The communication architecture between FileSure Server and FileSure workstations is a master/slave model. The FileSure server is the master and the workstations are the slaves. You define rules, alerts, jobs, etc. on the server and the workstations PULL them down every 20 minutes. The workstation also PUSHES its data logs to the server every 20 minutes. To deploy in a connected environment, you would just click on the “Workstations” menu in FileSure, and then click “Manage.” It will walk you through deploying FileSure to your workstations from the central location.

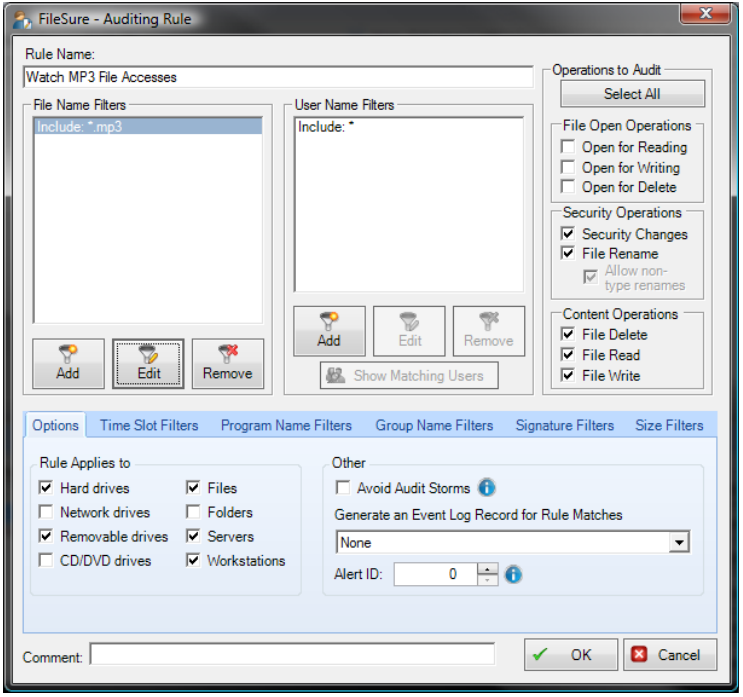
However, this architecture also allows the workstation to be disconnected from the server and continue to work correctly. If the workstation is unable to connect to the server to get any rule updates, it will just continue to use the current rules and try to connect again in a few minutes.

The same thing is true of log files; if the workstation is unable to push the logs to the server, it will continue to record activity just like normal and try again in a few minutes.

If your environment is disconnected but you need to deploy FileSure to a workstation, here is how to do it.

Step 1: Install the server version of FileSure on a computer.
You will use this computer to define the rules that should be applied to the workstations.

Step 2: Define the rules that you want.
Here is a screen shot of a sample rule to record activity on MP3 files anywhere on the computer.   When this rule is applied to a workstation, any accesses to an MP3 will be recorded by FileSure and stored in the data store.



Rule Name: Watch MP3 File Accesses

File Name Filters: Include: *.mp3

User Name Filters: Include: *

Operations to Audit

File Open Operations
- ☐ Open for Reading
- ☐ Open for Writing
- ☐ Open for Delete

Security Operations
- ☑ Security Changes
- ☑ File Rename
- ☑ Allow non-type renames

Content Operations
- ☑ File Delete
- ☑ File Read
- ☑ File Write

Rule Applies to
- ☑ Hard drives
- ☐ Network drives
- ☑ Removable drives
- ☐ CD/DVD drives
- ☑ Files
- ☐ Folders
- ☑ Servers
- ☑ Workstations

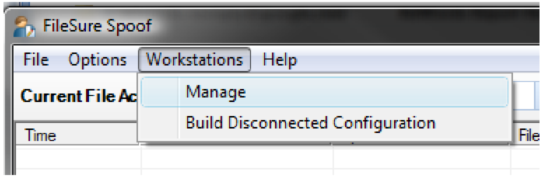
Other
- ☐ Avoid Audit Storms

Generate an Event Log Record for Rule Matches: None

Alert ID: 0

Comment:

Step 3: Build the disconnected configuration.
Under the workstations menu option, there are two choices: ‘Manage’ and ‘Build Disconnected Configuration’.



Typically, the ‘Build Disconnected Configuration’ option is used for workstations that will never be connected to the network, but it gives us a good starting point for picking up all the interesting configuration settings; so select the disconnected option and save the configuration to a file like ‘FileSureConfig.reg.’

Step 3a. Make custom configuration changes.
In a connected environment, FileSure Workstation pushes the audit logs to the master server for processing, but in a disconnected environment this isn’t possible, so when you build a disconnected configuration the domain credentials aren’t included. So we’ll need to add them by hand.

The easiest way is to export the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\ ByStorm Software\FileSure, and then copy the following lines from the exported file to the saved configuration file:

“DomainName"
"Password"
"UserName"

[Note: these fields are encrypted so they will look like: "UserName"="247343550B294BB3"]

Step 4: Install the configuration file and FileSure WorkStation on the workstation.
In the FileSure program folder (typically, C:\Program Files\ByStorm Software\FileSure) there is a file called ‘FileSureEP.MSI’. This is the installation program for FileSure Workstation.

Copy the disconnected configuration file (saved in step 3) and FileSureEP.MSI to the workstation.
Double click on the disconnected configuration file (‘FileSureConfig.reg’) to install the configuration on the workstation.
Double click on the FileSureEP installation package (FileSureEP.MSI) to install the workstation version of FileSure.

Step 5: All done
At this point the workstation is running FileSure enforcing the rules that you defined in Step 2 and saved in Step 3.