Basic Search using Sail Point

\*\* Need a Serving Blue ticket to get access to SailPoint. \*\*

URL : <https://mp-fam-a02/identityiqfam/v1/#/tasks/access-certification/overview>

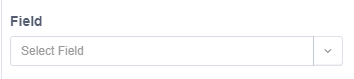
Main Page click to the Forensics tab



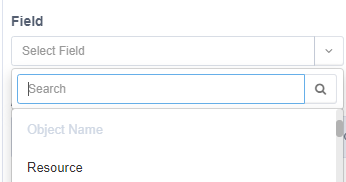
Basic search:

Clicking on the select field under the Field heading.

In this field you get different option to choose from depending what you researching…. For this simple search go to the field called Resource. The very first thing you do when start a new search….



Here you get a drop down menu and go to Resource or type Resource.



The next box it auto filled to “Any of”



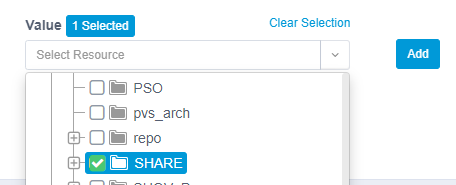
The Value field is another drop down menu. Here you pick the main Source that you searching for…



The majority will pick one of these two folders you looking for. (This example be the Share folder

\\Baz-filer01\Share)

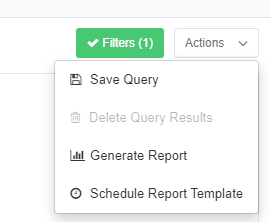




This is what it should look like when done. Move the mouse to the file path (highlighted) it will show the full path.



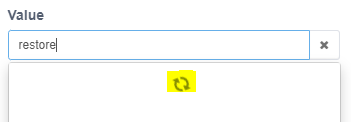
In the action field. You can save the query or create a report



Next step adding more filters to your search

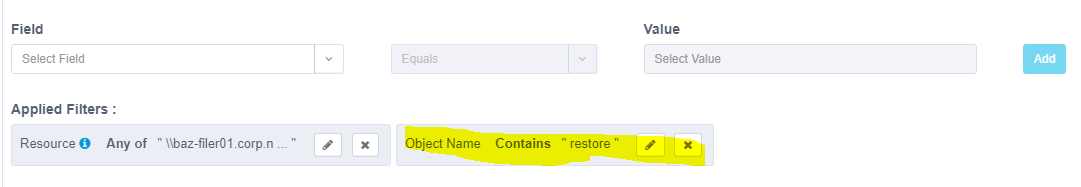
Go to the field name and choose object name the next box you can pick a Boolean type then the value

In the value should see a spinning circle

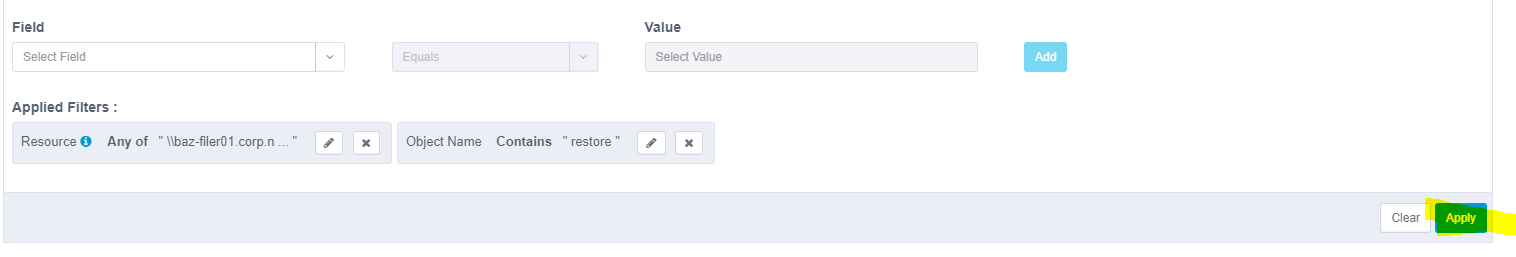


Here it searching for the name “restore” just click to open white space and it disappear

Now you click the blue add. Here you see the new filters that been highlighted.



Click the apply or if you want to change the date/time you can and then click apply

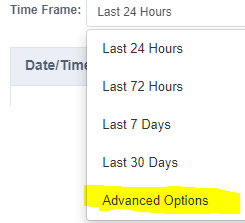


Next:

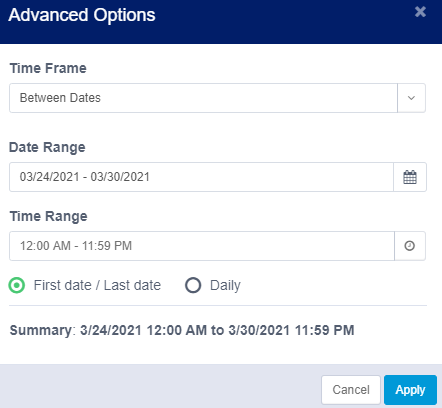
Now need to pick the time

Click the drop down arrow and you get another menu to choose from go to the Advanced Options



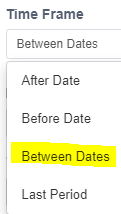


A pop up window should show

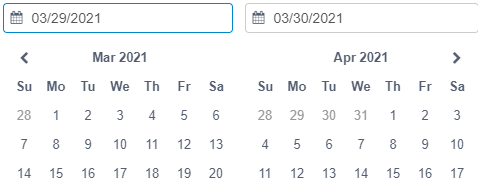


Here you can pick what date/time you looking for.

The Time Frame has a drop down menu. This one pick between date

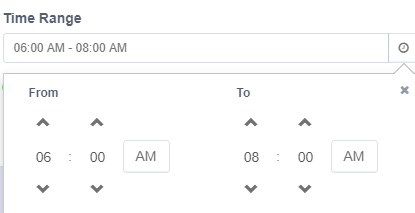


Date range

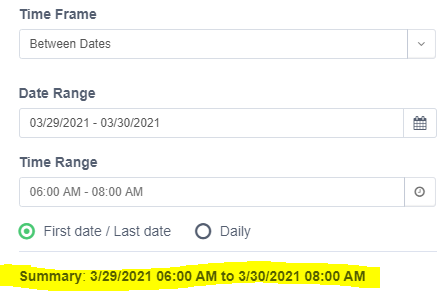


Here you can pick year or month and so for

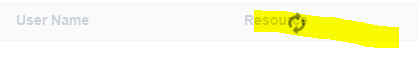
Time Range (here pick 6AM-8AM)



You should see the date/time summary



Click apply the start the search and see this circle moving in a circle it researching your basic parameter that you set. (Depending what you searching it might take some time to get the result back)



Final result:



At the bottom can go to other pages



In the Columns above the word action you get an drop down menu to pick which catalog you want to display.

