

FileSure

Be sure of your file integrity.

Copyright 2003-2007 ByStorm Software LLC.



Quick Start Guide

August 31, 2008

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.

© 2008 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

Introduction **1**

What Is FileSure?	1
Key Features of FileSure.....	1

Chapter 2

Getting Started Quickly **3**

Preinstalled Sample Rule.....	3
View Your Data	5
Real Time File Activity Monitor.....	5
Forensics Drill Down and Interactive Reports	6
Reports Interface	7

Chapter 3

Successfully Using FileSure **8**

Adding Your Own Rules.....	8
Common Tasks.....	9
Configuring FileSure	10

Chapter 1

Introduction

What Is FileSure?

The FileSure product audits file read, write, delete, deny, rename, and security setting change activities by user or by program accessing the information, and then records important details about the activities of interest. Add-on product FileSure Defend allows you to use the same process to block file accesses—reads, writes, copies and much more. FileSure Spoof allows you to misdirect access so the user does not know they are being blocked but is served a different file. FileSure Workstation puts the power of this solution onto every user machine with centralized data logs and viewing of activity.

To make this solution work, you define rules combining criteria to audit exactly what you need *and to ensure you don't get a lot of data you don't need.*

FileSure works with the file system, uses very few system resources, and does not rely on Windows Auditing.

Key Features of FileSure

- Simple, powerful, and flexible rules-based model
- Real-time file activity monitoring
- Encrypted and compressed audit logs to ensure data integrity
- Easy installation with no external database requirement
- Easy integration into existing server backup solutions
- Lightweight system that uses few system resources
- Support for rules based on domain group membership
- Built in real-time e-mail alerts
- Recurring automatic e-mail reports
- Integration with system monitoring tools through the Windows event log or syslog
- Service availability assurance through low-impact heartbeat

- Comprehensive logging of rules-model changes in the event log
- Console security for limited access to changing the rules model
- Comprehensive file auditing or protection, including reads, writes, deletes, renames, and security setting changes and denials
- Support for exporting audited data to .csv XML, HTML, Microsoft Excel, and Microsoft Access
- Automated publishing of auditing data to Microsoft Access
- Central rule management and distribution through a master server for multi-server environments and/or deployment to workstations
- Central auditing data storage through a master server location for multi-server environments and/or deployment to workstations
- IT compliance for various regulations, such as SOX, HIPAA, and GLBA
- Complimentary Web console add-on that allows others access to audit data directly from their workstations

Chapter 2

Getting Started Quickly

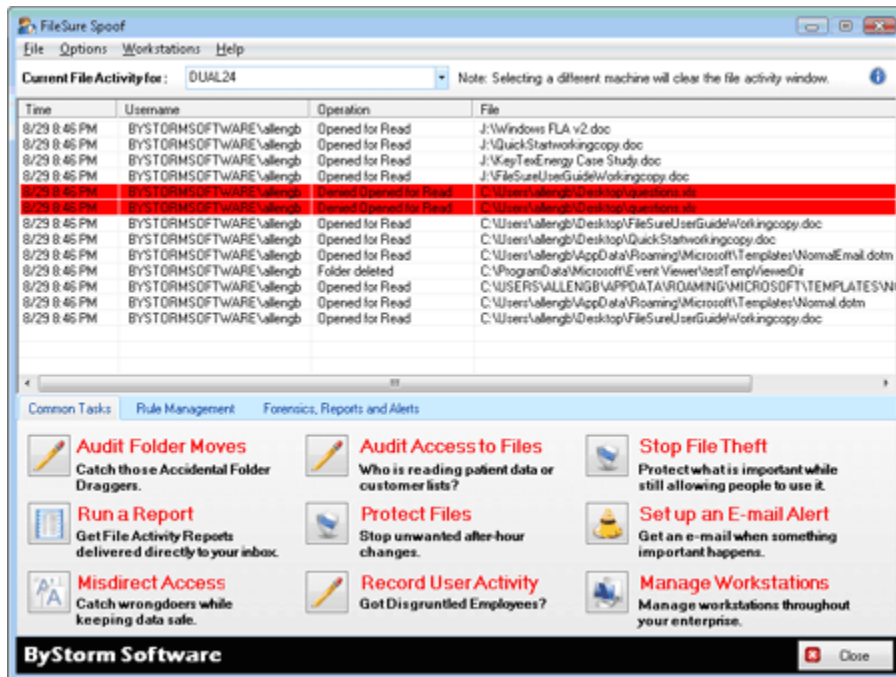
It takes almost no time to see FileSure in action. This guide will quickly show you how FileSure captures file accesses and how you can view the resulting information. This QuickStart Guide is focused on the main auditing functions of the standard version of FileSure. Please see the Common Tasks section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



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.

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.

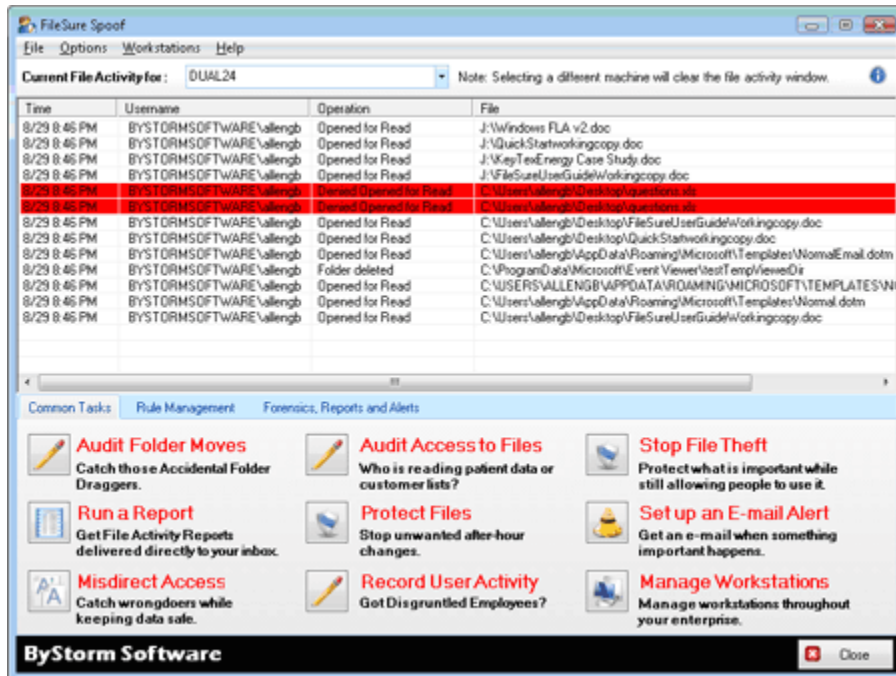
Any time you access any Microsoft Office files, FileSure will be recording the activity. Try a few different activities to any MS Office files you have such as renaming, moving, deleting, changing file security settings, etc. The next section tells you how to view your file access data.

View Your Data

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

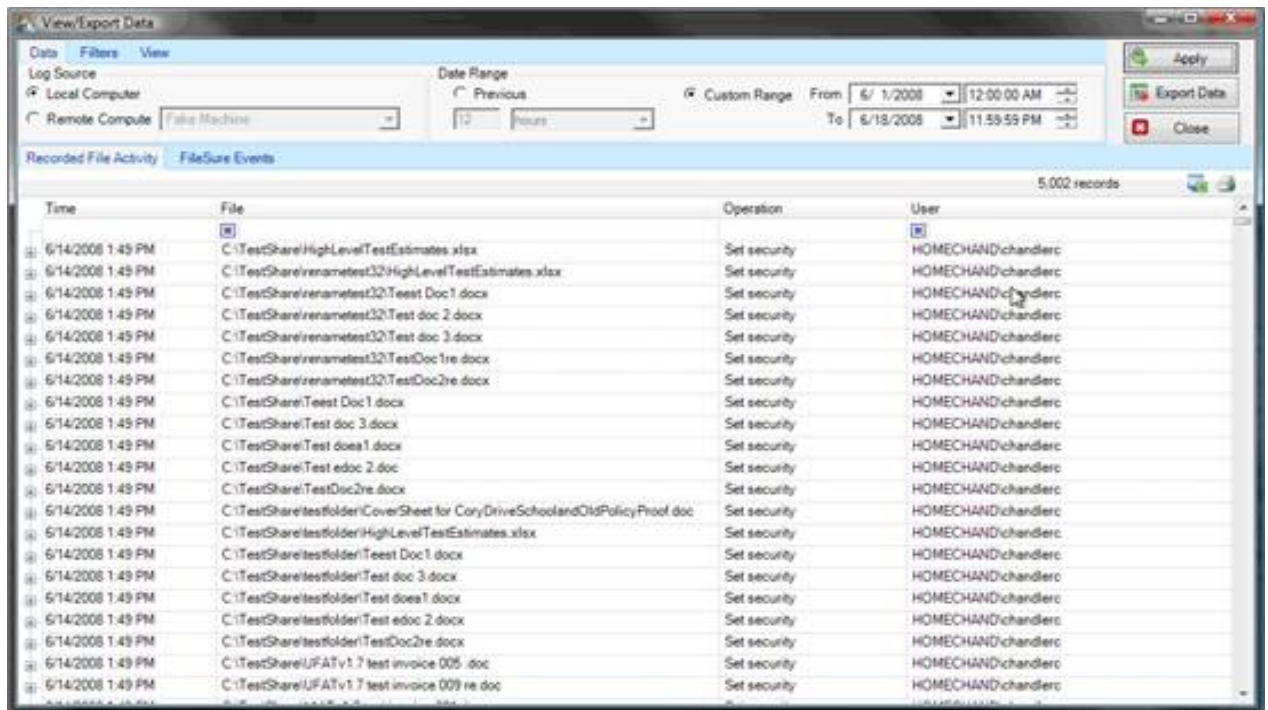
Real Time File Activity Monitor

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.



Forensics Drill Down and Interactive Reports

To review, filter, analyze, or export past file operations and activity, you can use the **Forensics, Reports, and Alerts Tab**. In the first section, Forensics, you design queries to return exactly the information you are seeking. The Forensics interface resembles the figure below.



The screenshot shows the 'View/Export Data' window in a forensic tool. It features a 'Log Source' section with 'Local Computer' selected and a 'Date Range' section with a 'Custom Range' from 6/1/2008 12:00:00 AM to 6/18/2008 11:59:59 PM. The main area displays a table of 'Recorded File Activity' with 5,002 records. The table has four columns: Time, File, Operation, and User. The data shows a series of 'Set security' operations performed by 'HOMECHAND\chandlerc' on various files in the 'C:\TestShare\testfolder\HighLevelTestEstimates.xlsx' directory.

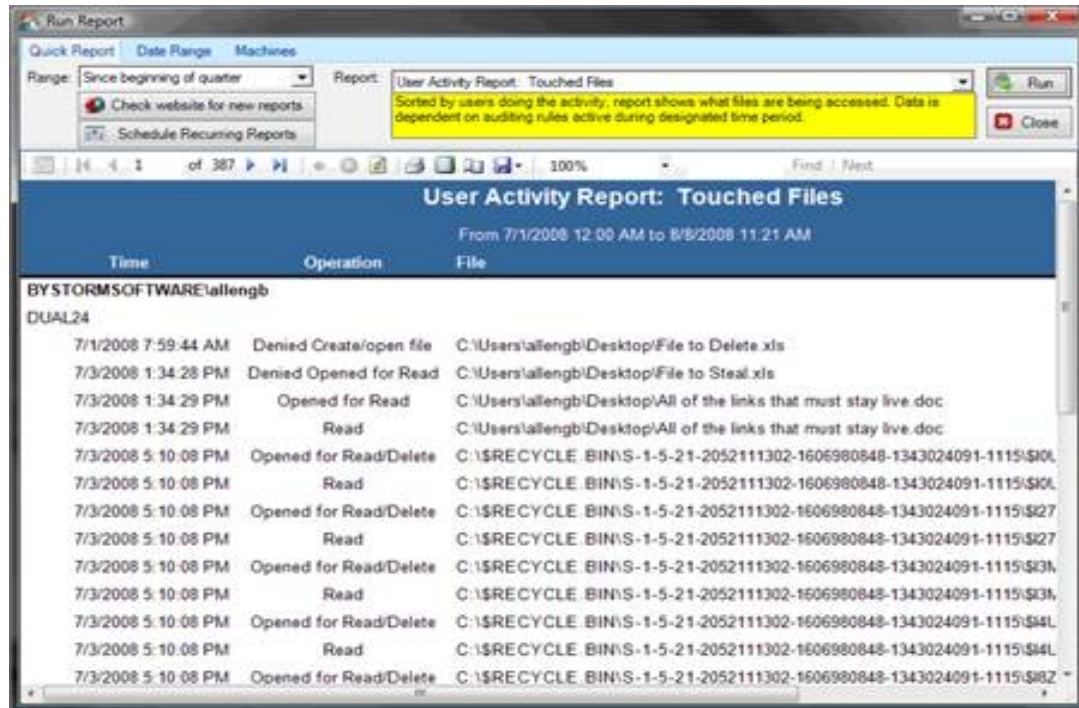
Time	File	Operation	User
6/14/2008 1:45 PM	C:\TestShare\HighLevelTestEstimates.xlsx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\renametest32\HighLevelTestEstimates.xlsx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\renametest32\Test Doc1.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\renametest32\Test doc 2.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\renametest32\Test doc 3.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\renametest32\TestDoc1re.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\renametest32\TestDoc2re.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\Test Doc1.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\Test doc 3.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\Test doca1.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\Test edoc 2.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\TestDoc2re.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\CoverSheet for CoryDriveSchoolandOisPolicyProof.doc	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\HighLevelTestEstimates.xlsx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\Test Doc1.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\Test doc 3.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\Test doca1.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\Test edoc 2.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\testfolder\TestDoc2re.docx	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\UFATv1.7 test invoice 005 .doc	Set security	HOMECHAND\chandlerc
6/14/2008 1:45 PM	C:\TestShare\UFATv1.7 test invoice 009 re.doc	Set security	HOMECHAND\chandlerc

To view file activity in the Forensics Interface:

1. On the main console, click **Forensics, Reports, and Alerts Tab**. Choose the **Forensics 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.

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.



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

1. On the main console, click **Forensics, 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. Five of the tasks can be performed with the original 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, FileSure Spoof, or FileSure Workstation.



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

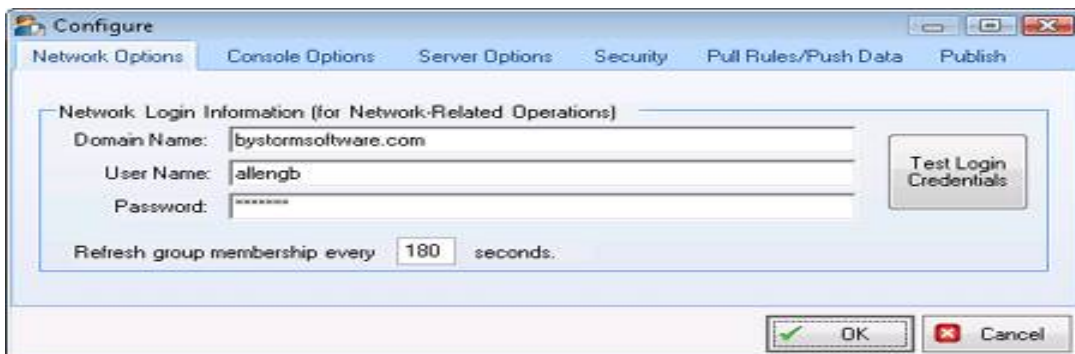
From this new rule you have created, and the trial rules preinstalled, you can see how variables are combined to make a useful and targeted rule by going into the Edit Rule interface and looking at what makes the rule work. Just go to the Rule Management Tab, highlight a rule and click **Edit Rule**.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

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.
- Select view filter types, such as wildcards or regular expressions.
- 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**.