ByStorm Software

www.bystorm.com

877-BYSTORM

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:

FileSure Spo	of			
<u>File</u> Options	Workstations Help			
Current File Ac	tivity for : DUAL24	-	Note: Selecting a diffe	rent machine will clear the file activity window.
Time	Usemame	Operation	File	
•				•
Common Tasks	Rule Management Forensid	cs, Reports and Alerts		
🖉 Aud	it Folder Moves	Audit Acc	ess to Files	Stop File Theft
Catch Dragg	those Accidental Folder gers.	Who is reading customer lists	ng patient data or ?	Protect what is important while still allowing people to use it.
Run	a Report	Protect Fi	les	🔌 Set up an E-mail Alert
GetFi delive	ile Activity Reports ered directly to your inbox.	Stop unwant changes.	ed after-hour	Get an e-mail when something important happens.
Loc	k file	Record Us	ser Activity	Manage Workstations
Prote acces	ct a file from any user ss,	GotDisgrunt	ed Employees?	Manage workstations throughout your enterprise.
ByStorm	Software			S Close

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.

🏡 FileSure - Defend Rule		
Pute name:		operations to Deny
Block Remote Access		Ueselect All
File name titlets Include: * Include:	ne filters ×	Access checks Read access Write access Delete access
		Status changes Create Delete Rename Security Changes
Add Edit Remove	Edit Remove Show matching users	Content operations File read File write
Options Time slot filters Program name filters	Group name filters 🦳 Signature fil	ilters Size filters Other
Rule applies to Bulk op Image: Hard drives Image: Files Image: Network drives Image: Folders Image: Removable drives Image: Servers Image: CD/DVD drives Image: Workstations Image: Driveless (VSS) Image: Servers	apply rule after a threshold has be ivate rule when the threshold of 20 matches with 60 minutes is re	een reached. thin eached.
Comment:		✓ OK 🛛 Cancel

- 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.

🏠 Add File Filter	
Please enter file or folder name filter:	6
 Include matching Files in Filter Exclude Files in Filter 	✓ Browse✓ OK✓ Cancel

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.
 - Click on the 'Program Name Filters' tab

Click the 'Add' button

vii.

Program Name Filters	Group Name Filters	Signature Filters	Si
		Add)

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.]

わ Add Program Filter	
Please enter program name filter:	6
Remote Access	•
 Include matching Programs in Filter Exclude Programs in Filter 	✓ OK Sancel

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.

Options	Time Slot Filters	Program Name
Rule Ap	plies to d drives work drives novable drives DVD drives eless (VSS)	Files Foldon Servers Workstations
Comment:		

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.

💦 FileSure - Defend Rule	
Rule Name: Block remote accesses	Operations to Deny Deselect All
File Name Filters Include: * Include: *	Access checks ▼ Read access ▼ Write access ▼ Delete access ▼ Create ▼ Delete ▼ Rename ① ▼ Allow non-type renames ▼ Security Changes Content operations ▼ File Read ▼ File Write
Options Time Slot Filters Program Name Filters Group Name Filters Signature Fi	Iters Size Filters Other
Include: Remote Access Ad Ad Ed Rem	d lit ove
Comment:	OK Cancel

Step 4: Activate the rule

Click on the ne	wly created rule to active it.	
1/5 11:50 AM	BISTORMSOFTWARE allenge Den	
1/0 11.06 AM	BTSTURMISUPTWARE vallenge Den	
•		
Common Task	s Rule Management Forensics, Rep	
Local Rules	Master Rules (Read-Only)	
🗌 Auditing Ru	le - Copy of Watch File Accesses	
Auditing Building Building Building	de Trial Pule for Local Machine - Audit Ar	
L 🔄 Auditing Ru	ule - Watch File Accesses	
Deny Rule	- Block remote accesses	
Deny Rule	- Lock File	
P		
ByStorm Software		

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.)

🏠 Add User Filter	
Please enter user name filter:	6
	•
 Include matching Users in Filter Exclude Users in Filter 	V OK Cancel

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.)

🏠 Add File Filter	
Please enter file or folder name filter:	6
C:\Users*	- Browse
 Include matching Files in Filter C Exclude Files in Filter 	✓ OK 🛛 Cancel

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.

わ FileSure - Defend Rule		_	
Rule Name: Block remote accesses			Operations to Deny Deselect All
, File Name Filters	User Name	Filters	Access checks
Include: *	Include: *		✓ Read access ✓ Write access ✓ Delete access
			Status changes ✓ Create ✓ Delete ✓ Rename ✓ Allow non-type renames
Add Edit	Remove	Edit Remove	Content operations
Options Time Slot Filter	Hogram Name Filters G	iroup Name Filters Signatur	e Fitters Size Filters Other
Sunday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday 120M	40M 80M	12PM 4PM	8PM 20M
Comment:			OK Cancel

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.)

わ Edit File Filter	
Please enter file or folder name filter:	6
*xls; *.doc; *.ppt; *.vsd; *xlsx; *.docx; *.pptx; *.vsdx	👻 📴 Browse
 Include matching Files in Filter Exclude Files in Filter 	✓ OK Sancel

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.