

Using Queries to create Smart Groups

Outside of creating queries for informational purposes, FileWave can help you create powerful, dynamic Smart Groups. The concept behind a Smart Group is to gather clients together who meet certain criteria. That would be, for example, all of the devices residing on a certain IP subnet. By adding Inventory queries to the criteria, then adding Filesets to the Group, you can create a Smart Group that will gather a Client device due to its meeting specified criteria, perform Fileset actions on that device, and as a result, the client no longer meets the criteria and drops out of the Group.

Example - Locating Filesets that contain SIP violations

Apple has released a security policy with OS X 10.11 called System Integrity Protection. In a nutshell, it says that no process will be able to have write access to any area of the OS that is protected. FileWave administrators may have scripts that violate this policy, and need to find out which are affected other than just seeing their Fileset(s) fail. There are two new fields in Inventory that identify whether or not a Mac has SIP active or not, and another field that identifies files that contain code that would violate the SIP rules. Here are the two query items:

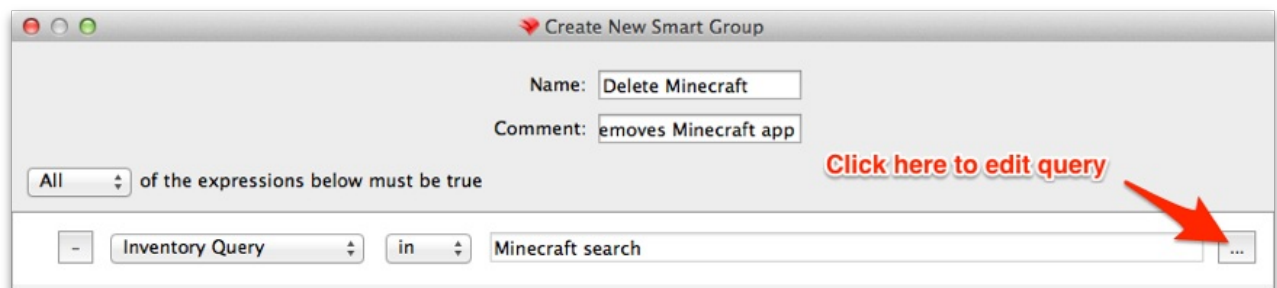


Two query items are shown in a list. The first item is "Fileset / OS X SIP Incompatible" with a dropdown set to "equals" and a value of "true". The second item is " / is system integrity protection enabled" with a dropdown set to "equals" and a value of "true". Both items have a "Not" checkbox on the left.

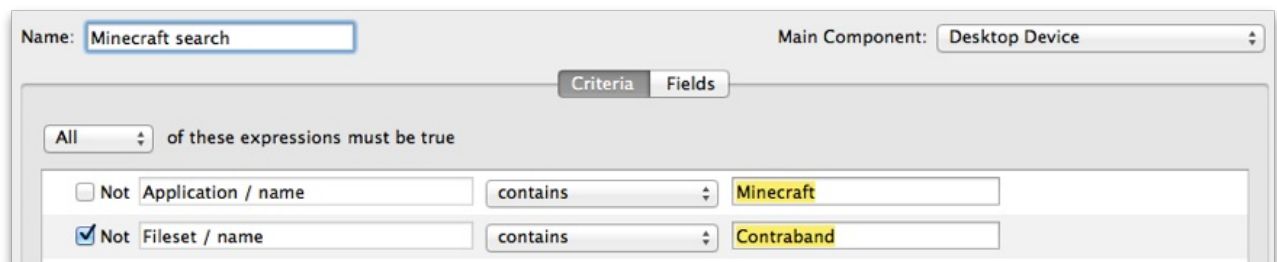
If you use either one of these to create a Smart Group, you will be able to rapidly identify your Macs that have SIP active, or your Filesets that have incompatible code in them. As you repair the Filesets, they will drop from that Smart Group. If someone turns off the SIP settings (not an easy task), the affected Mac will drop off that Smart Group.

Example - Removing contraband software

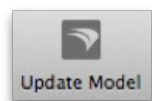
For example, you need to scan your clients for contraband software. If the client meets the criteria of having the software you are looking for, then you will have a Fileset execute that will remove that software. Since the Group is dynamic, as soon as the device responds that it no longer has the software and it has that Fileset installed, it will no longer qualify for that Group, and will drop out. Here is the workflow for setting this up:

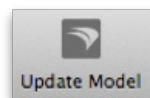
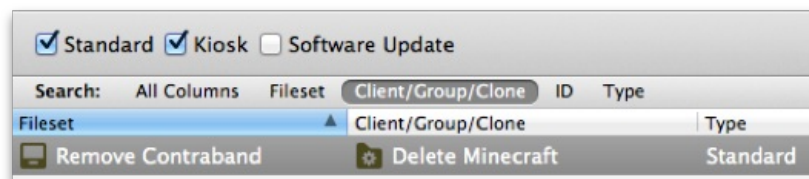
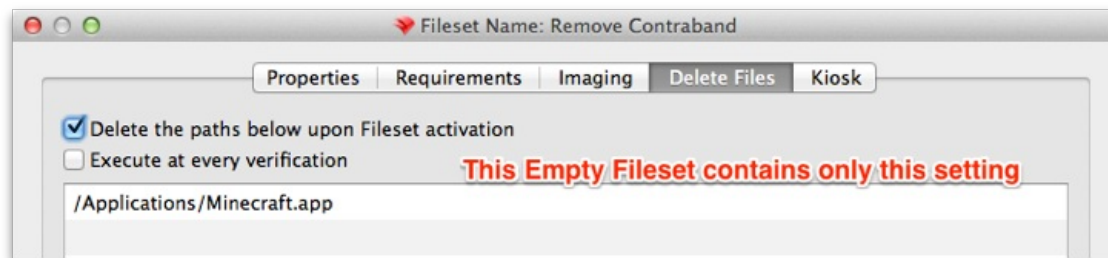


The "Create New Smart Group" dialog is shown. The "Name" field is "Delete Minecraft" and the "Comment" field is "removes Minecraft app". Below the fields, it says "All of the expressions below must be true". A red arrow points to a "Click here to edit query" link. Below the link, there is a query item: "Inventory Query" in "Minecraft search".



The "Minecraft search" criteria are shown. The "Name" field is "Minecraft search" and the "Main Component" is "Desktop Device". The "Criteria" tab is selected. It shows "All of these expressions must be true". There are two criteria: "Application / name" contains "Minecraft" and "Fileset / name" contains "Contraband". Both criteria have a "Not" checkbox on the left.





Once you have executed the Update Model command, the Fileset will execute and delete the software.

Revision #1

★ Created 12 July 2023 20:49:53 by Josh Levitsky

✎ Updated 12 July 2023 20:51:30 by Josh Levitsky