **+Request Access** under **SharePoint Resources**. The button changes from + Request Access (gray letters on a white background) to ✔ Selected (white letters on a green background) to indicate that this access requested is now selected.



2. Follow Steps 2-8 in Shares & Folders.

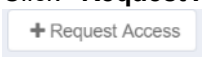
File Servers Tab

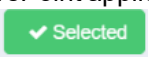
1. Click **+Request Access** under one of the displayed file server applications. The button changes from + Request Access (gray letters on a white background) to

(white letters on a green background) to indicate that this access requested is now selected.

2. Follow Steps 2-8 in Shares & Folders.

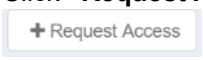
SharePoint Tab

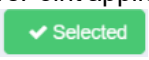
1. Click **+Request Access** under one of the displayed SharePoint applications. The button changes from 

(gray letters on a white background) to 

(white letters on a green background) to indicate that this access requested is now selected.
2. Follow Steps 2-8 in Shares & Folders .

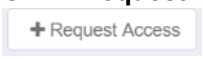
Exchange Tab

1. Click **+Request Access** under one of the displayed SharePoint applications. The button changes from 

(gray letters on a white background) to 

(white letters on a green background) to indicate that this access requested is now selected.
2. Follow Steps 2-8 in Shares & Folders .

Active Directory Tab

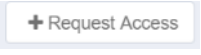
1. Click **+Request Access** under one of the displayed SharePoint applications. The button changes from 

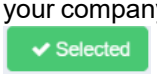
(gray letters on a white background) to 

(white letters on a green background) to indicate that this access requested is now selected.
2. Follow Steps 2-8 in Shares & Folders .

> Regarding Step 6, select one of the following permission types:
> CreateChild, DeleteChild, ListChildren, ReadProperty, WriteProperty, DeleteTree, ListObject, Delete, ReadControl, WriteDacl, and WriteOwner.

Other Applications Tab

1. Click **+Request Access** under one of the other applications (which depends on the applications available in your company). The button changes from 

(gray letters on a white background) to 

(white letters on a green background) to indicate that this access requested is now selected.
2. Follow Steps 2-8 in Shares & Folders.

> Regarding Step 6, select one of the available permission types, which vary, depending upon the application selected.