Using Access Filters to Limit Access in SkySpark

Security is of the upmost importance in applications such as SkySpark and we here at SkyFoundry take it very seriously. Using our tag-based record system, we easily enable you to control who can see what records based on simple filters.

An access filter allows the super user or any admin to control what users are able to access. Access to a project can be controlled on a per user basis at virtually any level.

Note that an admin can even control his or her own access filters.

How is an Access Filter Applied?

Find the Users app in the Host screen or any project:

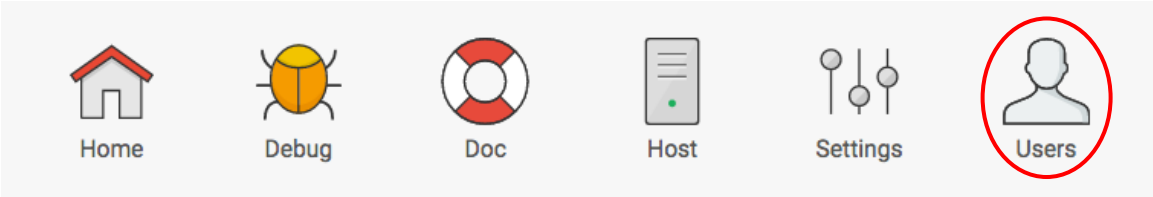

Figure 1: The Users app

Then, make a new user or double-click on the existing user that you want to experience the filtering.

Area intentionally left blank.

An access filter allows the super user or any admin to control what users are able to access. Here is an example:

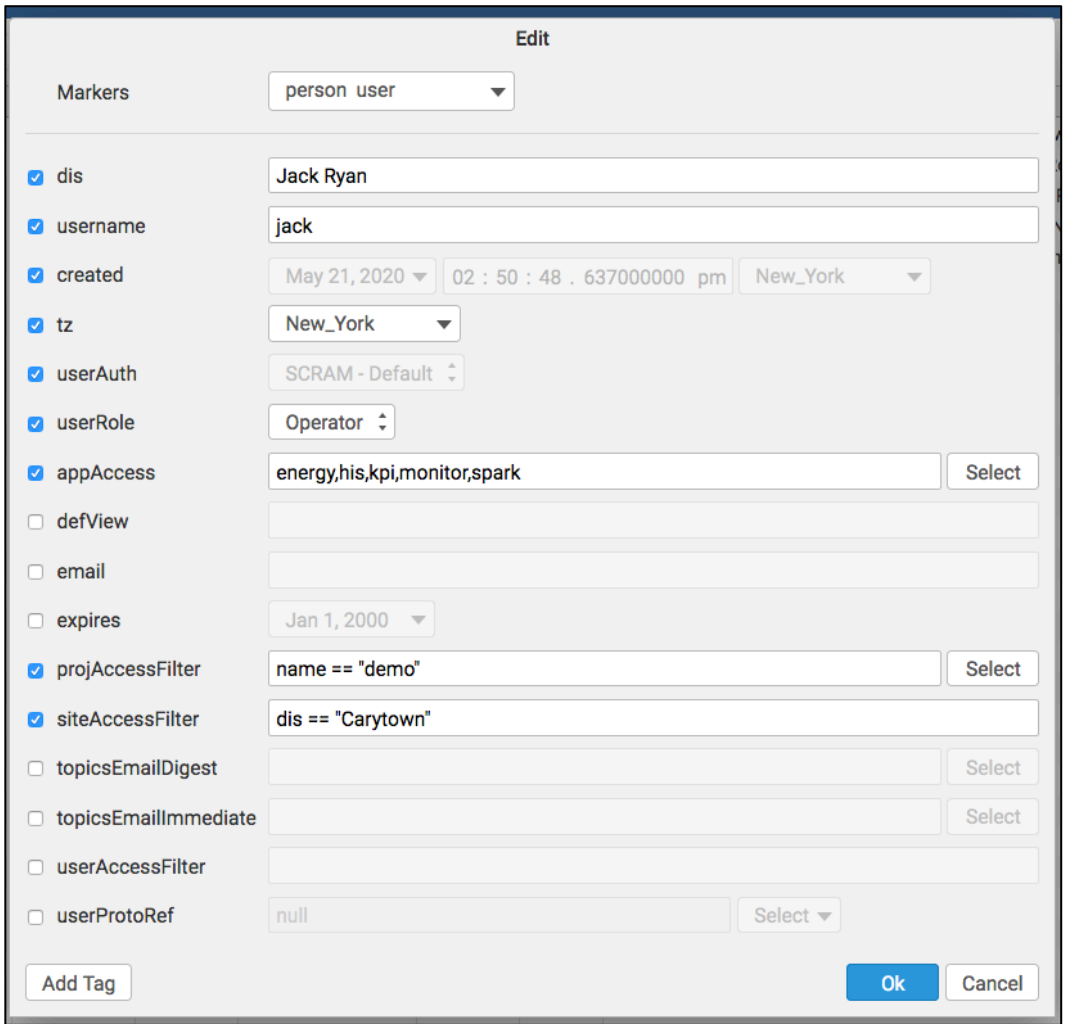

Figure 2: A user record inviting you to add filters

In this example, the appAccessFilter only lets this operator see the energy app, history app, kpi app, monitor app, and spark app. This person shouldn't be able to get into too much trouble!

This individual also only has access to the demo project by way of projAccessFilter and the filter name == "demo".

Also worth noting is that this entity is only expected to be working on Carytown via the siteAccessFilter: dis == "Carytown"

This should be plenty of access filtering, but did we stop there? No! Just in case you want to have more enjoyment with accessFilters, we allow you to make them out of any tag with the model {tag}AccessFilter: filter.

Any valid accessFilter that does not use the trap (->) operator can be used.

Here are some acceptable constructs:

== equals
!= not equal
< less than
<= less than or equal to
> greater than
>= greater than or equal to

And here are some accessFilters to try out:

pointAccessFilter: power
equipAccessFilter: meter
sparkRuleAccessFilter: hvac
sparkRuleAccessFilter: dis == “AHU Fan Failure”

and the recenty-added (at the time of this revision) userAccessFilter: dis == “Ben Linus” which makes sense if you want users to be invisible to some admins.