Quick Start Guide

March, 2010

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, BYSTORM SOFTWARE LLC PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of ByStorm Software LLC, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of ByStorm Software LLC. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

© 2010 ByStorm Software LLC, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

ByStorm Software, the ByStorm Software logo, FileSure, and UFAT-Audit are trademarks or registered trademarks of ByStorm Software LLC or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

Chapter 1
What Can FileSure Do for You? **1**

Chapter 2
Getting Started Quickly **3**
Preinstalled Sample Rule 3
View Your Data 5
Real Time File Activity Monitor 5
View Data, Search for Trends, and Create Reports 6

Chapter 3
Successfully Using FileSure **9**
Adding Your Own Rules 9
Common Tasks 10
Custom Rules 10
Configuring FileSure 11

Chapter 1

What Can FileSure Do for You?

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.

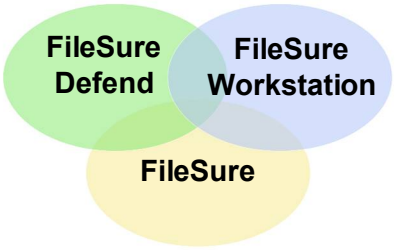
A solution that ignores internal threats to IP—employees who can read, change, rename, and delete sensitive files.

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.

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.

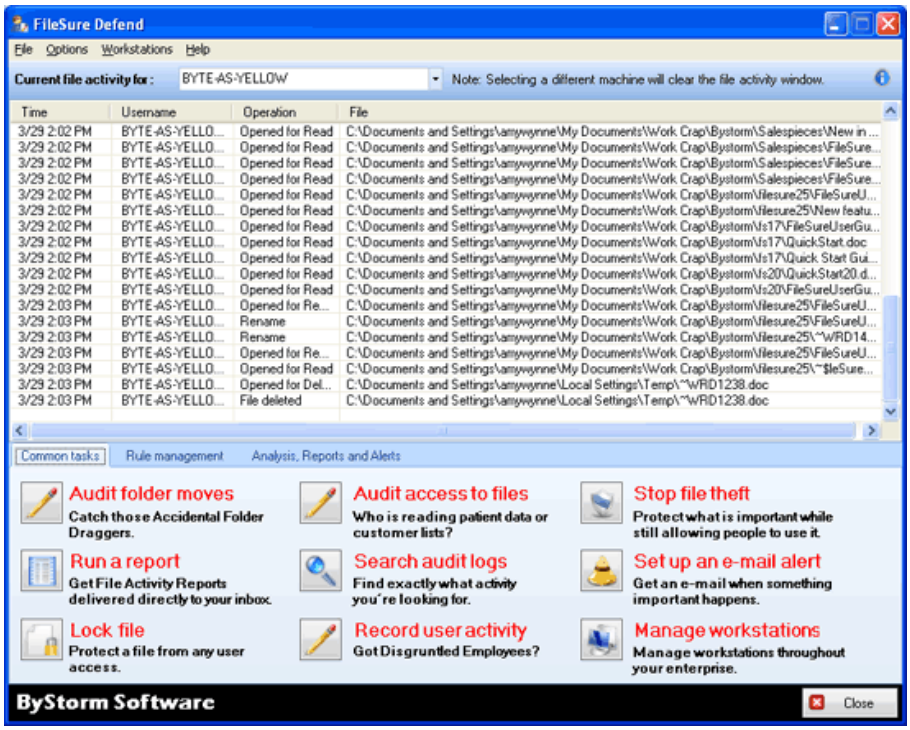
Chapter 2
Getting Started Quickly

It takes almost no time to see FileSure in action. This guide will quickly show you how FileSure captures file accesses and how you can view the resulting information. This QuickStart Guide is focused on the main auditing functions of the standard version of FileSure. Please see the Common Tasks section on page 9 for a note about FileSure Defend and Workstation.

Note
For detailed instructions on using FileSure, please see the User Guide located under the Help Menu in the product.

Preinstalled Sample Rule

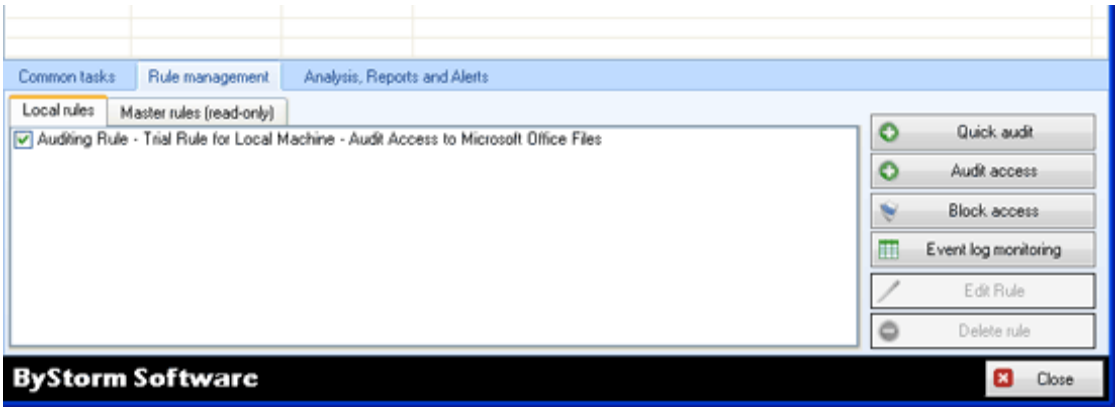
Once you've installed and opened FileSure, you should be looking at a window similar to the figure below.



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

To find the sample rule:

1. Choose the Rule Management Tab from the middle of the main interface. In the Local Rules screen you will see: "Trial Rule for Local Machine - Audit Access to Microsoft Office Files."
2. **Note that the checkbox next to this rule is enabled.** This rule is defining which ones, out of all the file operations happening on your machine, are being recorded to FileSure's audit log files.



Any time you access any Microsoft Office files, FileSure will be recording the activity. Try a few different activities to any Microsoft Office files you have such as renaming, moving, deleting, changing file security settings, etc. The next section tells you how to view your file access data.

Note

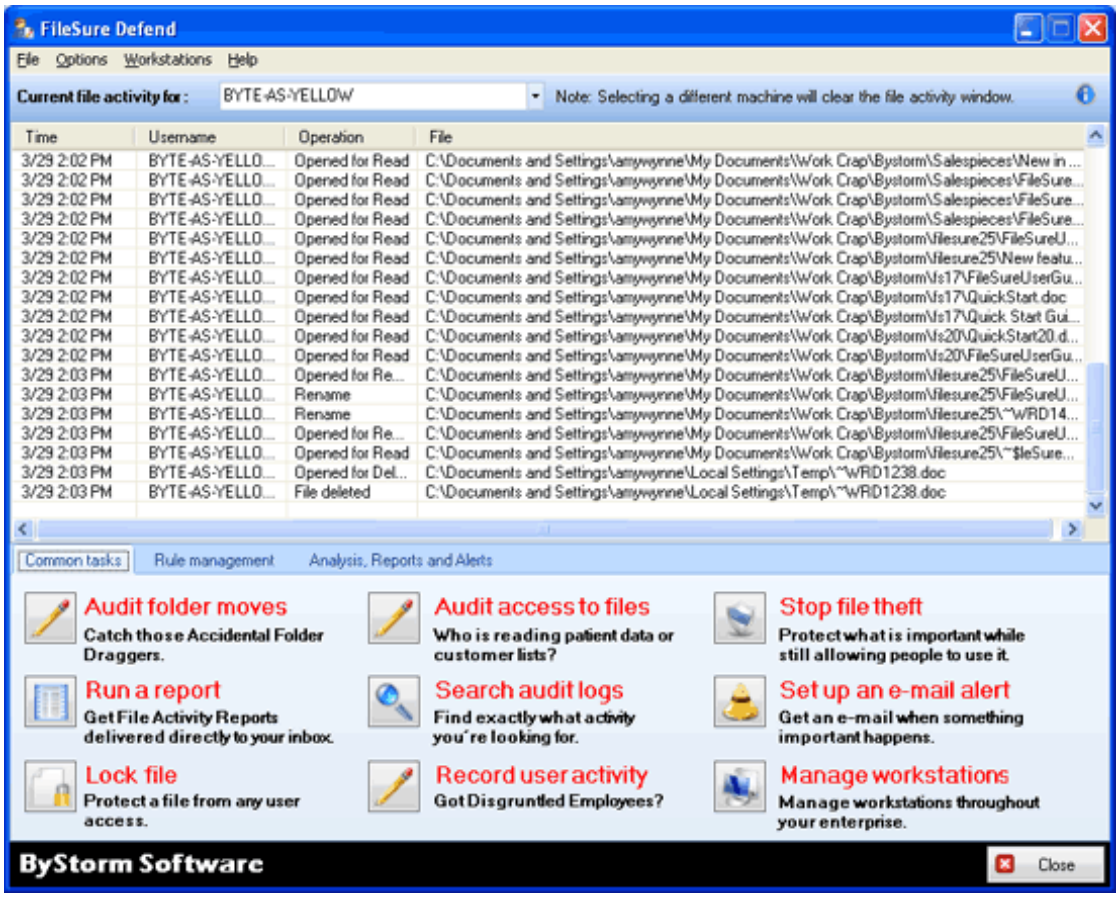
FileSure collapses duplicate operations into a single entry; this is done to reduce auditing noise. By default, if the same user accesses the same file within an hour, the second access will not be recorded. You can change this behavior on the Configure screen.

View Your Data

Within the product, there are three main areas for viewing the file activity FileSure is recording, as follows.

Real Time File Activity Monitor

Kind of like a file access status screen, the **Real Time Activity Monitor** shows you a list of file operations that match the activated rules as they happen. The Real Time File Activity Monitor resembles the figure below. If you had FileSure deployed to workstations, you would choose the source of the data from the drop down list at the top.



View Data, Search for Trends, and Create Reports

To review, filter, analyze, or export past file operations and activity, you can use the **Analysis, Reports, and Alerts Tab**.

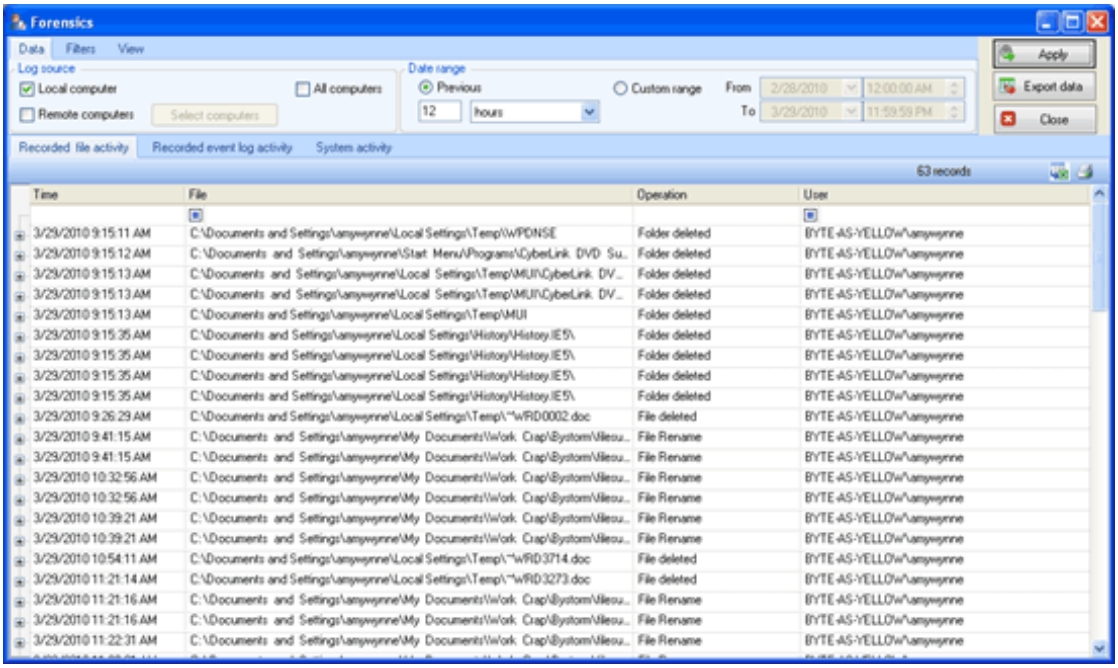
Analysis

In the first section, Analysis, you design queries to return exactly the information you are seeking by clicking **View Data**. You can also study trends to find information you may not have known how to find by clicking **Search for Trends**.

To use the View Data Interface:

1. On the main console, click **Analysis, Reports, and Alerts Tab**. Choose the **View Data** Button.
2. Choose the source of your data and specify a date range for your query (or use the default).
3. Define query filters to return exactly what you need from the audit data by going through options on the Filters and View tabs. For a description of the available filters, please see the User Guide.
5. Click **Apply** to display the data that matches the filter options you specified.

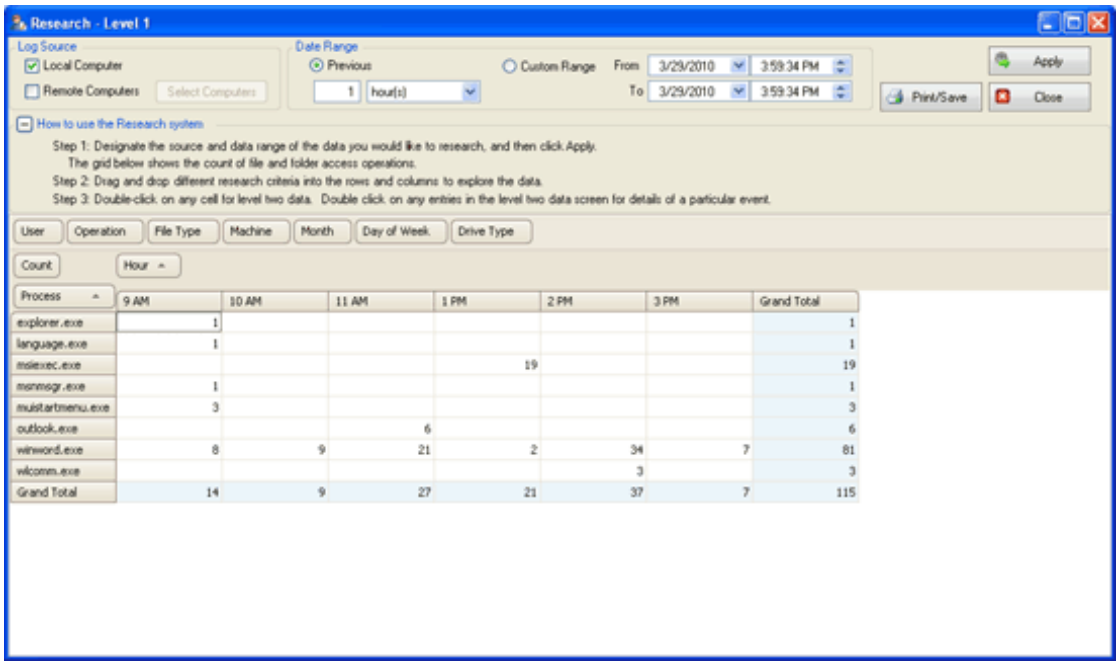
The View Data interface resembles the following figure:



To use the Search for Trends Interface:

1. On the Analysis Tab, click **Search for Trends**.
2. Choose the source machine for your data. Specify the date range for your query.
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.

The Search for Trends interface is similar to the following figure:



Reports Interface

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 Excel or Adobe Acrobat format.

Error! Objects cannot be created from editing field codes.

To create a report on file activity in the Reports Window:

1. On the main console, click **Analysis, Reports, and Alerts Tab**, and then click **Reports**.
2. Specify the date range for your report. You can enter a custom date range by choosing the Date Range Tab.
3. Choose a report from the Report drop-down list. The parameters of the selected report will show in a definition below the box. If you had FileSure deployed to Workstations you could choose the Machines Tab to choose the data source.
4. Click **Run Report.** You can then print or export the report information. You can also schedule recurring reports to be delivered to you via e-mail after entering your SMTP information.

Chapter 3
Successfully Using FileSure

FileSure's powerful ability to capture all file activity ***must*** be metered by your ability to target exactly what information you want—or else you will have too much information to serve most purposes.

You will easily accomplish this by:

- adding rules that explicitly match the information you need while excluding the information you don't, and
- configuring FileSure to respond to the unique needs of your work environment.

Adding Your Own Rules

When you create your own rules, you will be able to target what you want through:

- Filters indicating what files/folders to include or exclude
- Filters indicating what users/groups to include or exclude
- Filters indicating what type of file operation activity to include or exclude
- Filters indicating what devices to include or exclude
- Filters indicating what programs accessing the information to include
- Filters indicating what time of day you want rule matches
- Filters indicating what size of files to include . . . . and more

Before designing rules to run on your server environment, we highly recommend reading "Defining Targeted Rules Using Filters" in the User Guide, found under the Help Menu.

Common Tasks

Because rule creation is a bit of a learning curve, ByStorm Software has built a few shortcuts to create rules that are commonly needed.

Adding a rule through Common Tasks is simple and fast.

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 picklists, 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.

Note

From this new rule you have created, and the trial rules preinstalled, you can see how variables are combined to make a useful and targeted rule by going into the Edit Rule interface and looking at what makes the rule work. Just go to the Rule Management Tab, highlight a rule and click **Edit Rule**. This is the same interface you would use to design a custom rule of your own.

Custom Rules

If you want to create your own rule rather than using a Common Task, click onto the Rule Management Tab. For a rule that focuses on Auditing and Compliance, click **Audit Access**. For a rule that focuses on Security, click **Block Access**.

To add a new rule:

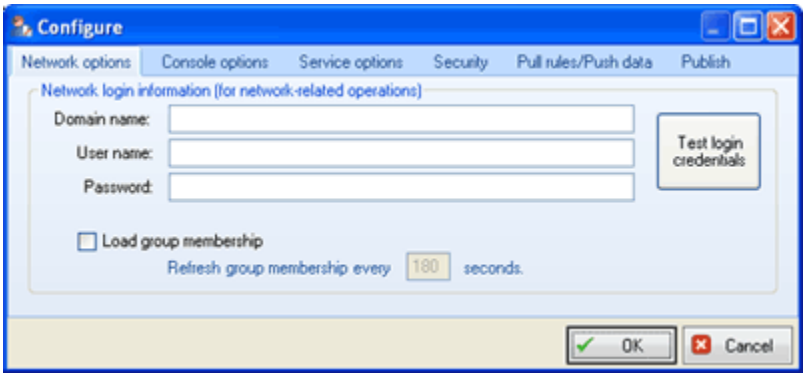
1. On the Rule Management Tab, click the **Audit Access** or **Block Access** button**.** Give your new rule a name.
2. Define your filters. You can filter by files, users, groups, types of file operations to monitor, and many other criteria. For details on how to plan the rules you need, please see the User Guide.
3. Write a comment describing your rule.
4. 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.*

Configuring 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.
- Turn on or off warning messages.
- Adjust service heartbeat options.
- 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" in the User Guide found under the Help Menu.**

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**.