



File Access Manager Resource Tab

Version: 8.4

Revised: March 27, 2023

Copyright and Trademark Notices

Copyright © 2023 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

- Resource Overview** 1
- Viewing Activities** 2
 - Resource Tree 2
 - Filter Parameters 4
 - Viewing the Permission Path 4
- Viewing Permissions** 6
 - Editing Permissions 6
- Data Tab** 9
- Alerts Tab** 11
- Owners Tab** 12
 - Adding Owners to Resources 12

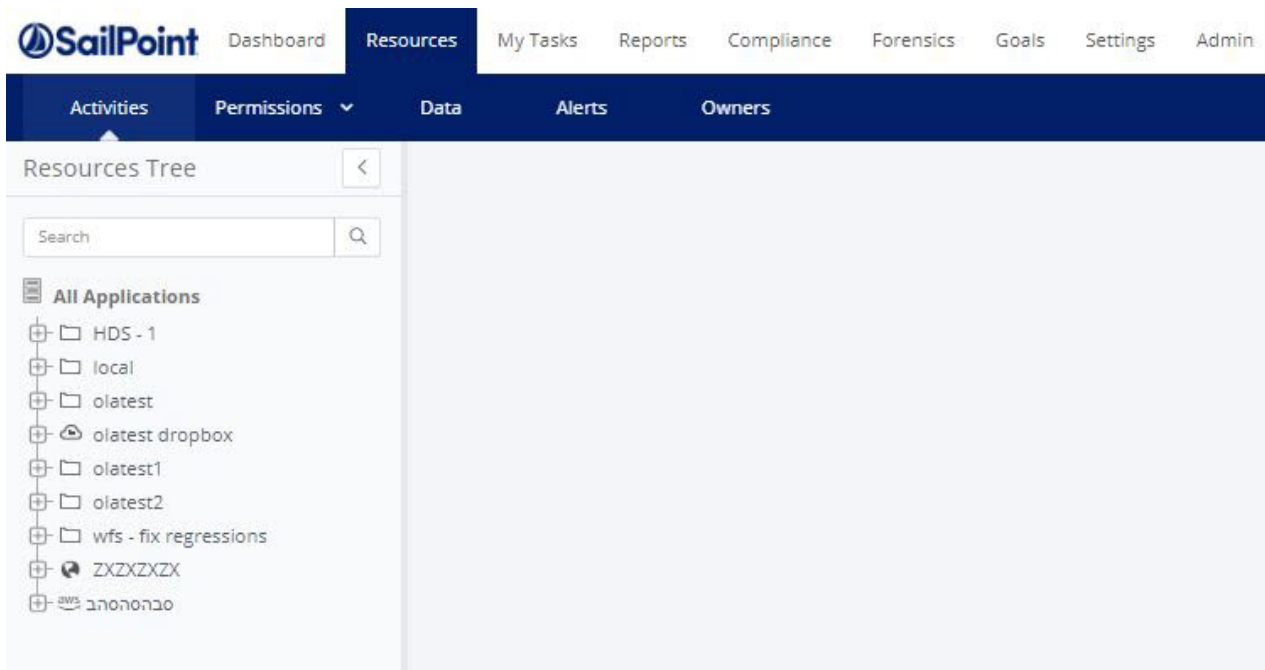
Resource Overview

The resource tab allows you to view different governance dimensions on managed resources within applications governed by File Access Manager. All onboarded applications will display within the resource tree on the left panel. Each application will have its own nested resource tree. A resource within an application can be a file share, folder, SharePoint site, database, storage object, etc.

Individual files are not represented as "resources" managed by File Access Manager, unless they have unique permissions assigned to them. In this case they will be represented as individual managed resources.

The Resource tab includes the following tabs:

- Activities
- Permissions
- Data
- Alerts
- Owners



Viewing Activities

After performing the crawler task, the Activities tab displays all of the aggregated data. Here you are able to view the most and least frequent users, resources, activity types, and can perform various actions. It provides a high level overview of activity trends and common usages as well as the most common actions taken on certain resources hierarchies.

Resource Tree

When a resource has been selected from the Resource Tree to the left, all information within that resource will display. A user can search for a resource, like a folder, share, site, or Personal Drive, in the search bar.

The screenshot shows the SailPoint interface with the following components:

- Resources Tree (Left):** A hierarchical tree view showing 'All Applications' and 'Data'. Under 'Data', 'Human Resources' is selected and highlighted in blue.
- Activities Tab (Right):** The 'Access Frequency' view for the selected resource. It shows a table of 'Most Frequent Users' with columns for rank, user name, activity count, and resource name.

Rank	User Name	Activity Count	Resource
1	Sarah Campbell (SERISarah.Campbell)	27 activities	Human Resources
2	Michelle Perez (SERIMichelle.Perez)	4 activities	Human Resources
3	Edward Baker (SERIEdward.Baker)	3 activities	Human Resources
4	Anthony Roberts (SERIAnthony.Roberts)	2 activities	Human Resources
5	Brian Nelson (SERIBrian.Nelson)	2 activities	Human Resources
6	Elizabeth Taylor (SERIElizabeth.Taylor)	2 activities	Human Resources
7	Ronald Mitchell (SERIRonald.Mitchell)	2 activities	Human Resources
8	Ruth Gonzalez (SERIRuth.Gonzalez)	2 activities	Human Resources
9	Christopher Clark (SERIChristopher.Clark)	1 activities	Information Technology

You can view the information by Users, Resources, or Actions.

- Users – displays users that have performed actions
- Resources – contained resources within this resource
- Actions – action performed within this resource

Note: You can display the content by either Most Frequent usage or Least Frequent usage.

Viewing Users

The three line menu to the right of each set of users provides a circular way to view the data associated with this high level resource.

When viewing users on a resource, all activities that particular user has done will display in blue under their name.

Click the blue activities link to see what that user has done on the resource.

Activities > Access Frequency

Resource: [Human Resources](#)
Application: Windows File Server | Path: \\ad-resource\Data\Departments\Human Resources

Start with: **Users** Resources Actions Most Frequent Least Frequent Timeframe: Last 30 Days

Most Frequent Users					
1	Sarah Campbell (SERI\Sarah.Campbell) 27 activities Human Resources		6	Elizabeth Taylor (SERI\Elizabeth.Taylor) 2 activities Human Resources	
2	Michelle Perez (SERI\Michelle.Perez) 4 activities Human Resources		7	Ronald Mitchell (SERI\Ronald.Mitchell) 2 activities Human Resources	
3	Edward Baker (SERI\Edward.Baker) 3 activities Human Resources		8	Ruth Gonzalez (SERI\Ruth.Gonzalez) 2 activities Human Resources	
4	Anthony Roberts (SERI\Anthony.Roberts) 2 activities Human Resources		9	Christopher Clark (SERI\Christopher.Clark) 1 activities Information Technology	
5	Brian Nelson (SERI\Brian.Nelson) 2 activities Human Resources				

Viewing Resources

A user can view the child resources nested under the current selected resource.

Activities Permissions Data Alerts Owners

Resources Tree

Search

- SERI Active Directory
- SharePoint Online
 - ClinicalTests
 - Community
 - DataAccessGovernance4All
 - FinanceInt
 - generalgroup
 - hub
 - HumanResources
 - HumanResourcesInt
 - HumanResourcesInternal
 - IIQ-FAM
 - IIQ-FAM-All
 - Microbiologie
 - o365_hr
 - search
 - securityiq.sharepoint.com**
 - securityiq-my.sharepoint.com
- SQL Server
- Windows File Server
- Data

Activities > Access Frequency

Resource: [securityiq.sharepoint.com](#)
Application: SharePoint Online | Path: https://securityiq.sharepoint.com

Start with: **Users** Resources Actions Most Frequent Least Frequent Timeframe: Last 30 Days

Most Frequent Resources					
1	Search 90 activities https://securityiq.sharepoint.com/search/...		6	Search 45 activities https://securityiq.sharepoint.com/sites/MichellesHRTeam/_catalo...	
2	PCI 57 activities https://securityiq.sharepoint.com/sites/HumanResources/Shared...		7	Search 45 activities https://securityiq.sharepoint.com/sites/appcatalog/_catalogs/mast...	
3	System 50 activities https://securityiq.sharepoint.com/search/_catalogs/masterpage/DI...		8	Search 45 activities https://securityiq.sharepoint.com/sites/generalgroup/_catalogs/m...	
4	Search 45 activities https://securityiq.sharepoint.com/_catalogs/masterpage/Display T...		9	Search 29 activities https://securityiq.sharepoint.com/sites/Comms/_catalogs/mastep...	

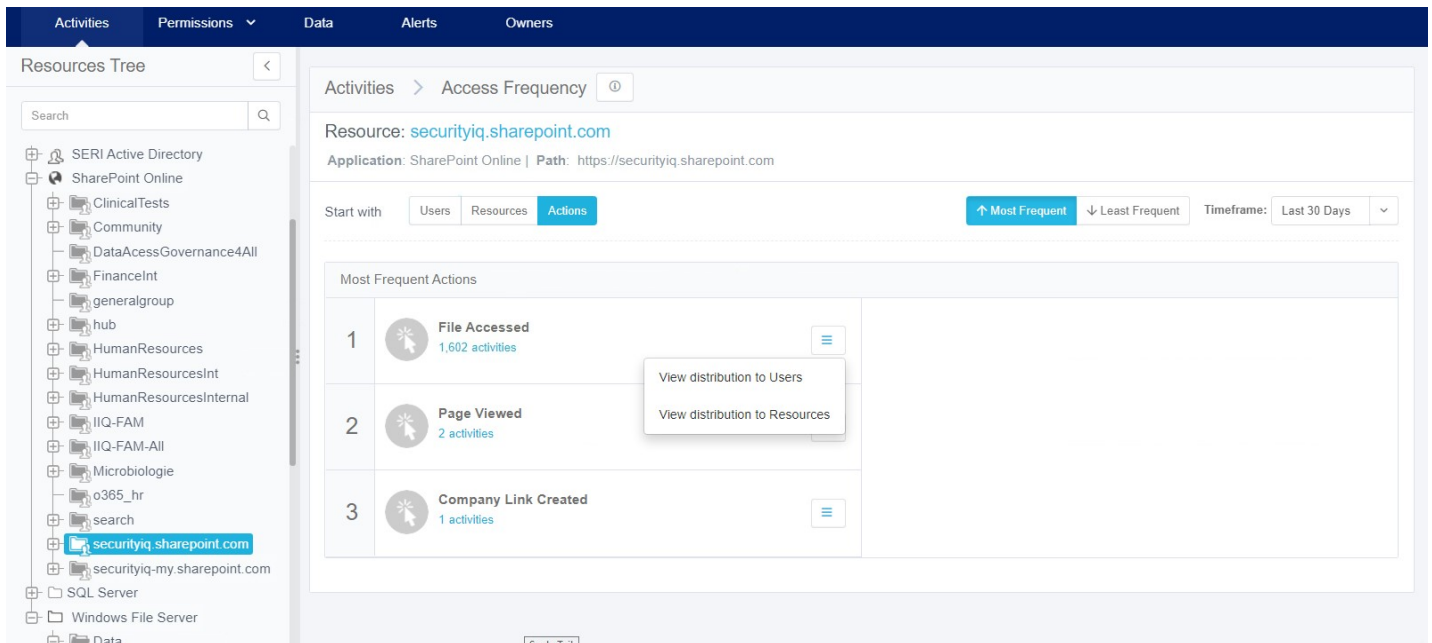
View distribution to Users

View distribution to Actions

Viewing Actions

When viewing actions on a resource, you are able to view the most and least frequent actions on a particular resource.

Clicking on the blue link below the action will display all actions performed and by who.



Filter Parameters

Select either **Most Frequent** or **Least Frequent** to change the order of what is displayed.

Click the **Timeframe** dropdown to change the duration of time to alter the displayed results.

Viewing the Permission Path

This function allows the user to view how someone has access to certain resources.

To view a permission path, click on the user name.

The colored legend at the top will provide additional context as to the frequency of usage on that particular permission. Namely, how long has it been since the user has used the permission or had access granted to it.

This colored legend helps identify stale and unused permissions that can be removed to reduce risk associated with unnecessary exposure and over-permissive and unused access.

The branches leading from the user to the resource will display in a color which corresponds to the legend.

Each branch represents an access path through which a user is granted access to the resource. That path can represent a direct permission, access granted through a group, or a nested group membership. Groups can be expanded to show the member and sub-groups nested under them.

User's Permission Paths [Close]

User: **SERI\Administrator** Resource: **Human Resources**
Application: Windows File Server | Path: \\ad-resource\Data\Departments\Human Resources

[Add Permission] [Revoke All Permissions] [Revoke Permission]

Stale Permission ● > 12 Months ● 6-12 Months ● 3-6 Months ● < 3 Months

```
graph LR; Root["Seri\Administrator  
Full Control"] --> Admin1["Administrato...  
ad-resource  
Owner"]; Root --> Admin2["Domain Admin...  
SERI  
Full Control"]; Root --> Admin3["Domain Admin...  
SERI  
Full Control"]; Root --> Admin4["Domain Admin...  
SERI  
Owner"]; Root --> Admin5["Enterprise A...  
SERI  
Full Control"]; Admin1 --> AdminFull["Administrato...  
ad-resource  
Full Control"]; Admin2 --> AdminFull; Admin3 --> AdminFull; Admin4 --> AdminFull; Admin5 --> AdminFull; AdminFull --> HR["Human Resour..."];
```

[Close]

Viewing Permissions

The Permission tab provides four different views on a resource:

- **Simple**—high level view. Shows who has direct access to what. You can filter the results by the permissions type (menu on the left panel).
- **Tree**—gives the view from a resource perspective on the entire resource. Each user within the resource will have a three line menu displayed next to their name.
- **Overexposed**—accessible by everyone or a larger part of the organization. The definition for overexposed can be configured through the Overexposed Resources section within the General tab under Settings. There are three different scope or view types:
 - Unique Permissions or Sensitive Data
 - Unique Permission only
 - Sensitive Data only
- **Excess**—view users who overlap and have redundant access paths granting similar or excessive permissions to the same resource.

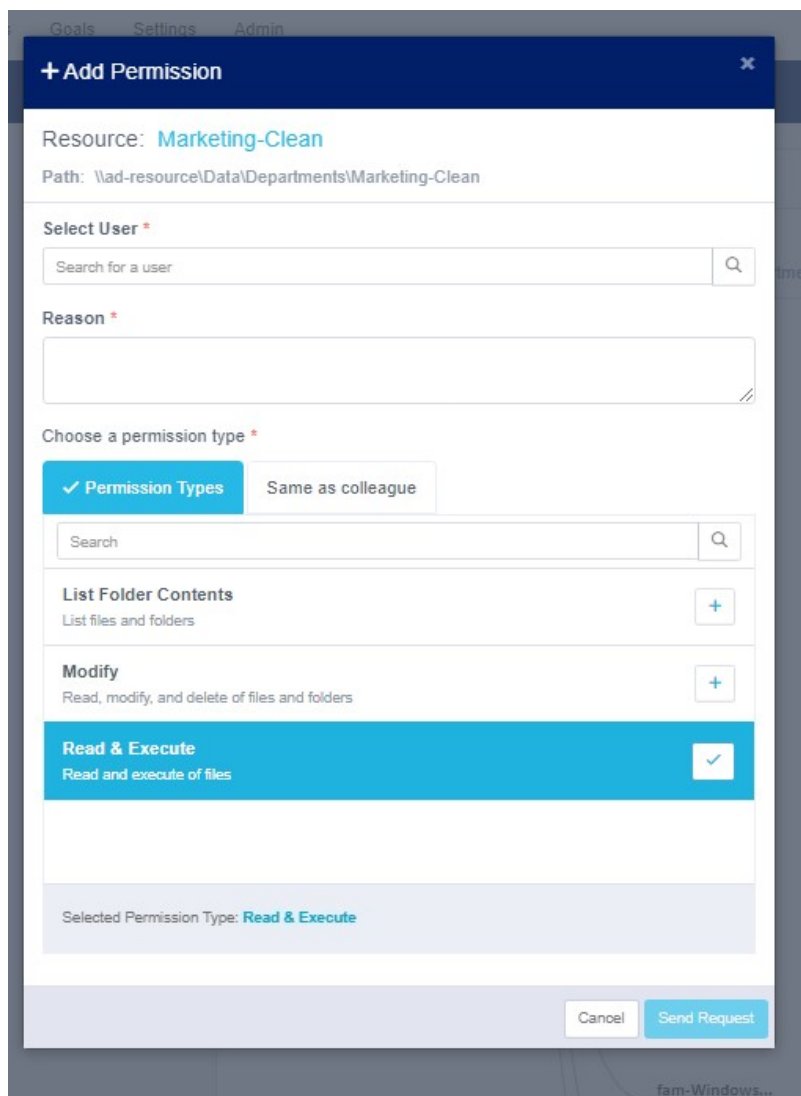
Editing Permissions

File Access Manager supports OOTB and custom fulfillment of removing permissions.

An administrator can change the permissions level a user has by clicking **Add Permission** or **Remove Permissions**.

Complete the following to edit permissions:

1. Search for the user you are adding permissions for.
2. Provide a reason why they are being granted the permissions.
3. For the Permission Type, a user can choose between either **Permission Type** or **Same as Colleague**.
 - Permission Type—choose between the various actions types to give permission.
 - Same as Colleague—search for a colleague give the same access as that person.
4. Click **Send Request** to initiate an Access Request on this new permission.



Goals Settings Admin

+ Add Permission ✕

Resource: [Marketing-Clean](#)
Path: \\ad-resource\Data\Departments\Marketing-Clean

Select User *

Search for a user

Reason *

Choose a permission type *

Permission Types Same as colleague

Search for a user

<input type="checkbox"/>	Koch, Regan (SERI\Regan.Koch)	<input type="button" value="+"/>
<input type="checkbox"/>	English, Donovan (SERI\Donovan.English)	<input type="button" value="+"/>
<input checked="" type="checkbox"/>	Snow, Kelly (SERI\Kelly.Snow)	<input type="button" value="✓"/>
<input type="checkbox"/>	Booth, Myra (SERI\Myra.Booth)	<input type="button" value="+"/>
<input type="checkbox"/>	Wade, Ramona (SERI\Ramona.Wade)	<input type="button" value="+"/>

Data Tab

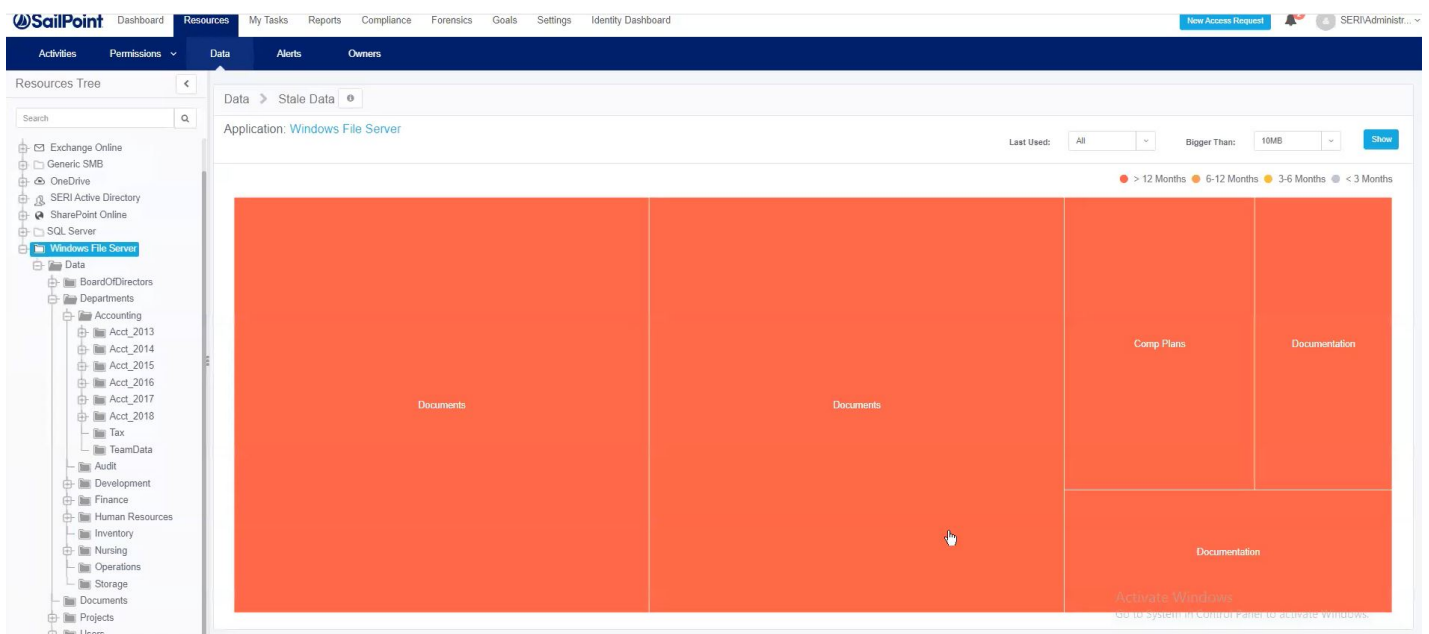
This tab helps identify the data distribution, the data level of staleness, and the usage frequency all from within a certain resource.

Each rectangle represents a contained / nested resource. Usage information is aggregated and presented based on the most recent usage of data within each resource.

A heat map will display the resources from a hierarchical point of view.

The resources will display in blocks of color based on when the last time they were accessed. The color legend is above the heat map to the right.

Note: The size of the block indicates the size of the folder.



Clicking a block will display the data analysis dialog which provides insight as to what type of content is within that resource block, what type of sensitive information is within the block and who is the owner of the resource block.


Data Analysis Last used 24 months ago

Resource : [Comp Plans](#)

Path : \wad-resource\Data\Departments\Human Resources\Comp Plans


Sensitive Data (24 of 11)

- ICD
- PII
- PCI Credit Card Types
- PHI



Content (15.50MB)

- Documents
- Other



Current Data Owners:

[Michelle Perez](#), [Sarah Campbell](#)

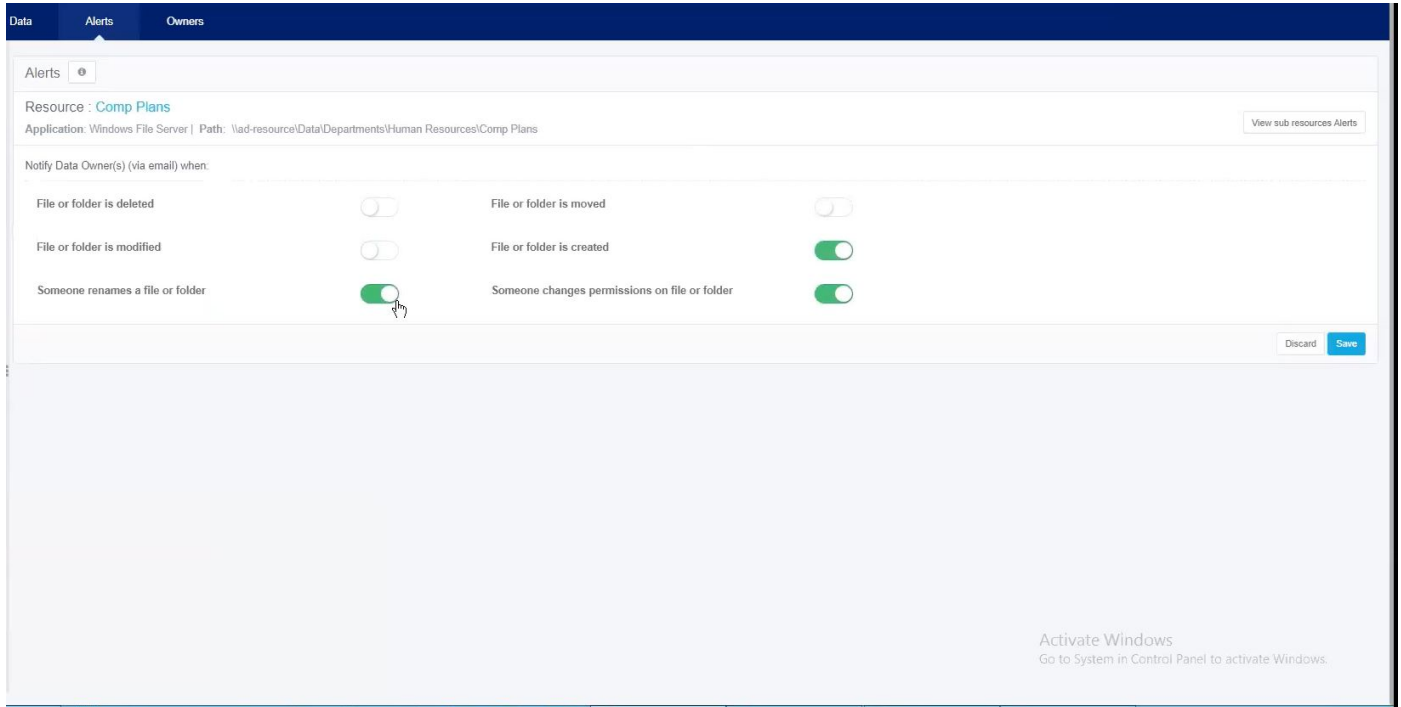
* The information relates only to files within the resource (not sub-resources)

Close

Alerts Tab

The Alerts tab allows you to enable or disable already preset alerts.

To add or edit alerts for the Resource tab, navigate to **Compliance > Alert Rules**. For more information on how to create or edit alerts, see the Alerts Guide.



Owners Tab

The Owners tab provides visibility into the ownership status of the data within a resource.

This view shows all the users and owners of a particular resource. The user also has the capability to alter data owners here.

With the Usage percentages displayed, File Access Manager provides activity information to help the user make a more informed decision about who own certain folders within a resource.

To fine tune the data displayed, use the Usage Statistics bar to have more refined data. You can adjust the timeframe or the actions performed within the folder.

Adding Owners to Resources

Within the table of displays a list of the most active users on a resource. If a user is not selected as an owner, click the **+Add Owner** button to add them.

If a user is not listed within the table and need to be added as an owner to the resource, click **Add New Owner** within the Current Owners window and search for them.

The screenshot shows the 'Owners' tab interface. On the left is a 'Resources Tree' with 'Human Resources' selected. The main area displays 'Usage Statistics' for the resource 'Human Resources' (Application: Windows File Server | Path: \\ad-resource\Data\Departments\Human Resources). The usage is shown as a pie chart and a table. The table lists users and their usage percentages, with 'Owner' status indicators.

Users	Department	Usage	Owner
Sarah Campbell (SERI\Sarah.Campbell)	Human Resources	58.4%	✓ Owner
Edward Baker (SERI\Edward.Baker)	Human Resources	8%	+ Add Owner
Michelle Perez (SERI\Michelle.Perez)	Human Resources	8%	✓ Owner
Anthony Roberts (SERI\Anthony.Roberts)	Human Resources	4.4%	+ Add Owner
Brian Nelson (SERI\Brian.Nelson)	Human Resources	4.4%	+ Add Owner
Others		16.8%	

On the right, the 'Current Owners' window shows two owners: Michelle Perez (SERI\Michelle.Perez) and Sarah Campbell (SERI\Sarah.Campbell), both associated with Human Resources. There is an '+ Add New Owner' button in the top right of this window.