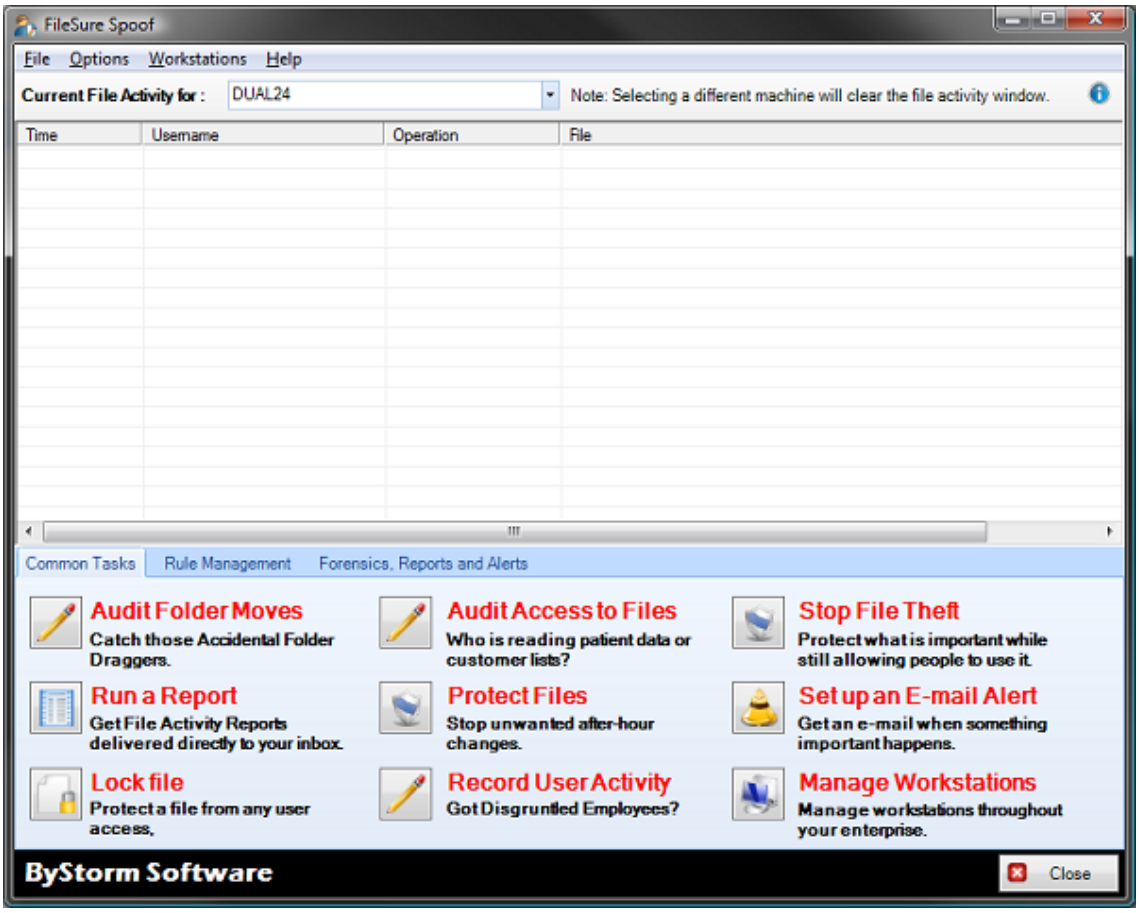
While you can disable administrative shares completely, many enterprise tools (like Microsoft System Management Server) rely on them to manage workstation deployments. By using FileSure, you can block remote accesses made by users yet allow these management tools to get through.

In this document, we will detail step by step how to configure FileSure for this.

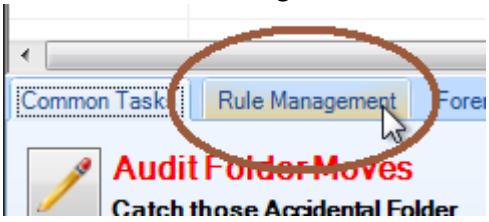
Step 1: Install FileSure on a central computer.
This computer will be used to define the rules that should be applied to the workstations. It will also receive all the audit logs from each of the workstations.

Step 2: Start the FileSure Console
Start the FileSure console by clicking Start->All Programs->ByStorm Software->FileSure. You should see a screen similar to this one:

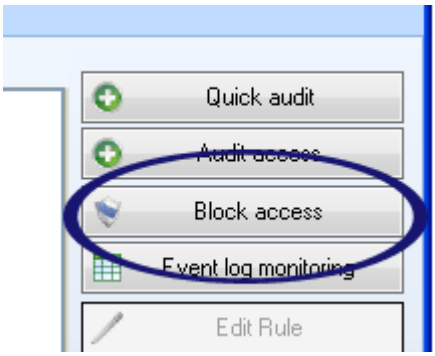


Step 3: Define a rule that will block all remote access.
We need to create a rule that will block network access of files for all users. Use care to define the rule completely and accurately; if you don't, you could lock yourself out of Windows completely, even if you're an Administrator.

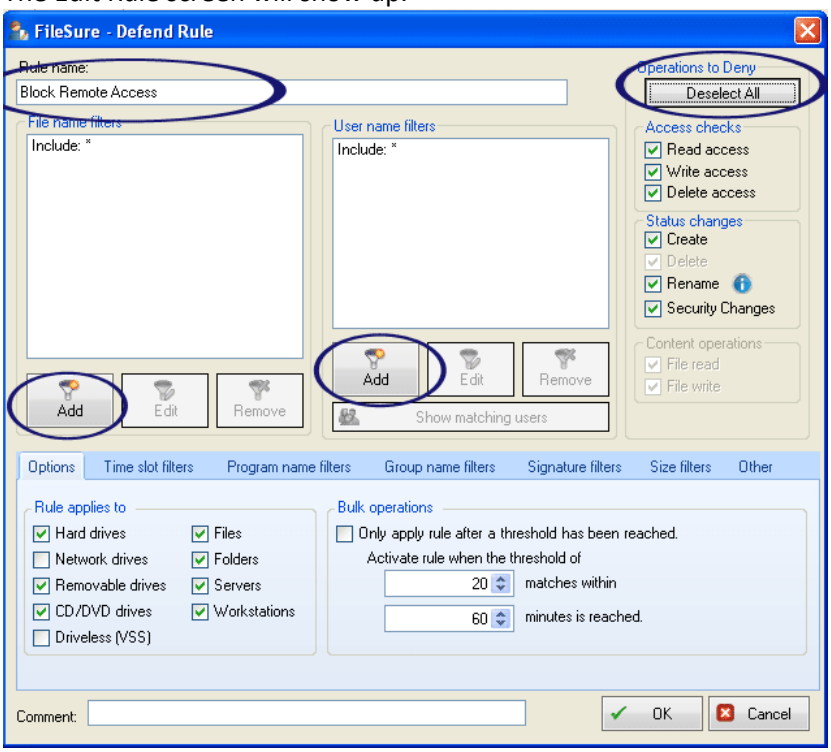
i. Click on the Rule Management tab



ii. Click on the “Block access” button.

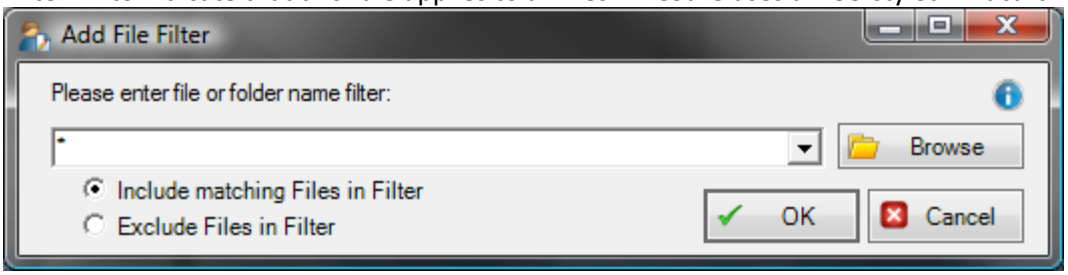


The Edit Rule screen will show up.



iii. In the Rule Name field circled above, type, ‘Block remote accesses’

iv. Click the Add button in the ‘File Name Filters’ area, circled above
Enter ‘*’ to indicate that this rule applies to all files. FileSure uses a DOS-styled wildcard for matching files.

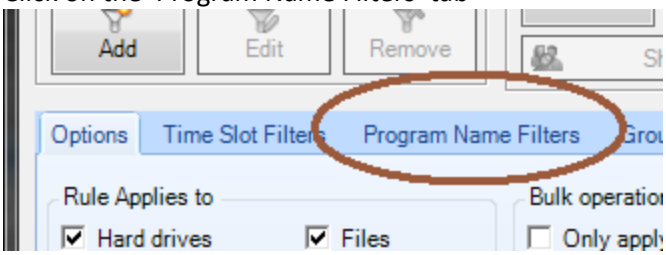


Click OK.

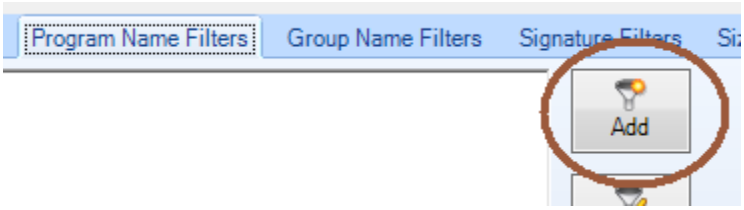
v. Click the Add button in the ‘User Name Filters’ area, circled above
Enter ‘*’ to indicate that this rule applies to all users. FileSure uses a DOS-styled wildcard for matching users.
Click OK.

vi. Click the ‘Select All’ button in the ‘Operations to Deny’ area, circled above, to indicate that we want to deny all access to the files.

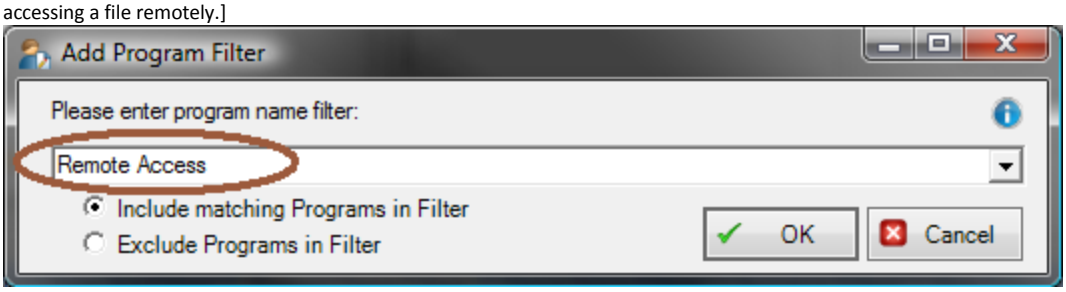
vii. Click on the ‘Program Name Filters’ tab



Click the ‘Add’ button

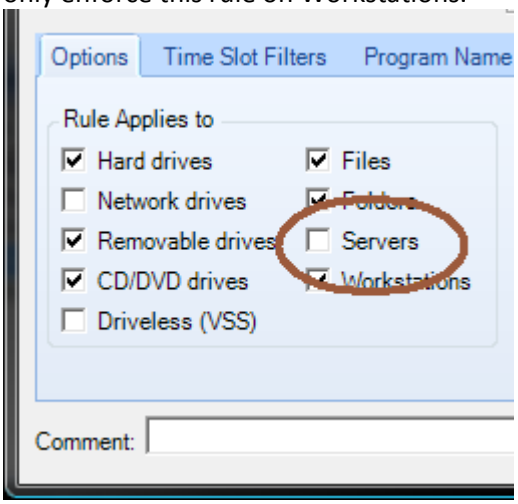


Enter ‘Remote Access’ to indicate that this rule applies to files accesses made from remote computers.
[Note: we use a program filter here since we determine network access by looking at the program name. It’s not possible to know what program is accessing a file remotely.]

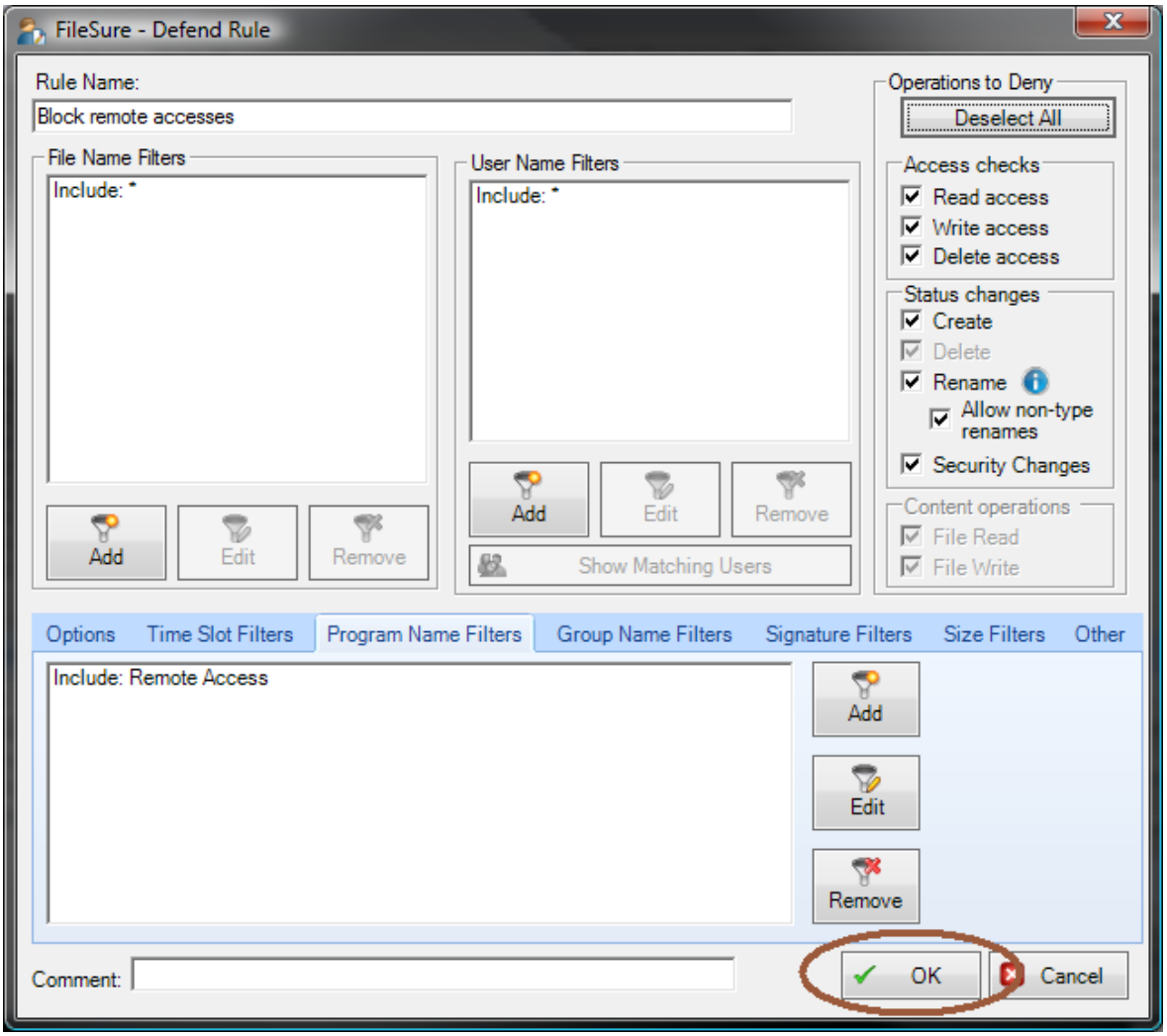


Click OK.

viii. If you installed FileSure on a computer that needs to allow remote access, like a network server, you’ll need to uncheck the ‘Servers’ checkbox in the ‘Rules applies to’ area. By unchecking ‘Servers’, you are telling FileSure to only enforce this rule on Workstations.

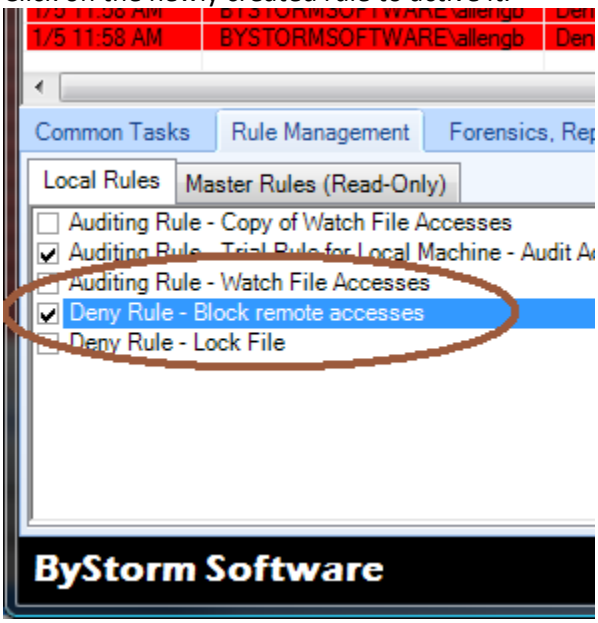


ix. Check all the settings to make sure that everything is correct, then click OK to save the rule. Just a reminder, this is a powerful deny rule that if set up incorrectly could block YOU from reading any file and basically locking Windows.



Step 4: Activate the rule

Click on the newly created rule to active it.



Step 5: Tweaking the rule

At this point, FileSure is blocking **all** remote file accesses, but that means that we will also be blocking the management tools that need remote access to work. If we provide a way for these tools to get through so they can do their job, we also run the risk of compromising the files we're trying to protect.

I'm going to run through the pros and cons of several options, and you can decide which option(s) fits into your environment best.

Option 1: Block all remote file accesses except for the user accounts used by management tools.

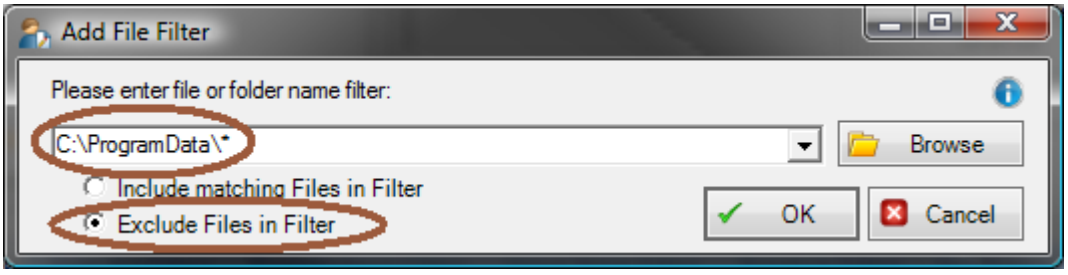
- **Pro**: This method is easy to understand and covers all the files regardless of the workstation drive configuration.
- **Con**: Someone could access the protected shares if they log on with the credentials of the management tools.
- **Con**: All the accounts used by management tools would need to be excluded. If all the accounts are members of a domain group, that group could be excluded but then have to monitor the group membership.

In the screen shot below, I have defined that any user named 'SMSUser' will be excluded. (See Step 3.v above on how to add a user name filter.)

Option 2: Block all remote file accesses except to the folders that the management tools use.

- **Pro**: This method is easy to understand and doesn't open a direct security hole.
- **Con**: It could be difficult to define what folders need to be excluded since each management tool has different requirements.
- **Con**: This will require a somewhat standard workstation configuration, but that's probably ok since the management tools probably already require a standard configuration.

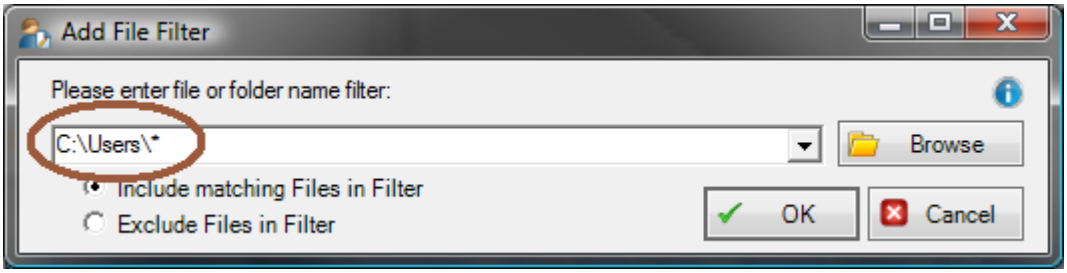
In the screen shot below, I have defined that access to the folder 'C:\ProgramData' is allowed by adding an exclude file filter. (See Step 3.iv above on how to add a file name filter.)



Option 3: Only block remote access to user specific folders.

- **Pro**: This method is probably the safest since the management tools shouldn't access user specific folders (e.g. C:\Users*) remotely.
- **Con**: Unfortunately, this method probably doesn't work well in the real world since users put data all over their hard drives.
- **Con**: This will require a somewhat standard workstation configuration, but that's probably ok since the management tools probably already require a standard configuration.

In the screen shot below, I have defined that access to the 'C:\Users*' be denied. It's important to note that this should be the only file filter instead of an additional one since file filters can overlap. (See Step 3.iv above on how to add a file name filter.)



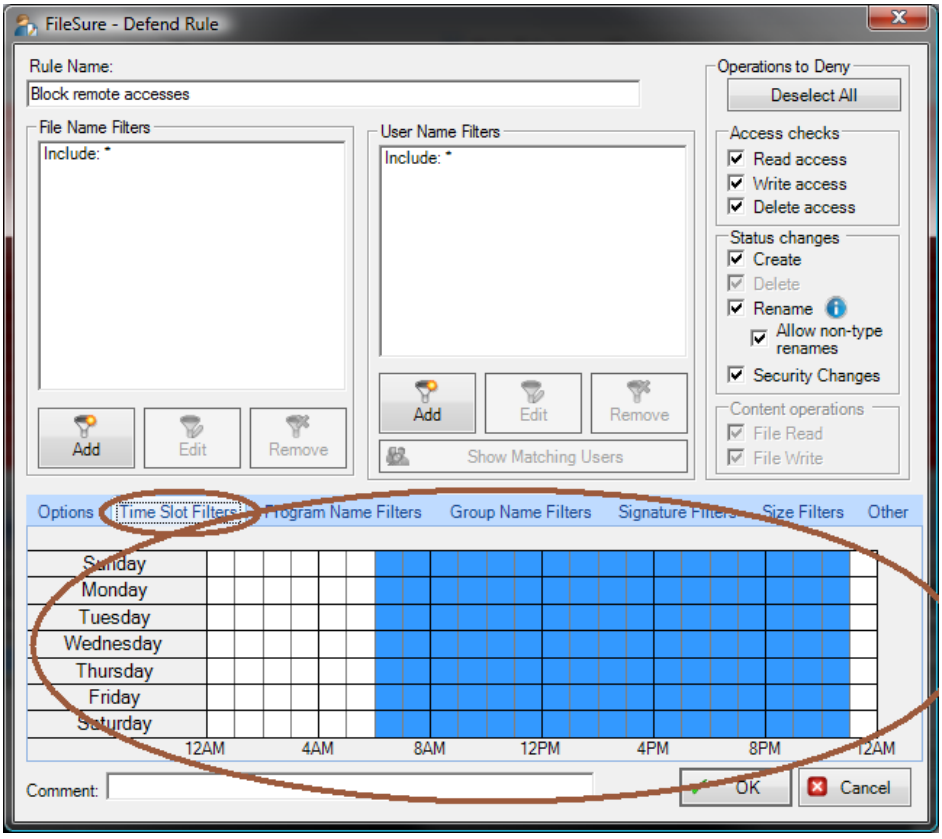
Option 4: Block all remote access based on the time of the day.

Pro: This method is nice because most management tools are configured to do their work in the middle of the night when no one is in the office.

Pro: It's easy to understand and set up.

Con: It doesn't work at all if the management tools need to work while users are in the office.

In the screen shot below, I have defined that the rule will be active from 6AM to 11PM, which means that remote access will be allowed from 11PM to 6AM and blocked the rest of the time.



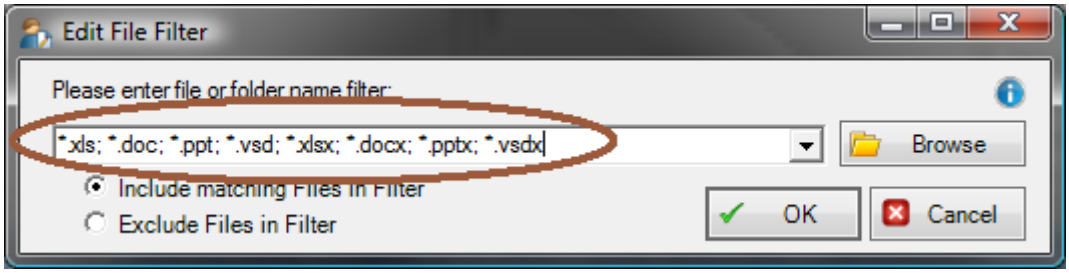
Option 5: Block remote access to protected file types

Pro: This method is easy to understand, set up and should work well since users and management tools use different types of files.

Con: It might be difficult to determine all the types of files that need to be protected from remote access; however that might not be a major problem since most companies standardize on applications.

Con: There could be protected files that the management tool needs to access remotely.

In the screen shot below, I have defined that remote access to all Microsoft Office files be denied. It's important to note that this should be the only file filter instead of an additional one since file filters can overlap. (See Step 3.iv above on how to add a file name filter.)



By using one or a combination of the methods above, you can configure he rule to allow remote access when and to whom you want and block everyone else.

Step 6: All done

Congratulations! You can successfully configured FileSure to block remote file accesses while allowing management tools the access that they need. The audit log will contain details on any denied accesses including what file, who did it and when it happened.