

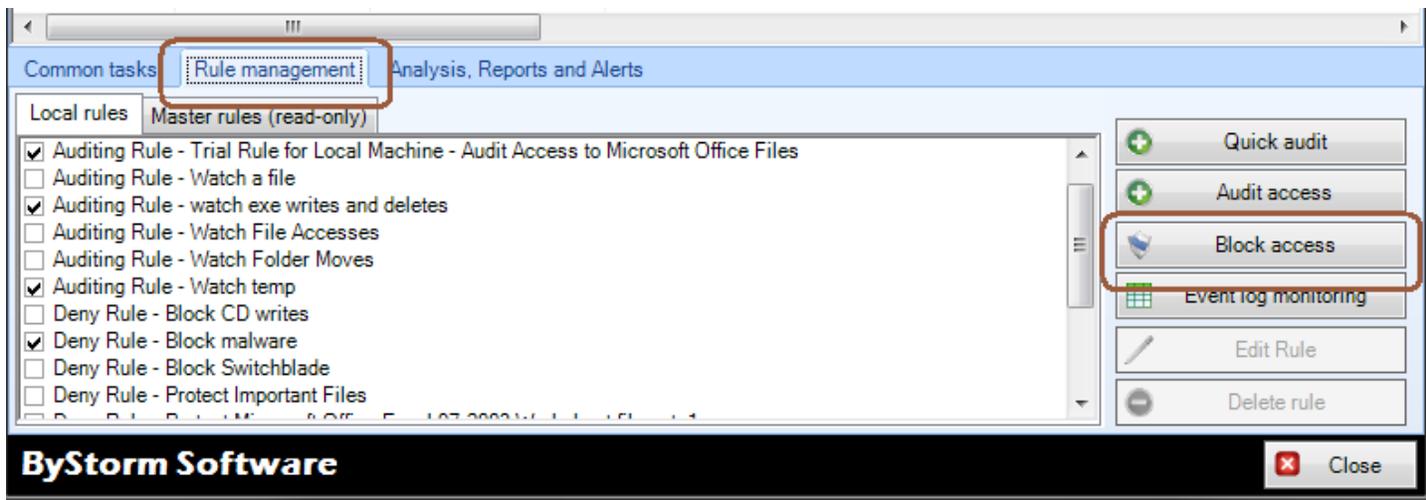
FileSure by its very nature gathers information that is sensitive. For example, even knowing that a file called Q4Layoffs.xls exists could be damaging. Since the FileSure console provides a method for querying the audit logs, anyone with access to the console itself could find information that shouldn't be seen.

The console is typically installed on a server and usually only administrators have the ability to run programs on the server, but in large IT groups, there could be tiers of administrators. Maybe you want only some administrators to be able to use the FileSure and block all the others.

One possible solution is to use Windows security and put a deny ACE on the FileSure.exe file. Problem with that approach is we're dealing with Administrators, so if they want, they can just remove the ACE and open the program.

A better approach is to use FileSure Defend itself to prevent prying eyes from reading the FileSure.exe. This How-to will show you how to configure FileSure Defend to block all Administrators except for a certain few from starting the FileSure console.

1. Start the FileSure console and click the 'Rules management' tab, then click the 'Block access' button.

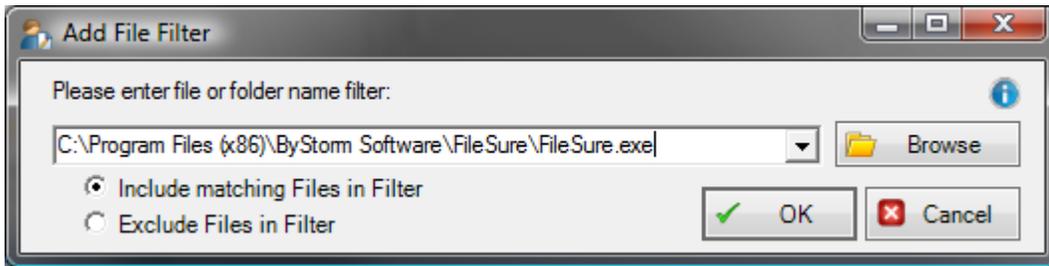


2. On the Defend rule screen, you make the following changes:
  - a. For the 'Rule name' enter 'Block read access to the FileSure Console'
  - b. Under 'Operations to Deny' check 'Read access'
  - c. In the 'User name filters' section, click the 'Add' and add an include filter of '\*' to cover all users
  - d. Click Add again and this time add an exclude filter for the users you want to allow access to, in my example, I'm going to exclude my account.



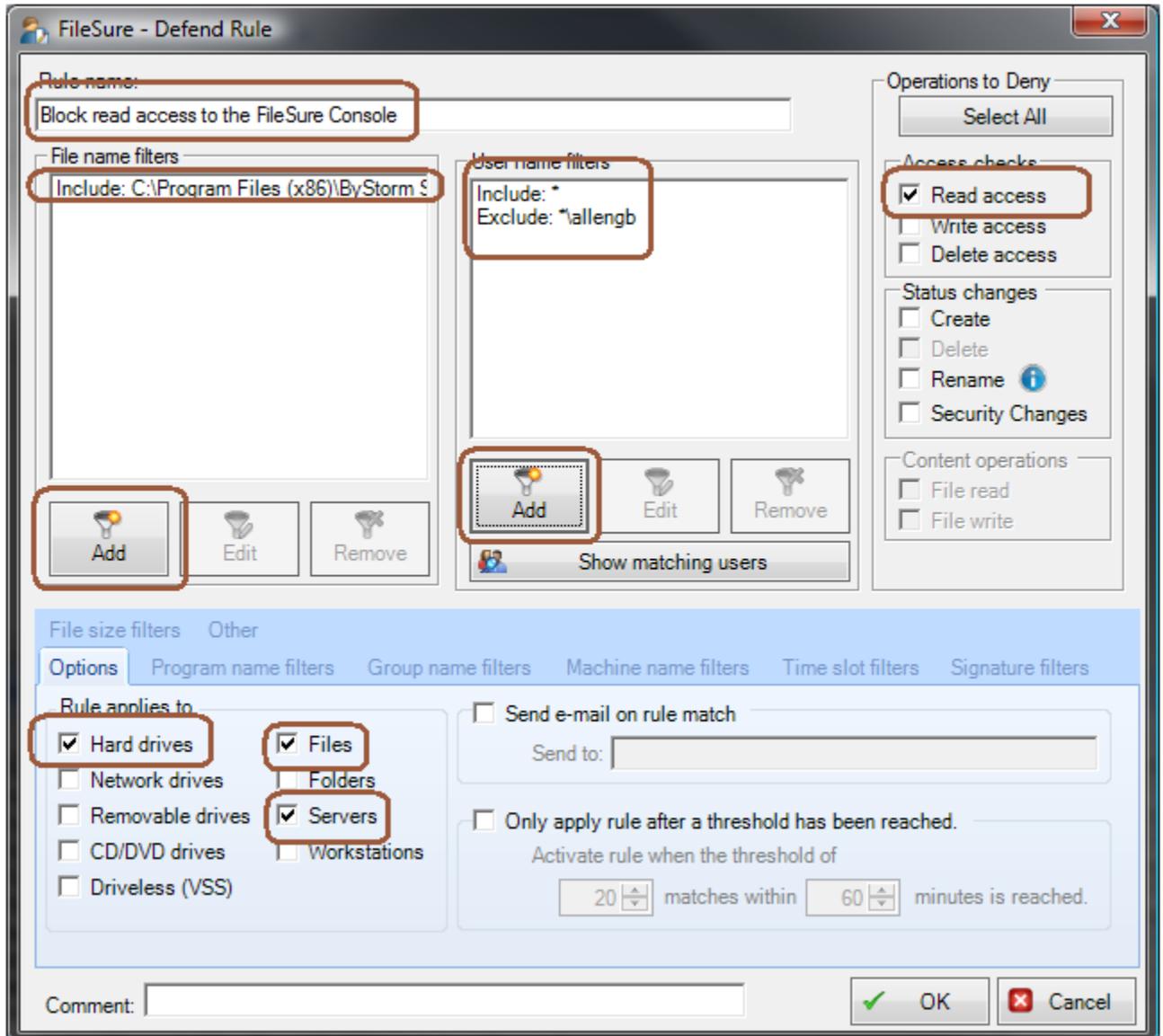
- e. In the 'File name filters' section, click the 'Add' button and enter the path to the FileSure console executable file. In my case 'C:\Program Files (x86)\ByStorm

Software\FileSure\FileSure.exe'

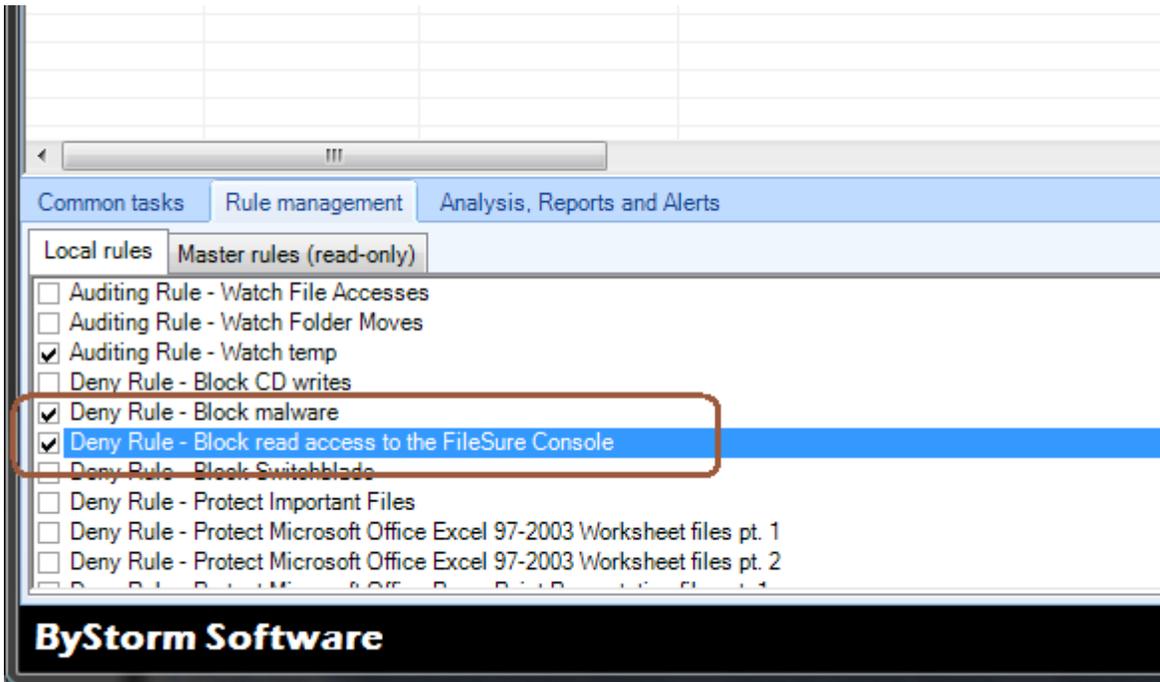


- f. In the 'Rule applies to' area, uncheck everything except 'Hard drives', 'Files' and 'Servers'.

When all these changes are made, your rule should look something like this:



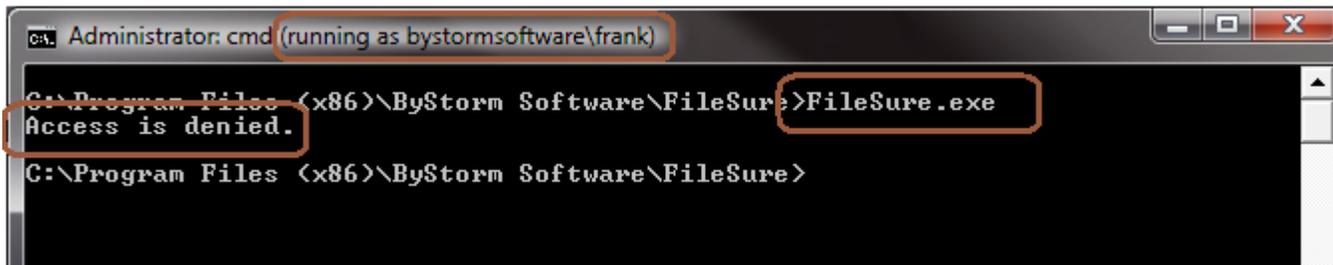
3. Click 'OK' to close the rule screen and find the newly created rule and click the checkbox to turn it



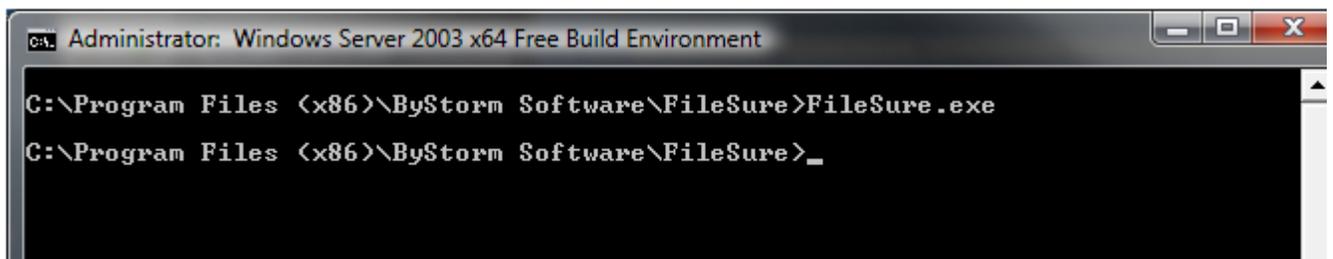
on.

At this point, FileSure Defend is blocking any user (including Administrators) except allengb from running FileSure.exe. Let's test it:

Frank, like me, is an Administrator and here is screen shot of Frank attempting to start the console.



Here is the same command running for me (allengb)



When the FileSure console comes up, you'll see that FileSure recorded that Frank attempted to start the console but was

denied.

The screenshot shows the FileSure Defend application window. At the top, there is a menu bar with 'File', 'Options', 'Workstations', and 'Help'. Below the menu bar, there are two tabs: 'Real-time monitor' and 'Managed machine status'. A dropdown menu shows 'Current file activity for : DUAL24' with a note: 'Note: Selecting a different machine will clear the file activity window.' Below this is a table with the following data:

Time	Username	Operation	File
3/4 11:44 AM	frank	Denied Opened for Re...	C:\PROGRAM FILES (X86)\BYSTORM SOFTWARE\FILESURE\FILESURE EXE

Below the table, there are three tabs: 'Common tasks', 'Rule management', and 'Analysis, Reports and Alerts'. The 'Common tasks' tab is active and contains several task cards:

- Audit folder moves**: Catch those Accidental Folder Draggers.
- Audit access to files**: Who is reading patient data or customer lists?
- Stop file theft**: Protect what is important while still allowing people to use it.
- Run a report**: Get File Activity Reports delivered directly to your inbox.
- Search audit logs**: Find exactly what activity you're looking for.
- Set up an e-mail alert**: Get an e-mail when something important happens.
- Lock file**: Protect a file from any user access.
- Record user activity**: Got Disgruntled Employees?
- Manage workstations**: Manage workstations throughout your enterprise.

At the bottom left, the 'ByStorm Software' logo is visible. At the bottom right, there is a 'Close' button.