



# File Access Manager

## Getting Started

Version: 8.3 Revised: March 29, 2022

This document and the information contained herein is SailPoint Confidential Information

---

## Copyright and Trademark Notices.

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive Identity” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

# Contents

---

<b>Contents</b> .....	<b>iii</b>
<b>User Types</b> .....	<b>1</b>
Administrator .....	2
Compliance Manager .....	2
Data Owner .....	2
Auditor .....	2
Other Users .....	2
<b>Navigation</b> .....	<b>3</b>
<b>The File Access Manager Web Interface</b> .....	<b>5</b>
Data Owner Dashboards .....	5
<b>Interface Languages</b> .....	<b>6</b>
<b>Navigating the Data Grid</b> .....	<b>8</b>
<b>Time and date format</b> .....	<b>9</b>
<b>Notifications</b> .....	<b>10</b>
<b>Dashboard Overview</b> .....	<b>11</b>
Administrator Tab .....	11
Data Owner Tab .....	19

## User Types

File Access Manager is pre-configured 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.

The user types are:

- Administrators
- Compliance Managers
- Data Owners
- Auditors
- Other Users

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

- Data Owners see a limited version of the dashboards that is relevant to the capability
- The Compliance Manager cannot access the **Alert Rules** under the **compliance** menu
- Compliance Managers have access to the Data Classification Forensics page only.
- 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 Manager database.

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.

## Administrator

- The first screen that administrators see is **Dashboard**.
- Users with Administrator capability can access all screens.
- Administrators have the full scope, meaning that they have access to all data.
- Administrators can access all pages and buttons that data owners can access, including general settings, configurations, and the definition and management of crowd sourcing elections and goals.

## Compliance Manager

- The first screen that campaign managers see is **My Tasks**.
- Campaign Managers can access the tabs **My Tasks, Reports, Compliance, Forensics, and Settings**.

## Data Owner

- 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.

## 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.

## Other Users

- The first screen that most 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

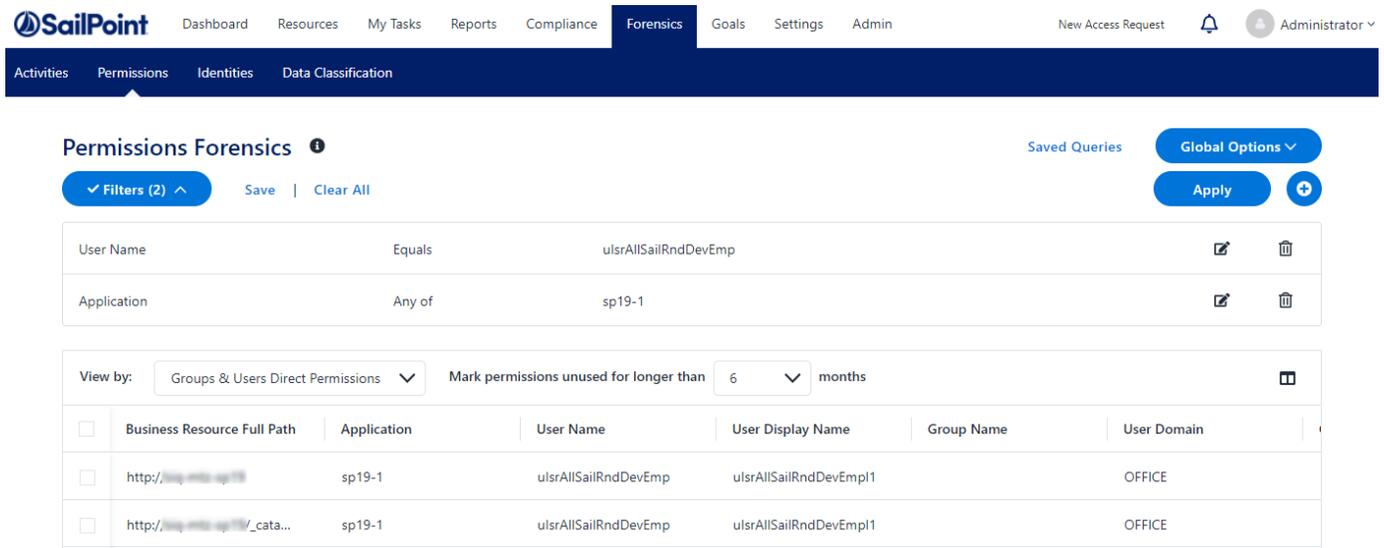
# Navigation

This section describes the main user interface of the File Access Manager business website, as well as its 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 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.

## The File Access Manager Web Interface

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

## Interface Languages

The File Access Manager business 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.

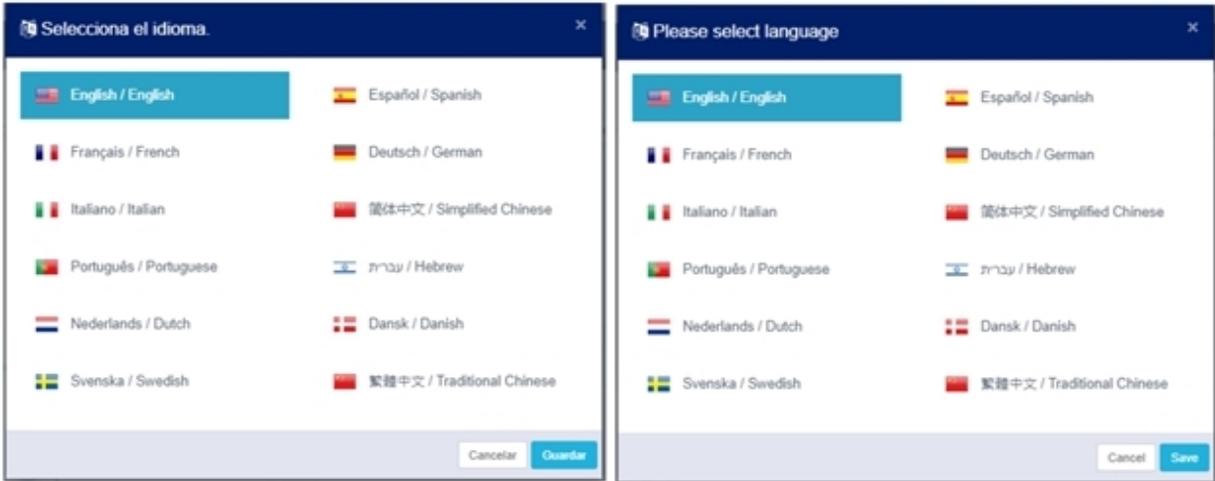
In case the current language is not set to a language you understand:

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 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 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.



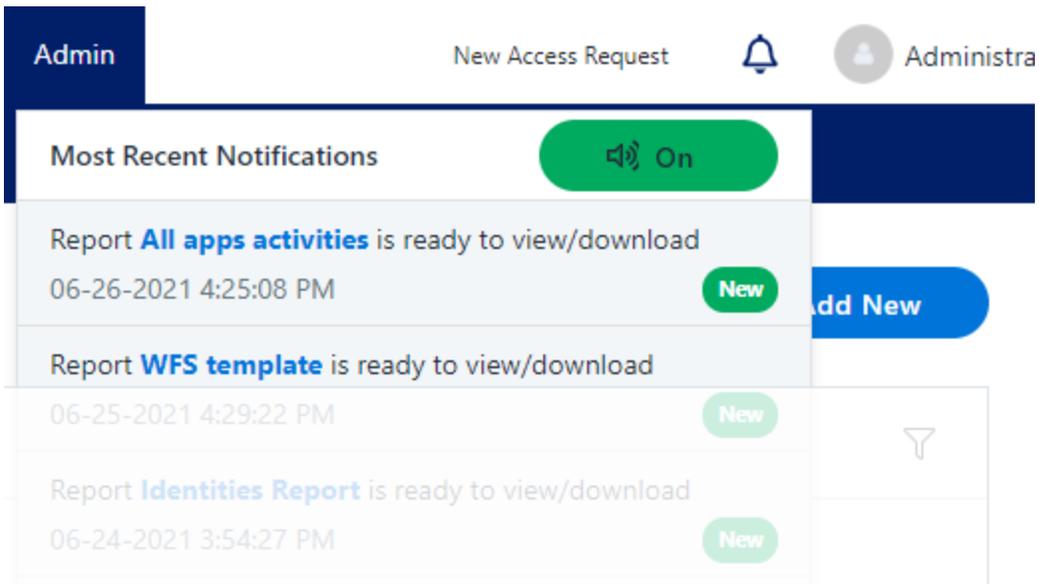
## Notification Panel

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 Overview

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.

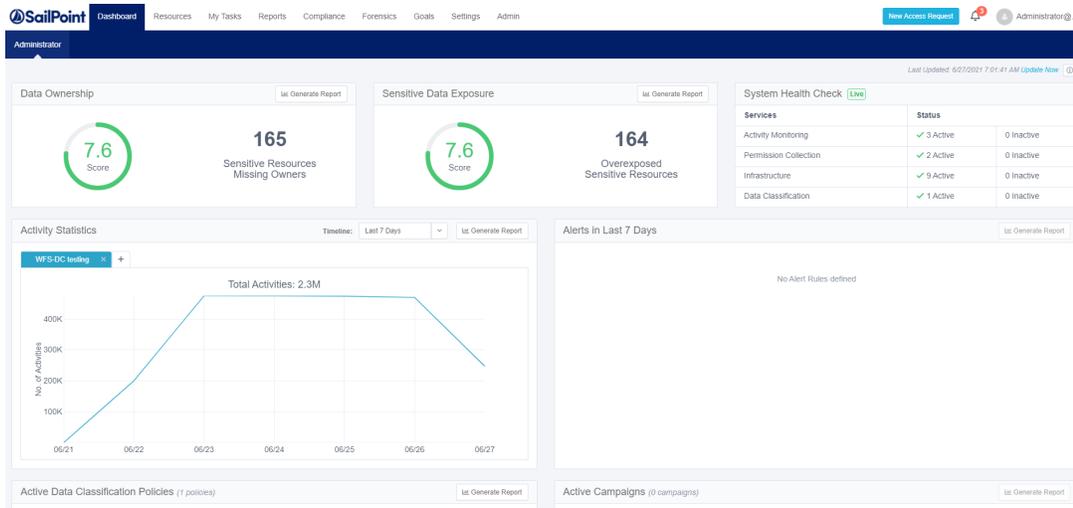
The File Access Manager Dashboard provides a bird's eye view of data vulnerabilities, so that data administrators and data owners can determine what actions to take to safeguard resources, and to prevent data from further exposure.

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:

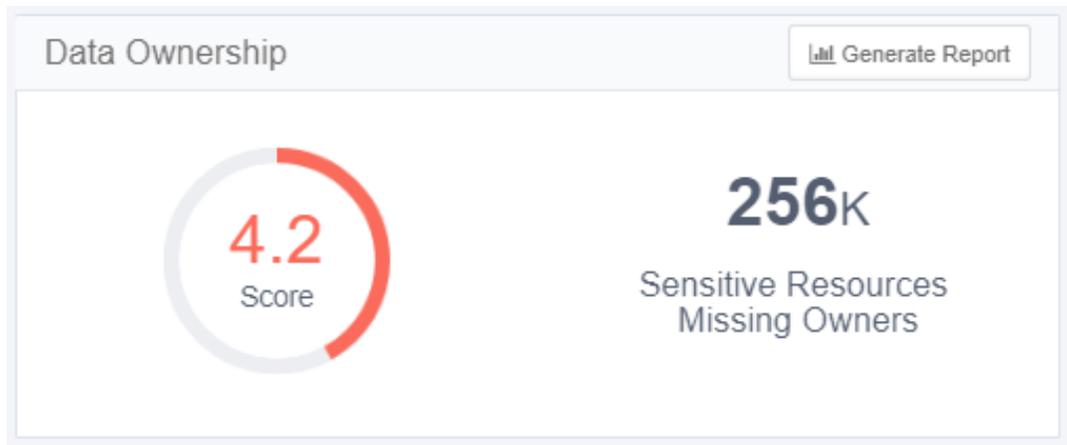
- A score of 0 to 5 displays in red, and indicates a high risk
- A score of 5.1 to 7.5 displays in yellow, and indicates a medium risk
- A score of 7.6 to 10 displays in green, and indicates a low risk

#### 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).



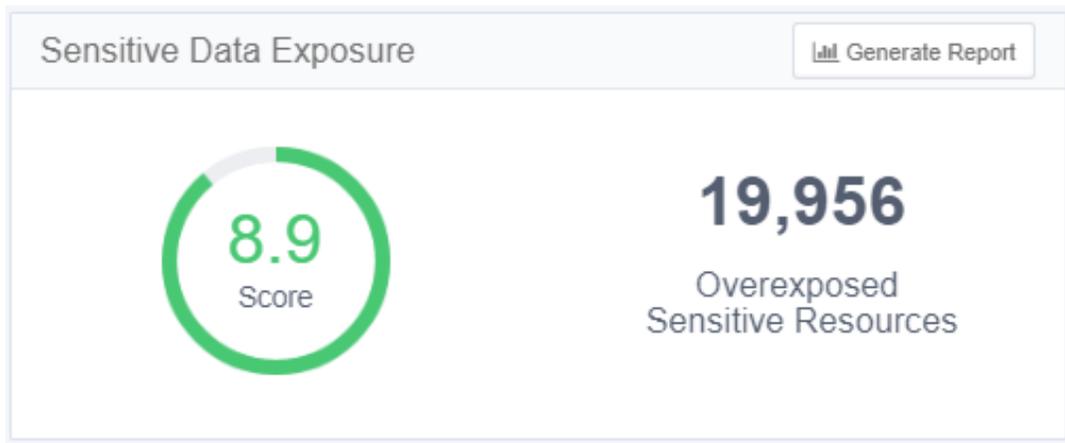
### Sensitive Data Exposure

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 "[Data Ownership](#)".

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.

## Dashboard Overview

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.

Services	Status	
Activity Monitoring	✓ 50 Active	⚠ 5 Inactive
Permission Collection	✓ 350 Active	⚠ 31 Inactive
Infrastructure	✓ 46 Active	0 Inactive
Data Classification	<i>Not Installed</i>	-

### ⚠ Activity Monitoring Inactive Services

✓ Service 'Permission Collection' is being restarted. You will be notified when the restart is completed..

Status	Service	Server Name	Action
Not Responding	Agent	Window Server 1	
Broken	Dummy Exchange	server2	<input type="button" value="Start"/>
Not Responding	Dummy SP	server3	<input type="button" value="Start"/>
Not Responding	EMC CELERRA_CIFS very long name for test...	server4	<input type="button" value="Start"/>
Not Responding	Exchange 2010	server5	<input type="button" value="Start"/>
Broken	Dummy AD	server6	<input type="button" value="Start"/>
Broken	Dummy Exchange	server7	<input type="button" value="Start"/>

## 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**

“Data Ownership” 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**

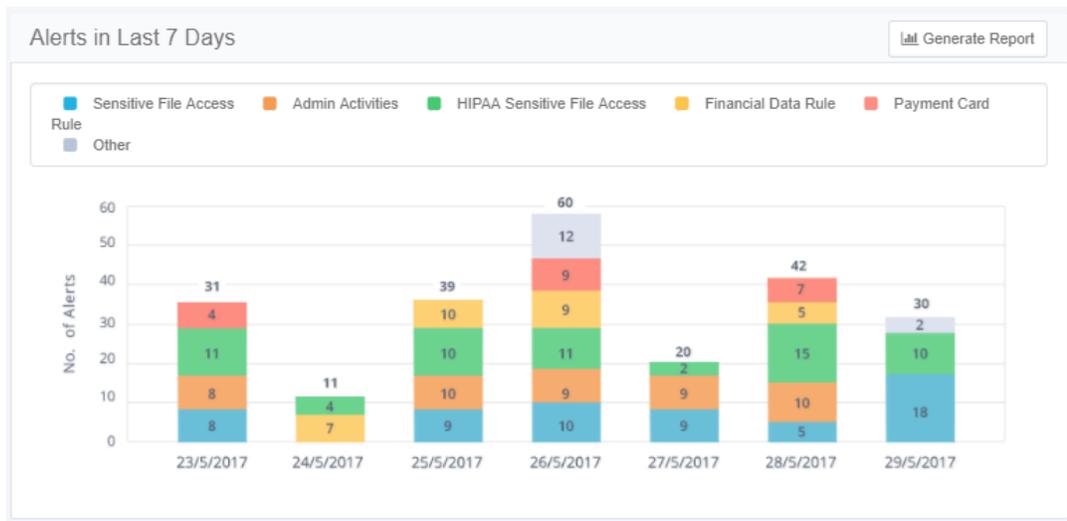
Section “Data Ownership” describes this tab.

**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 “Data Ownership” 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.

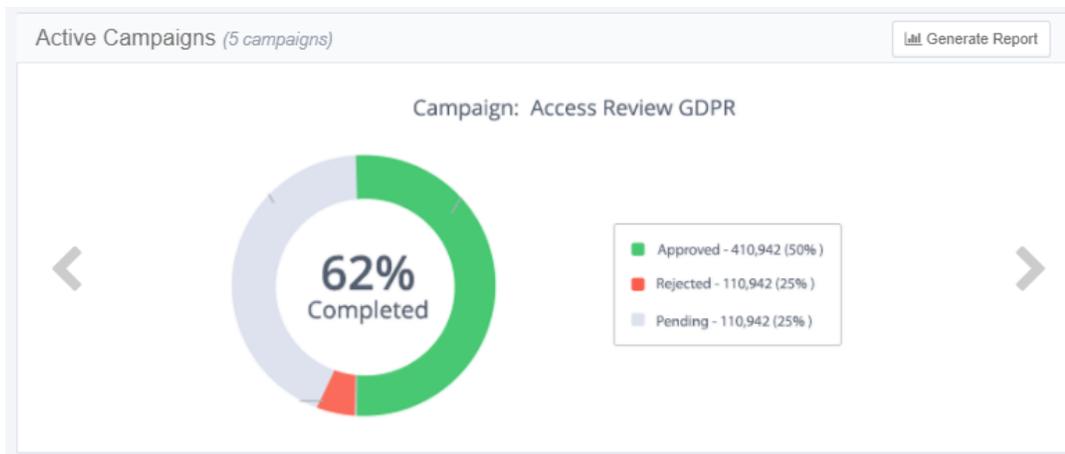
**Generate Report**

Section “[Data Ownership](#)” 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.

Top Sensitive Resources by Activity		Timeline: Last 7 Day: <span>▼</span>
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 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.”

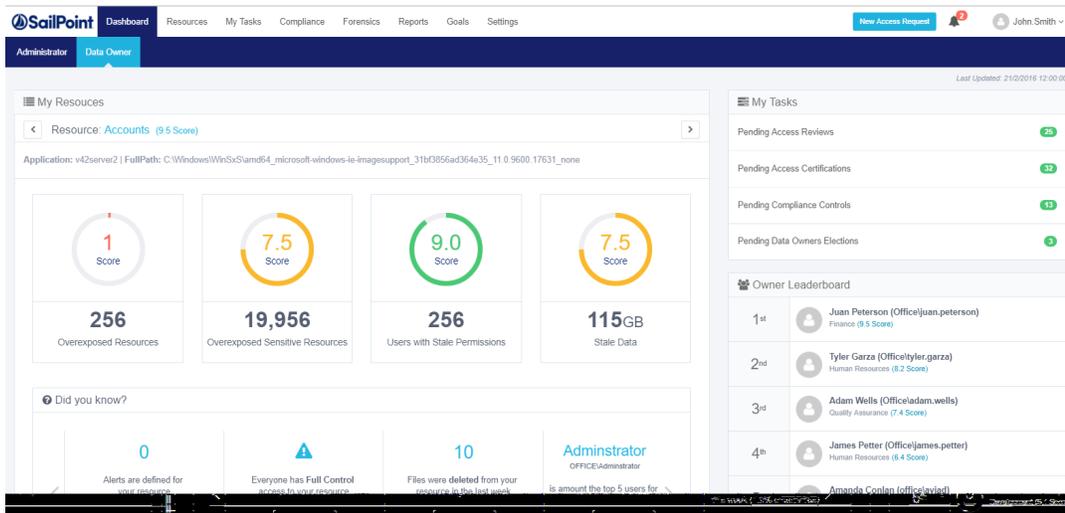
This widget is updated once a day (default). Click “Update Now” to refresh the data.

Top Users with Pending Tasks		
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

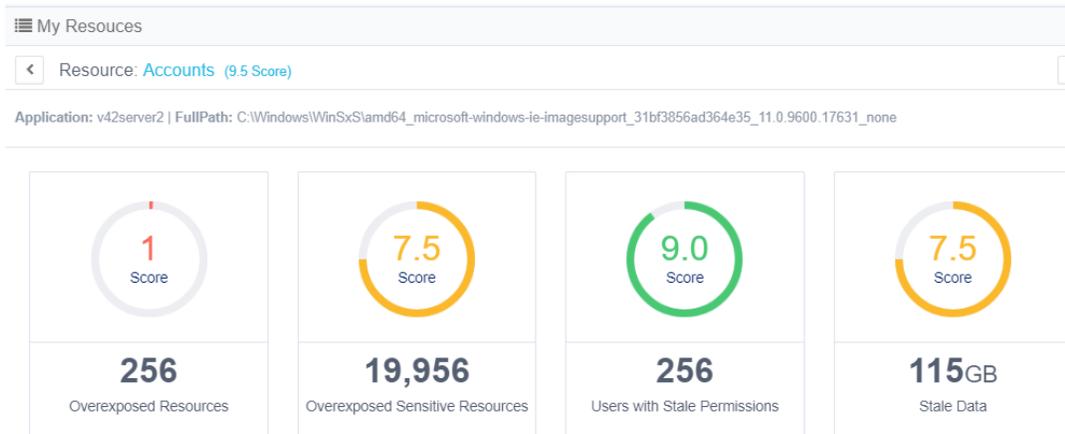


The following subsections describe each of the Data Owner Dashboard sections in detail.

### 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.

## Dashboard Overview

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:

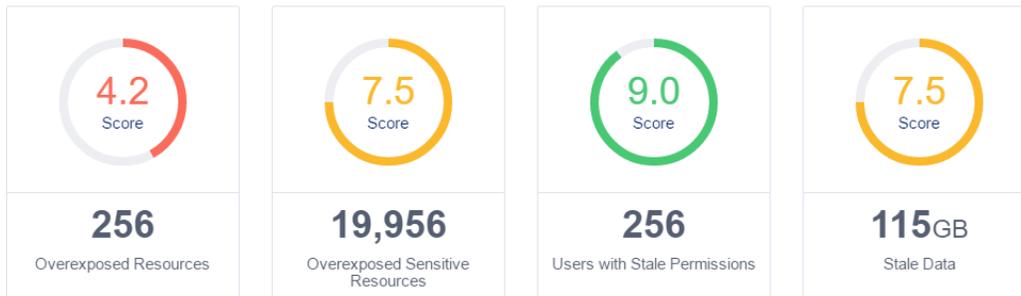
- Overexposed Resources
- Overexposed Sensitive Resources
- Users with Stale Permissions (permissions older than 12 months)
- Stale Data (data older than 12 months, expressed in number of megabytes or gigabytes)
- The color-coded scores are:
  - **Red** (0-5)
  - **Yellow** (5-7.5)
  - **Green** (7.5-10)

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



Permission > Overexposed View

Resource: Audit Admin  
Application: v42server2 | Path: z:\logial-drive-mapping-example (View full path)

Scope: Unique Permissions or Sensitive Data | Permission Type: Create folders / Append Data

Full Path	Permission Subject	Permission Type
z:\logial-drive-mapping-example-1 (View full path)	localhost\Users	Read & Execute
z:\logial-drive-mapping-example-2 (View full path)	Everyone	Modify
z:\logial-drive-mapping-example-3 (View full path)	localhost\Users	Full Control
z:\logial-drive-mapping-example-4 (View full path)	Everyone	Create folders / Append Data

Show 25 Per Page | Showing 1-25400 Results

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

## Dashboard Overview

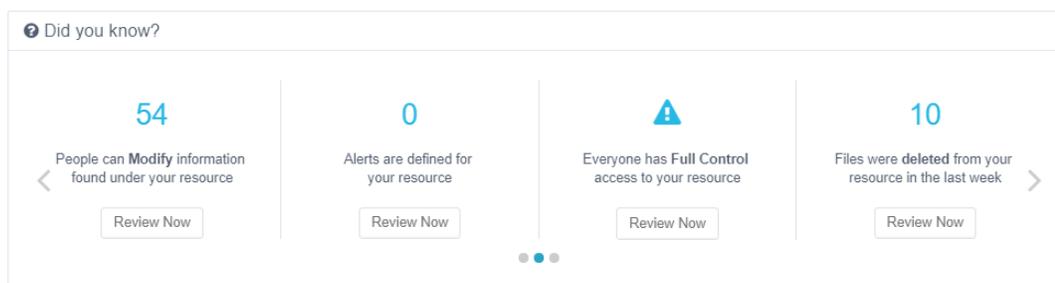
Full Path	Permission Subject	Permission Type
z:\logial-drive-mapping-example-1 <a href="#">(View full path)</a>	localhost\Users	Read & Execute
z:\logial-drive-mapping-example-2 <a href="#">(View full path)</a>	Everyone	Modify
z:\logial-drive-mapping-example-3 <a href="#">(View full path)</a>	localhost\Users	Full Control
z:\logial-drive-mapping-example-4 <a href="#">(View full path)</a>	Everyone	Create folders / Append Data

Show 25 Per Page Showing 1-25/400 Results < 1 2 3 4 5 >

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.

My Tasks	
Pending Access Reviews	25
Pending Access Certifications	32
Pending Compliance Controls	13
Pending Data Owners Elections	3

### 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).

Owner Leaderboard	
1 <sup>st</sup>	 <b>Juan Peterson (Office\juan.peterson)</b> Finance (9.5 Score)
2 <sup>nd</sup>	 <b>Tyler Garza (Office\tyler.garza)</b> Human Resources (8.2 Score)
3 <sup>rd</sup>	 <b>Adam Wells (Office\adam.wells)</b> Quality Assurance (7.4 Score)
4 <sup>th</sup>	 <b>James Petter (Office\james.petter)</b> Human Resources (6.4 Score)
5 <sup>th</sup>	 <b>Amanda Conlan (office\aviad)</b> Development (5.1 Score)
128 <sup>th</sup>	 <b>Me</b> Development (3.2 Score) <span>↑ Your ranking has gone up</span>