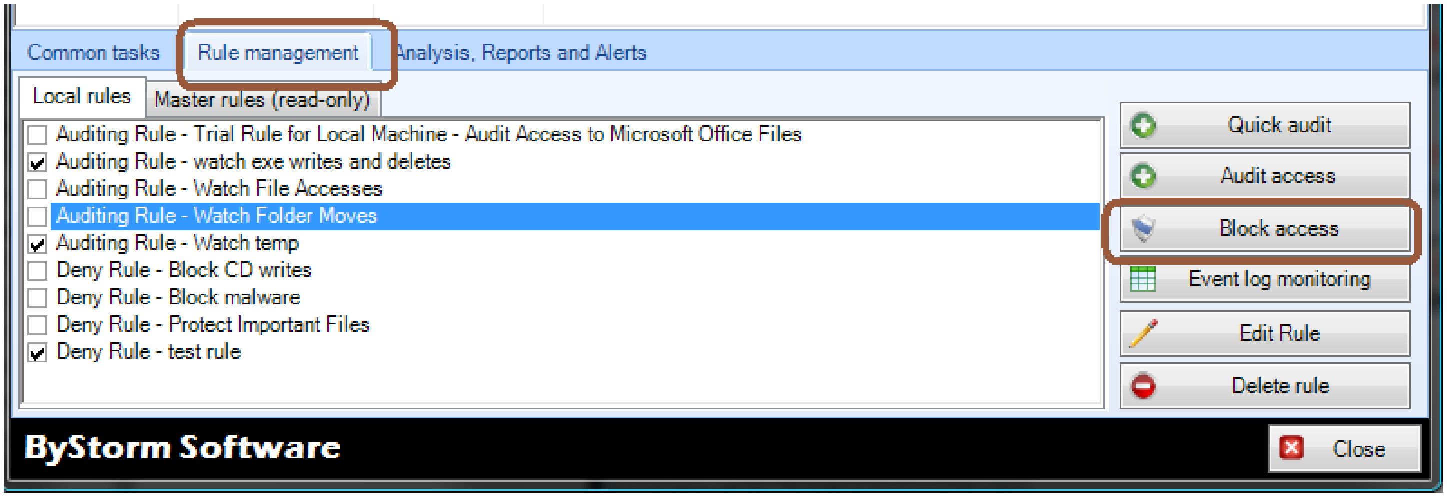
We’ve all been here, you spend hours, or maybe days, to get a computer working correctly for a client only to have them logon (as an Administrator) and mess it up somehow. Maybe, he was installing some new nifty-biff program to track his dog, or maybe he wanted to play a DVD (which installed a DRM Root-kit) or maybe he was just using the computer and some web-based malware exploited his security privilege and completely messed the computer up.

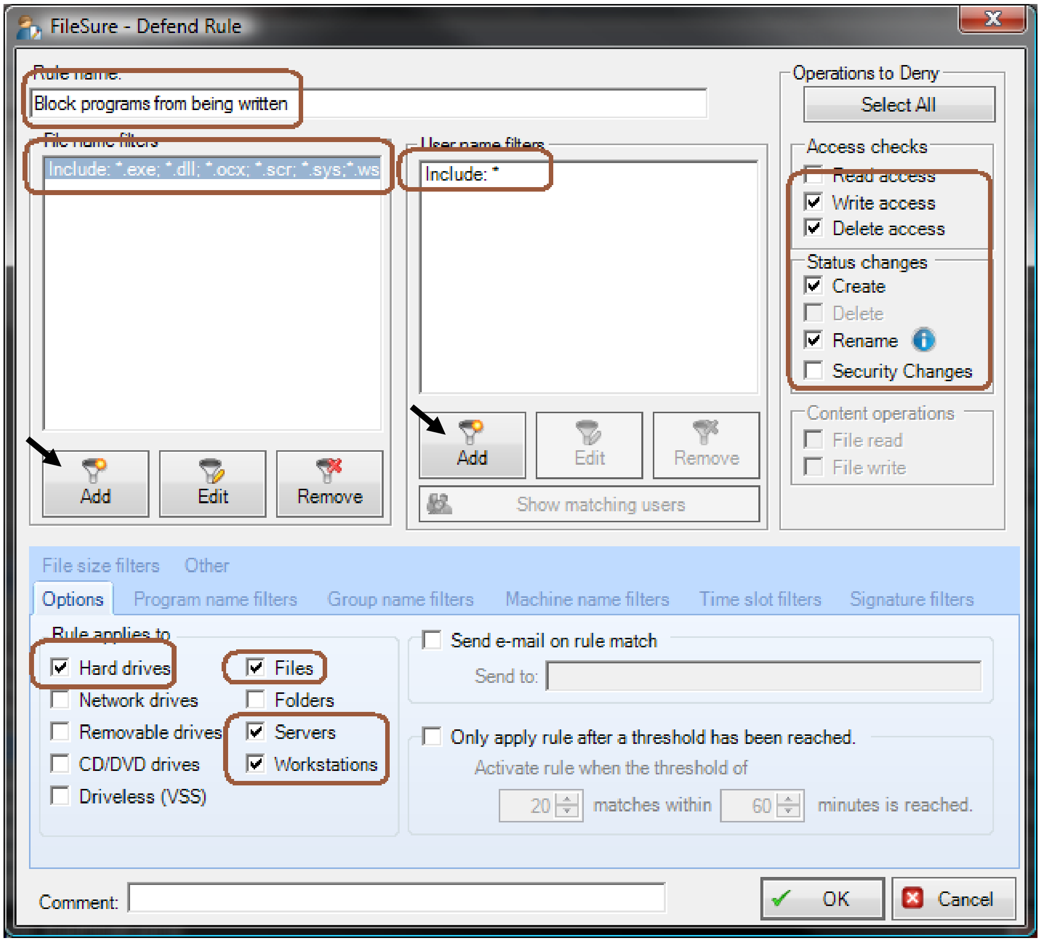
Whatever the case, this document will explain how to use FileSure to product the computer from ‘unauthorized programs’ getting installed. This set up will also protect against most malware and virus, even those that virus scanners haven’t written a signature for.

1. Install FileSure on the computer to be protected. [Note: If you need to protect multiple computers, you can install FileSure on a central server and use FileSure workstation to protect each machine.]



☐ Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files
☑ Auditing Rule - watch exe writes and deletes
☐ Auditing Rule - Watch File Accesses
☐ Auditing Rule - Watch Folder Moves
☑ Auditing Rule - Watch temp
☐ Deny Rule - Block CD writes
☐ Deny Rule - Block malware
☐ Deny Rule - Protect Important Files
☑ Deny Rule - test rule

2. Click the Rule management tab on the main FileSure console and then click the Block Access button to bring up a ‘Defend rule’ dialog. Refer to the picture below for the next several steps.



Rule name: Block programs from being written

File name filters: Include: *.exe; *.dll; *.ocx; *.scr; *.sys;*.ws

User name filters: Include: *

Operations to Deny

Access checks
☐ Read access
☑ Write access
☑ Delete access

Status changes
☑ Create
☐ Delete
☑ Rename
☐ Security Changes

Content operations
☐ File read
☐ File write

Rule applies to
☑ Hard drives
☐ Network drives
☐ Removable drives
☐ CD/DVD drives
☐ Driveless (VSS)
☑ Files
☐ Folders
☑ Servers
☑ Workstations

☐ Send e-mail on rule match
Send to:

☐ Only apply rule after a threshold has been reached.
Activate rule when the threshold of 20 matches within 60 minutes is reached.

Comment:

3. Name the rule by typing ‘Block programs from being written’ in the ‘Rule name’ area.

4. Add a file name filter. Click the ‘Add’ button in the ‘File name filters’ area.

5. Enter the filter of ‘*.exe; *.dll; *.ocx; *.scr; *.sys;*.wsh; *.lnk; *.bat; *.cmd’ indicating that this rule will only apply to files with those extensions. Normal users shouldn’t be writing any of these file types.[Note: this may not be a complete list of extensions to block, but as of this writing it’s a pretty good list]

6. Add a user name filter for all users. Click the ‘Add’ button in the ‘User name filters’ area.

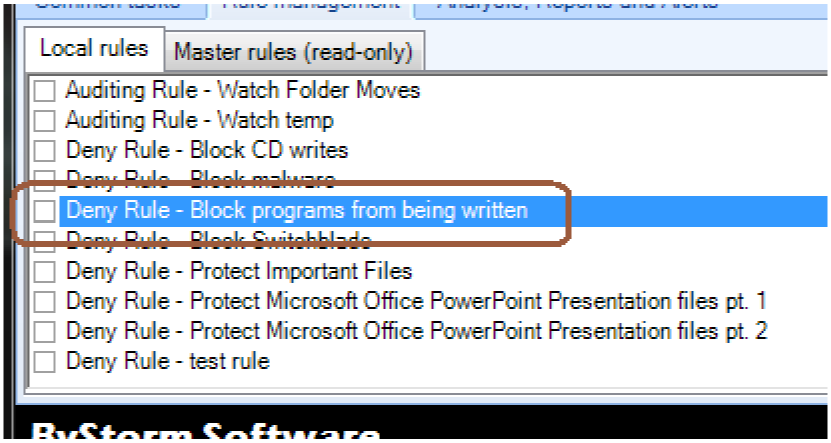
7. Enter the filter of ‘*’ for all users, make sure that the ‘Include matching Users in Filter’ is checked. [Note: you could exclude your user id here which would allow you to make changes, but no one else.] Click ‘OK’

8. Select the operations we want to block, which is ‘Write access’, ‘Delete access’, ‘Create’, and ‘Rename’. This means that no executables can be written, deleted, created or renamed while the rule is active.

9. On the ‘Options’ tab in the ‘Rule applies to’ area, ensure that ‘Hard drives’, ‘Files’, ‘Servers’ and ‘Workstations’ is checked.

10. Click ‘OK’ to close the dialog.

11. Find the new ‘Block programs from being written’ rule in the ‘Local rules’ list



☐ Auditing Rule - Watch Folder Moves
☐ Auditing Rule - Watch temp
☐ Deny Rule - Block CD writes
☐ Deny Rule - Block malware
☐ Deny Rule - Block programs from being written
☐ Deny Rule - Block Switchblade
☐ Deny Rule - Protect Important Files
☐ Deny Rule - Protect Microsoft Office PowerPoint Presentation files pt. 1
☐ Deny Rule - Protect Microsoft Office PowerPoint Presentation files pt. 2
☐ Deny Rule - test rule

12. Click the checkbox next to the rule and accept the ‘Please verify’ message.

13. Sit back and relax, your environment is safe from unwanted program changes and any new malware.