Employees need access to files to work—you need to ensure those files stay safe and on premises.

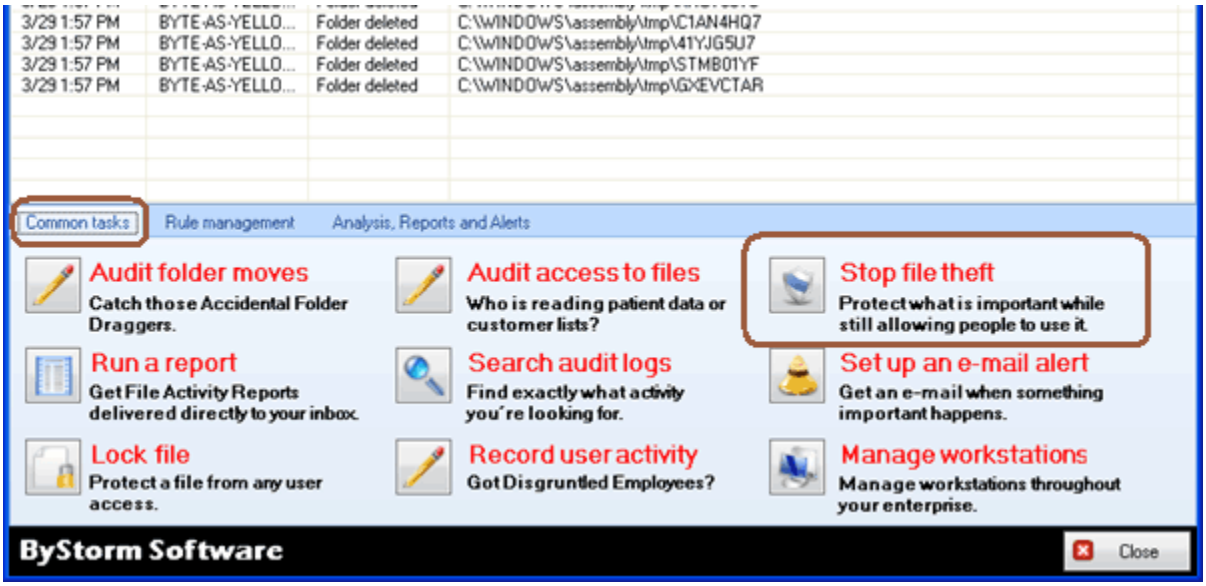
FileSure handles this problem by its unique ability to block access by program type. How?

- A file that can ONLY be accessed by the program in which it normally runs cannot be accessed to be moved or copied (or otherwise altered) by any external program. This is the safest route. It involves making a "white list" of programs authorized to open protected file types, and then blocking all others.

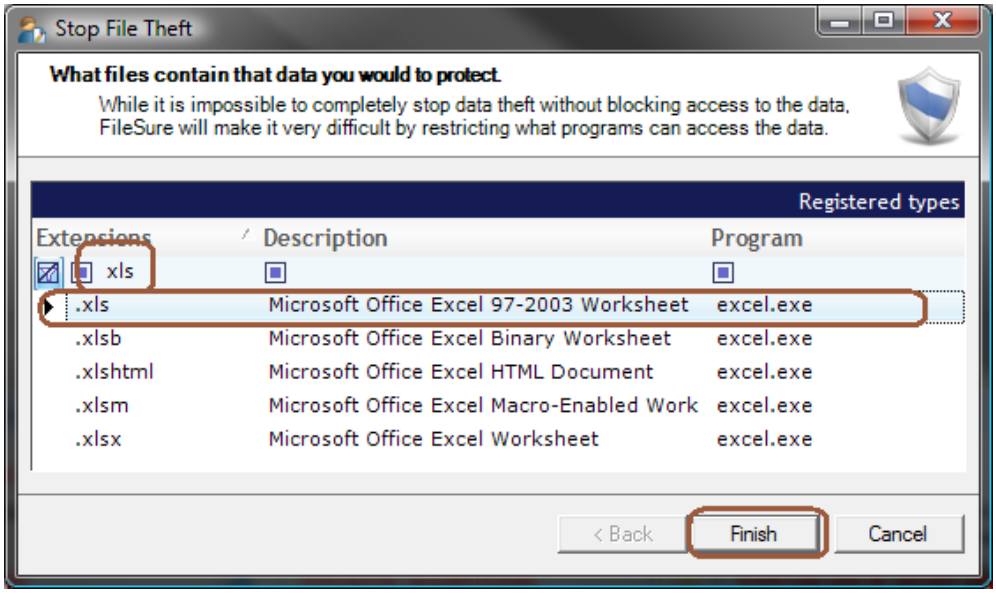
To protect all files of chosen types from theft while allowing authorized access:

Use the 'Stop File Theft' wizard on the 'Common tasks' area tab:

1. On the 'Common tasks' tab, click the 'Stop file Theft wizard'



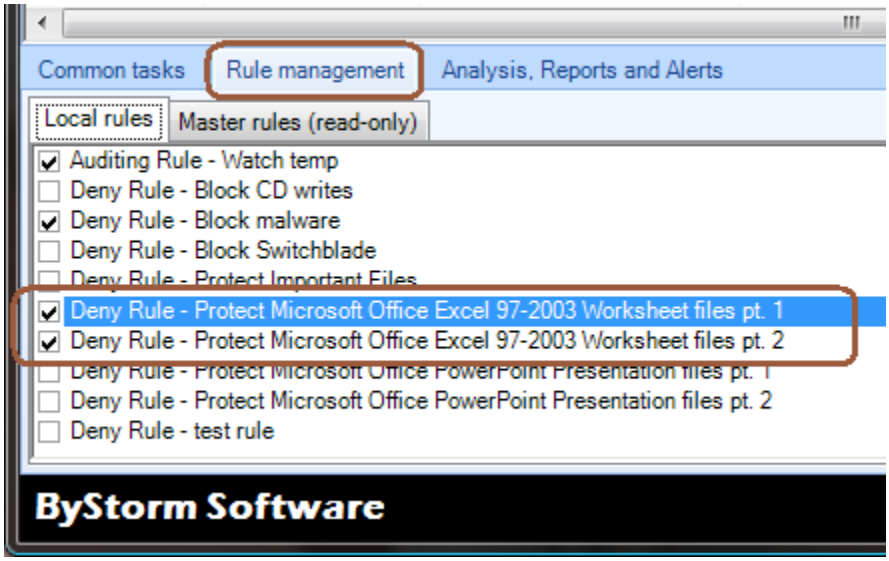
2. This will bring up a single page wizard where you are able to select what types of files you want to protect from theft. Here I filtered the list down to extensions that include an 'xls' and then I select the Microsoft Office Excel 97-2003 Worksheet entry and click Finish. See next page for illustration.



This wizard will build 2 rules:

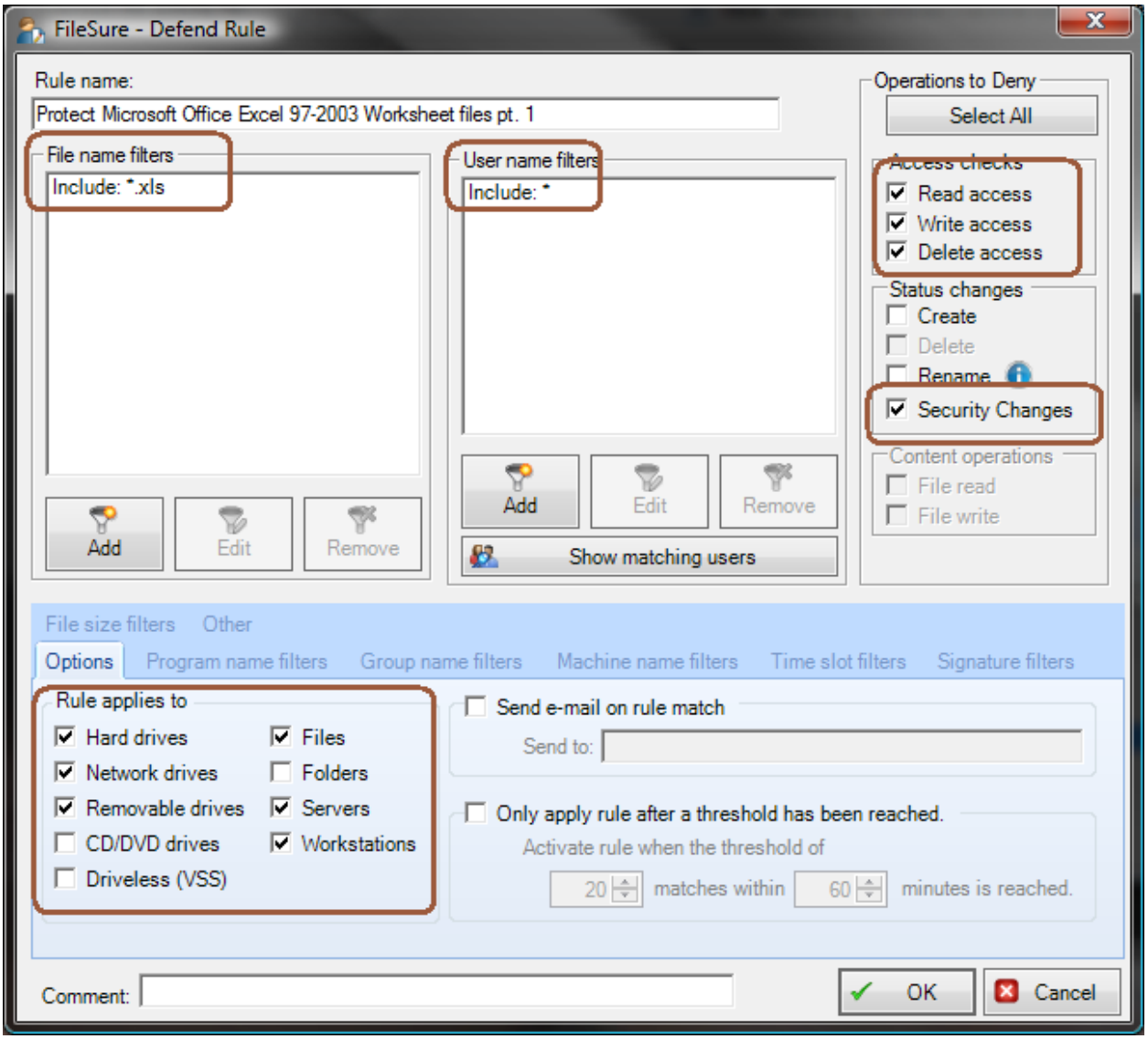
One rule blocks all access to the named file type ***with the exception of the program listed as its default program*** (excel.exe, in my example) and the other closes the 'Save as' hole, where the 'allowed' program could do a 'Save as' directly to the removable drive.

3. You can see the rules on the 'Rules management' tab

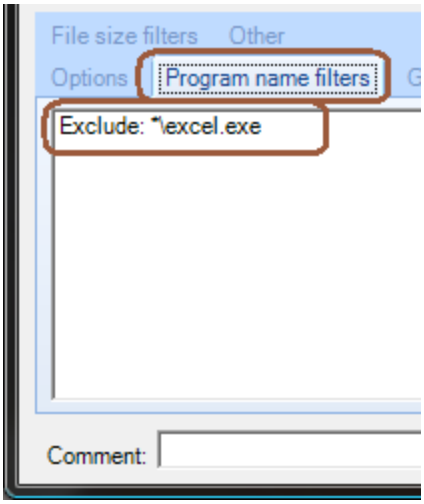


4. Select the first rule ('Deny Rule – Protect Microsoft Office Excel 97-2003 Workstation files pt.1) and click 'Edit rule' you'll see the details of how the rule works.

The wizard has built a rule that denies reading, writing, deleting or changing security on any XLS (*.xls) file stored on a hard drive, a removable drive and on the network. This rule applies to all users (*)



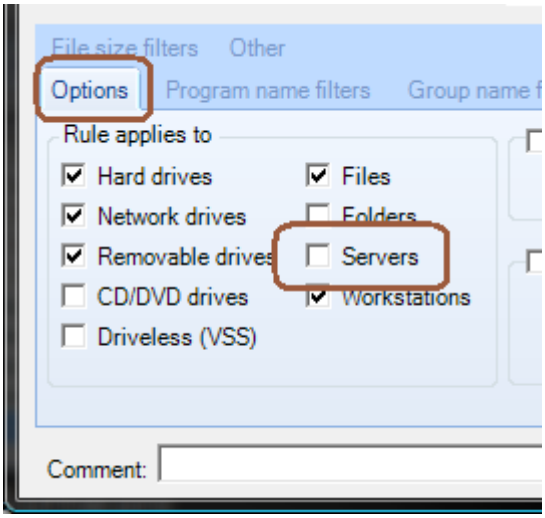
By denying read access, basically no one would be able to access the file at all. Click on the 'Program name filters' and you'll see the exclude filter that keeps this rule from applying if the program being used is '*\excel.exe'.



This single rule blocks all access to *.xls files by anyone unless they are using Microsoft Excel (*\excel.exe).

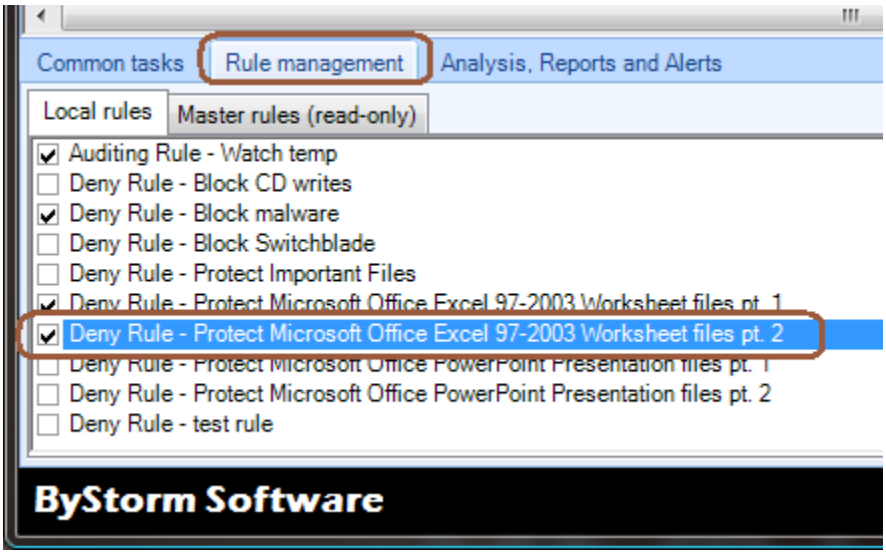
Let's make a small change to the rule as it's only intended to run on the workstation. Click on the 'Options' and uncheck

'Servers'.

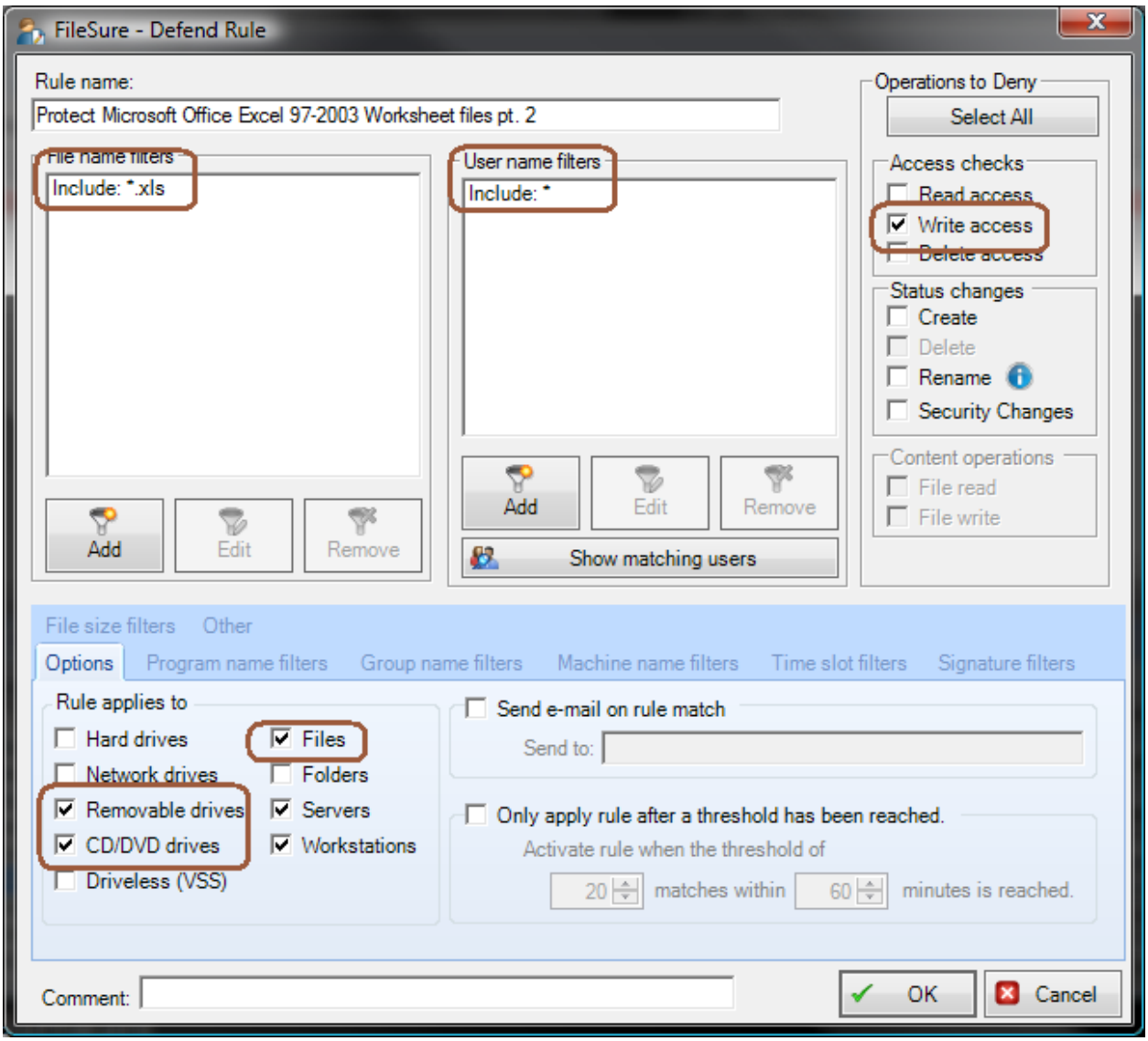


Click 'OK' to save the changes.

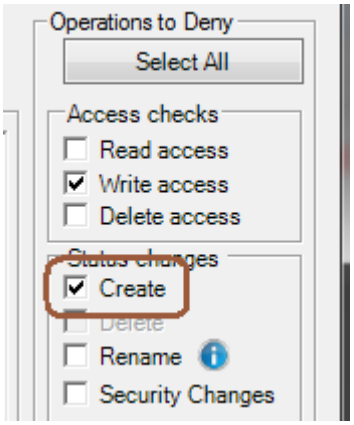
5. Now, let's take a look at the second rule. Click on the 'Rules management tab', select the 'Deny Rule – Protect Microsoft Office Excel 92-2003 Worksheet files pt. 2' rule and click the Edit button.



This rule prevents *.xls files from being written to a removable drives and applies to all users.



There is a known issue with this rule, we need to address. The wizard correctly defined that writes to removable drives should be blocked, but didn't block creating new files.



6. Check the 'Create' option, to block xls files from being created on removable drives.

Click OK to close the Edit rule screen.

That's it. When you deploy FileSure to the workstations, this rule will be pulled from the server and enforced.

FileSure Defend is blocking access to the protected data. No Microsoft Excel files may be emailed, sent by FTP, or saved or copied to USB devices or CD/DVDs—but normal file access is still allowed by authorized users for viewing and editing.

The only risk remaining is closing the holes inside the allowed program. In the example of Excel, you should set up rules to block ‘Save as’ or exports to non-xls types, like .123.