FileSure	How to prevent Administrators from ru	How to prevent Administrators from running the FileSure console	
ByStorm Software	www.bystorm.com	877-BYSTORM	

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.

<		Þ.
Common tasks Rule management Analysis, Reports and Alerts		
Local rules Master rules (read-only)	-	
Auditing Rule - Trial Rule for Local Machine - Audit Access to Microsoft Office Files	0	Quick audit
Auditing Rule - Watch a file	0	Audit access
Auditing Rule - watch exe writes and deletes	V	Audit access
🗌 Auditing Rule - Watch File Accesses 🔤	-	Block access
Auditing Rule - Watch Folder Moves		Diocit doctas
Auditing Rule - Watch temp		Event log monitoring
Deny Rule - Block CD writes		5 5
Deny Rule - Block malware	1	Edit Rule
Deny Rule - Block Switchblade		
Deny Rule - Protect Important Files	0	Delete rule
ByStorm Software		🛛 Close

- 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.

윩 Edit User Filter	
Please enter user name filter:	0
*\allengb	-
<ul> <li>Include matching Users in Filter</li> <li>Exclude Users in Filter</li> </ul>	V OK Cancel

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'

🂫 Add File Filter	
Please enter file or folder name filter:	6
C:\Program Files (x86)\ByStorm Software\FileSure\FileSure.exe	▼ Erowse
<ul> <li>Include matching Files in Filter</li> <li>Exclude Files in Filter</li> </ul>	✓ OK Cancel

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:

わ FileSure - Defend Rule	<b>×</b>
Block read access to the FileSure Console       File name filters       Unclude: C:\Program Files (x86)\ByStorm \$	Operations to Deny Select All
Exclude: *\allengb	Status changes
Image: Show matching users	Content operations
File size filters       Other         Options       Program name filters       Group name filters       Machine name filters       Time slot	filters Signature filters
Rule annlies to       Image: Send e-mail on rule match         Image: Hard drives       Image: Folders         Image: Network drives       Image: Folders         Image: Removable drives       Image: Folders         Image: CD/DVD drives       Image: Vorkstations         Image: Driveless (VSS)       Image: Vorkstations	n reached.
Comment:	OK Cancel

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

•	III		
Common tas	Rule management	Analysis, Reports and Ale	erts
Local rules	Master rules (read-only)		
Auditing F	ule - Watch Folder Moves ule - Watch Folder Moves ule - Watch temp e - Block CD writes e - Block malware	S	
Deny Rul	- Block read access to t	he FileSure Console	
Deny Rule - Protect Important Files     Deny Rule - Protect Microsoft Office Excel 97-2003 Worksheet files pt. 1     Deny Rule - Protect Microsoft Office Excel 97-2003 Worksheet files pt. 2			
ByStor	m Software		

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.

Administrator: cmd (running as bystormsoftware\frank)	
G:\Program Filos (x86)\ByStorm Software\FileSure>FileSure.exe Access is denied.	<u>^</u>
C:\Program Files (x86)\ByStorm Software\FileSure>	

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.

🐴 FileSure Defend			
<u>File Options Workst</u>	ations <u>H</u> elp		
Real-time monitor Ma	inaged machine status		
Current file activity for :	DUAL24	<ul> <li>Note: Selecting a c</li> </ul>	different machine will clear the file activity window. 🛛 🕕
Time Usernar	me Operation	File	
3/4 11:44 AM frank	Denied Opene	for Re C:\PROGRAM FILES (X86)\BY	STORM SOFTWARE\FILESURE\FILESURE.EXE
			4
Common tasks Rule n	management Analysis, Re	orts and Alerts	
Audit folde	ermoves	Audit access to files	Stop file theft
Catch those A	Accidental Folder 🧾 🦉	Who is reading patient data or customer lists?	Protect what is important while still allowing people to use it
	ort 🔽	Soarch auditloge	Sotup on a mail alort
Get File Activ	vity Reports	Find exactly what activity	Getan e-mail when something
delivered din	ectly to your inbox.	you're looking for.	important happens.
Lock file		Record user activity	Manage workstations
Protect a file	from any user 🥖	Got Disgruntled Employees?	Manage workstations throughout
D. CA			
Bystorm Soft	ware		Close Close