User Guide

March, 2010

Contents

Chapter 1
Introduction **1**
What Is FileSure? 2
FileSure for Auditing 3
FileSure Workstation 3
FileSure Defend 3
Key Features of FileSure 3
How FileSure Helps You 5
Workstation Support 5
Comprehensive Regulatory Compliance and IP Protection 5
Data Loss Prevention 5
Integration 6
New in this Version of FileSure 6

Chapter 2
Installing and Starting FileSure **9**
Requirements 9
Installing FileSure 10
Starting FileSure 11

Chapter 3
Using FileSure **13**
Understanding the Rules Model 13
FileSure Product Family Options 14
Seeing Rules in Action Immediately 14
Common Tasks 15
Adding Custom Rules 15
Quick Audit Interface 15
Audit Access (or Block Access) Interface 16
Event Log Monitoring Interface 16
Enabling, Editing or Deleting Rules 17
Designing Targeted Rules Using Filters 18
File and Folder Name Filters 18
User and Group Name Filters 19
Operations to Audit (or Block) 19
Options Tab (Audit/Block Access Rule Creation Window) 21
Time Slot Filters 21
Program Name Filters 21
Group Name Filters 22
Signature Filters 22
Size Filters 22

"Other" Tab....23
Real-Time Monitoring and Notification Options....24
Event Log and Syslog....24
FileSure E-mail Alerts....24
Accessing and Using the File Activity Information....28
Using the View Data Interface....29
Using the Search for Trends Interface....30
Using the Reports Window....30
Using the Web Console....31
Working with Audit Data Log Files....33
Customizing FileSure....35
Managing Workstations with FileSure....36

Chapter 4
Windows and Features Detailed **37**
Navigating the Main Console....37
Common Tasks Tab....38
Rule Management Tab....39
Quick Audit Button and Interface....40
Audit Access Button and Interface....41
Block Access Button....47
Event Log Monitoring Button....48
Edit Rule Button....50
Delete Rule Button....50
Analysis, Reports and Alerts Tab....50
Analysis Tab / View Data Button....51
Analysis Tab / Search for Data Button....54
Reports / Reports Button....56
Reports / Scheduled Reports Button....58
Alerts....61
Summaries (found within the Alerts interface)....64
Options Menu→The Configure Interface....66
Network Options Tab....66
Console Options Tab....66
Service Options Tab....67
Security Tab....69
Pull Rules/Push Data Tab....70
Publish Tab....70
Workstations Menu→The Manage Interface....71
Add Workstation Button....71
Workstation Process Protection....72
Server FileWall®....72
Deploy/Remove Button....73

Chapter 1
Introduction

Track files, keep them safe, prove they're safe, do it simply.

FileSure audits and reports targeted file accesses *and stops unauthorized accesses before they happen*.

FileSure is more secure than signature-based security *which can be outwitted by encryption or out-maneuvered by secure FTP*.

FileSure blocks file copies to USB drives *and protects against loss via webmail, IM, secure FTP, and more*.

FileSure is installed and working in under 5 minutes with a proprietary, alter-proof database. *No consultants, external databases, or steep learning curves.*

Get you compliant, stop any loss, never stop your employees' work:

Use it for simplified compliance with HIPAA, Sarbanes-Oxley, and more.

Use threshold alerts to be notified of suspicious behavior as it occurs.

Deploy FileSure on workstations as well as servers and regulate all file activity centrally.

Allow broad access to files but disable the ability to copy, move, or delete files.

Or, just lock down file access completely by criteria you choose.

FileSure is NOT:

An expensive, complex solution requiring hardware and storage requirements.

A solution based on comparing snapshots of sensitive files.

A solution that ignores internal threats to IP—employees who can read, change, rename, and delete sensitive files.

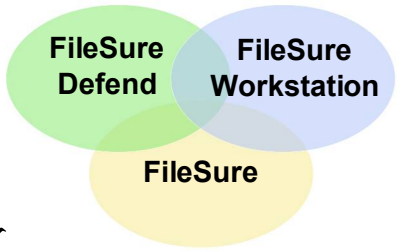
A solution reliant upon Windows Auditing.

Just a solution for auditing, just a solution for blocking pen drives, or just a solution for data loss prevention.

No other product offers our noise-free auditing and reporting or our patent-pending security technology—let alone both together in one solution: FileSure.

What Is FileSure?

The FileSure solution—three products in one, just add on what you need:



You need a solution that will . . .

Install safety protocols fast with no external database or lengthy learning curve

Allow access to files but block the ability to steal them

Stop data loss via pen drives or from employee laptops

Loss Prevention

Full system protection from data removal via secure ftp transfers, email and more

Endpoint Security

Integrated workstation protection from file loss or theft via external drives

Centralized Control of Security

FileSure

Easily Scalable

Audit Workstations, Too

Auditing

Targeted auditing and reporting of all file access and usage for regulatory compliance

Have one solution for auditing and loss prevention

Monitor file use on laptops / workstations

Quickly print a report proving HIPAA *compliance*

Find misplaced files and folders fast

Alert me when someone accidentally deletes a lot of files

All this at less cost than the competitors . . . and so unbelievably easy to use.

FileSure for Auditing

The FileSure product audits file read, write, create, delete, deny, rename, and security setting change activities by user, and then records important details about the activities of interest. The product works by capturing every file operation as it occurs and applying rules to determine which operations should be audited.

The powerful rules model gives you the flexibility to closely audit specific activity types, files, and user accounts. You define rules and combine criteria to audit exactly what you need. FileSure also helps you eliminate noise, such as event storms caused by virus scanners and backup products.

FileSure Workstation

FileSure can be run just on your servers—or for seamless protection can be deployed onto your users' machines with **FileSure Workstation**. Rules you design are centrally managed and pulled onto users' machines; their audit data is pushed back for your central viewing and reporting. FileSure works even when workstations are disconnected from the server.

FileSure Defend

Building on this targeted and responsive rules model, **FileSure Defend** allows you to create very selective rules which stop unwanted file access or theft activities.

Combined with FileSure Workstation, you can get protection from file copies all the way down to a pen drive on a workstation. You can also allow full access to files but block the ability to remove them in any way.

FileSure Defend and **FileSure Workstation** are built upon the core FileSure auditing product. They may be purchased from the start or as upgrades.

Key Features of FileSure

Software and Usage Features

- Easy and fast installation with no external database requirement
- Encrypted and compressed audit logs to ensure data integrity and ease of use
- Does not rely on Windows Auditing
- Lightweight solution that uses few system resources
- Easy integration into existing server backup solutions
- Integration with system monitoring tools through the Windows Event Log and Syslog
- Console security for limited access to program configuration and settings

- The ability to block the FileSure service from being stopped by any user
- Service availability assurance through low-impact heartbeat
- Central control and storage through a master server location for multi-server environments or for workstation deployment

Auditing and Compliance Features

- Simple, powerful, and flexible rules-based model
- Real-time file activity monitoring
- Comprehensive file auditing, including reads, writes, creates, deletes, renames, security setting changes and denies
- Targeted filters let you pinpoint activity by things like domain group membership, time of day, program accessing the file, usage behavior, thresholds, and much, much more.
- Instant or recurring reports delivered to your inbox and saved at a central location
- Saves desired Windows event log entries with the secure data store
- Support for exporting audited data to .CSV, XML, HTML, Microsoft Excel, and Microsoft Access
- Automated publishing of auditing data to Microsoft Access if you desire for easy external application integration (like our web console).
- Comprehensive logging of any FileSure rule changes in the Event Log, Syslog and Data store.
- IT compliance for various regulations, such as PCI, SOX, HIPAA, and GLBA
- Audits workstations as well as servers, still runs even when disconnected from servers.
- Can audit on non-Windows NAS.
- Complimentary Web console add-on that allows others access to audit data directly from their workstations if you choose

Security and Data Loss Prevention Features

- Threshold-based e-mail alerts to activities you flag
- Ground-breaking “Search for Trends” interface lets you find security issues you weren’t looking for
- Locks down file access by type of access: reads, writes, creates, deletes, renames, security setting changes, etc.
- Targeted filters let you choose who can access what by things like user, domain group membership, time of day, program accessing the file, usage behavior, thresholds, and much, much more.

- Allows normal use of files, but blocks the ability to remove or copy them in any way
- Blocks file access on workstations as well as servers, even when they are disconnected from the server
- Stops copies to external drives, CD/DVDs, webmail, secure FTP, and much more

How FileSure Helps You

Workstation Support

FileSure has the availability to deploy onto users' workstations. This makes a seamless and simple auditing and security solution with centralized management. View real-time file activity on any managed machine from your desk, stop unwanted file copies, easily find lost files and folders, and much, much more.

Comprehensive Regulatory Compliance and IP Protection

FileSure was designed especially for compliance and will quickly help you with many regulatory standards (PCI, Sarbanes-Oxley, HIPAA, GLBA, etc.).

- You may audit any sort of operations on any files or folders, including reads and denies, and see who has done the operations and when.
- You may audit for certain types of operations, such as abnormal access patterns—alerting you to bulk transfers, for example.
- You may save specific Windows event log entries into the data store, allowing capture of logons and logoffs, and remote control events indicating what computer is doing the remote control.
- You may audit file use on workstations and laptops as well, from a central location (requires FileSure Workstation).
- You can prove compliance with fast and simple reports.
- You may be alerted to activities you have flagged, real-time.
- You can trust FileSure's proprietary, encrypted and tamper-proof datastore
- You only have to see what you want, not all the clutter.

Data Loss Prevention

When you apply the ability to block file access (FileSure Defend) to the already powerful auditing model, you have a very specific and powerful weapon against all kinds of IP loss and theft.

- You may allow access to files, but block the ability to steal them.
- You may block access to certain files, file types, or folders for certain users.
- You may block data loss from pen drives or employee laptops (requires FileSure Workstation).
- You may lock down sensitive files completely.

Integration

If you decide not to use FileSure's powerful built-in threshold alerting, you can integrate FileSure with event monitoring products, such as Microsoft Operations Manager, Kiwi SysLog. When a file operation passes the rule model, FileSure can generate an event log or syslog entry with the important information. This event can then be captured by the event monitoring product and passed into your existing system monitoring processes.

FileSure also allows you to automatically publish information to a Microsoft Access database if you choose. This publish feature provides a powerful mechanism for integrating with various IT systems you already have in place. With this integration, you get a comprehensive solution that works with your existing systems and processes. Publishing the data logs allows safe and targeted access to the information by any other authorized staff members so they might answer their own questions about "what files has Sam accessed," or "who was the last person to view budget.xls."

New in this Version of FileSure

New in this version of FileSure is yet another way of accessing and using the activity data you've gathered. In the previous version we added multi-faceted data drill-down, recurring e-mailed reports, and e-mailed alerts to real-time activities you designated.

In 2.5, we present the **Search for Trends interface**.

Truly groundbreaking, the **Search for Trends** section of FileSure 2.5 allows you to ***find problems you didn't know to look for.*** Essentially organized to present data by "counts" of file or folder operations, this research function lets you see usage trends by user—and then filter by time, file type, the program accessing the files, and much, much more. The result? You find abnormalities you wouldn't have otherwise seen. And since the data is all there and available, once you find that abnormality it is just a double-click to drill down and pinpoint the exact details of time, machine name and more.

Also new in this version:

- A quick wizard that easily allows a file to be locked down from all access
- The ability to block the FileSure service from being stopped by any user
- A web proxy feature for auditing/protecting environments using a web proxy server

- The ability to include workstation log data when publishing to Access database
- The ability to capture windows event log entries and store them with the FileSure data store
- The ability to monitor when files are created as well as opened or read, etc
- The choice of the “driveless” drive type to the drive filters (VSS)
- The ability to not only choose which file extensions you want to block renames “from,” but to also choose not to have any files renamed “to” certain file types.

Chapter 2
Installing and Starting FileSure

This section guides you through the installation process. Review the requirements and then install the product.

Requirements

The following table summarizes the minimum requirements—for both servers and workstations running FileSure.

Category	Minimum Requirement
Memory	512 MB
Hard disk	1 GB
Operating system	One of the following operating systems and service packs (32 and 64 bit): • Windows 2000 SP4 Rollup 1 or later • Windows XP SP2 or later • Windows 2003 SP1 or later • Windows 2008 • Windows Vista • Windows 7
Supporting software	Microsoft .NET Framework 2.0 or later

For FileSure Workstation—To use the Server FileWall® there is an OS requirement of Windows Server 2008, Windows 7, or Vista

Installing FileSure

Install FileSure on each server you want to audit. Make sure each managed server meets the minimum requirements summarized in the previous section. Note that if this is a trial, you can also install FileSure on your local machine and explore most functionality. For FileSure Workstation, you will deploy to slave workstations from a master server.

To install FileSure:

1. Log on as an administrator on the server.
2. Run the `FileSure.exe` file.
3. Follow the instructions until you have finished installing the product.

The installation program installs the product and starts monitoring file activity. This activity is monitored with and without the user interface open. The installation program also creates the following shortcuts in the ByStorm Software program group on your Start menu:

FileSure
Starts the FileSure user interface. This user interface allows you to create rules, configure the product, and view file activity.

FileSure User Companion
Only for use if you have a Technical Support issue. This product collects information and communicates with ByStorm Technical Support staff, helping them diagnose any issues that you may experience.

FileSure User Guide

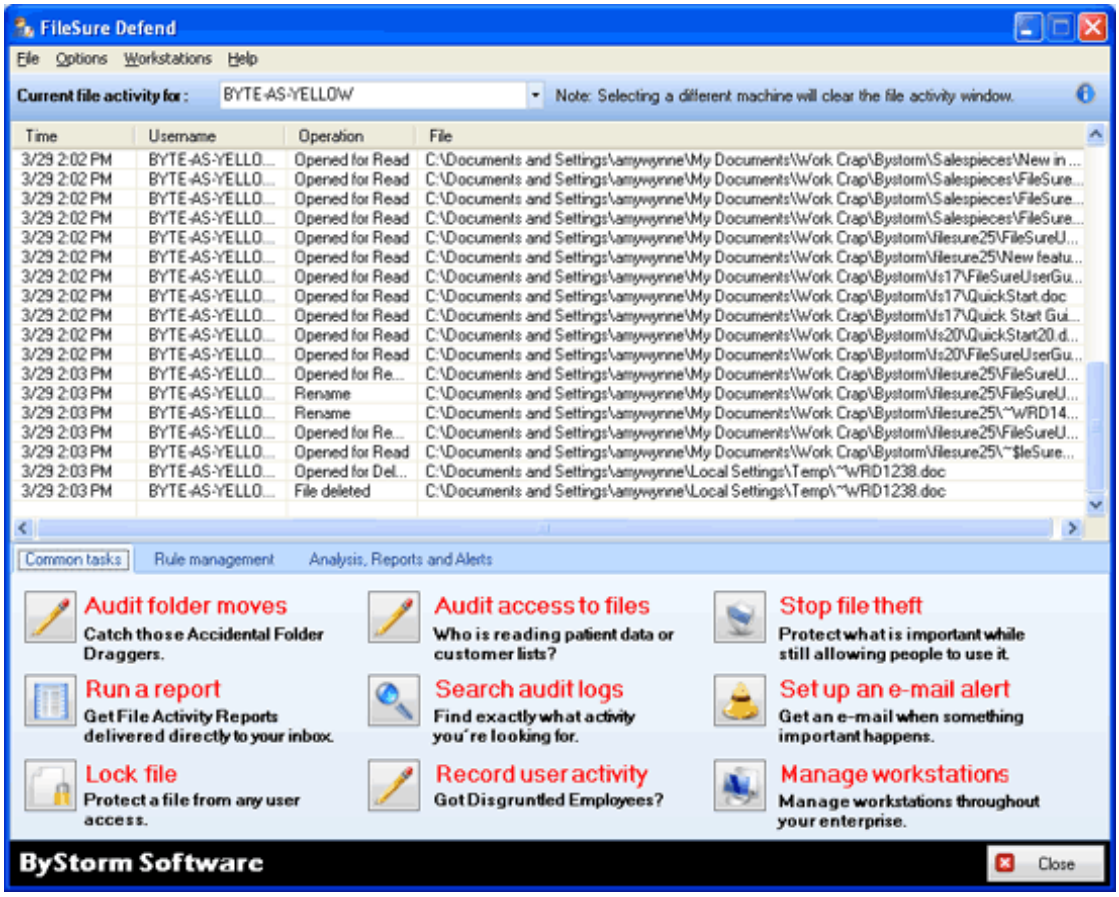
User documentation.

FileSure QuickStart

QuickStart guide for FileSure.

Starting FileSure

To start the product user interface, click **FileSure** in the **ByStorm Software** program group of your Start Menu. A window similar to the following figure will appear.



Chapter 3
Using FileSure

This section outlines the overall process for using the product. Chapter 4 shows and describes the different interfaces you will encounter.

Note
To follow a QuickStart program instead—look under Help→ QuickStart on the FileSure product for an easy start guide.

Understanding the Rules Model

On the bottom of the Main Console Window you'll find common tasks you can perform with FileSure. You'll also find a tab for creating and managing the rules that make FileSure work, and a tab for Analysis, Reports, and Alerts. Before describing how to set up FileSure to achieve your goals, it is important to understand the overall rules model that powers FileSure.

FileSure's powerful rules model allows you to define exactly which files, folders, and devices to monitor. You can also define which user accounts to monitor, which helps you reduce auditing noise and focus on specific activity. You can further filter accesses by time of day, program running the file, size of files, file signatures, and much more. Configuration options allow you to further define duplicate activity and consolidate that activity.

Note

It can be tempting to audit activity on all files and folders for all user accounts. However, this type of auditing will capture thousands of file accesses every hour that are useless—which inflates audit log size, hides the risky activity you need to capture, and, depending on the volume, could result in FileSure affecting runtime performance of your server. To avoid this, you'll use simple "include" and "exclude" filters.

For example, you might include only your critical files and folders, and then exclude user accounts for automated services, such as virus scanners and backup products. You want to audit people, not services. To further reduce noise, you would leave audit storm protection on and focus on specific risky operations. For more on this, see the section on Defining Targeted Rules Using Filters on page 14.

FileSure Product Family Options

All FileSure add-on products (Defend, Workstation) operate using this same core rules model. This user guide focuses largely on the original FileSure product, because if you understand how to make and manage auditing rules, you will subsequently understand how to make rules which restrict file access, and know how to use rules on Workstations as well as servers.

When this rules model is modified to *restrict* file access, you have a powerful and flexible security tool. That is **FileSure Defend**. **FileSure Workstation** allows you to deploy FileSure with rules you have created onto all Workstations and manage your auditing and protection activities locally from a master server.

Seeing Rules in Action Immediately

Once you start the program, FileSure is already monitoring file activity and storing log data based on one, preinstalled sample rule. The sample rule records activity for MS Office Documents. FileSure will immediately begin to store and display file access information that matches the rule criteria.

You can see this rule on the Rules Management Tab in the Local Rules screen. The sample rule is called "Trial Rule for Local Machine - Audit Access to Microsoft Office Files." By highlighting the rule and selecting **Edit** you can see the filter choices that make this rule work. You can also disable the rule by unselecting the checkbox next to its name.

You can keep a list of many rules—and activate or deactivate them as you choose. ***FileSure will only return matching data (or restrict access, etc) when a rule is turned on.***

Common Tasks

To begin building rules that achieve your security goals, check the Common Tasks Tab on the main console. You may be able to quickly set up the rule you need through a scenario-based wizard. Five of the tasks can be performed with the core version of FileSure, "Audit Folder Moves," "Audit Access to Files," "Record User Activity," "Run a Report," and "Set Up an E-mail Alert." The program will prompt you to enter network information for the user activity task.

The remaining tasks configure rules using FileSure Defend or FileSure Workstation.

To Use a Common Task:

1. Click the task description that most closely resembles what you need to accomplish
2. Follow the wizard directions. For interfaces with pick lists, you may use shift or control to choose more than one item.
3. The wizard will automatically close and show you your new rule listed in the Local Rules screen—already activated and working. You may highlight the name of your rule and click **Edit Rule** to view or change the rule configuration details.

Adding Custom Rules

All custom rule creation is found on the "Rule management" tab. Here you make rules telling FileSure to audit file use, restrict file use (FileSure Defend), and monitor specific event log items.

You have two choices when adding a new auditing rule: Quick Audit or Audit Access. Quick Audit allows you to make a simple auditing rule based on the type of file or files you want "watched" and their location. The rule will default to recording most types of file access activities by all.

The Audit Access button allows you to define the full range of rule characteristics such as which specific file operations to record, which users or groups to target with this rule, and more. There is no Quick Block option, because when you are denying access you need to pay close attention to your filters.

Note
Regardless how you create any rule, you can access and configure the rule with the full range of functionality through the Edit Rule interface. Thus, Quick Audit rules are not limited in functionality in the long term.

Quick Audit Interface

Adding a rule through the Quick Audit interface is simple and fast.

To add a new rule:

1. On the Rule Management Tab, click **Quick Audit**. Give your new rule a name.
2. Specify what files you want watched, either by the file type (extension) or the file name characteristics (begins with, ends with). Clicking any "i" will give you filtering examples.
3. Choose the location of the files you want to monitor.
4. Click OK. You will see the rule you have defined in the Local Rules list—and it will already be activated and monitoring matching file activities. Quick Audit is only available for Auditing Rules, not to block access.

Audit Access (or Block Access) Interface

Adding a rule by clicking on **Audit Access** or **Block Access** allows you to control all filtering options related to that specific rule. ***Block Access will only be enabled if you have purchased FileSure Defend.***

To add a new rule:

1. On the Rule Management Tab, click **Audit Access/Block Access**. Give your new rule a name.
2. Define your filters. You can filter by files, users, groups, types of file operations to monitor, location of activities, time of day, program accessing the file, file signatures, file size and even the behavior of the users (audit storms). For details on how to plan and activate the rules you need, please see Designing Targeted Rules Using Filters on page 14.
3. Choose whether or not to have the matches from this rule written to the Windows Event Log. You may also create an Alert ID to be written to the audit log upon any rule matches. You could then create an alert for FileSure to email you upon x number of incidences of that Alert ID in the Audit log. For more information on either of these choices, see Real Time Monitoring Options on page 20.
4. Write a comment describing your rule.
5. Click OK. You will see the rule you have defined in the Local Rules list. *You will need to choose to activate the rule by checking the checkbox next to it.*

Event Log Monitoring Interface

Event log monitoring allows you to define certain events you want captured and stored in the audit logs with your other file activity. Instead of several rules, event log monitoring is essentially either on or off, and there is a list of events you want noted by FileSure. You will always access Event log monitoring settings through the main button.

To use Event Log Monitoring:

1. On the Rule Management Tab, click **Event log monitoring**.

2. Click the box to enable event log monitoring.
3. Define your criteria for choosing events to record. You may choose Application, Security, or System in the first column, and type directly into remaining fields using standard FileSure wildcard naming conventions, event log IDs, etc.
4. You may also select events directly from the Event log via the **Select from Event Log** button at the bottom of the interface.

Enabling, Editing or Deleting Rules

Once you create a rule, its name will be listed in the Local Rules Section on your Main Console Window. You choose to enable or disable rules by merely clicking on the box next to the rule name. Rules take effect the moment they are enabled.

To edit a rule, you would select the rule (whether it is enabled or not) and then choose the **Edit Rule** button. This will give you the **Audit/Block Access Rule** window interface, so you can both see the current rule parameters and change them.

To delete a rule, you would select the rule (whether it is enabled or not) and then choose the **Delete Rule** button.

Rules appearing to users in the Master Rules Section are not available for enabling, editing, or deleting except at the master server where they were created.

Note
You will not see a "rule" in the rules screen for Event Log Monitoring. You can edit your choices directly from the Event Log Monitoring button.

Designing Targeted Rules Using Filters

The filter functions allow you to design rules that pinpoint exactly the information you need—and eliminate distracting auditing noise. The sections below take an in-depth look at how to use these filters to your best advantage.

File and Folder Name Filters

File name filters allow you to audit your sensitive files and folders without collecting unimportant data and noise. These filters also reduce any performance impact associated with auditing activities. For example, you can exclude activity on operating system files, `.exe` files, `.dll` files, and temporary files. You can also exclude activity by users on the files in their own home directories.

You can use wildcard characters in file and folder names. An asterisk (`*`) matches zero or more characters. A question mark (`?`) matches any single character. The following table identifies several example filters and what they match.

Filter	Matches	Does Not Match
`*`	All files and folders, regardless of their name	
`*\*.doc`	All `.doc` files on any drive and in any directory on the server	`IT.dot`
`*\T*.xls`	All `.xls` files whose name starts with the letter `T` on any drive and in any directory on the server	`IT.xls`
`C:\*\???.xls`	All `.xls` files whose name without the file extension has 3 characters on the C: drive, such as `C:\Test\SOX.xls`	`IT.xls` `D:\SOX.xls`
`*\H*`	All files and folders whose name starts with the letter H on any drive and in any directory on the server, such as `D:\Test\Houston` folder and `C:\Test\HR.xls` file	`C:\IT-Hou`

User and Group Name Filters

At its most basic, this filter lets you choose a particular user to watch. But its effects can also be very broad. For example, you can exclude activity by antivirus or backup product accounts, effectively targeting just human actions. You can also leverage your existing user groups to target types of employees for rules that, when combined with file types or locations, make very specific screening searches.

You can use wildcard characters in user account and group names. An asterisk (*) matches zero or more characters. A question mark (?) matches any single character. The following table identifies several example filters and what they match.

Filter	Matches	Does Not Match
*	All accounts, regardless of their name	
Hou*	All accounts that start with Hou, such as Hou, HouPaul, and Hou-IT	Holland IT-Hou
H?????	All accounts with 6 character names that start with H, such as Hilton and Hou-IT	HouPaul IT-Hou
???-	All accounts with 3 characters and then a hyphen (-) in their name, such as Hou-IT and Houston-Paul	HouPaul IT-Hou

Operations to Audit (or Block)

You can specify exactly which file operations to audit (or deny, if you are making a Block Access rule). These options help you limit auditing noise and focus on the specific operations that interest you. For example, Sarbanes-Oxley auditors closely evaluate **write** operations for spreadsheets. IT professionals tend to watch **security change**, **rename**, and **delete** operations for folders. Healthcare professionals often focus on who is **reading** patient data.

Note
The **Access Checks** are security checks to ensure a user account has permission to perform an action. The **Content Operations** (File ...) are the actions when they occur on the file or folder itself. With some caching mechanisms, some file activity requests may be served through the cache and no Content Operation may actually occur. This typically doesn't occur in a server environment.

Review the following operation descriptions to make sure you select the correct operations to audit in each rule:

Read Access
A security check to make sure the user account has permission to read the file.

Write Access
A security check to make sure the user account has permission to modify the file.

Delete Access
A security check to make sure the user account has permission to delete or rename the file or folder.

Create
A change in status resulting in the creation of a file (during the open process)

Delete
A permanent deletion of a file or folder. When a file or folder is moved to the recycle bin, the file or folder is actually renamed rather than deleted.

Rename
A change to the name of a file or folder. This activity occurs when the file or folder is saved with the new name, or deleted to the recycle bin.

You may deny changing the file extension in any renames (i.e. renaming Work.exe as work.tif)

Security Changes
A change to the security settings for a file or folder, such as changing the access control list (ACL) for a file or folder.

File Read
An operation that views the contents of a file or folder. If a request to view the contents of a file or folder is served from the cache, this operation type may not occur on the computer. Most file read operations for files accessed over the network are not served from the cache.

File Write
An operation that modifies and saves the contents of a file or folder. If a write request is served from the cache, this operation type may not occur. Most file write operations for files accessed over the network are not served from the cache.

Note
FileSure also shows when a user has been denied access to a file. This is an automatic feature than accompanies any of the Access Check operations. Your audit report will show a "Deny" if the user failed the security checks for any of the operations you were auditing. This feature does NOT require FileSure Defend.

Options Tab (Audit/Block Access Rule Creation Window)

Rule Applies to . . .

Specify which devices you should audit for each rule. For example, you can exclude file activity for CD and DVD drives. You can also choose whether the **File name filters** you specified should match files, folders, or both. Lastly, you designate whether this rule is just for servers, workstations, or both.

Note
You cannot audit Write activity to a CD or DVD since there is no file system on those devices until AFTER the data has been written.

Bulk Operations

You may designate to enact a rule only for bulk file operations. Define how many of the rule matches must occur within a certain amount of time before the rule "counts" the operation as a match. You might allow users to email three Excel spreadsheets a day before a match occurs, allowing normal day-to-day work to happen but protecting against theft.

Time Slot Filters

The rule you are creating/editing will only return matches/restrict access during the hours you designate by clicking on the time slot grid or on a day of the week. Any time highlighted in blue will be the time the rule is active, any white area is inactive. Exception: If **NO** time is designated, the *filter* is inactive and the rule is "on" at all times.

Program Name Filters

Program Name Filters work just like file name and user name filters—but apply to the program being used to open/access a file. If you add a program filter of '*\excel.exe', the rule would then only apply when Excel.exe was used.

One way this can be useful would be with FileSure Defend. If you were to add a filename filter of *.xls for all users, and then have all programs EXCEPT excel.exe be included in the rule (exclude '*\excel.exe'), the result would be: only excel.exe would be able to open an xls. file.

Note
Program name filters are generally only useful on workstations since program names aren't passed to the server on remote file accesses. There are a few programs that run on the server and in those cases, program filters could be useful.

Group Name Filters

Group Name Filters Tab allows you to specify the names of the groups whose members should be included or excluded from matching this rule. You can use wildcard characters, such as an asterisk (*) by default. To use group memberships, specify network credentials on the Network Options tab of the Configure window (choose Options from the top main menu).

Signature Filters

Signature Filters allow rules to match based on the actual contents of a file. Signatures are defined as a series of numbers (bytes) in the following format:

XXXX: AA BB CC DD EE FF AA & XXXX : 11 22 33 44 55 66

"XXXX" is the byte offset to start looking for matching bytes. "AA BB CC DD etc…" are the bytes to look for in hexadecimal format.

This is an advanced feature that can be used with **FileSure Defend** to stop file theft. Here's how…Say we want to protect XLS files from theft so we create a simple rule. Block file reads on XLS files to all programs EXCEPT excel. If someone were to override the extension of the file allowing the XLS file to be saved as a non-protected type like ".jpg" then this filter would not work. It's really an xls file, but they saved it as a jpg. ***By using a signature, FileSure can scan the file regardless of the name and determine if it really is an excel file or not.***

To enable file signature filters for your rule:

1. On the Signature Filters Tab, click **Add.**
2. Choose a predefined signature to match the file type you are trying to protect. You can also check the web for new predefined signatures.
3. If a predefined signature doesn't work and you need help creating a custom signature, contact ByStorm software support at support@bystorm.com or visit the ByStorm Software Forum at ww.bystorm.com/forum.
4. Choose whether you want this to be an "include" or "exclude" filter.
5. Click OK. You will see the filter in the signature filters tab window.

Note

For performance, FileSure only scans the first 4,000 bytes of a file for a signature.

Size Filters

This option allows you to define filters based on file size; useful if you only care about large files. For example, if you are attempting to protect models in spreadsheets with 100,000 cells, you probably don't care about someone e-mailing an .xls file that is 50k in size.

"Other" Tab

Audit Noise Reduction

When auditing file operations, many common activities can create auditing noise known as an *audit storm*. An audit storm occurs when the same user generates 100 or more file operations within 30 seconds. For example, when a user copies several folders that contain many files, a large number of file operations occur. To limit this noise, FileSure can automatically avoid an audit storm by temporarily excluding that user account from the rule until the storm is over, and then reactivating that user account in the rule. You select whether to enable this feature for each rule.

Also on this tab you can choose to write matches to the event log, and create an alert ID. Both of these choices are covered in the Real Time Monitoring Options section on page 20.

Advance Rename Options

When using **FileSure Defend**, if you select the "Rename" option under "Options to Deny," the Advance Rename Options become enabled.

Allow renames with the same file extension is the default setting: it means that if you have specified .xls in the file filter (above on the screen) while you cannot change budget.xls to budget2.txt, you CAN change budget.xls to budget2.xls.

Deny changes "to" chosen extension(s), again assuming .xls is chosen in the file filter, allows you to not only deny changing any .xls file to any other file extension, but it also will deny changing budget.txt to budget.xls.

Advanced Alerting Support

Generate an event log record on rule match: You can configure FileSure to generate a Windows event when an operation matches a specific rule. You choose whether to write to the Event log or not for each rule, and define the type of event to generate, such as Information, Warning, or Error.

Alert ID: This can directly align an alert to rule filters you've established. For example, you might not care if X user copies 25 files during the day, but would be very concerned if it happened after hours. You could create a rule to match when X user copies files, enable a time slot filter for after hours, and then set that Alert to whatever number you choose, say 5. You could then create a simplified summary that alerts you based on the Alert ID 5—*which only matches to that user's file accesses happening after hours.*

However, care needs to be taken when assigning Alert IDs: Make sure the ID is not based on rules that overlap.

More on both of these Alerting options in the next section: Real-Time Monitoring and Notification Options.

Real-Time Monitoring and Notification Options

FileSure offers several ways to be notified, at the time it occurs, about activity that concerns you. If your organization makes use of an event log monitoring system, FileSure can write to the event log. If you use a syslog monitoring system, FileSure writes to the syslog. If you don't use any monitoring system, FileSure gives you a very powerful one built in that support thresholds.

Event Log and Syslog

You can configure FileSure to generate a Windows event when an operation matches a specific rule**. In the Audit Access/Block Access interface, under the "other" tab, you choose whether to write to the Event log or not for each rule, and define the type of event to generate, such as Information, Warning, or Error.**

When a file operation matches a defined rule that generates a Windows event, FileSure writes the captured information about the operation in the Windows Application log. Then, you can configure your monitoring solution, such as Microsoft Operations Manager, to respond to the generated events. This integration helps you monitor file and folder activity in real time while limiting the auditing noise in your monitoring solution.

If you have Event Log notification turned on, then FileSure automatically also writes to the syslog. So, if you use a syslog monitoring system, the information will be there for you to pull from.

FileSure E-mail Alerts

Alerts are e-mails that are sent when a "threshold" is met of whatever activity you designate. A threshold might be "tell me when X user copies more than 25 files." To have the information about that user and their file copying activity in a form the alert engine can check for your threshold, FileSure uses alert Summaries (queries) you define.

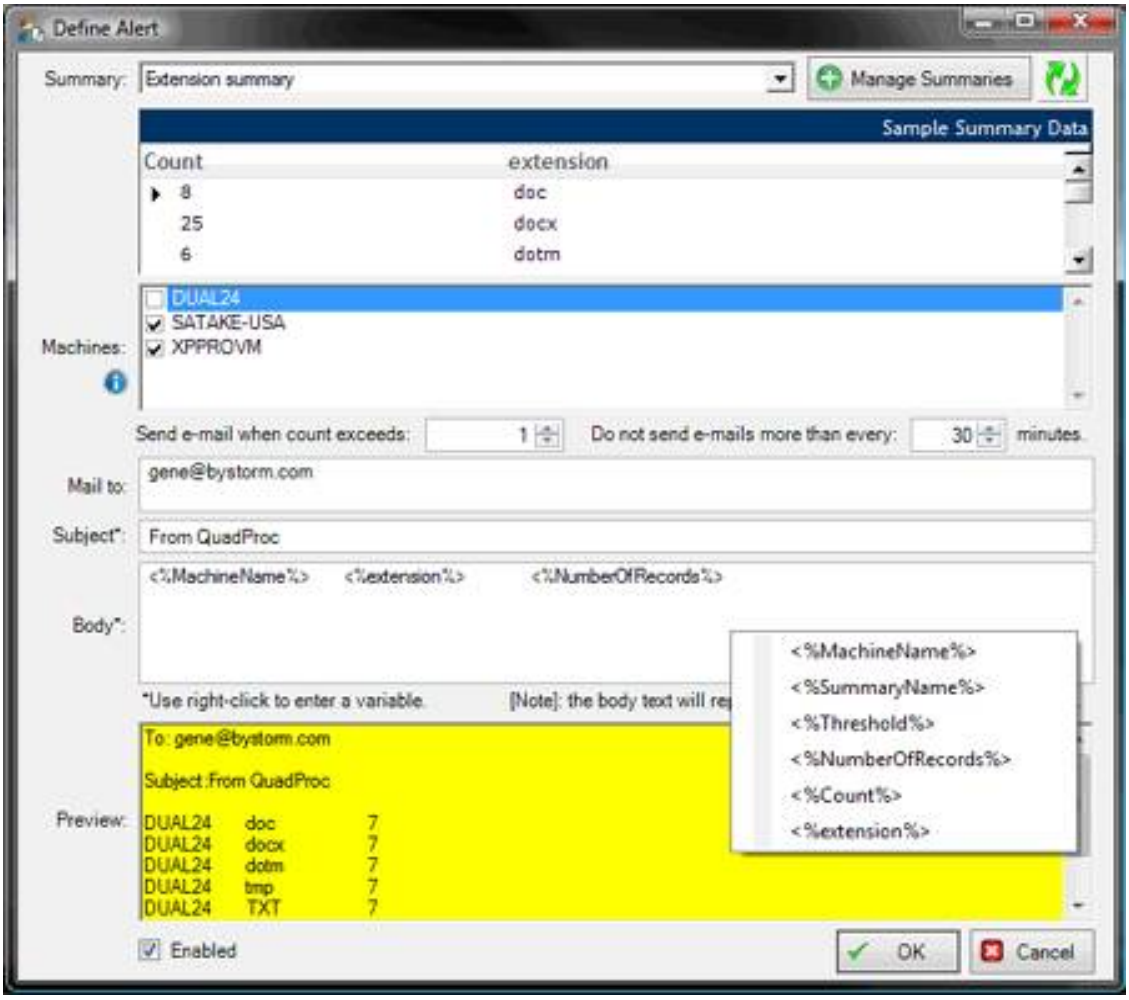
For your convenience, FileSure has a few preloaded summaries to choose from. You will need to activate them before you can schedule an alert based on their results.

To add an E-mail Alert:

1. On the Analysis, Reports and Alerts Tab, click **Manage Alerts**
2. Any previously configured Alerts would show up in the Manage Alerts Window for you to enable or disable with a check mark. Click the **New** button to add a new Alert.
3. You should now be in the Define Alerts interface. Since Alerts are based on summaries, you have to have a summary enabled to define an alert. Any previously configured summaries would show up in the drop box at the top (and any sample data would show up in the Define Alerts Window—having been pulled from the local machine). *If you are just starting, you have no summaries enabled,* so you need to click **Manage Summaries**.
4. Now you have a choice between a preloaded summary, and a custom summary. These instructions use a preloaded summary. To create a summary, see detailed information in the next section. Enable a summary by clicking the **Enabled** box and then clicking **Close**.
5. Back at the Define Alerts interface, you can see your new summary by clicking the refresh icon in the top right corner. After a few seconds, you should see a window similar to the figure below. Choose what machines you want this summary activated for from the Machines window. Set the threshold by picking a number in the count box, and designate a timeframe for not getting repeated e-mails in the "do not send" email box.

   Then, create the E-mail you want to receive. Both the subject and the body allow you to insert a "variable." You can access the variable list via a right click.

   There are 4 built in variables:
   <%SummaryName%> --- the summary name (in our example….Extension Summary by User)
   <%Threshold%> -- the threshold amount (in the figure below, 5)
   <%NumberOfRecords%> --- the number of records that PASS the threshold
   <%MachineName%> -- the machine that the summary came from
   The rest of the variables come from the summary, so in the figure below, <%Count %>, <%userName%>, <%extension %>.
6. Click OK. You will see the Alert you have defined in the Manage Alerts list. *Your alert will already be enabled.*



Defining a Custom Summary

Within the Alerts Interface, go to the Manage Summaries dialog. It can be accessed by choosing **Manage Alerts, New,** and then **Manage Summaries**.

Summaries are SQL select statements that are executed by the FileSure service after every consolidation phase and published on named pipe to be consumed by the alerting engine. As writing SQL statements can be complex, ByStorm Software has provided some standard summaries for you to choose. These instructions are for writing your own summary instead.

The FileSure data store is based on the public domain SQLite SQL database engine, so Summary queries are similar to standard SQL format, but there are small differences. In most cases, these differences won't be noticed.

While it is possible to enter any valid select statement into a query definition, to be a summary the first return value must be a number, and typically this is the threshold value.

For example:

```
select count(*) Count from AuditingRecords;
```

would be a valid, albeit not very useful, summary. This summary would just count up all the records.

Here is a more useful summary:

```
select count(exeName) Count, exeName from AuditRecords where exeName
<> "" group by Upper(exeName) order by Count desc;
```

This summary would return a list of programs used to access audited files and how many times they were used. While more useful, still not very useful since we don't have a time constraint so the counts wouldn't be quantitative.

Up to this point, the strings are standard SQL. But we need to set how much data we need; for this we use the built-in variable OldestRecordAge, like this:

```
'and eventTime > OldestRecordAge'
```

We use the eventTime to limit the dataset that is processed. When the summary is processed by the FileSure service, OldestRecordAge will be replaced with eventTime of the first record that should be processed. Here is the final statement:

```
select count(exeName) Count, exeName from AuditRecords where exeName
<> "" and eventTime > OldestRecordAge group by Upper(exeName) order by
Count desc;
```

You can add other fields to be published as part of the summary that might be of interest. In the above example, we've included the name of the program that was used when the file was audited.

Summaries are stored in the registry and all pulled down as part of the 'master-slave' system. So summary changes will be reflected only after they slave machine pulls the rules from the master. Since the local machine doesn't have to rely on the master-slave model to get the summary changes (they were made locally) they will be reflected on the next summary update, which is on every consolidation pass.

Summary creation to meet your needs is an advanced topic, and if you need more assistance please visit the ByStorm Software Forum at www.bystorm.com/forum or contact ByStorm Software customer service at support@bystorm.com.

Note

On the rule Audit/Block Access rule creation window under the "Other" tab you have a choice to make an Alert ID. This can directly align an alert to rule filters you've established. For example, you might not care if X user copies 25 files during the day, but would be very concerned if it happened after hours. You could create a rule to match when X user copies files, enable a time slot filter for after hours, and then set that Alert to whatever number you choose, say 5. You could then create a simplified summary that alerts you based on the Alert ID 5—*which only matches to that user's file accesses happening after hours.*

However, care needs to be taken when assigning Alert IDs: Make sure the ID is not based on rules that overlap.

- For example, you could have one rule to watch *.doc files and another to watch Office files. FileSure does NOT check all the rules but instead stops after finding the first matching rule. If the Alert ID was set to 223 on the watch *.doc rule, and the first matching rule was the Watch Office Files rule, the desired Alert ID of 223 would not be written
- Most of the time, Alert IDs should be unique. If you have 3 different rules with the same Alert ID, you won't be able to tell which rule generated the alert.

Accessing and Using the File Activity Information

FileSure is designed to allow you to view, print, and export your file activity information in many different formats. Filters are available to allow you to quickly target only the information you need from the rule matches that have been recorded or activity that has been denied. Within the product, there are six main ways to view the file activity FileSure is recording, as follows.

Real Time File Activity Monitor

Displays a list of file operations that match the defined rules as those operations occur. This list contains only the activities that occur while the user interface is open. If the list is empty, you either have no rules turned on or your rules are currently finding no matches. If FileSure is deployed to workstations, you may choose which machine's activities you view from the top drop-down box.

Analysis—View and Trends

To review, filter, analyze, or export past file operations and activity, you can use the Analysis section for two more ways to view your data.

In the **View Data** interface, you design queries to return exactly the information you are seeking. This window supports your internal auditors during internal investigations, and allows you to export data in comma-separated value (`.csv`), XML, HTML, Microsoft Excel or Microsoft Access format for external auditors.

In the Search for Trends interface, you have to ability to return information you may not have been looking for. Essentially organized to present data by "counts" of file or folder operations, the Search for Trends function lets you see usage trends by user—and then filter by time, file type, the program accessing the files, and much, much more. This allows you to find abnormalities you wouldn't have otherwise seen. Once you find that abnormality, it is just a double-click to drill down and pinpoint the exact details of time, machine name and more.

Reports and Scheduled Reports

This window allows you to query the results of past file auditing activities based on date and a pre-defined report setting, the fourth way of looking at your data. The information is returned in a report format, and can be printed or exported in Excel or Adobe Acrobat format. You may also schedule recurring reports to be automatically pulled and delivered via e-mail and saved in a central location in .XLS, .PDF, .CSV, .XML, or .HTML format.

Notes

In all data viewing screens, remember the filters you are choosing are defining what data you want *from the data that has already passed the test of your designated rule matches*. In other words, the data returned is always dependent on the rules that were activated at the time period you are querying. Make sure you remember what rule filter matches created the data when you design or use the different view queries.

FileSure 2.5 still supports the **Web Console**. This gives you a fifth interface option for viewing the returned data—and allows other authorized users to access the data via an intranet web console.

For real-time protection and integration, the sixth way you can use audit data is by using FileSure's built-in **E-mail Alerts** or by extracting data written to either the event log or the syslog into your own alerting system. Please see "Email Alerts" in the previous section [page 20] for instructions on setting up FileSure Alerts, and contact ByStorm Customer service or visit www.bystorm.com/forum if you need more information on integrating FileSure with your other security products.

Using the View Data Interface

To view file activity:

1. On the Analysis Tab, click **View Data**.
2. Choose the source machine for your data. The machine list is populated by what machines have pushed their data to the server. Specify the date range for your query. The default filter displays activity from the previous 12 hours.
3. Click the Filters Tab at the top left to define security, operation, and program filters.
4. Click the View Tab to designate the drive type(s), and choose output view options.

5. Click **Apply** to display the data that matches the filter options you specified.
6. At the top of the viewing screen, please note you can switch tabs to view recorded file data, event log activity (if you have event log monitoring turned on), and system data related to the FileSure service.

Using the Search for Trends Interface

To search file activity for abnormalities:

1. On the Analysis Tab, click **Search for Trends**.
2. Choose the source machine for your data. The machine list is populated by what machines have pushed their data to the server. Specify the date range for your query. The default filter displays activity from the previous 1 hour.
3. Click **Apply** to display the data that matches the filter options you specified.
4. In the display screen, you will see counts of data. Drag and drop research criteria headings into the column or row areas to clarify the counts by those criteria. For example, dragging "Process" into the column heading area will separate the file activity count by processes that used them.
5. Double click on any item to drill down to the level two research information screen. Double click on any item on level two to see level three specifics on that item.

Using the Reports Window

To create a report on file activity:

1. On the Analysis Reports and Alerts Tab, click **Reports**.
2. Specify the date range for your report. Choose a report from the Report drop-down list. The parameters of the selected report will show in a definition below the box.
3. For custom date range, choose the Date Range Tab, and if FileSure is deployed to workstations, click the Machines Tab to choose a data source for the report inquiry. The machine list is populated by what machines have pushed their data to the server.
4. Click **Run.** You can then print or export the report information.

To schedule recurring e-mail reports:

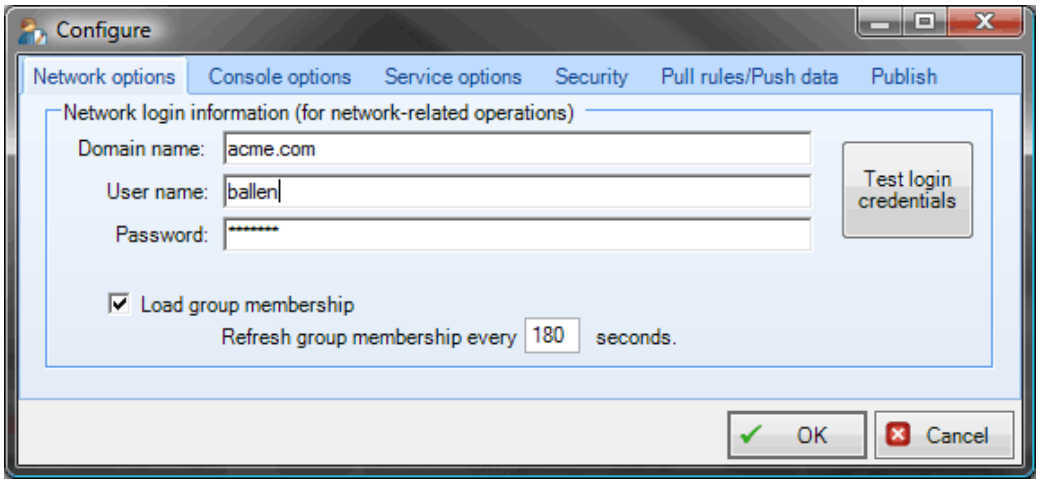
1. On the Analysis Reports and Alerts Tab, click **Reports**.
2. Choose **Schedule Recurring Reports** on the Run Report Interface (or choose **Scheduled Reports** from the Reports Section). Make a name for your new e-mail report job and choose whether this job will be enabled immediately or you will turn it on later.
3. Set criteria for your report as in the previous section. You can add an additional user filter in this interface. For help with wildcard filters please click the "i" button.
4. Determine delivery email address(es), and choose what days of the week to receive the report.
5. Choose **OK.** Your report will now be listed in the Scheduled Reports window. ***Be Sure to set FileSure SMTP settings; your mail can not be delivered without this information.***

Using the Web Console

The audit log web console was developed to allow end users to view the audit logs of a server without having to get a report emailed to them or ask the Security Administrator to generate the desired data. Another feature of the Audit log web console is that the audit log doesn't get "stale" like a scheduled report can.

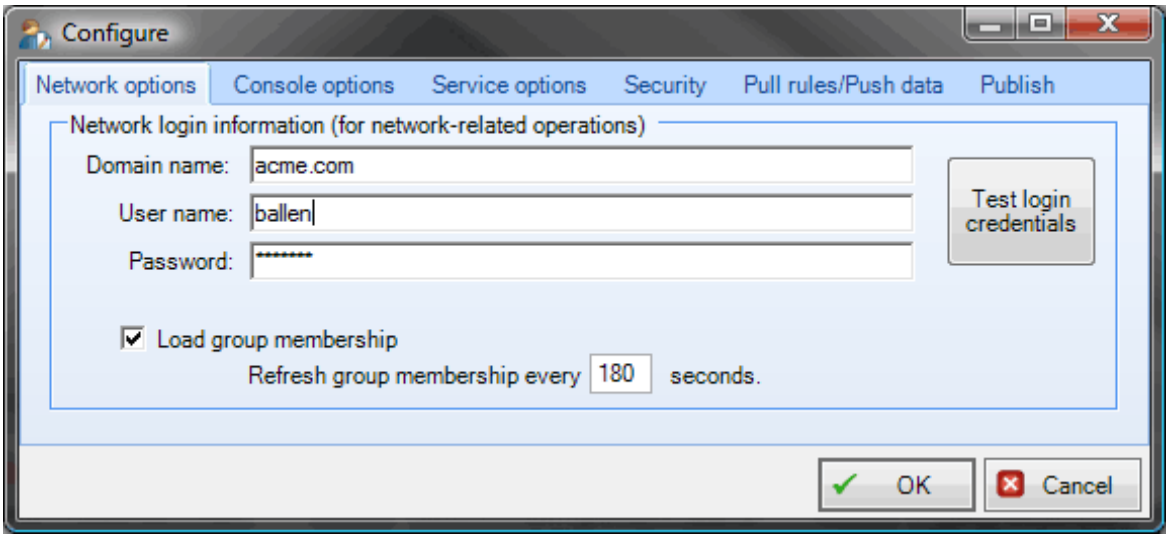
Define Publish Settings

The Audit log web console relies on the **Publish** feature of FileSure, located under Options→Configure. The Publish feature generates a Microsoft Access database on a regular basis to a location of your choosing. In the dialog below, we want to publish the last 30 days of auditing data every 30 minutes to the network path of \\ByStorm01\c$\Inetpub\wwwroot.



Configure Network Options

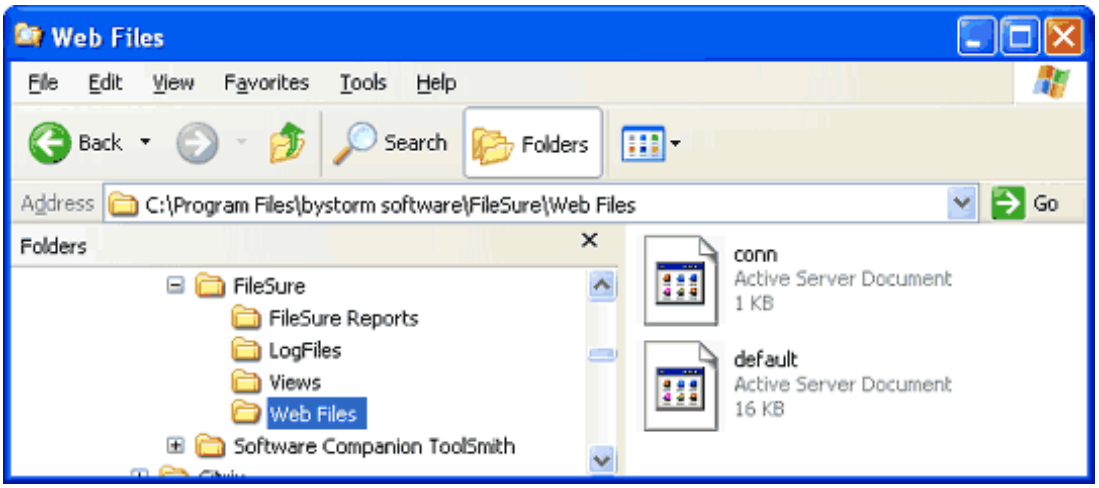
Since we are publishing to a "network" path, the service needs to be configured to allow access to the network. This is done via the Network Options tab on the Configure dialog, as shown here.



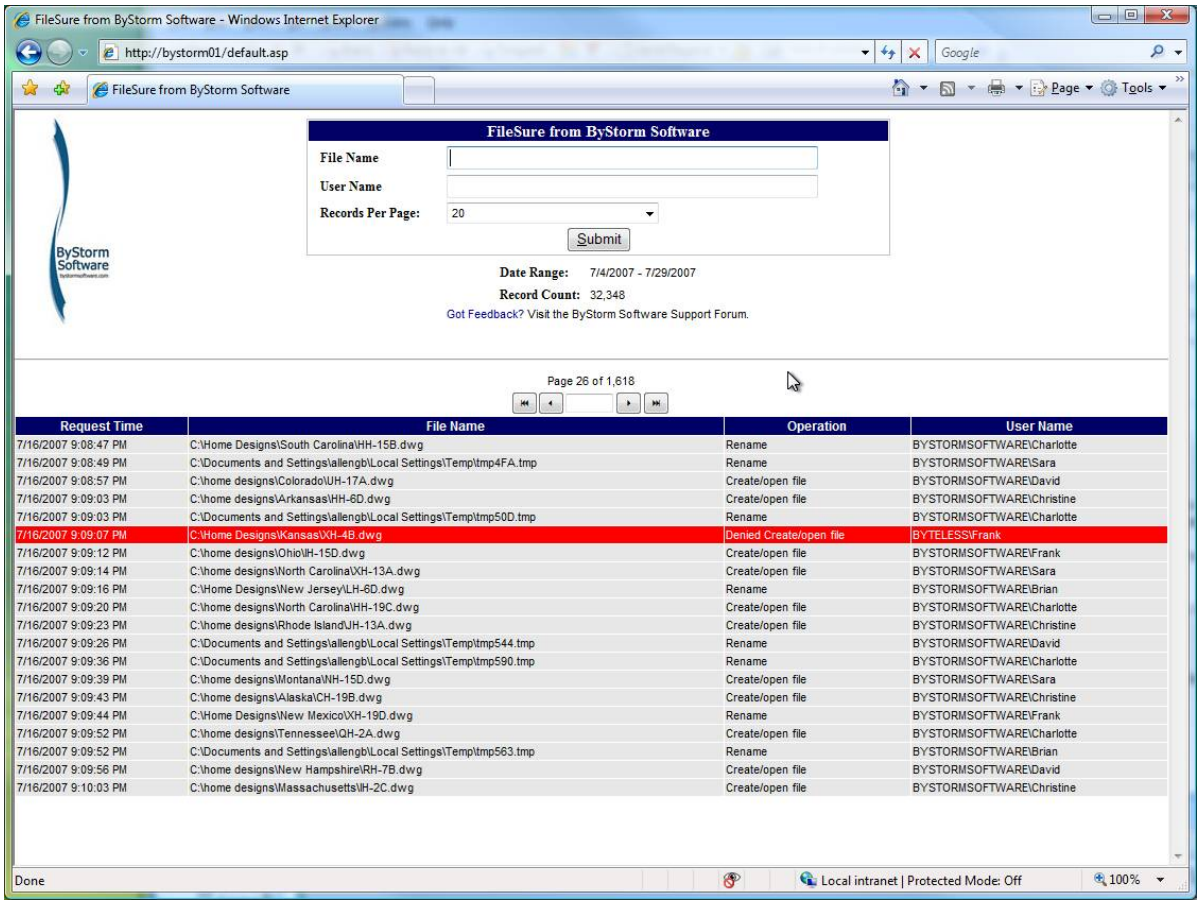
Set up Web Files

From the previous two steps, a Microsoft Access Database (filename: FileSure.mdb) should now be created every 30 minutes (if possible). By recreating the file every time, the integrity of the audit log is ensured.

We now need to set up the web pages to use this published data. There are 2 files included with the FileSure installation **that need to be copied to a Virtual directory of IIS.** You can find them in the "Web Files" folder under installation directory, shown here:



In this example, we're publishing directly to the virtual directory (\\ByStorm01\c$\Inetpub\wwwroot) so no modification to the web pages is needed. Here is example of what the web console looks like:



If you aren't publishing directly to the IIS virtual folder, the **conn.asp file** contains location of the access database. Your webmaster should be able to change the location for you.

If you would like to limit what users can see in the auditing log, the **conn.asp file** also contains this information. Your webmaster should be able to add any view rules you need (this requires knowledge of the SQL 'like' statement)

Working with Audit Data Log Files

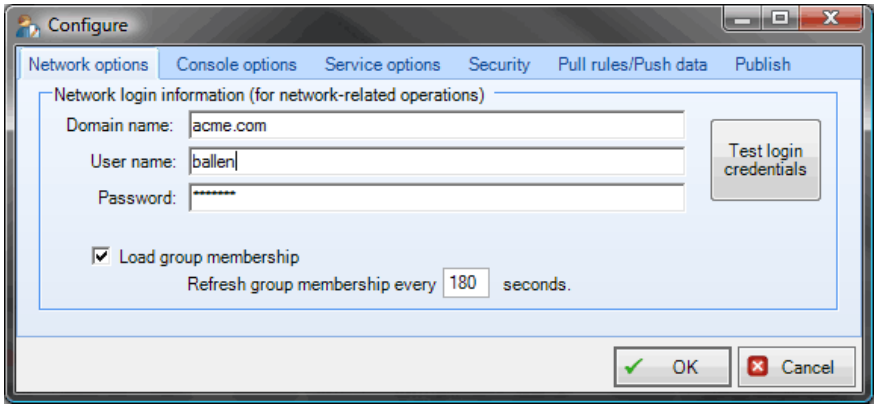
FileSure creates compressed, encrypted log files to protect the recorded audit data. These files are stored in the `Program Files\ByStorm Software\FileSure\LogFiles` folder. The name of each log file indicates the month and year of the audit data stored in that file. For example, the `FA0610.bsa` file contains audit data from October 2006. The `FA0611.bsa` file contains audit data from November 2006.

Customizing FileSure

FileSure provides many customization options to support your specific needs. The customization options include several important areas:

- Specify network credentials used to collect group membership information. The credentials are used for ALL network operations and will be used by workstations to pull rules and push data.
- Turn on or off warning messages. Hide start-up splash screen. Enable Web Proxy.
- Adjust service heartbeat options. Choose whether the FileSure service may be stopped manually or not.
- Specify the period of time during which FileSure should treat multiple open/create, read, or write events by the same user on the same file as duplicate events and consolidate them.
- Choose performance settings that affect all rules, such as ignoring file accesses by the OS, backup procedures, or file types you designate.
- Define security settings enabling access by different local groups.
- Configure rule sharing and log publishing from a central server.
- Control audit log consolidation and publishing activities, such as if and how often you want to publish the audit log information to Microsoft Access.
- For more information about the configuration options on each tab, see “Options Menu→The Configure Interface” on page 62.

The Configure window is similar to the following figure.



To customize FileSure options:

1. On the Options menu, click **Configure**.
2. Select the tab with the options you want to change.
3. Specify the appropriate values, and then click **OK**.

Managing Workstations with FileSure

If you have upgraded to FileSure Workstation, you can monitor file activity and protect IP resources not only on the server but on individual Workstations. This means finding mis-saved or "accidentally-dragged" folders on the users' local machines and protecting files from being saved to pen drives after being copied from network drives to the desktop. This powerful solution is managed locally through the Manage Workstations interface.

To manage FileSure workstation deployments:

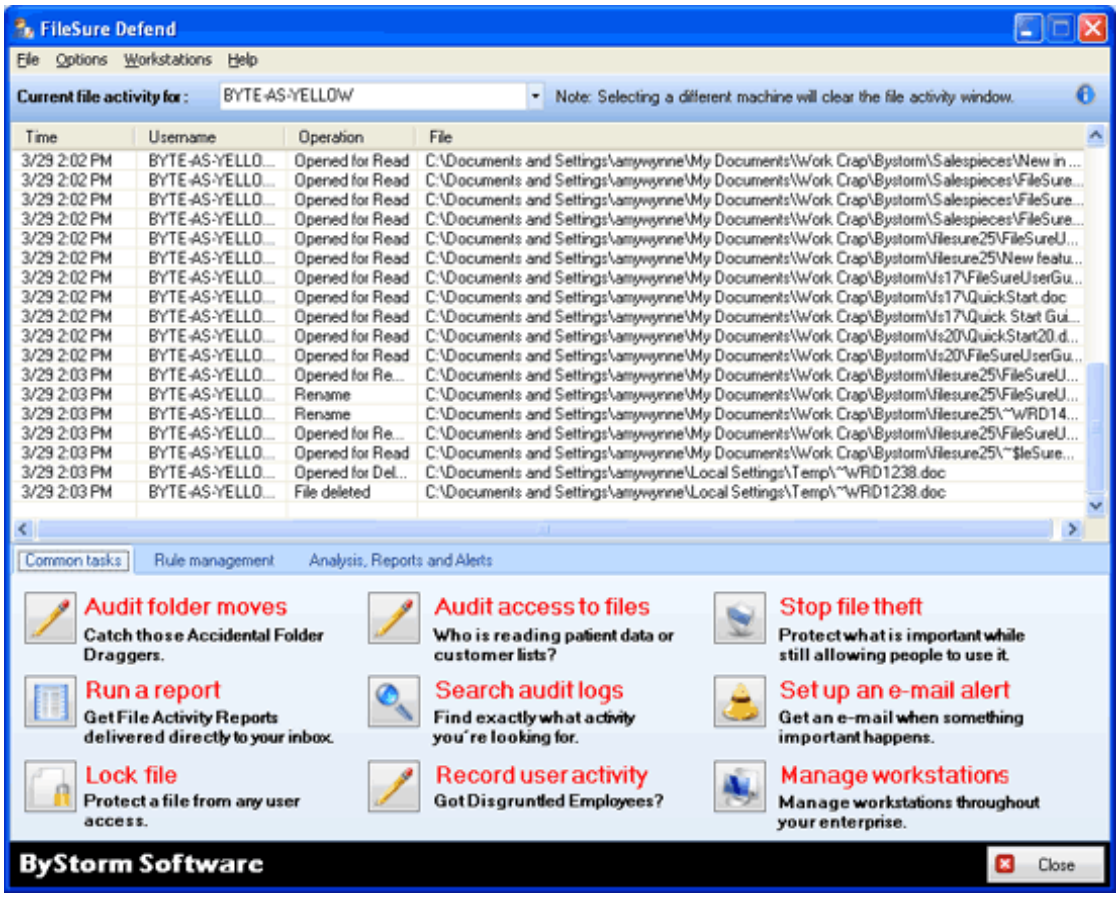
1. On the Workstations menu, click **Manage**.
2. Add or Remove workstations within the FileSure deployment. You may also turn on and exempt machines from the FileSure FileWall®. For more information on all these topics, please see Workstations→The Manage Interface on page 67.
3. Specify the appropriate values, and then click **Close**.

Chapter 4

Windows and Features Detailed

Navigating the Main Console

The Main console window allows you to monitor what is happening on any machine running FileSure when the activity occurs, quickly set up common auditing and protection tasks, view what rules are currently in effect, add/edit/delete rules, and return auditing data in many different forms.



The fields on this window are defined as follows:

Current File Activity Monitor

Displays a list of file operations that match the defined rules as those operations occur for whatever server or workstation is listed in the dropdown box. This list contains only the activities that occur while the user interface is open. If the list is empty, you either have no rules turned on for the destination machine, or your rules are currently finding no matches.

The dropdown list does not indicate that a machine is running, merely that it is one on which you have FileSure deployed. If a machine is off when you choose it but subsequently turned on, the activity monitor will begin giving results.

Data Found Behind the "i" Button

Total file operations intercepted
Specifies the total number of file activities that FileSure evaluated on the computer.

Rule Matches
Specifies the number of file activities FileSure evaluated and found that they match one or more defined rules.

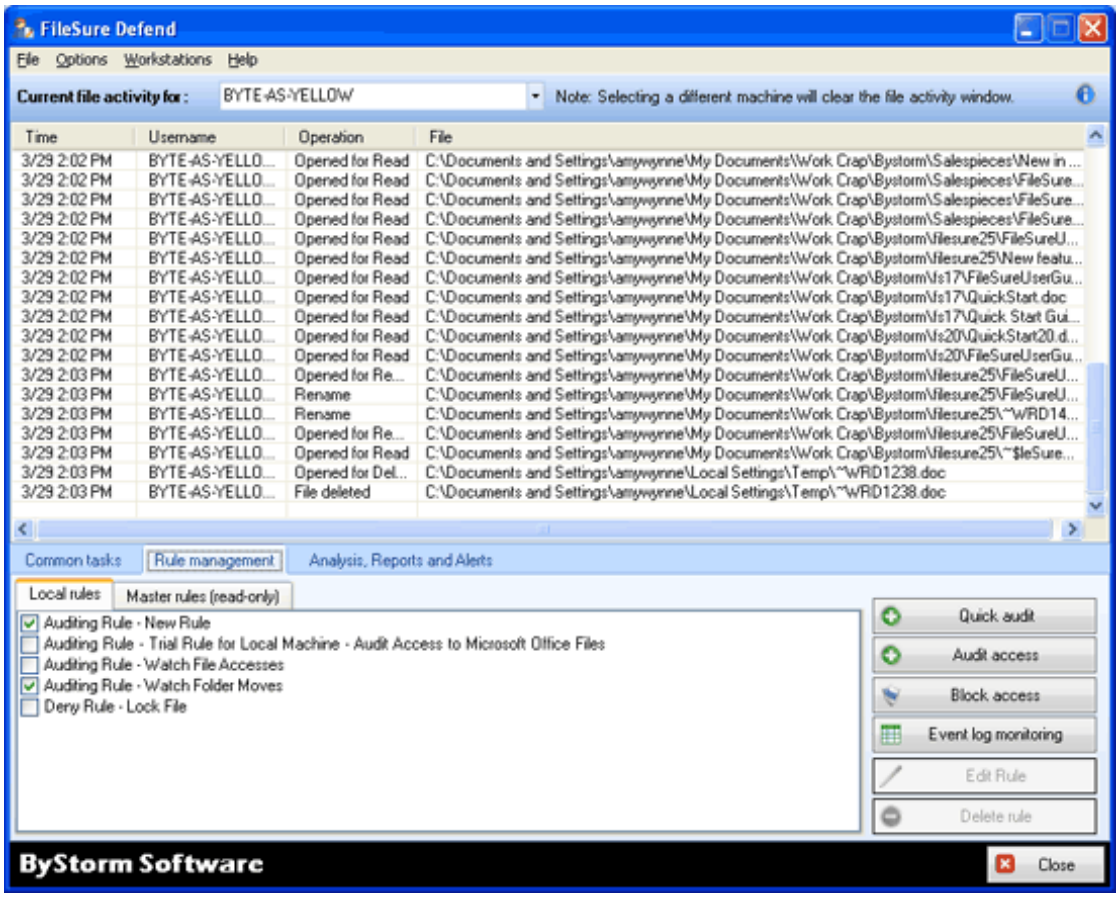
Time since last group membership load
Specifies the time that has passed since the last time FileSure reloaded the group membership information. To make sure group membership rules are validated correctly, FileSure reloads group membership information at the interval specified on the Network Options tab of the Configure window. You can modify this interval for your specific needs. This process runs in a low priority thread to ensure it does not hinder performance. If you do not have any group membership rules defined, FileSure does not need to load group membership information.

Time since last audit consolidation
Specifies the time that has passed since the last time FileSure consolidated the audit logs. You can configure this time period on the Server Options tab of the Configure window. Changes to server settings require you to restart the service. To ensure the audit log consolidation process does not hinder performance, this process uses a low priority thread to compress and encrypt the events in the main auditing logs. This thread sleeps for 30 seconds between passes.

Common Tasks Tab

To enable easy access to commonly-needed features, click on any of the scenario-based choices for wizard-style set-up of FileSure's various functions.

Rule Management Tab



Local Rules

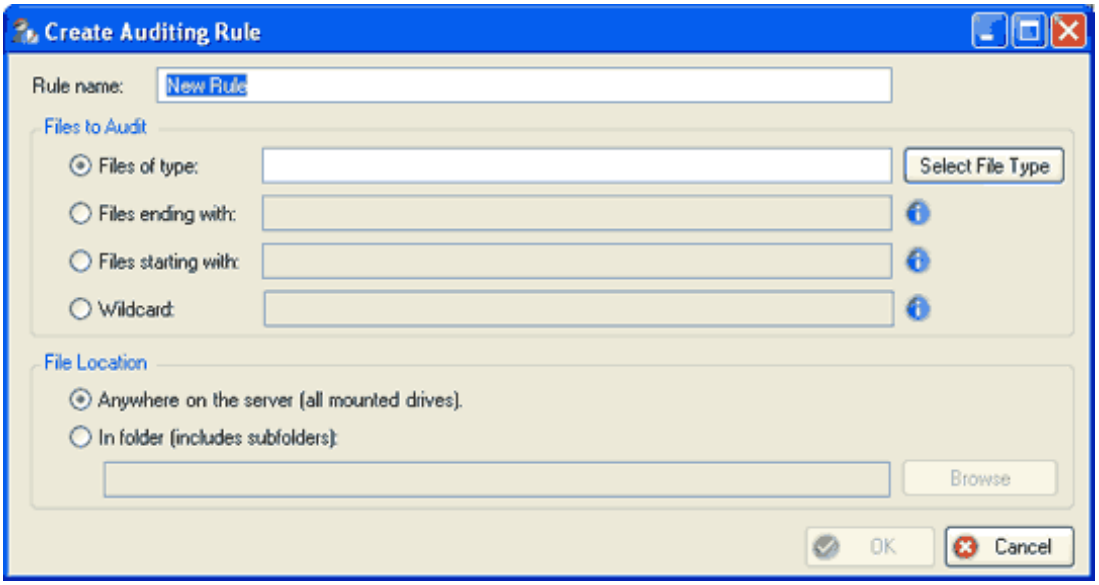
Lists the rules defined on the local computer. You can enable or disable a defined rule using the check box next to the rule. You'll see a sample rule has been created for you. The sample rule is enabled by default.

Master Rules

Lists the rules imported from the master server. These rules are read-only on computers other than the master server. You can modify, enable, or disable these rules only from the master server.

Quick Audit Button and Interface

Clicking Quick Audit will give you a simplified Auditing Rule interface. The window is similar to the following figure.



The fields on this window are defined as follows:

Rule Name

Specifies the name of the rule to help you identify it. This value is recorded with event log entries related to this rule.

Files to Audit

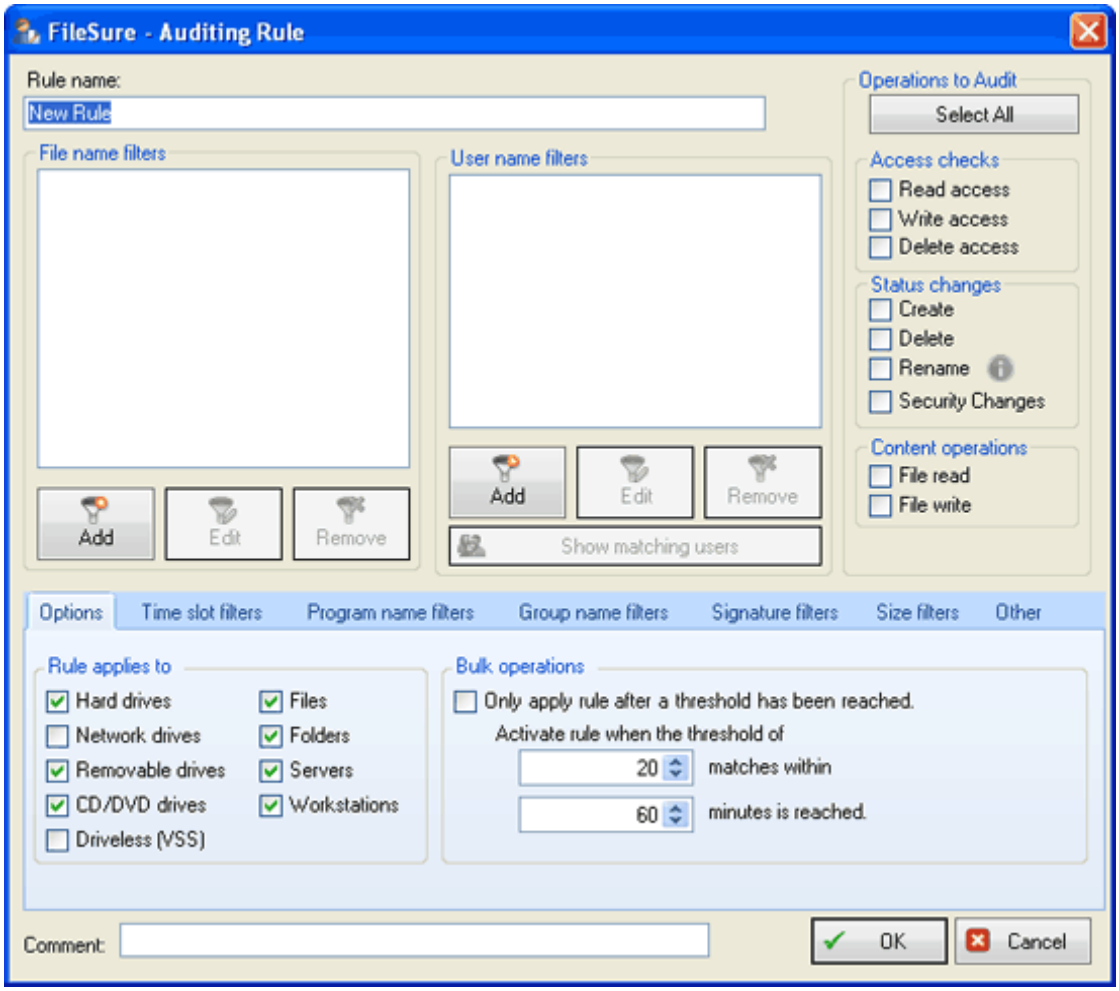
This section allows you to add simple filters that instruct FileSure what specific files or types of files to track. Click the "i" for instructions on how to use each filter type and for examples.

File Location

This section allows you to choose the location of the files you want FileSure to audit.

Audit Access Button and Interface

Clicking Audit Access will give you the Auditing Rule Window. The Auditing Rule window is similar to the following figure.



The fields on this window are defined as follows:

Rule Name

Specifies the name of the rule to help you identify it. This value is recorded with event log entries related to this rule.

File name filters

Specifies the names of the files to include or exclude from matching this rule. You can use wildcard characters, such as an asterisk (*) by default. For example, to include all .XLS files whose name starts with HOU, specify *\HOU*.XLS as an include filter. Click on the "i" to see a key for how to configure wildcard filters.

User name filters

Specifies the names of the user accounts to include or exclude from matching this rule. You can use wildcard characters, such as an asterisk (*) and question mark (?). For example, to include all user accounts, specify * as an include filter. Click on the "i" to see a key for how to configure wildcard filters.

Operations to Audit

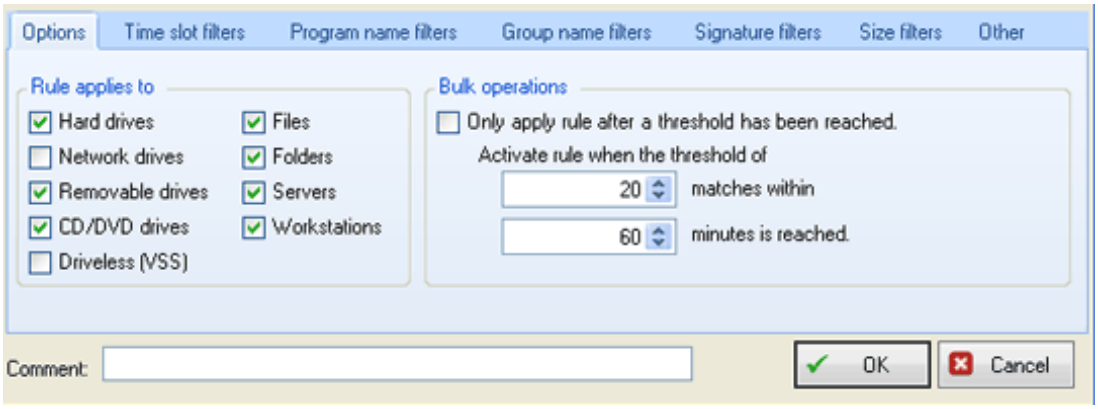
Specifies the types of file operations, such as Read and Write, to audit. Many auditors focus on Write, Rename, Delete, and Set Security operations.

Comment

Specifies additional information about the rule to help you clearly identify its purpose. This information is not recorded with the rule and is not used during the processing of the rule.

The tabs at the bottom of this window give additional options and filters for the rule:

Options Tab



Rule Applies to . . .

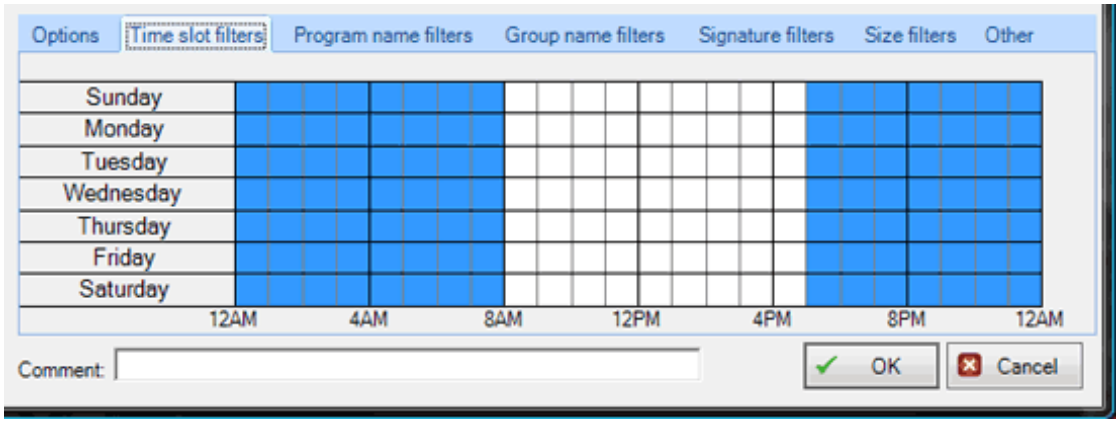
You can refine a rule to apply to only files or only folders (or choose both), and you can specify which device types to audit. If you are using FileSure Workstation, you may also designate to monitor servers or workstations with this rule.

Bulk Operations

You may choose to ignore activity unless it matches criteria indicating a bulk file transfer/delete. Set how many of the designated operations have to happen within a timeframe before FileSure considers the operations to be a rule match. You might allow users to email three Excel spreadsheets a day before a match occurs, allowing normal day-to-day work to happen but protecting against theft.

Time Slot Filters Tab

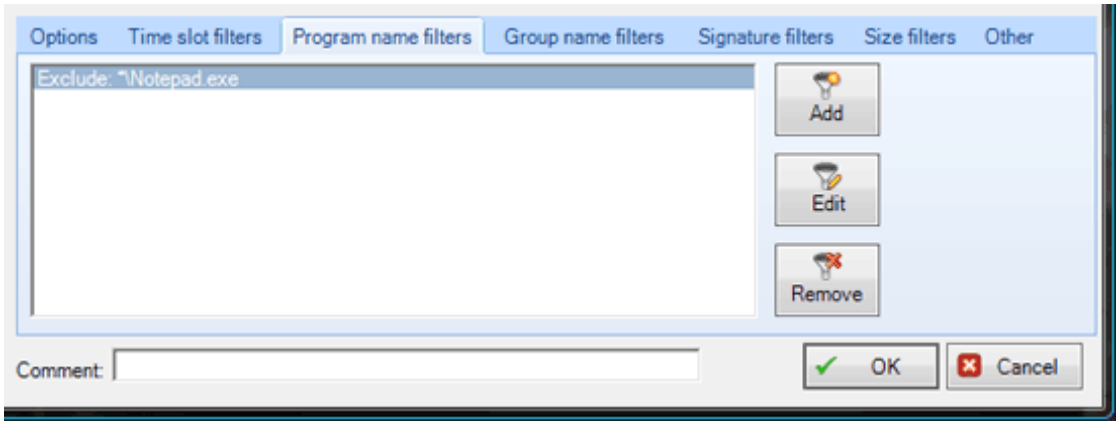
Designate a timeslot during which the rule will be active. The Time Slot Filters tab interface is similar to the figure below:



If no timeslot filters are selected, the rule will be in effect at all times.

Program Name Filters Tab

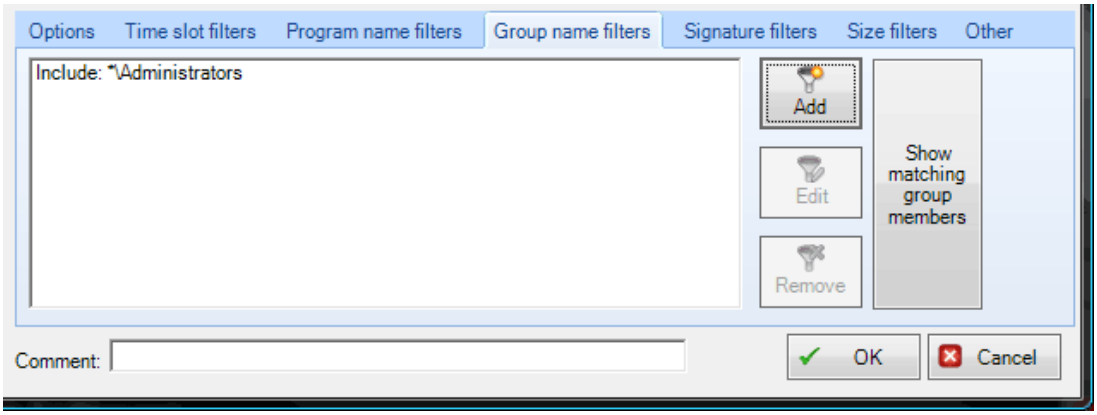
The Program Name Filters interface allows you to specify the programs to include or exclude from matching this rule. You can use wildcard characters, such as an asterisk (*) and question mark (?). A program filter of '*\excel.exe', creates a rule which only applies when *\excel.exe is used. The Program Name Filters Tab interface is similar to the figure below:



Note
For the most part, program name filters are only useful on workstations because program names aren't passed to the server on remote file accesses. For applications that run on the server, program filters could be useful.

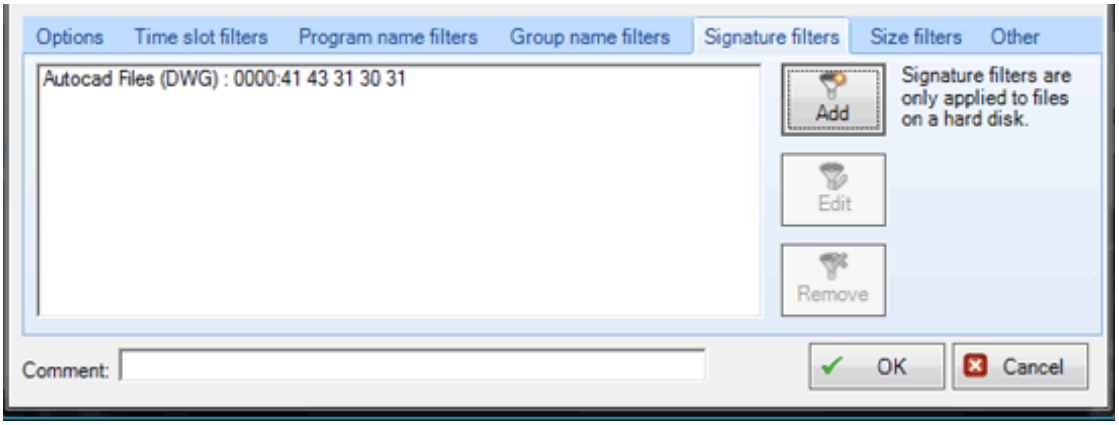
Group Name Filters Tab

Group Name Filters Tab allows you to specify the names of the groups whose members should be included or excluded from matching this rule. You can use wildcard characters, such as an asterisk (*) by default. To use group memberships, specify network credentials on the Network Options tab of the Configure window. Group Name Filters Tab interface looks similar to the figure below:



Signature Filters Tab

Signature Filters allow rules to match on the actual contents of a file. This is an advanced feature that will be used to stop file theft. The Signature Filter tab interface looks similar to the figure below:



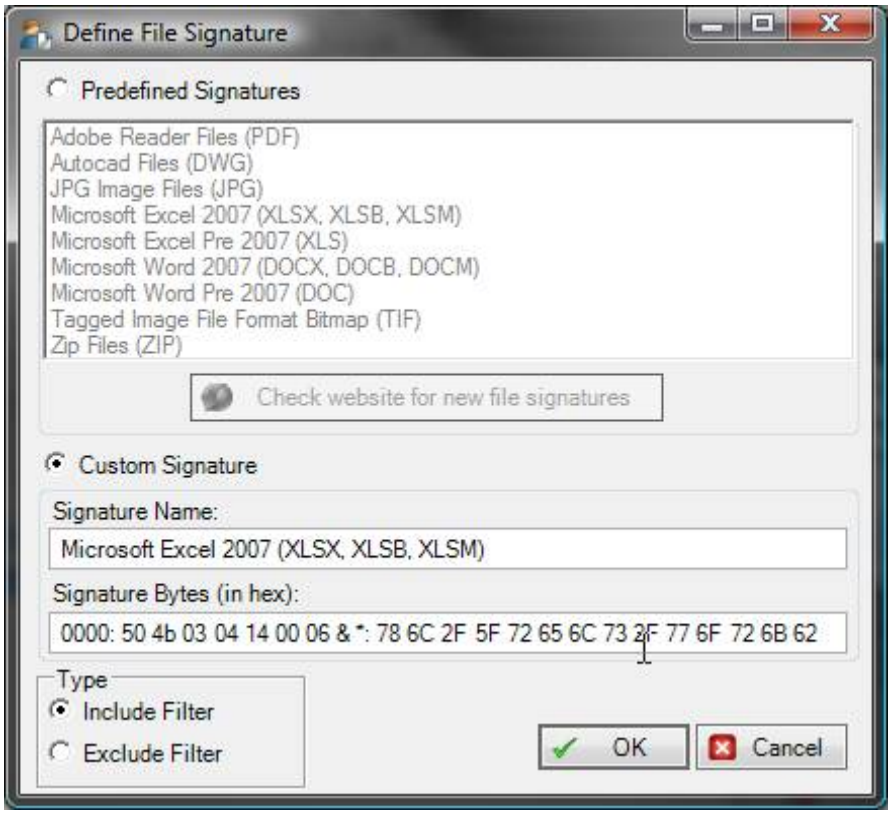
Signatures are defined as a series of numbers (bytes) in the following format:

XXXX: AA BB CC DD EE FF AA & XXXX : 11 22 33 44 55 66

"XXXX" is the byte offset to start looking for matching bytes. "AA BB CC DD etc..." are the bytes to look for in hexadecimal format.

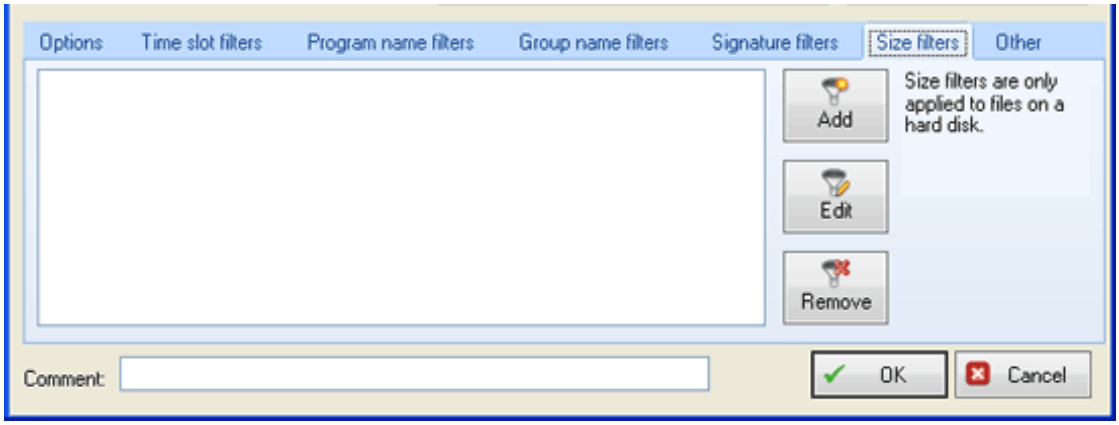
By using a signature, this feature allows FileSure to scan the file regardless of the name/file extension and determine what type of file it really is (so getting around security placed on filetypes/files with certain extensions can not be accomplished by renaming the file type).

ByStorm Software has pre-loaded some signatures based on common file types that you can select. Contact ByStorm Customer Service or visit the ByStorm User Forum at www.bystorm.com/forum if you need additional help with this feature. Choosing **Add** will give you access to those preloaded signatures in an interface similar to the one below:

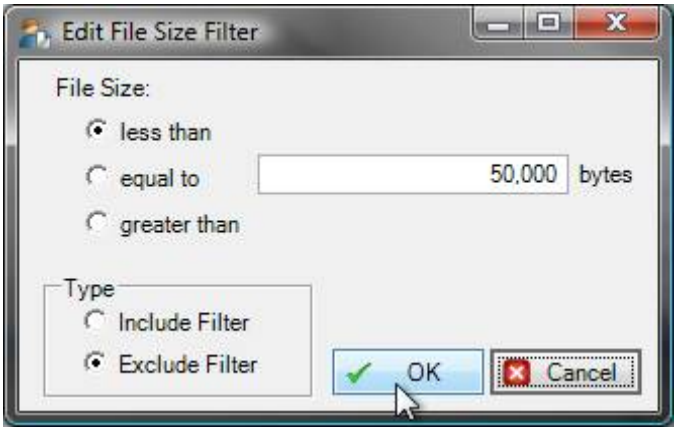


Size Filters Tab

Defining a Size Filter Allows you to audit/protect data based on file size; useful if you only care about large files. For example, if you are attempting to protect your energy trading models that contain over 100,000 cells, you probably don't care about someone e-mailing an xls file that is 50k. The Size Filters Tab looks similar to the figure below:



Choosing **Add** or **Edit** will give you this interface to define your size filter:



Other Tab

The "Other" Tab will resemble the picture below:

Audit Noise Reduction

When auditing file operations, many common activities can create auditing noise known as an *audit storm*. An audit storm occurs when the same user generates 100 or more file operations within 30 seconds. For example, when a user copies several folders that contain many files, a large number of file operations occur. To limit this noise, FileSure can automatically avoid an audit storm by temporarily excluding that user account from the rule until the storm is over, and then reactivating that user account in the rule. You select whether to enable this feature for each rule.

Advanced Rename Options

This feature will only be enabled in the Block Access interface.

Advanced Alerting Support

You can elect to have an event log entry generated when the rule is matched. Choose the log to which to write the event in the adjacent pick list box.

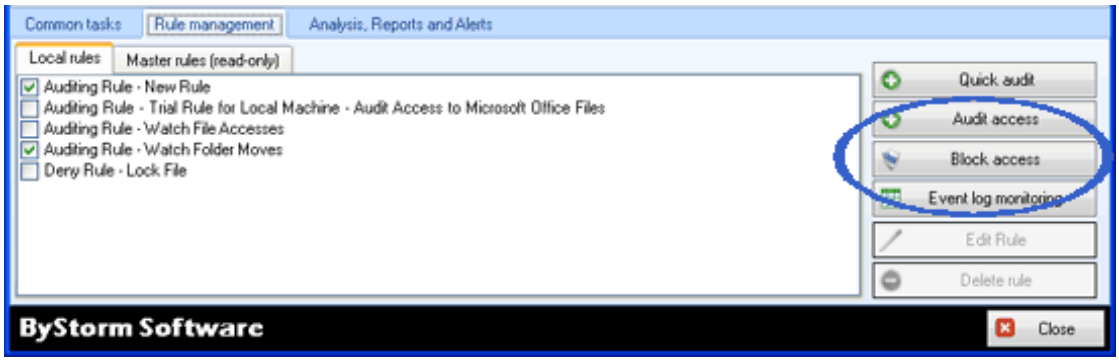
The Alert ID is written to the audit log if the associated rule matches. If you have a rule that matches *.doc files and the Alert ID is set to 223; whenever a doc file is read, the alert ID of 223 will be written to the audit log. Corresponding Alerts can be written to activate based on that ID, eliminating the need for complicated sql statements when creating an Alert.

Caution

Care needs to be taken when assigning Alert IDs:

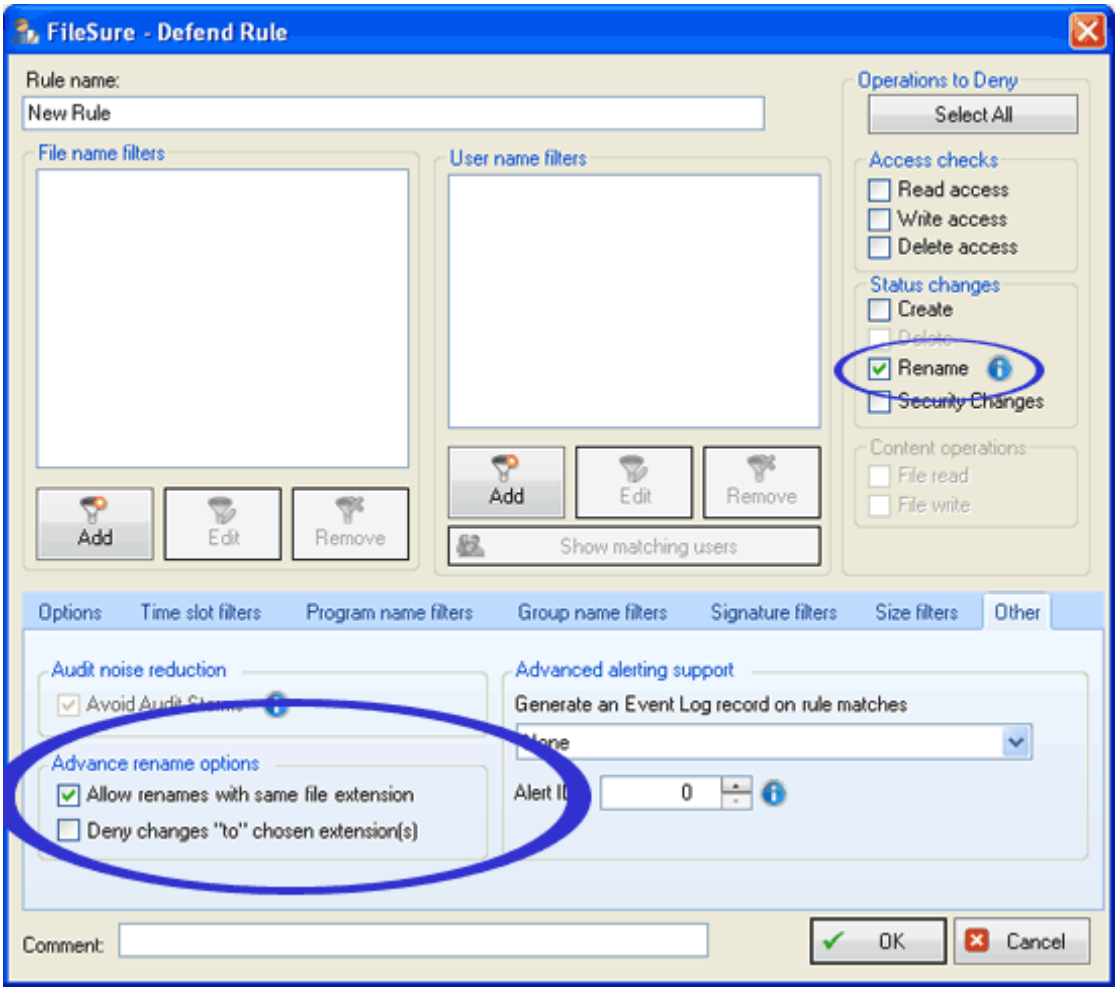
- Make sure the ID is not based on rules that overlap. For example, you could have one rule to watch *.doc files and another to watch Office files. FileSure does NOT check all the rules but instead stops after finding the first matching rule. If the Alert ID was set to 223 on the watch *.doc rule, and the first matching rule was the Watch Office Files rule, the Alert ID would not be written
- Most of the time, Alert IDs should be unique. If you have 3 different rules with the same Alert ID, you won't be able to tell which rule generated the alert.

Block Access Button



If you upgrade to FileSure-Defend, this button allows you to configure rules which block access. Block Access Rules are designed the same as Audit Access Rules, but will actually *block* user access based on the criteria you have provided. Blocked access is also recorded in the auditing log.

Almost all the filter configuration choices are the same as with the Auditing Rules. One exception would be on the "Other" tab, Advanced Rename Options. It will look similar to the following figure:



Allow renames with the same file extension

When blocking renaming of files (by clicking "Rename" under operations to deny, above), you may choose to allow files to be renamed if they have the same file extension. So, text.doc could be changed to text1.doc.

Deny changes "to" chosen extension(s)

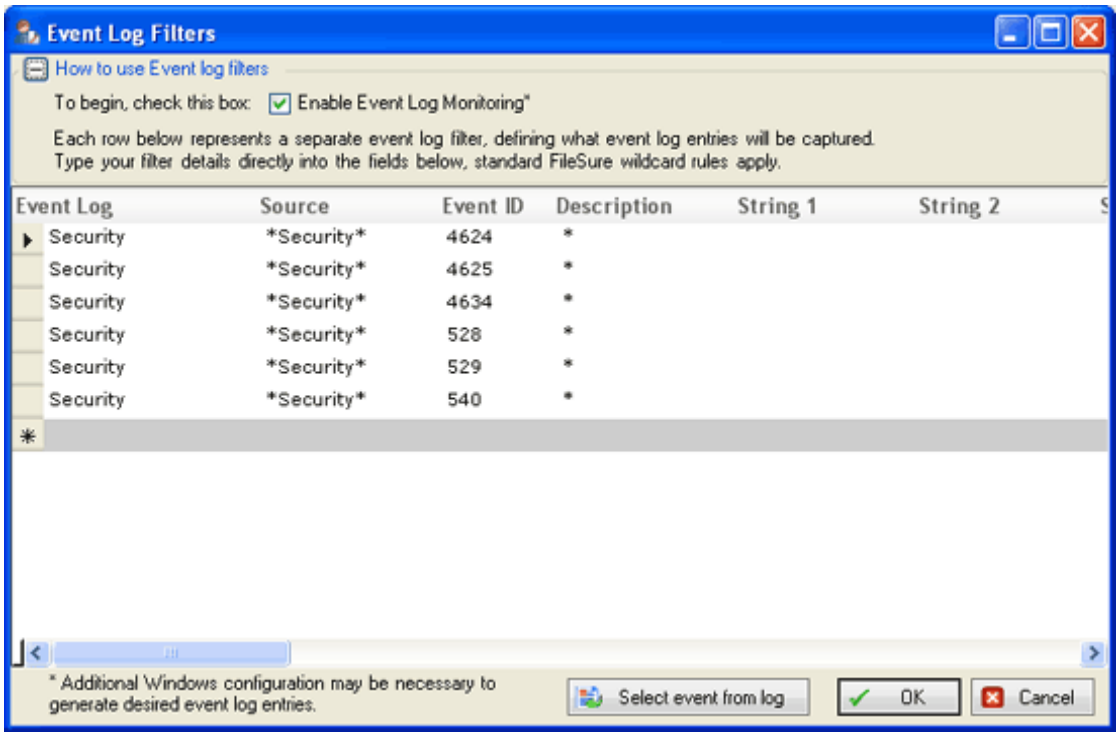
If *.xls were in the file name filter window above, renames of any files currently of the .xls type would be denied. Clicking this box would also deny any changes of files TO the .xls type. So, text.doc could not be changed to text.xls.

For more information on FileSure Defend, please visit www.bystorm.com.

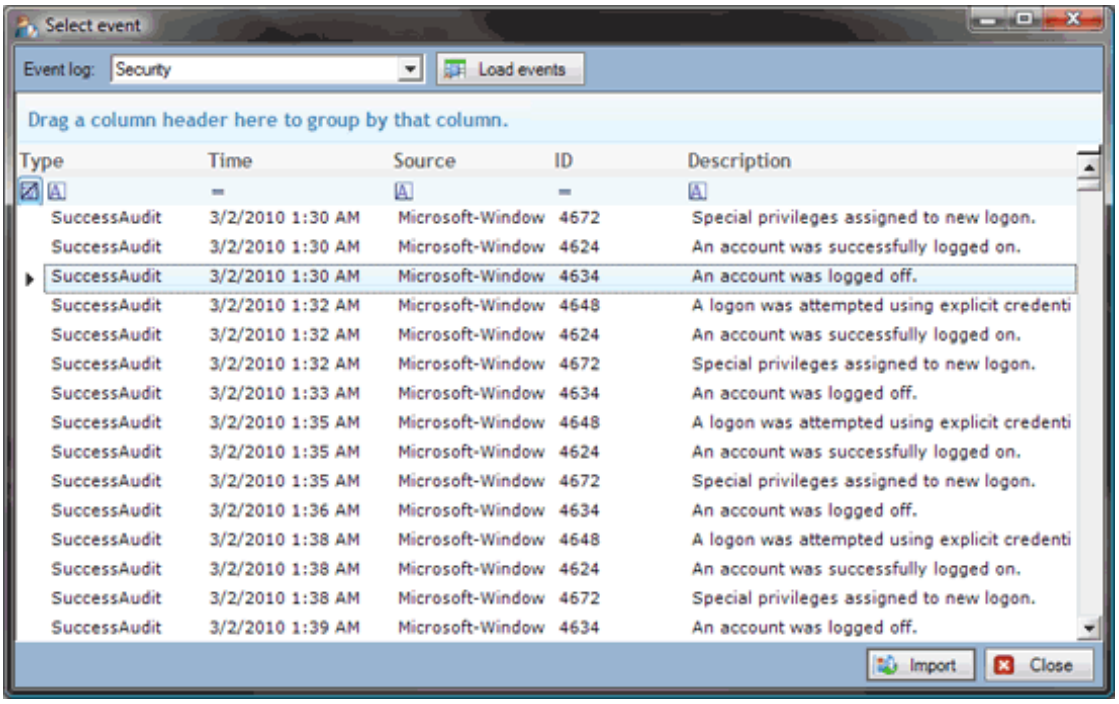
Event Log Monitoring Button

Choosing this button will open the Event Log Monitoring interface. Here you can choose Windows events to save with your auditing data and view within FileSure. Event log filters are managed by using an editable grid. Each row is a unique event log filter.

By defining what event log, source, event ID that you are interested in recording, FileSure can intercept and record those events in the datastore. The Source, Description and all the 'Replacement' strings fields support the standard FileSure wildcard matching system. The Event Log Monitoring interface resembles the image below:



You may also choose events to record by browsing the event log via the **Select event from log** button. That interface resembles the following:



Edit Rule Button

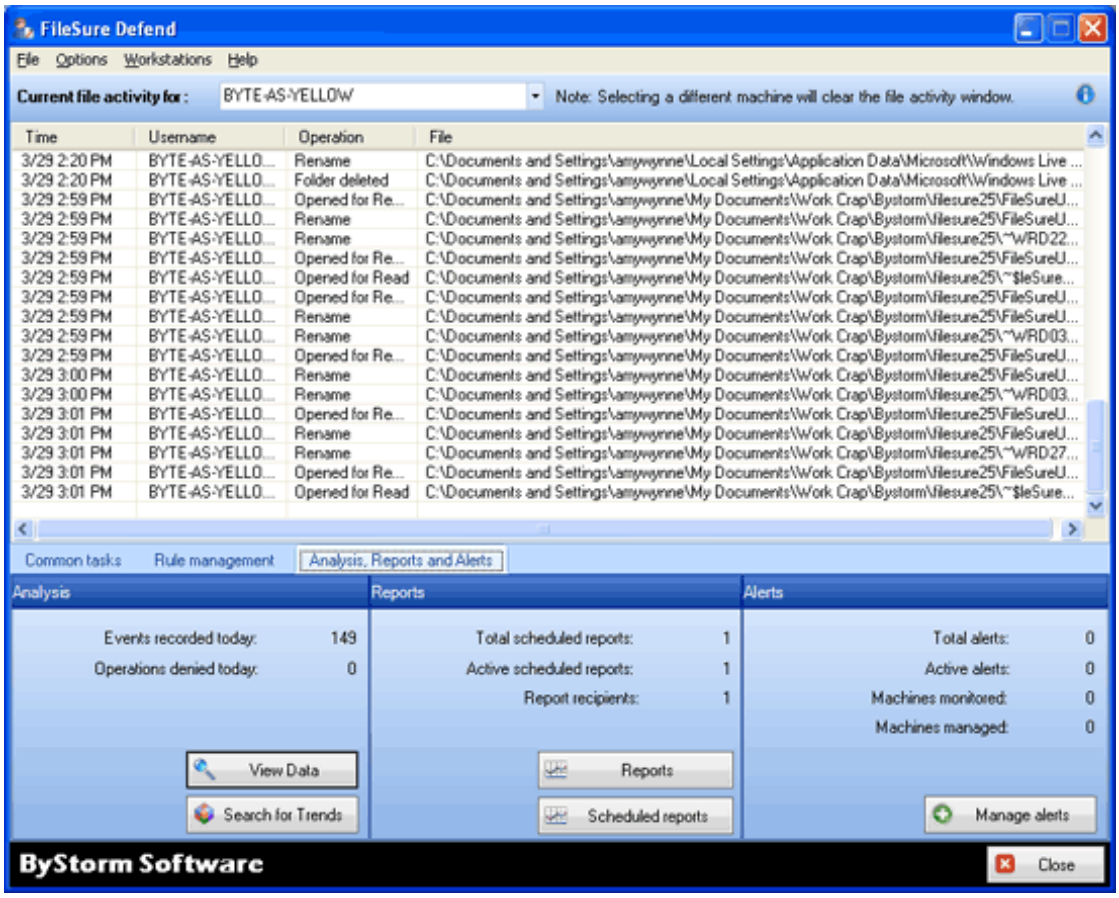
Selecting the Edit Rule Button opens the Advanced Rule interface for whatever rule is selected. If it is an Auditing Rule, the Auditing Rule window will open (and for a Block Access Rule, the Block Access Rule window will open, etc.), displaying all current configuration choices for that rule. You may edit any filter or performance choices, and clicking OK will save the new settings under the old rule name.

Delete Rule Button

Selecting the Delete Rule Button will delete any rule you have highlighted.

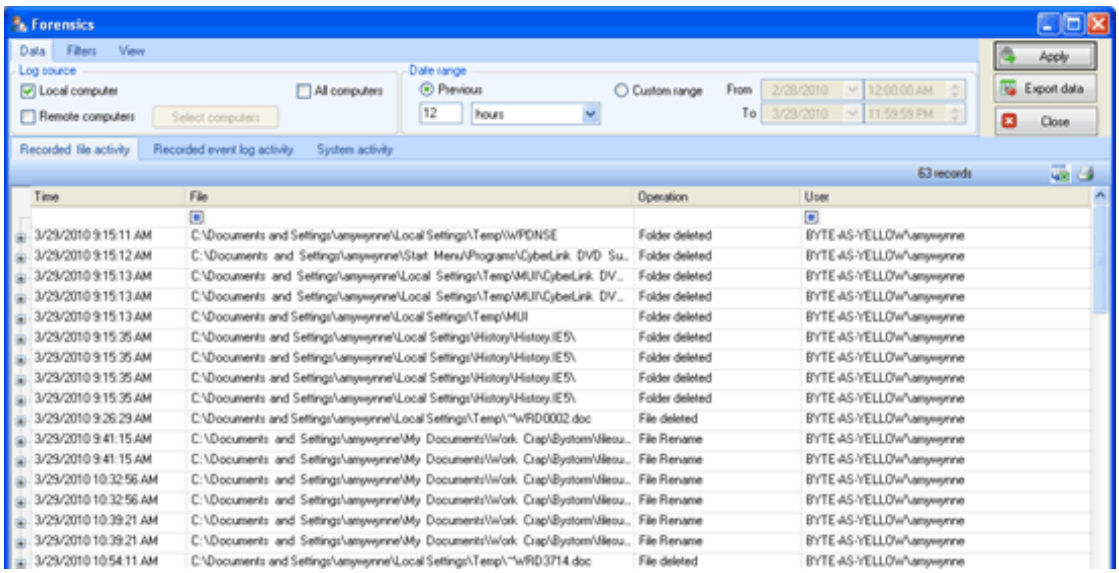
Analysis, Reports and Alerts Tab

The following figure is similar to the third tab on the main screen, or the Analysis, Reports, and Alerts Tab. Here you search data, configure reports, and define alerts.



Analysis Tab / View Data Button

Clicking on the View Data button allows deep exploration into audit data and export of selected information. The View Data interface is similar to the following figure:



Access high-powered filters through the tab control at the top of the window. The tabs are as follows:

Data Tab

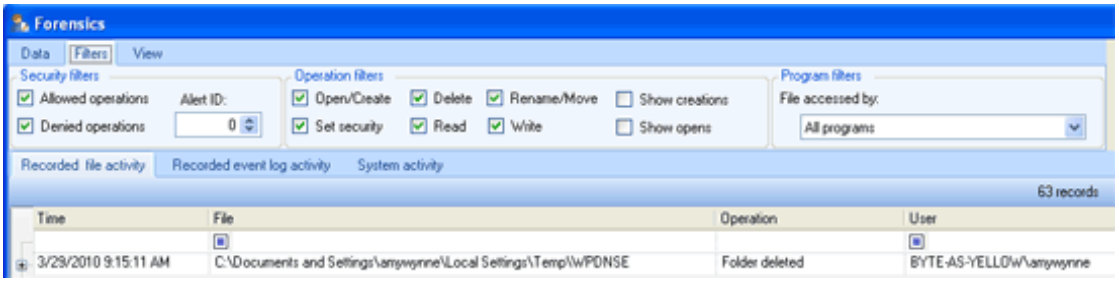
This is where you define the data source and the date range.

Log Source
Select either a local machine or a remote computer.

Date Range
Specify the time period from which to return file operations.

The Filters Tab

This tab has 3 filter groups: Security filters, Operation filters and Program filters, and is similar to the figure below.



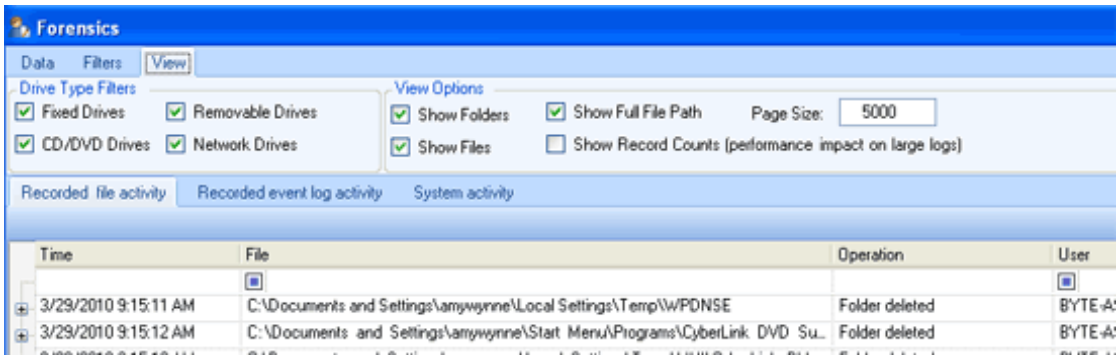
Security Filters
Make selections to show or hide data as it relates to its security status (denied, allowed, or related to a particular Alert ID).

Operation Filters
Make selections to show or hide data based on what type of record it is (a file rename, delete, open/create, etc).

Program Filters
Make selections to limit the data based on the program that actually accessed the data. This option has limited use on servers and is mostly intended for workstation logs since program name isn't recorded on remote file accesses (in other words, if you open a file on the network with WinWord, FileSure running on the server isn't going to know it was WinWord that was used to open the file).

View Tab

This tab offers two more choices to define your data query, and is similar to the following figure:



Drive Type Filters

Make selections to pinpoint operations on certain drives, like file writes to removable drives.

View Options

Choose whether or not to return and display the full file path in the query, choose between files or folders or both, show record counts, and determine output page size.

Returning View Results

To query the server and display all rule match data that agrees with the specified filter options, click **Apply**.

To export the results for use with other programs, such as Microsoft Excel, click **Export Data**.

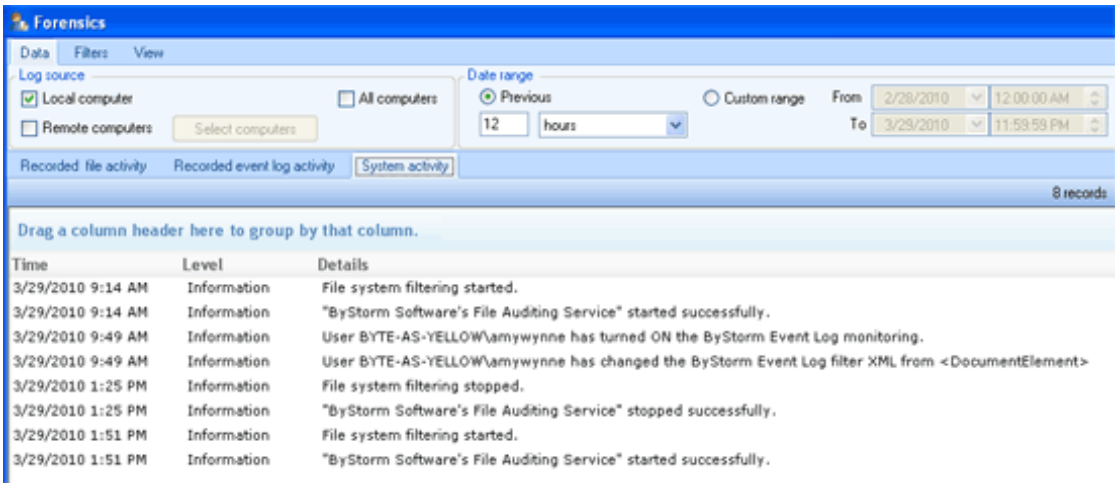
Recorded File Activity, Recorded Event Log Activity, and System Activity Tabs

Recorded File Activity is your logged data, based on the rules you've created.

Recorded Event Log Activity is any event log data you have chosen to collect via the Event Log Monitoring feature.

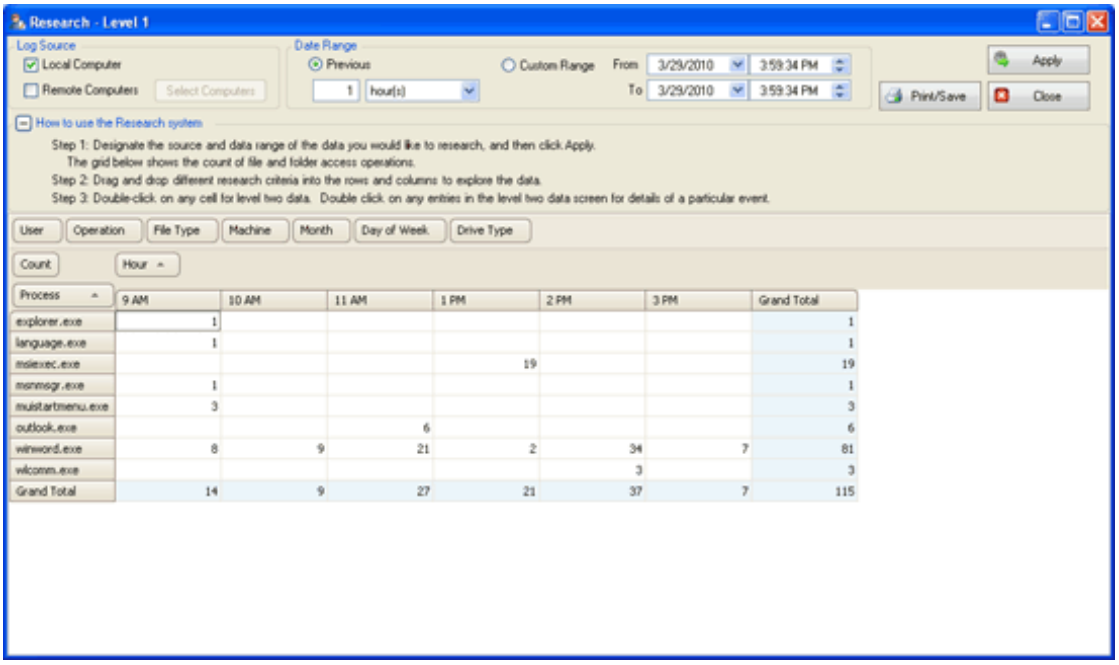
System Activity is FileSure system events written to the event log, broadcast to syslog servers and written to the datastore. These tabs let you choose to view either your file query activity, your recorded event log activity, or the FileSure system events of note that have occurred during the designated period.

A view with the System Events tab selected is similar to the following figure:



Analysis Tab / Search for Data Button

The **Search for Trends** Button allows you to easily research your data and discover abnormalities you wouldn't have otherwise seen. The Search for Trends interface resembles the image below:



Log Source

Select either a local machine or a remote computer.

Date Range

Specify the time period from which to return file operations.

To query the server and display all rule match data that agrees with the specified filter options, click **Apply**.

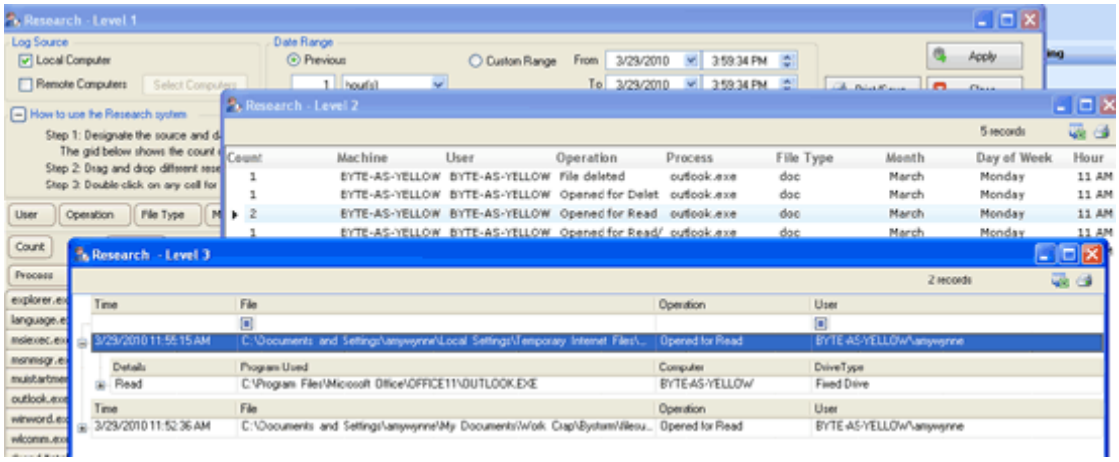
To print or save the results for use at another time, click **Print/Save**.

Research Criteria

Once the data is presented in the view screen, you can drag and drop several research criteria to better see trends and abnormalities. In the image above, twelve hours worth of file operations on a local machine are sorted by the processes that affected them and the time it happened.

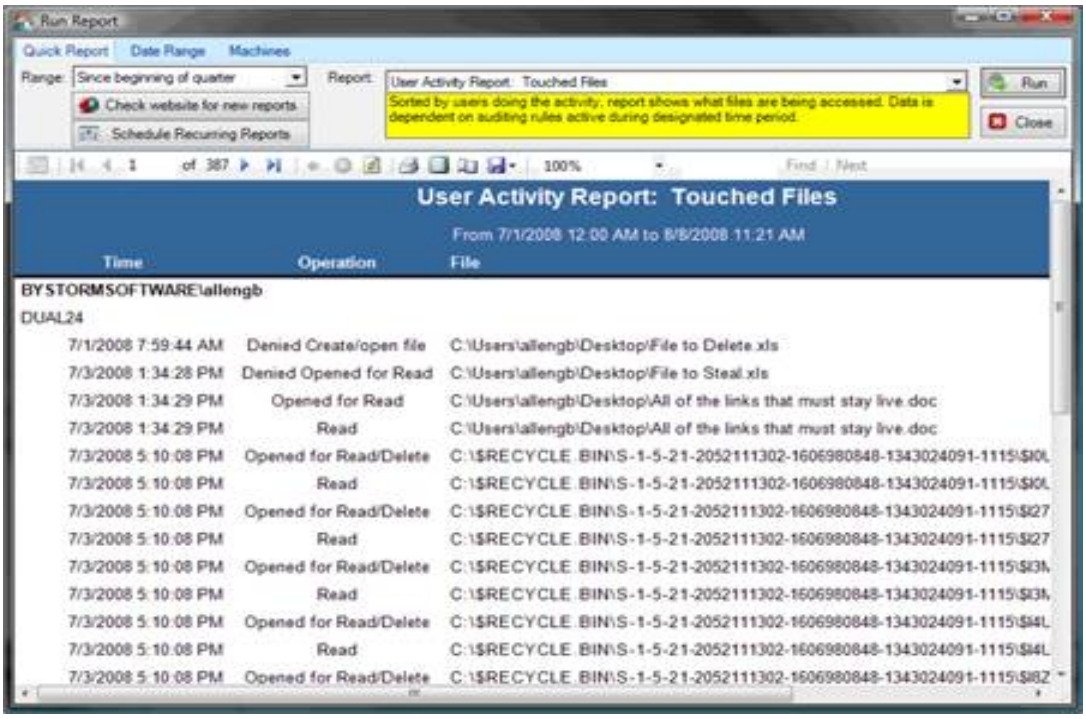
Three Levels of Drill-Down

Double-click on any item in the screen for level two data information. Double click on any item in the level two screen for level three specifics, similar to the image below:



Reports / Reports Button

The Reports section has access to both the **Reports** Button and **Scheduled Reports** Button. Choosing the **Reports** Button will give you the Reports window. This window allows you to query the results of past file auditing activities based on date and a pre-defined report setting. The information is returned in a report format, and can be printed or exported in Microsoft Excel or Adobe Acrobat format. The Reports window looks similar to the picture below.



There are three tab choices available in configuring a report, as follows:

Quick Report Tab

Uses set date ranges and predetermined reports to quickly return the information you are seeking.

Range

Specifies the time period during which to report on file operations that matched enabled rules.

Report

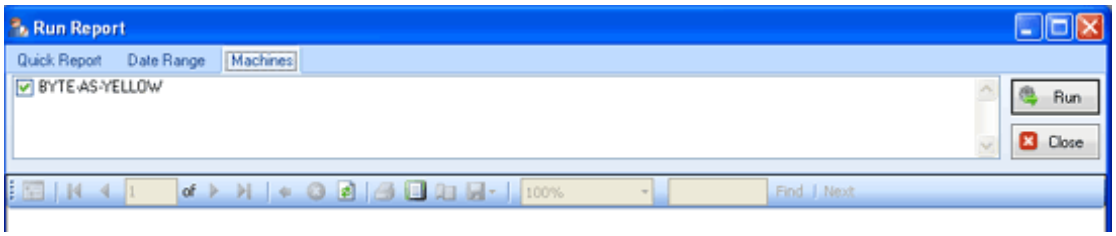
Specifies the parameters of the query that will be returned, and how the information will be displayed. New reports are added periodically, and can be added at your request. New reports are easily found by clicking **Check Website for New Reports.** Report descriptions appear below the pick list box when you select a report.

Date Range Tab

Similar to the figure below, the Date Range Tab gives a full range of date and time choices for setting your report parameters.

Machines Tab

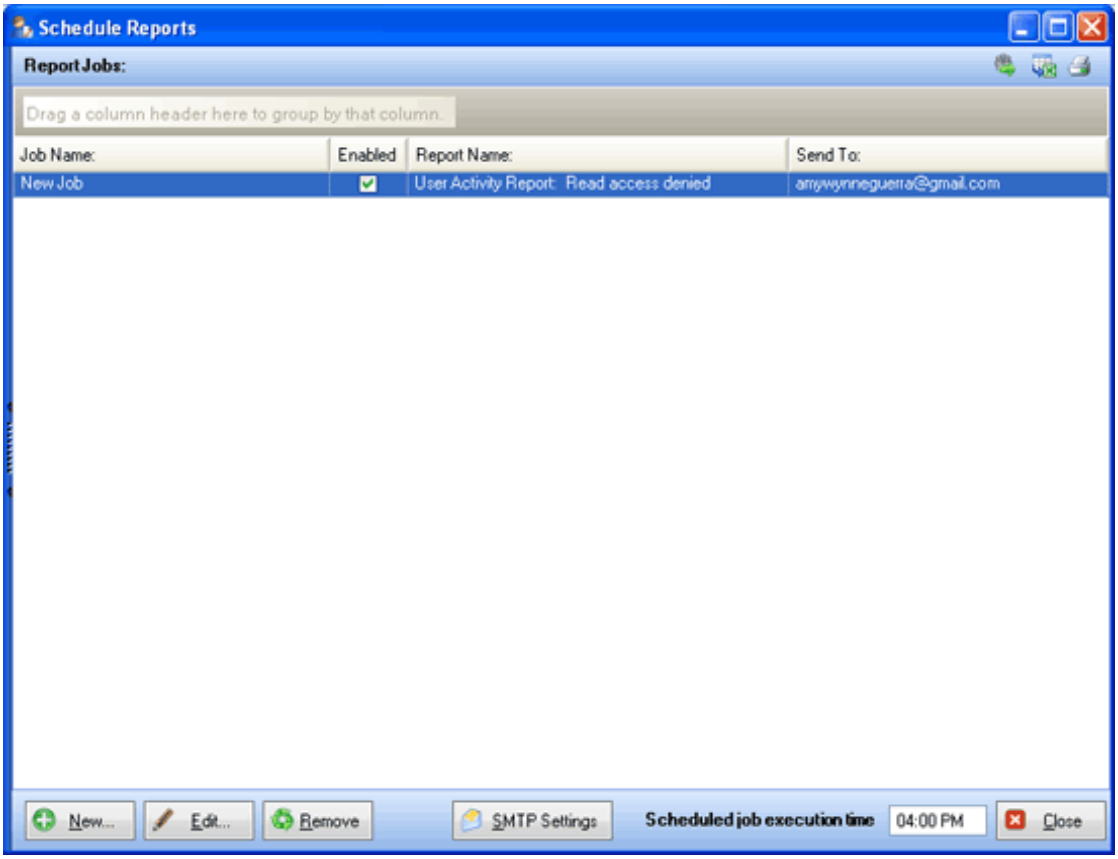
Similar to the figure below, the Machines Tab allows for selection of the source of the data you would like the report to pull from. The available sources will be the local machine and all slaves using this machine as a master.



To query the server and display all rule match data that agrees with the specified report options, click **Run**.

Reports / Scheduled Reports Button

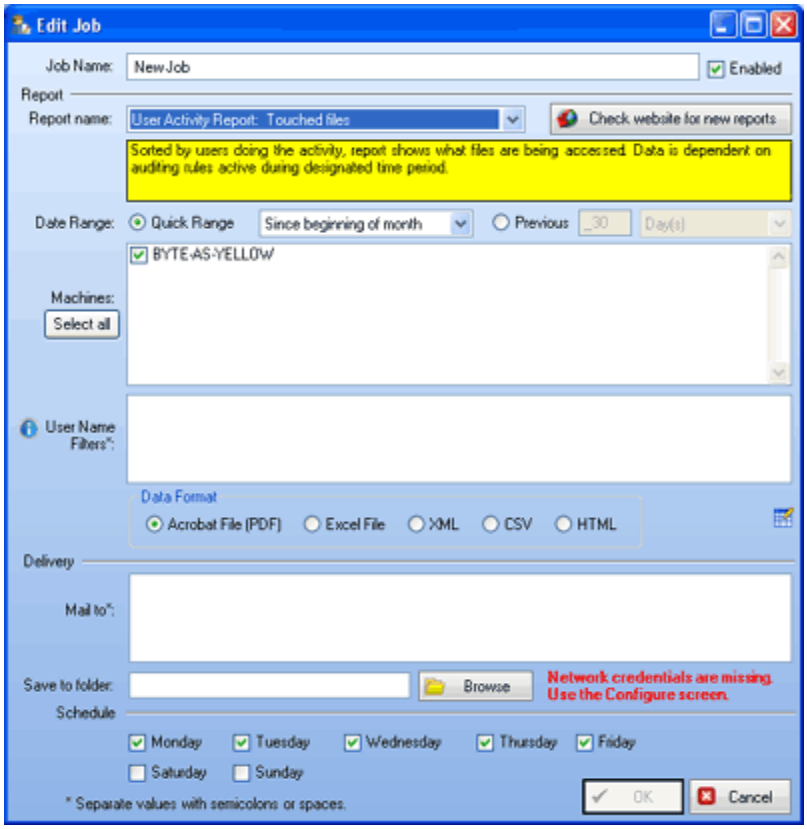
Choosing the Scheduled Reports Button from the Reports section allows creation and management of recurring emailed reports. The interface is similar to the following figure:



In the Job window, all preconfigured and scheduled reports available are listed. You can then enable or disable those reports. To set up a report, use the buttons at the bottom of the dialog.

New or Edit Buttons

Choosing New or Edit will bring up a similar dialog, allowing you to specify the criteria for the report you want to have scheduled. The dialog is similar to the figure below:



Job Name

Create a name for this scheduled report, will be what is listed in the Job window for enable/disable function.

Report Name

Specifies the name of the report that will be used in this recurring job. New reports are added periodically, and can be added at your request. Report descriptions appear below the pick list box when you select a report.

Date Range

Specifies the time period during which to report on file operations that matched enabled rules.

Machines

Select the machines whose usage data you want included in this report. The machine choices will be the local machine and managed workstations.

User Name Filters

Limit the report to only apply to certain users if you choose. FileSure wildcard characters apply, click "i" for help.

Data Format

Reports may be emailed in several different formats.

Mail to:

Designate email addresses to receive reports, separating multiple addresses with semicolons or spaces.

Save to Folder

Designate a folder if you would also like reports saved to a central location when the scheduled report is run.

Schedule:

Select which days you want the reports run/sent.

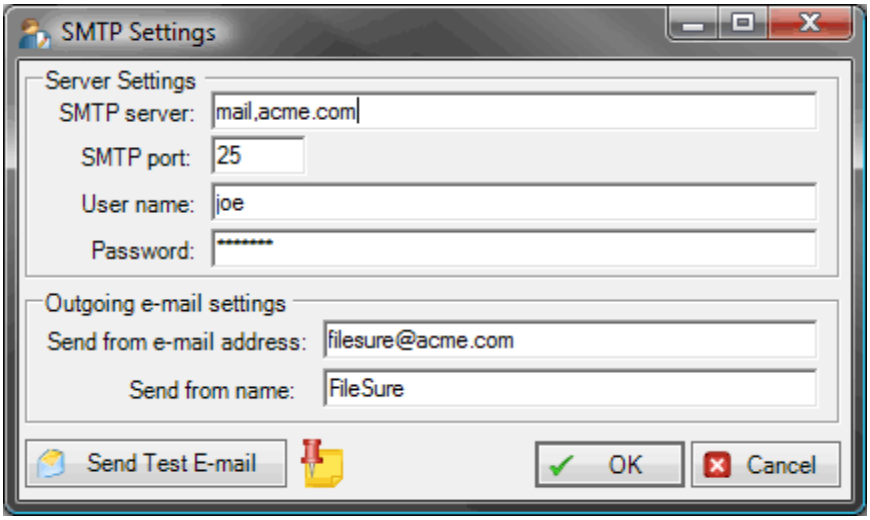
Note:
The small grid button to the right of the Data Format section is an advanced feature. It allows for the OVERRIDE of the default sql query for that report. Please contact customer support if you need assistance with custom reports.

Remove Button

If you have a job selected in the Job window, you can then delete that job and all associated scheduling by clicking the **Remove** button.

SMTP Settings Button

A one-time set-up for all scheduled reports (and alerts), this interface, similar to the figure below, tells FileSure how to deliver all the scheduled emails.



Server Settings

Tell FileSure how to access your mail server to send scheduled reports and alerts.

Outgoing E-mail Settings

Designate a “from” address and a “from” display name for the mail that FileSure sends.

Send Test E-mail

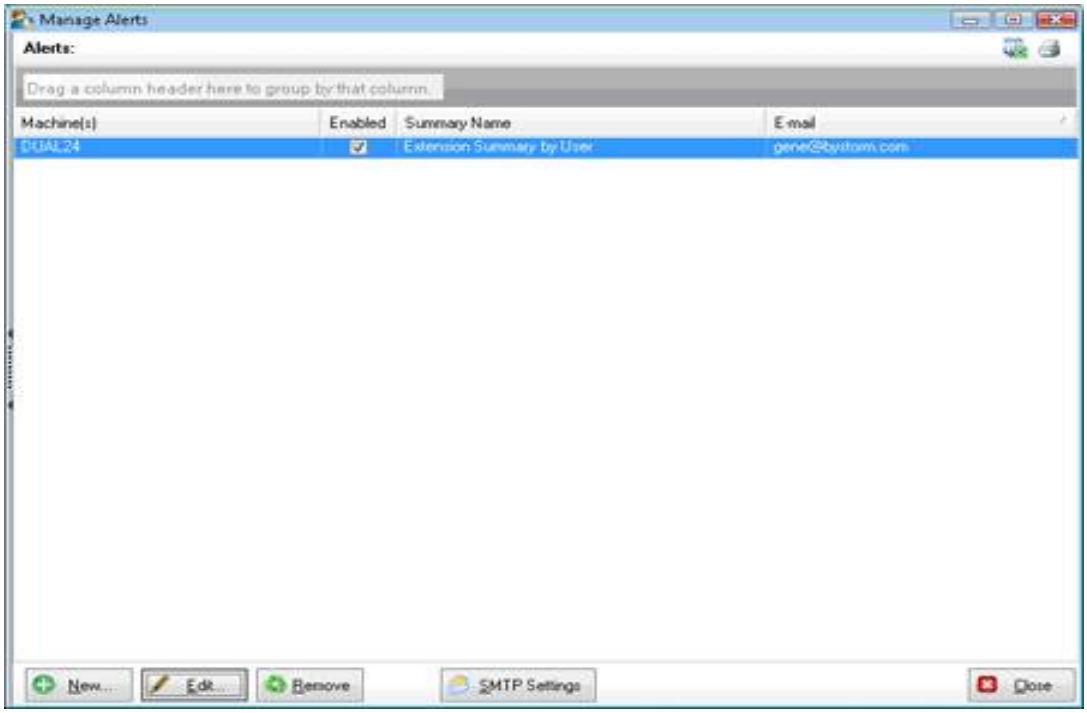
Clicking this sends a test email TO the assigned “from” address. Please use a mail client to check and see if the send was successful.

Set the **Scheduled Job Execution Time** in the bottom right corner.

View a current version of the report from any scheduled job by highlighting the job in the Job window and clicking on the first icon in the upper right corner (the **Run Job Now** icon). You may also **Export** the report or **Quick Print** from the other two icons.

Alerts

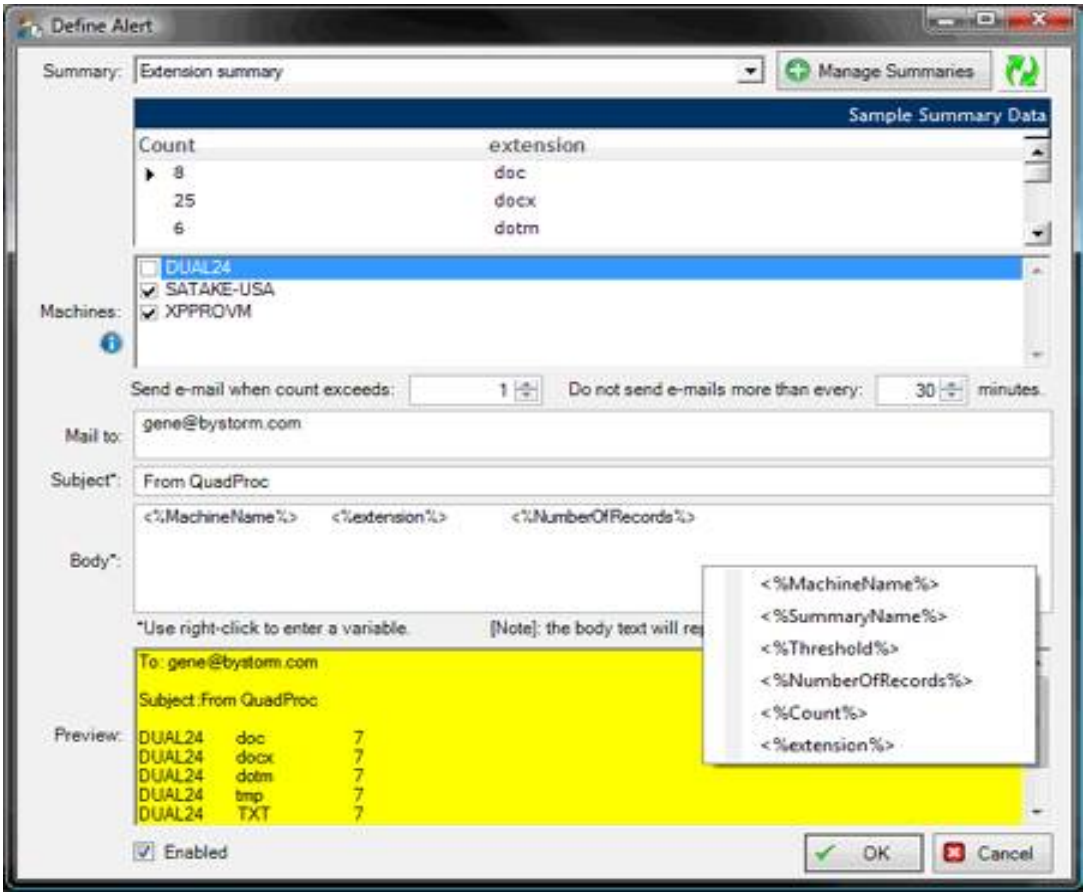
Alerts are e-mails that are sent when a "threshold" is met. Clicking the alerts button will launch the Manage Alerts dialog, similar to the figure below:



The figure shows one alert defined, enabled, and selected. You can enable and disable the alert by clicking the **Enabled** checkbox. To set up an alert, use the buttons at the bottom of the dialog.

New or Edit Buttons

Choosing New or Edit will bring up the Define Alert dialog, allowing you to specify the criteria for the alert you want to define. The dialog is similar to the figure below:



Summary

Select from a drop down list of published summaries. Summaries are published by the FileSure Service and are data queries upon which thresholds may be set to generate the alerts. Summaries can be managed via the **Manage Summaries** button and you can refresh the drop down via the **Refresh icon**. Please see the next section for the Summaries interface.

The Sample Summary Data area will be populated based on the LOCAL FileSure Service.

Machines

The Machines list shows the current machine and all the currently managed workstations. The Alert will be based on activity from all checked machines.

Mail to

Designate email addresses to receive the alerts, separating multiple addresses with semicolons.

Subject and Body

Designate a subject and a body for the e-mail alert. Both the subject and the body fields allow you to insert a variable that will populate the field with dynamic information from the specific alert event. You can access the variable list via a right click.

There are 4 built in variables:

- <%SummaryName%> --- the summary name (in our example….Extension Summary by User)
- <%Threshold%> -- the threshold amount (in our example….5)
- <%NumberOfRecords%> --- the number of records that PASS the threshold
- <%MachineName%> -- the machine that the summary came from

The rest of the variables come from the summary, so in our example, <%Count %>, <%userName%>, <%extension %>.

Preview

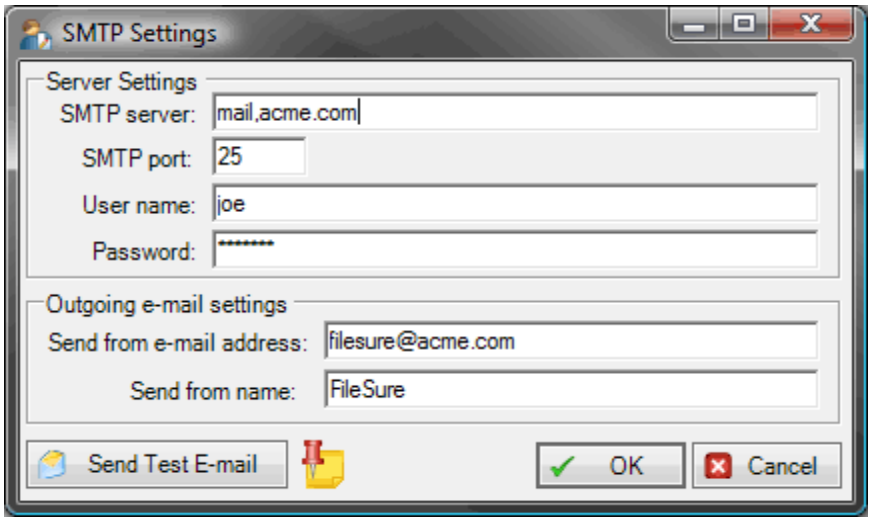
Allows preview of the alert formatting with information pulled from the local machine.

Remove Button

If you have an alert selected on the manage alerts dialog, you can then delete that alert by clicking the **Remove** button.

SMTP Settings Button

A one-time set-up for all scheduled alerts (and reports), this interface, similar to the figure below, tells FileSure how to deliver all the scheduled emails.



Server Settings

Tell FileSure how to access your mail server to send scheduled reports and alerts.

Outgoing E-mail Settings

Designate a “from” address and a “from” display name for the mail that FileSure sends.

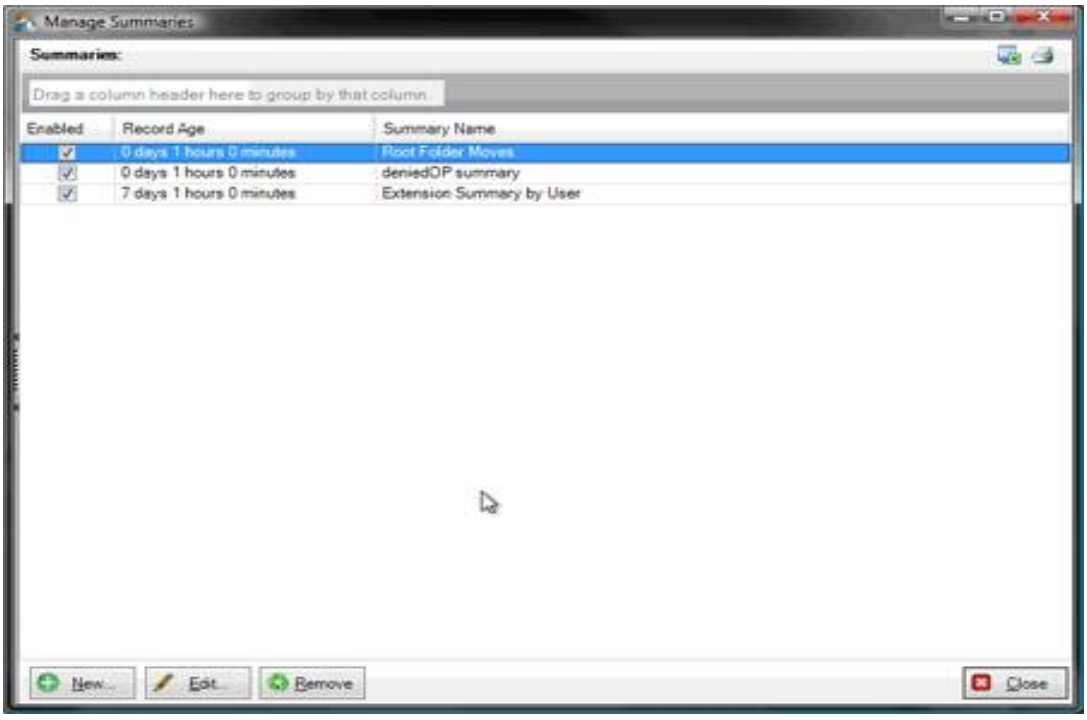
Send Test E-mail

Clicking this sends a test email TO the assigned “from” address. Please use a mail client to check and see if the send was successful.

Export saves the grid as a Microsoft Excel file. You may also **Quick Print** from icons in the upper right corner of the Manage Alerts dialog.

Summaries (found within the Alerts interface)

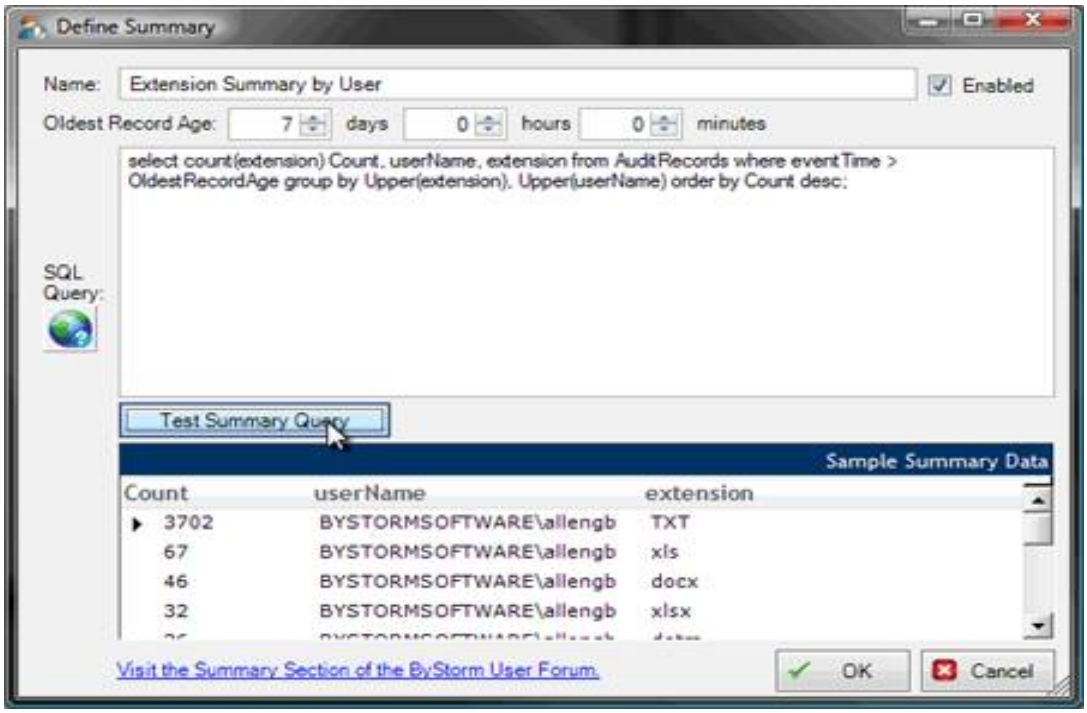
Clicking the alerts button will launch the Manage Alerts dialog, similar to the figure below. It lists all the summaries, record age and whether or not they are enabled.



You can enabled or disable the summary with the **Enabled** checkbox. Enabled summaries are published by every machine running FileSure, disabled summaries are not published. To set up a summary, use the buttons at the bottom of the dialog.

New or Edit Buttons

Choosing New or Edit will bring up the Define Summary dialog, allowing you to create or change a summary. The dialog is similar to the figure below:



Name

Create a name for the summary which will be displayed in the list of choices on the Manage Alerts interface.

Oldest Record Age

Indicate how far back in the audit log you want to pull data for your summary.

SQL Query

Enter the SQL query to deliver the desired results in this field. For help with this, see "Defining a Summary" in Chapter 3 of this User Guide.

Test Summary Query

View sample data from the query you have designed pulled from the local machine.

Remove Button

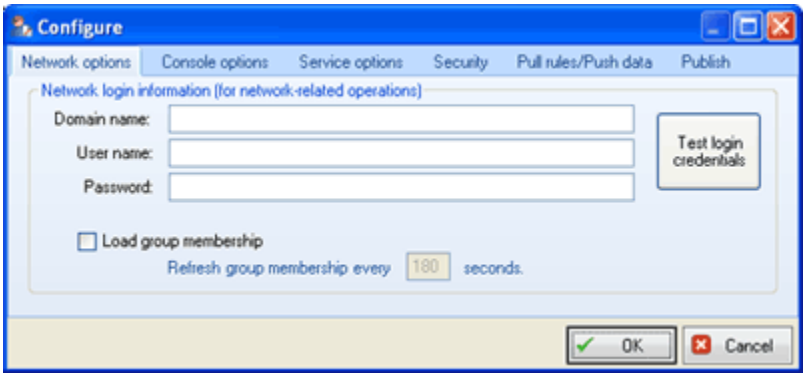
If you have a summary selected on the manage summaries dialog, you can then delete that summary by clicking the **Remove** button.

Options Menu→The Configure Interface

The Configure window allows you to specify several configuration options. The Configure window can be found by accessing the top menu, under Options. The following sections summarize the tabs on the Configure window.

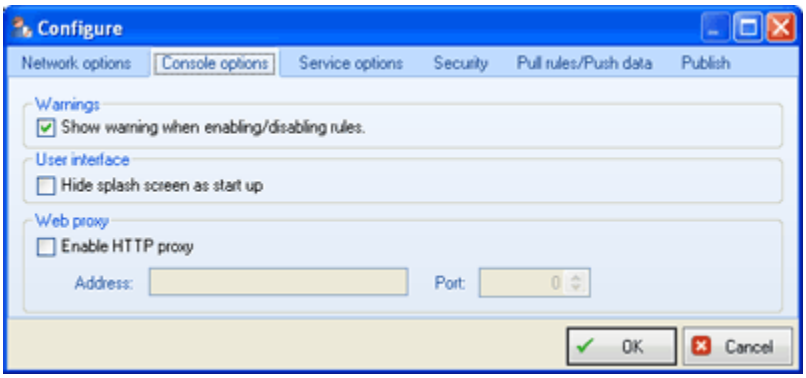
Network Options Tab

The Network Options tab of the Configure window allows you to specify the credentials that FileSure will be used to make network connections; these credentials will be used by the local instance of FileSure, slave FileSure servers and managed FileSure workstations. The Network Options tab is similar to the following figure.



Console Options Tab

The Console Options tab is similar to the following figure.



The fields on this tab are defined as follows:

Warnings

Specifies whether FileSure displays a confirmation message when a user enables or disables a rule.

User Interface

Turn on or off the ByStorm Software splash screen upon startup. This is a very handy if you're remote controlling FileSure over a slow link.

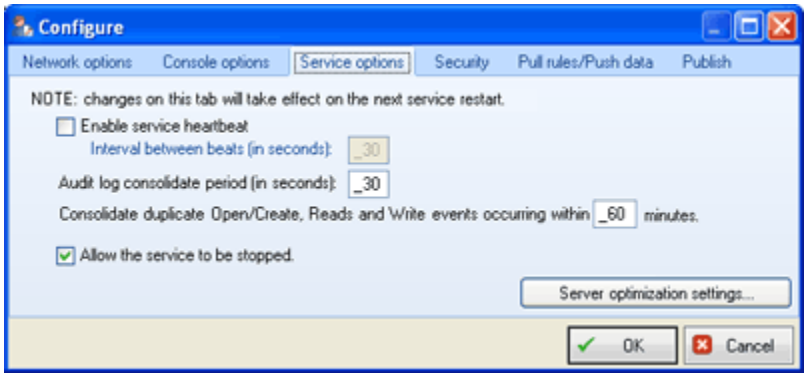
Web Proxy
Extends use of FileSure in environments using a Web Proxy server.

Service Options Tab

The Service Options tab of the Configure window allows you to specify heartbeat and audit log consolidation settings. You can also specify the time period during which FileSure ignores duplicate events. During the specified time period, if the same user opens the same file with the same permissions more than once, FileSure records only the first file access.

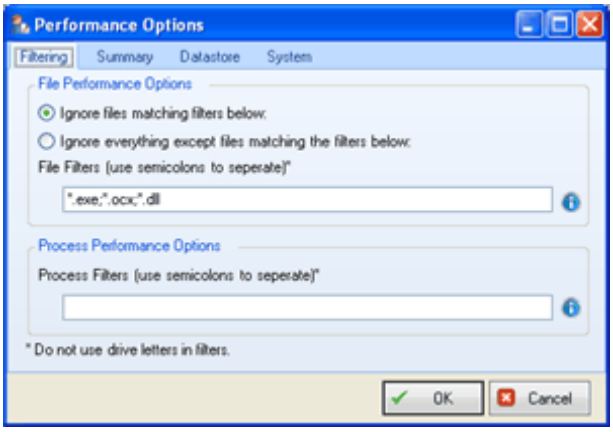
For additional security, if you would like to make it so no user can stop the FileSure service; uncheck the box that allows the service to be stopped.

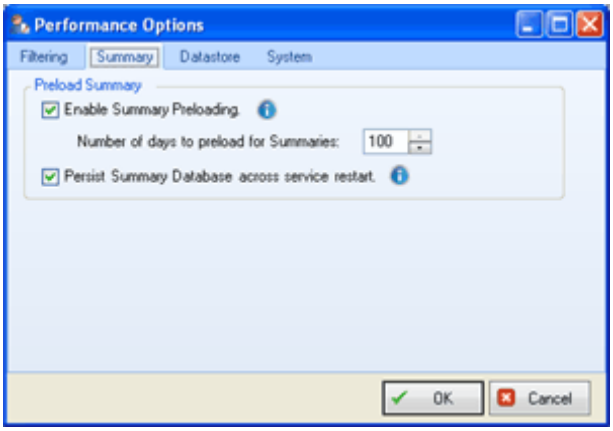
If you change any settings on this tab, you need to stop and restart the FileSure service for your changes to take effect. The Service Options tab is similar to the following figure.

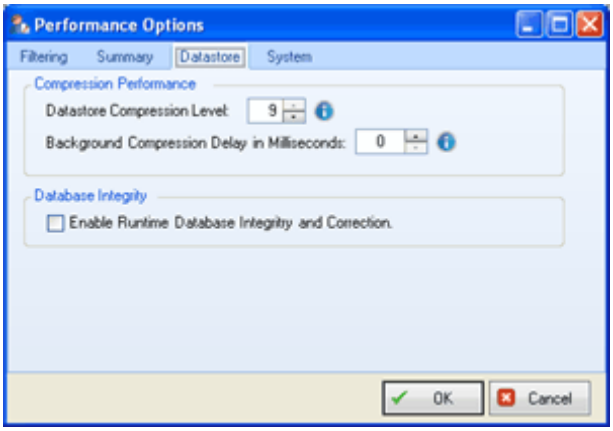


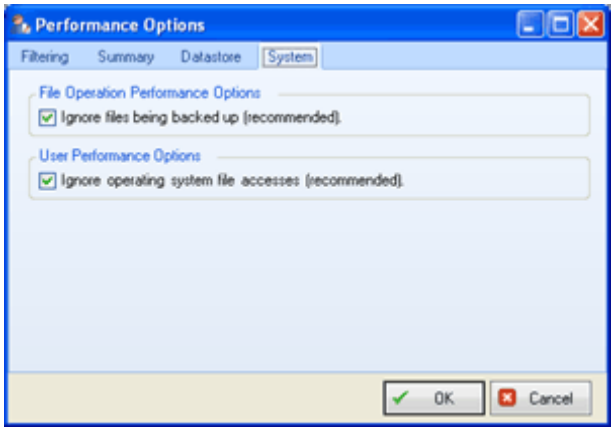
Server Optimization Settings Window

Also found on the Server Options Tab (pictured above) is a button to access the Server Optimizations Window. The choices on this window allow you to further reduce auditing noise and increase overall system performance by filtering out common types of file accesses that do not generally hold any bearing on file security—such as system-generated file accesses. It also allows advanced options for summaries that affect their availability for alert queries, and allows you to control the level of compression of your data stores. The Server Optimizations Window is similar to the following figures:


Performance Options
Filtering
Summary
Datastore
System
File Performance Options
Ignore files matching filters below:
Ignore everything except files matching the filters below:
File Filters (use semicolons to seperate)"
.exe;.ocx;*.dll
Process Performance Options
Process Filters (use semicolons to seperate)"
* Do not use drive letters in filters.
OK
Cancel


Performance Options
Filtering
Summary
Datastore
System
Preload Summary
Enable Summary Preloading.
Number of days to preload for Summaries:
100
Persist Summary Database across service restart.
OK
Cancel

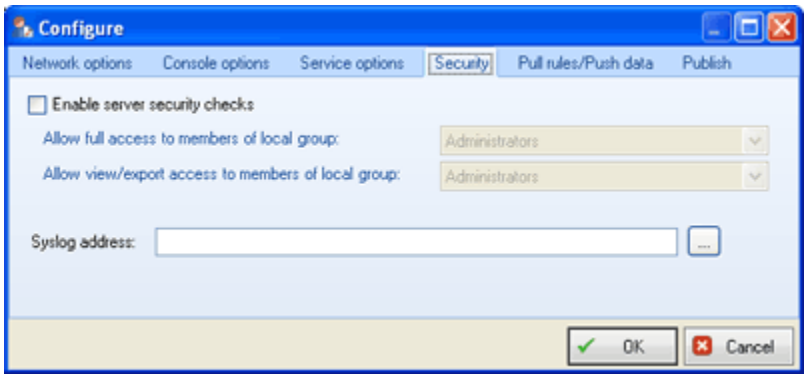

Performance Options
Filtering
Summary
Datastore
System
Compression Performance
Datastore Compression Level:
9
Background Compression Delay in Milliseconds:
0
Database Integrity
Enable Runtime Database Integrity and Correction.
OK
Cancel



Security Tab

The Security tab of the Configure window allows you to specify who can change rules and who can view previously recorded audit data. Local groups provide access control levels. By default FileSure broadcasts syslog messages to "ALL;" if you would like to focus this, enter the IP address of your syslog here.

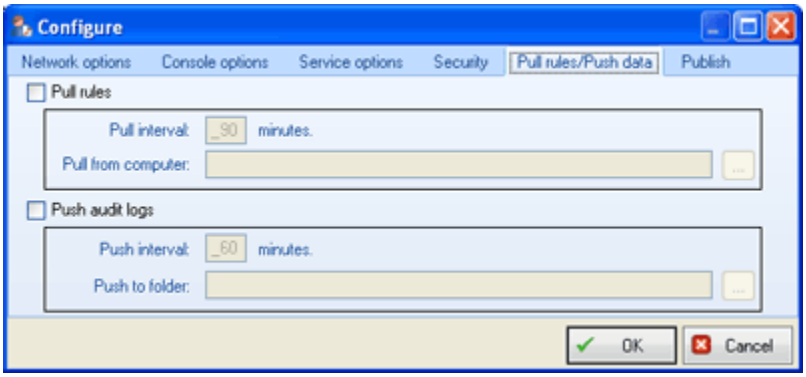
The Security tab is similar to the following figure.



Pull Rules/Push Data Tab

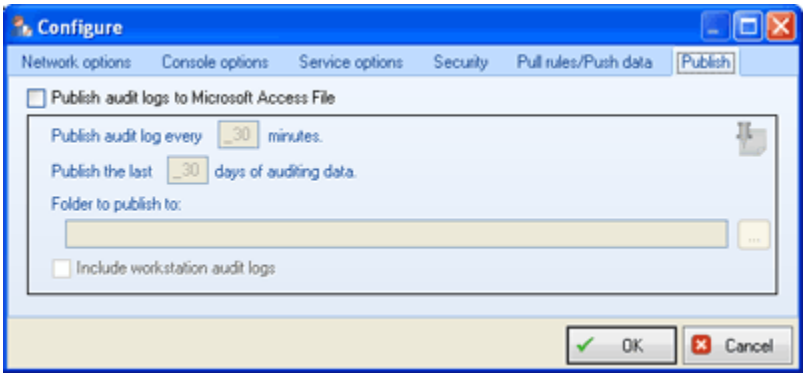
The Pull Rules/Push Data tab of the Configure window allows you to specify whether you import rules from a master server. The imported rules are shown on the Master Rules tab of the Main window and you cannot edit them. On the master server, these rules are shown on the Local Rules tab and you can edit them.

This tab also allows you to specify whether you want to back up audit logs to a remote location. You can specify a folder on a remote computer using a UNC specification, such as *computer**share*. FileSure will take saved audit log files and copy them at your chosen interval to the location you designate. The Pull Rules/Push Data tab is similar to the following figure.



Publish Tab

The Publish tab of the Configure window allows you to specify whether FileSure publishes audit data to a Microsoft Access file. To ensure data integrity, FileSure deletes the existing Access file and recreates it with the complete data on the defined interval. The Publish tab is similar to the following figure.



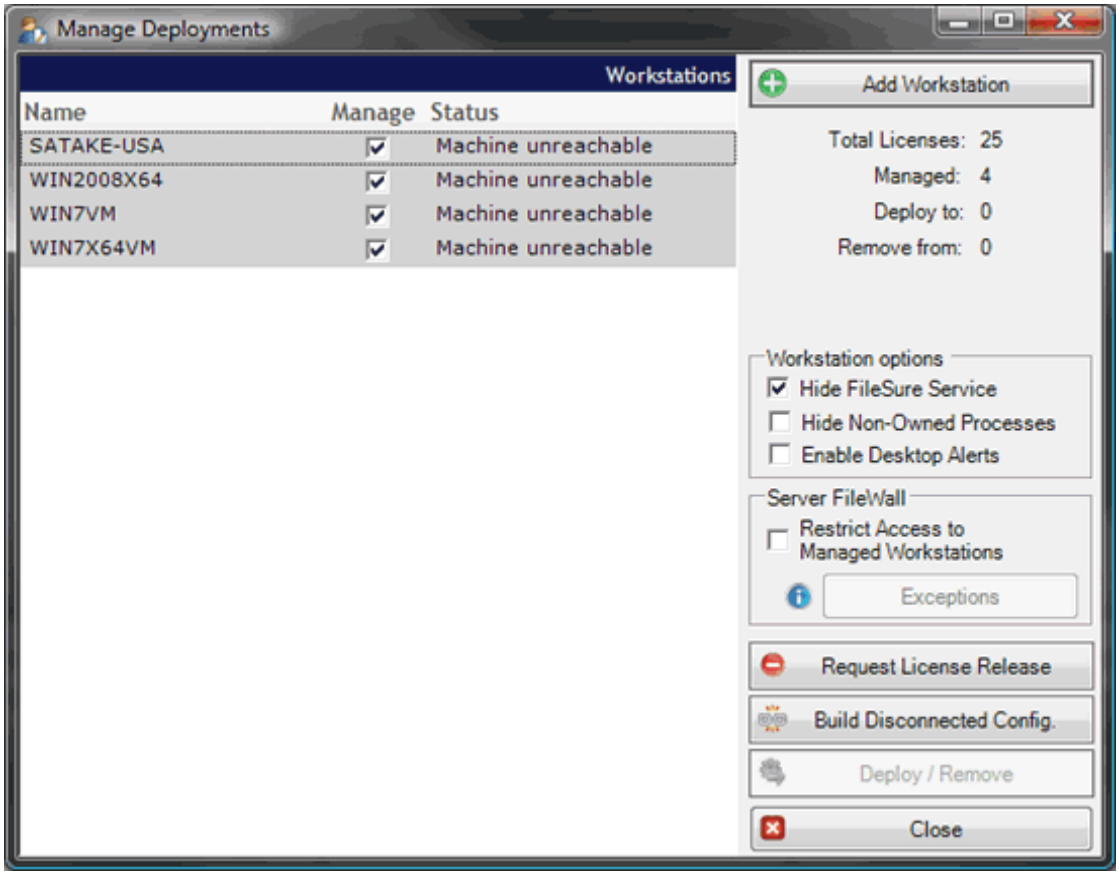
You can include workstation audit logs in the Access file by checking the Include workstation audit logs box.

If you want to use the Web Console to allow real-time viewing of the contents of the Access file on your intranet, please see “Using the Web Console” section of this document on page 27.

Workstations Menu→The Manage Interface

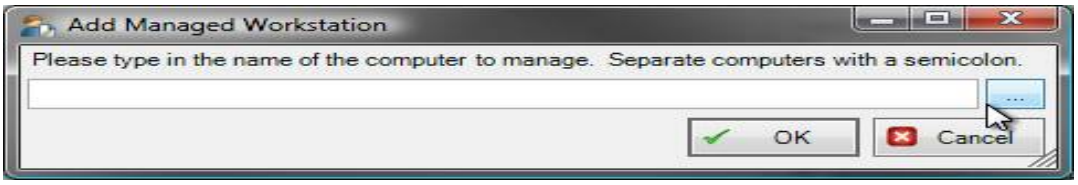
A FileSure license can support X number of workstation licenses if you have upgraded to FileSure Workstation. You add workstations and manage them through this interface.

The architecture of 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. The Manage Deployments interface looks similar to the following figure:



Add Workstation Button

Clicking Add Workstation gives you an interface similar to the figure below. You either browse or type in workstations on which you want FileSure deployed.



Workstation Process Protection

Enable or disable "Hide FileSure Service" with the first checkbox. Hiding FileSure on the workstations is an additional security level which masks FileSure from the workstation user. This protects the service from being discovered or killed via the Task Manager.

Enable or disable "Hide Non-Owned Processes" with the second checkbox. Hiding non-owned processes is similar to the first item but hides ***all*** tasks that are not owned by the user from showing up in the Task Manager.

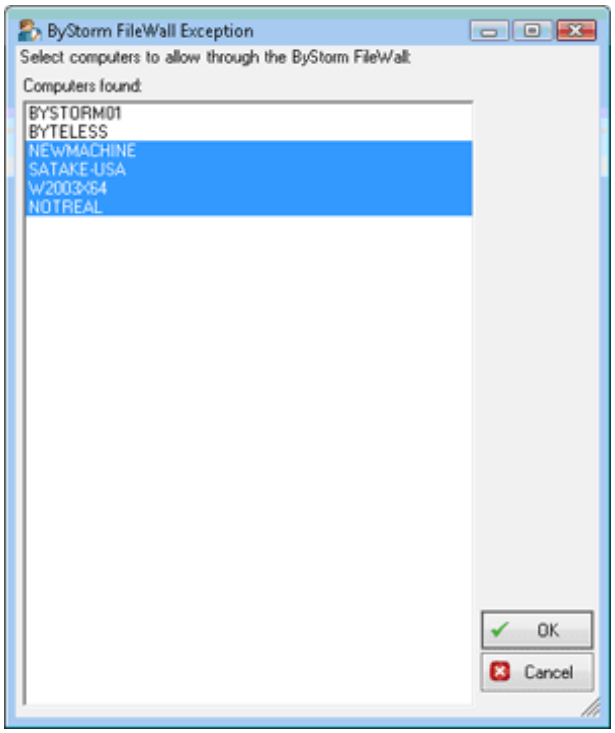
Server FileWall®

Enabling this checkbox engages the *ByStorm FileWall*®. Only managed workstations will be allowed access to the server. You can allow non-managed machines explicit access with the **Exceptions** button.

The ByStorm FileWall® only runs on Vista, Windows Server 2008, and above.

This feature prevents someone from engaging data theft by connecting an unauthorized computer on which FileSure is not deployed.

The **Exceptions** button dialog looks similar to the following:



Deploy/Remove Button

For any workstations listed in the display window and enabled (checked), FileSure will either deploy itself to that workstation and add it to the managed machines, or remove itself from that workstation and take it out of the list of managed machines.