Network-attached storage appliances are great things; offering an easy way to expand or consolidate your file servers onto a stand-alone device that just plugs into your network.

But how do you audit or secure it?

NAS appliances run streamlined operating systems and for the most part, implement Microsoft Windows-styled (NTFS) auditing and security systems. On NAS devices based on Windows Storage Server, the underlying file system actually is NTFS; but on UNIX-based NAS devices, they usually emulate NTFS.

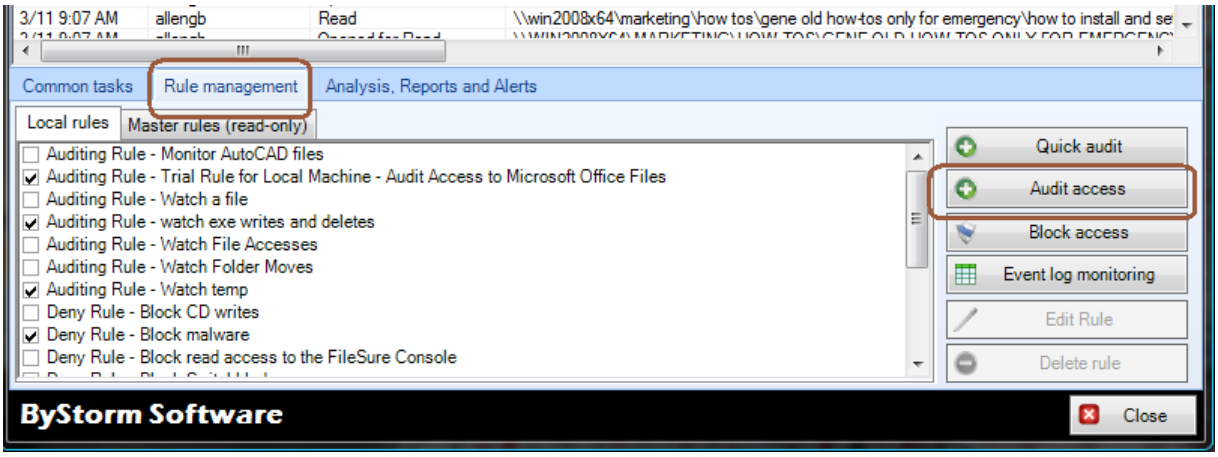
On Windows-based NAS appliances, you can install FileSure directly on the NAS and make use of all its features.

On UNIX-based NAS devices (e.g. NetApp Filer), FileSure can't be installed directly on the server and your only option for server-based file auditing and security is to rely on the emulated NTFS access control list model…which is troublesome at best.

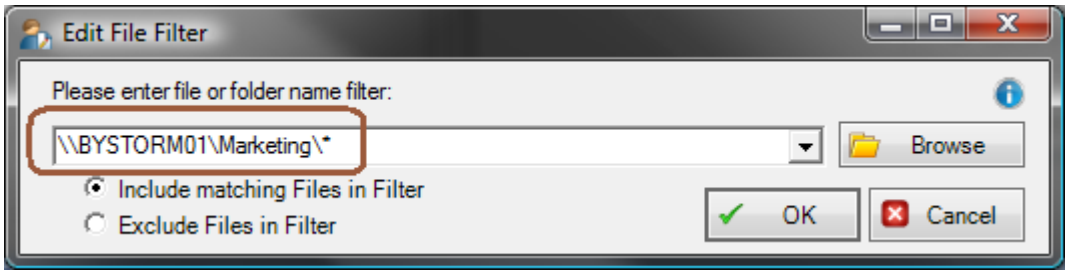
But, there is a way to benefit from the power of FileSure with your UNIX-based NAS and that's by using **FileSure for Workstations** instead. FileSure can handle file operations when they occur **on** the machine where FileSure is installed and file operations made **from** the machine where FileSure is installed.

In this 'How-to', I'm going to show you to audit a Network-attached storage appliance using FileSure for Workstations.

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

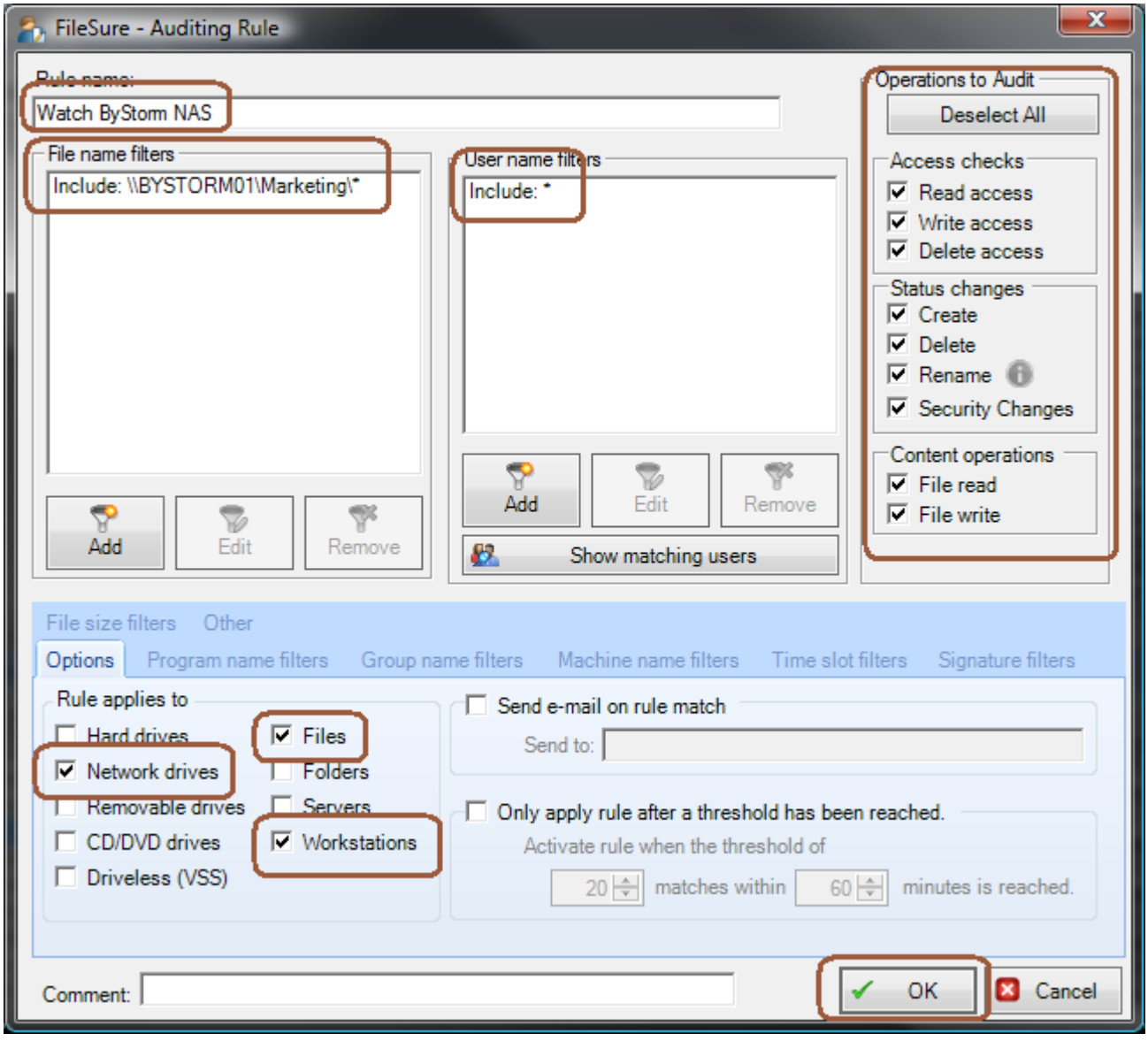


2. On the Auditing rule screen, make the following changes (see figure next page):
   a. For the 'Rule name' enter 'Watch NAS'
   b. Under 'Operations to Audit' click the 'Select All' button.
   c. In the 'User name filters' section, click the 'Add' and add an include filter of '*' to cover all users
   d. In the 'File name filters' section, click the 'Add' button and enter the UNC path to the NAS share you want to audit. [Note: you have to use a UNC since mapped drives can be different for each user.]

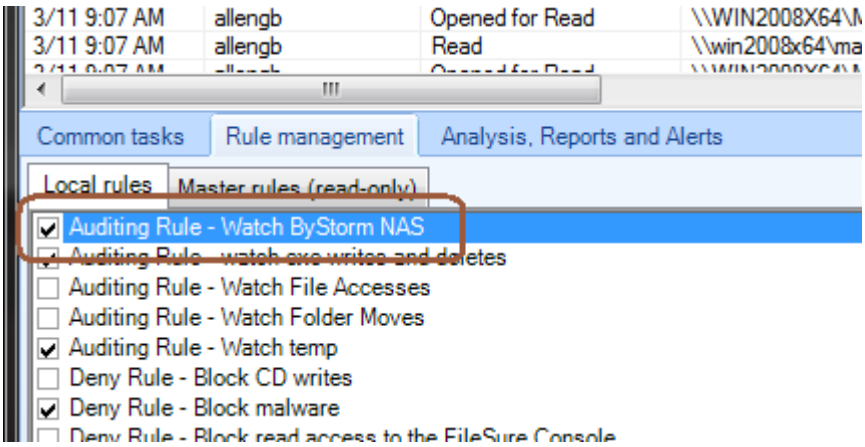


e. In the 'Rule applies to' area, uncheck everything except 'Network drives', 'Files' and 'Workstations'.

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

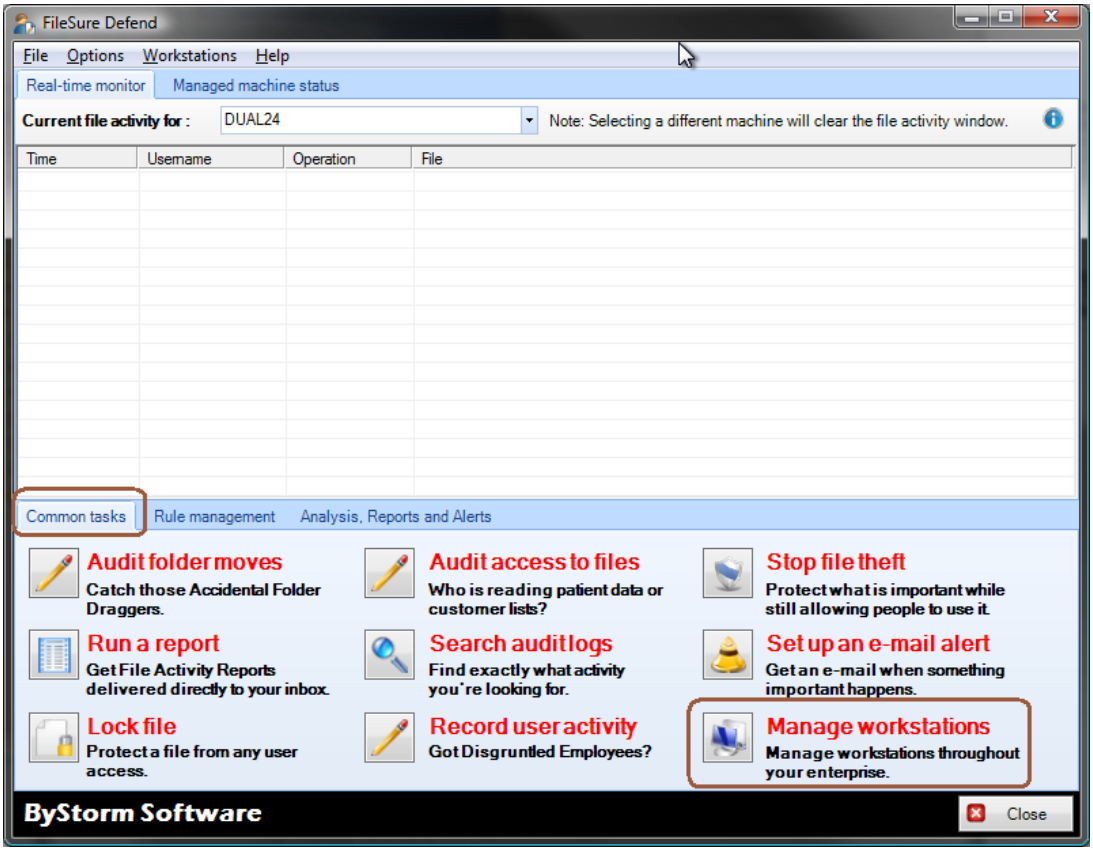


3. Click ‘OK’ to close the rule screen and find the newly created rule and click the checkbox to turn it on.

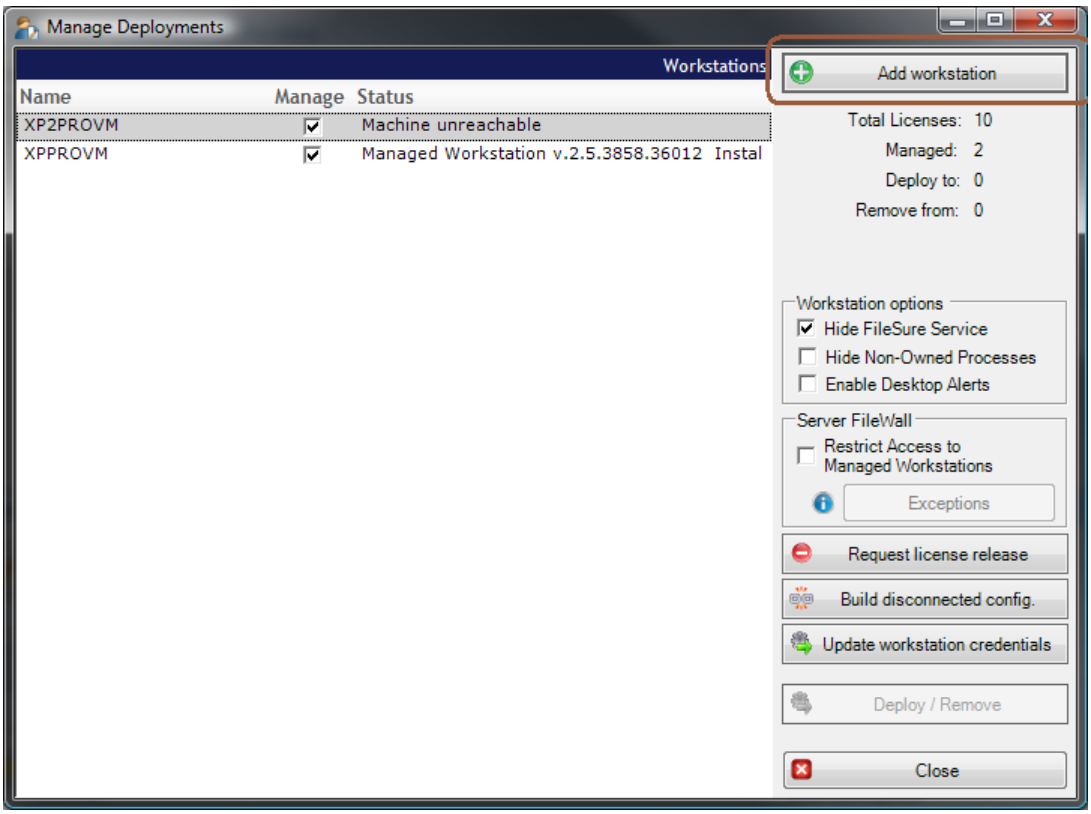


Now we have a workstation rule defined to watch all files on the Marketing share on our NAS (\\ByStorm01\Marketing), but we need to deploy FileSure to the workstations that access that share.

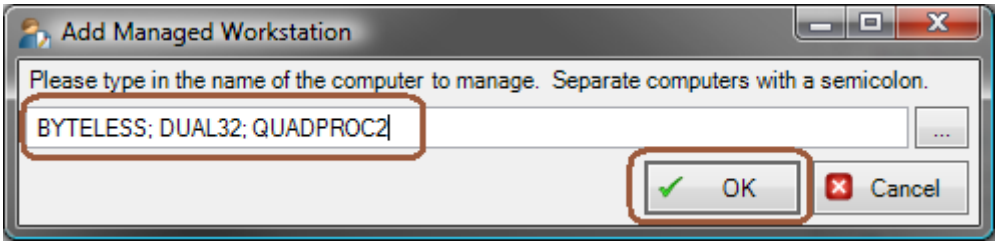
4. On the main console screen, select the ‘Common tasks’ and click the ‘Manage workstations’ button.



5. This will bring up the ‘Manage Deployments’ screen, click ‘Add workstations.’



6. This will bring up the ‘Add Managed Workstation’ screen. On this screen enter the workstations you want to monitor and click OK.



7. Click the ‘Deploy/Remove’ to install FileSure for Workstation on the workstations you have listed.

The managed workstations will pull their rules, configuration and summaries from the server and push their back logs to the server so they can be used for searching, researching or reporting. All activity from that NAS will be monitored.