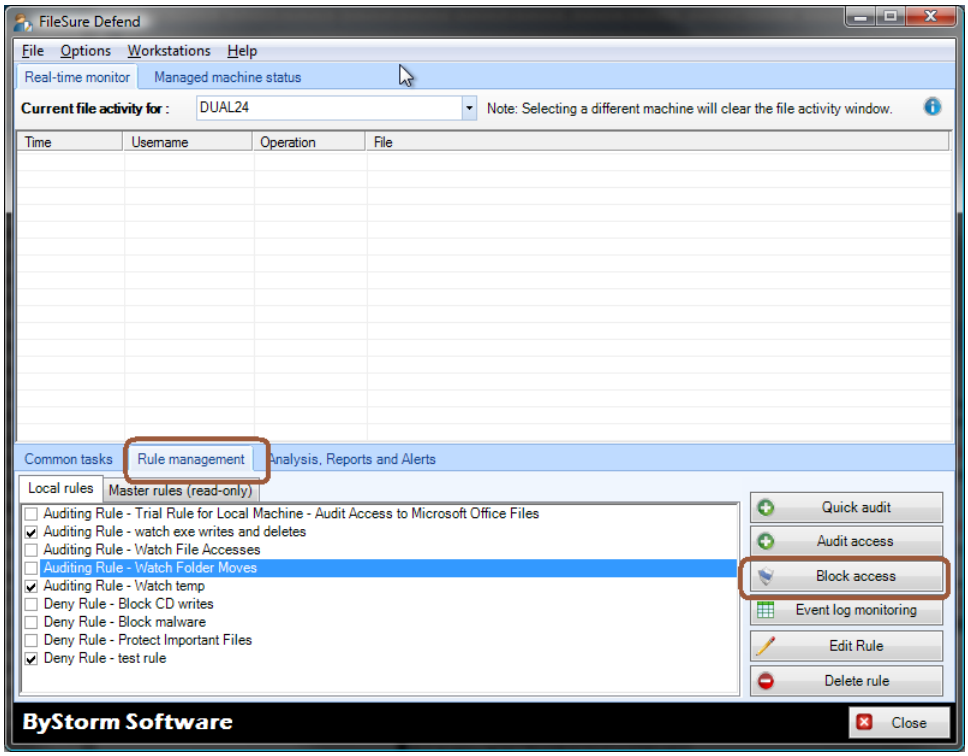
There are several solutions on the market to stop file copying to USB drives; some options are even built right into Windows. For most people, the complete lock down of USB drives isn't very attractive since USB drives are so useful. This opened up a space for other USB theft products, ranging from 'Endpoint management' products that report on what USB devices are being used to 'White-list' based systems where you define a list of 'Allowed USB devices' and some that combine both techniques. The thing is . . . it doesn't matter what the device is, it matters what files are vulnerable.

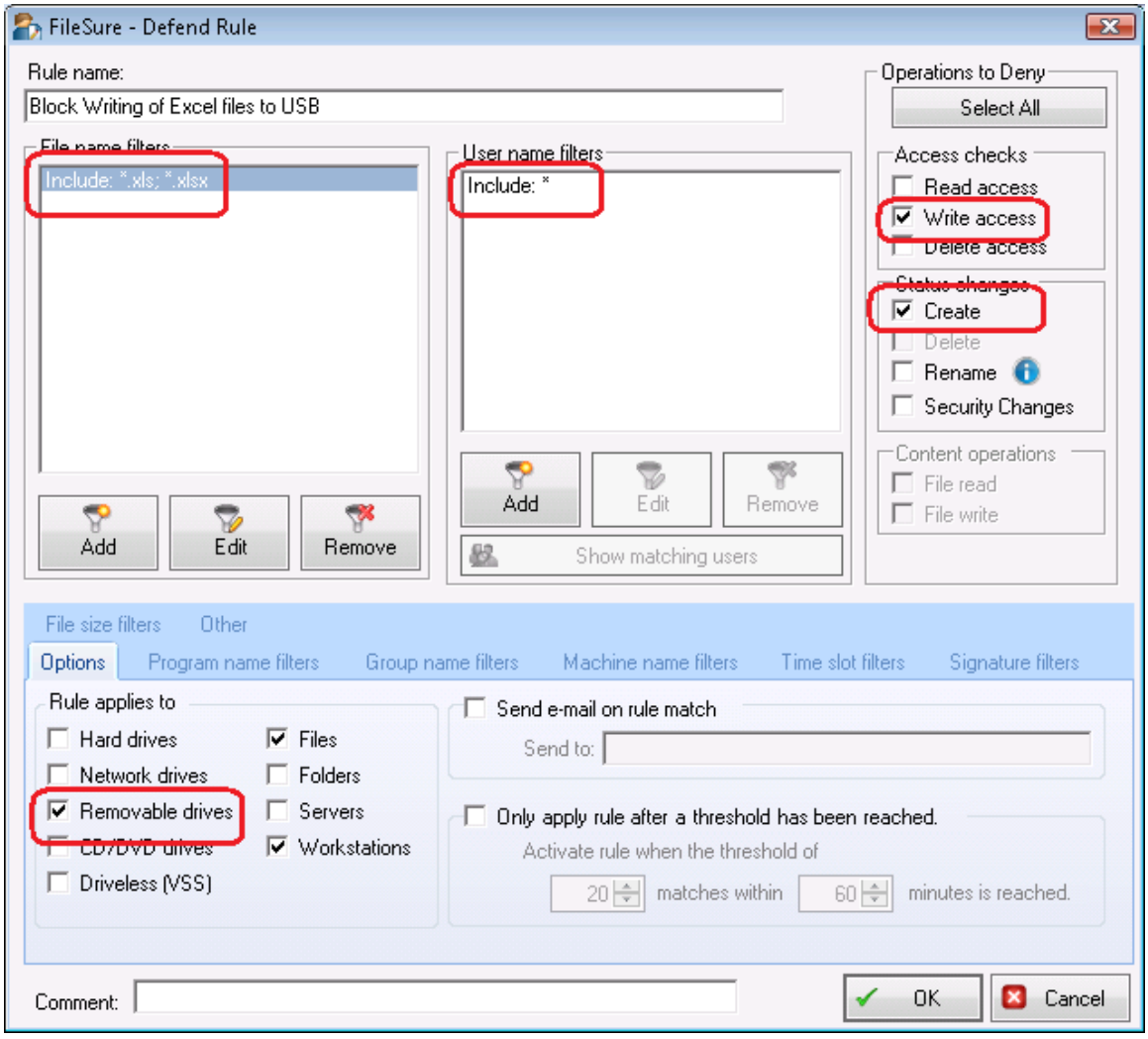
How we do it: FileSure starts with the files. You can determine what files you don't ever want leaving and block those from being copied TO a USB drive, period (while still leaving them otherwise available to authorized users). Or you can record or block all USB copies. You can see or block any files coming in to your environment FROM a USB drive. FileSure can also block against the powerful USB Switchblade attack where malicious data comes from the USB drive onto the computer (see the "Block Switchblade Attacks" how-to document for this).

Specifically, how to do it: Here is a screenshot defining a rule that blocks the writing of Microsoft Excel files to a removable drive using FileSure Defend. All we do is block files with the extensions XLS and XLSX from being created or written to on a removable drive, and we apply it to all users.

Step 1: On the mail FileSure console, click the "Rule management" tab and then click the "Block Access" button:



Refer to the picture below for the next several steps:



Step 2: Name the Rule “Block Writing of Excel Files to USB”
Step 3: Click “Add” under file name filters and “include” .xls & .xlsx
Step 4: Under Operations to Deny, check Write access and Create
Step 5: On the “Options” tab choose Removable drives, Files, and we want it to work for things on Workstations as well as the server
Step 6: Click OK
Step 7: Find the “Block Writing of Excel Files to USB” rule on the rules list and enable it.

Of course, you could choose specific files, things in a certain folder, different users or groups, times of day, or more to pinpoint exactly what you are trying to accomplish with the USB write block.

Whatever choice of security you choose, FileSure records the activity, can alert on it, reports on it and archives it centrally forever in an encrypted data store.