

AirZip™ FileSECURE™ Release 2 Author

Getting Started Guide

1 Welcome to AirZip™ FileSECURE™

FileSECURE is an essential application for securing as well as sharing confidential and sensitive information without giving up control.

The FileSECURE Author is an application used to protect and share sensitive information. The Author allows the setting of access permissions that determine who and how others can use protected information. Author also provides the ability to change permissions and track how protected files are used.

When you install FileSECURE Author, you also install FileSECURE Reader. The FileSECURE Reader is an application used to access protected information. The FileSECURE Reader ensures the information is used only as you intended and only by authorized users.

FileSECURE Author works in conjunction with a FileSECURE Server. The FileSECURE Server is the repository for file encryption keys, permission assignments, and user account information. This data determines who has access to which files and what access they have.

What this guide provides

Section 2 WHAT FILESECURE ALLOWS YOU TO DO

Section 3 GETTING STARTED WITH FILESECURE

Section 4 PROTECTING FILES

Section 5 USING DISKSECURE FILES

Section 6 EMAILING SECURED AND UNSECURED FILES

Section 7 TRACKING FILES

Section 8 CONTROLLING PERMISSIONS ON FILES YOU HAVE DISTRIBUTED

Section 9 USING SECURED FILES

Section 10 WORKING OFFLINE



System Requirements

System Component	Minimum System Requirements
FileSECURE Author plus Reader	Microsoft Windows XP, 2000, ME, and 98. Installation requires approximately 25 MB of disk space for Author plus Reader.

2 What FileSECURE allows you to do

FileSECURE enables you to persistently secure information with strong encryption. FileSECURE Author features an intuitive point-and-click, drag-and-drop interface for securing, un-securing, viewing, editing, and deleting secured files with a standard Windows interface. It also makes it extremely easy to email secured files to other FileSECURE users and to track how secured information is accessed and used.

In order to use FileSECURE, your system administrator must provide you an Account ID and Password.

Persistently protect any file

[FileSECURE](#) enables you to secure any file stored on your computer, files that you share with others by placing them on web servers, or files that you exchange internally or externally. When you use [FileSECURE](#) to secure files, only authorized individuals may access them and only with the permissions you assign. When you secure a file, you determine the files access permissions:

View	Allows others to view the contents of a file.
Print	Allows others to print paper copies of a file.
Copy/Save	Allows others to select and copy portions of the file (or the entire file) to the clipboard or to save unencrypted (vulnerable) copies of files.
Control	Allows others to change permission assignment or to revoke all permissions.

You also may set an **Available On** date and time when you want others to be able to access a file only after a certain point in time, or an **Expire On** date and time, when you want others to be able to use a file before a certain point in time.

Automatically protect files with DiskSecure

[DiskSecure](#) allows you to automatically secure files in specific directories on your local disk drive. Each time a file is added to a directory configured for [DiskSecure](#), [FileSECURE](#) secures the file with a specified set of permissions and shreds the original vulnerable file.

Email secured files

[FileSECURE](#) allows you to email secured files to other authorized users via a convenient email feature. [EmailSecure](#) also allows you to secure the body of email messages in addition to attachments.

Access secured files

You and those to whom you send secured files use [FileSECURE Reader](#) to access them. When you send secured files to others, you decide the access permission those users will have. When other people send you files securely, they decide which type of permissions to give you. You may only be able to view a secured file on your monitor. In this case you will be unable to copy and paste content from the file, or print or save the contents to your hard disk. When viewing files, screen print and screen capture programs are disabled. You will only be able to copy and paste content from the file, print the file, or save its contents to your hard disk if you have been specifically assigned those permissions. If you are granted the save as permission, you will be able to save the file in its original form and use it as if you received the original.

Edit secured files

If you are the author for a file (the person who secured the file) or have **Copy** permissions for a file, you may open a secured file directly using a native application and save the file in its original format.

Changing permissions

If you are the author or have **Control** permissions for a file, you may use [FileSECURE](#) to change permissions or expire files at any time.

Tracking secured file usage

If you are the author or have **Control** permissions for a file, you may use [FileSECURE](#) to inspect what has happened to the secured file using [FileSECURE Tracking](#).

Logging into multiple FileSECURE Server Accounts

[FileSECURE](#) enables you to have accounts on many [FileSECURE](#) Servers for the purpose of securing files or accessing files that others secure and make available to you.

3 Getting Started with FileSECURE

Download the FileSECURE Software

To download and install the [FileSECURE Author](#) and [Reader](#), go to

<http://www.airzip.com/FileSECUREAuthor2>

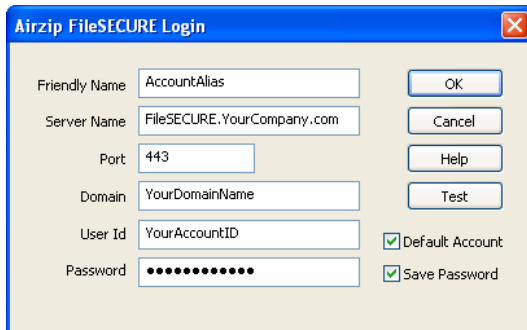
Starting FileSECURE Author

After installation, **AirZip FileSECURE Author** may be opened from the start menu by selecting **Start > Programs > AirZip FileSECURE > Author**.

Authenticating with the FileSECURE Service

To use **AirZip FileSECURE** to protect files, open protected files, or change configuration information, you first authenticate with a **FileSECURE Server** using an Account ID and Password that has been provided to you. **FileSECURE Servers** store your Account information, file encryption keys, and file Permissions. The Server verifies through your account information that you are who you say you are and determines what you are allowed to do through a process called authorization. The **FileSECURE Server** determines your authorization by examining Server restrictions, User and Group rights, and Security Category

Permissions associated with the task you are attempting to perform.



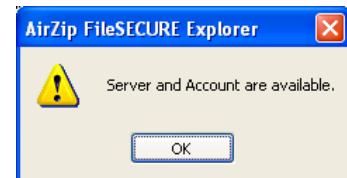
FileSECURE makes it easy for you to have different Accounts. For example, you may be securing information using an Account associated with your organization's own Server while viewing information using Accounts associated with several other **FileSECURE Servers**.

Note: Your Account information (Server Name, Port Number, Domain Name, your Account ID, and your Password) must EXACTLY match the Server's info. Please refer to your account activation info should you have problems connecting to a Server.

Normally, the Server, Port, and Domain are automatically configured when you receive the first protected file secured by a particular Server. Once you have authenticated, **FileSECURE** remembers your account

information and may automatically log you into the Server if you have asked **FileSECURE** to remember your password.

After entering the account information, it is a good idea to use the **Test** function to confirm its accuracy. If your account information is entered properly, the Test will show that the Server and Account are available as shown to the right.




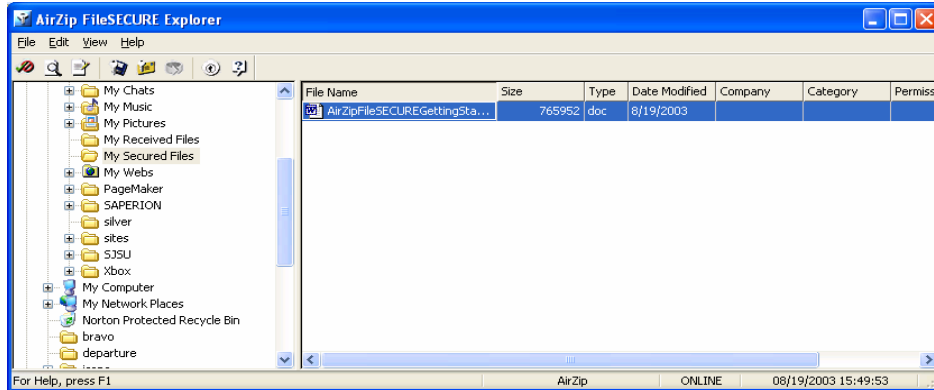
The first time that you logon you may be asked to change your password before continuing to use **FileSECURE**. For better security, you should change your password to one that only you know as soon as possible. It is wise to select a password that contains both letters and numbers and is at least 8 characters in length.

Generally you will be required to logon only once each time you use **FileSECURE**. You may save your password so that **FileSECURE** automatically logs onto the appropriate **FileSECURE Server Account** each time you use **FileSECURE**.

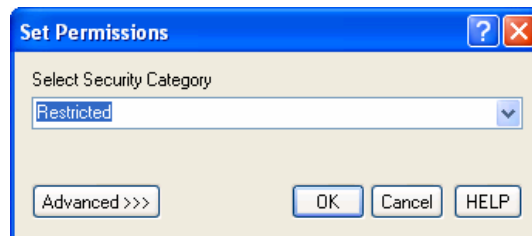
Use **FileSECURE Online Help** to learn more about Logging on for the first time, the Test Connection feature, changing Account Profile information such as your Email Address and Password, and about logging onto different servers.

4 Protecting files

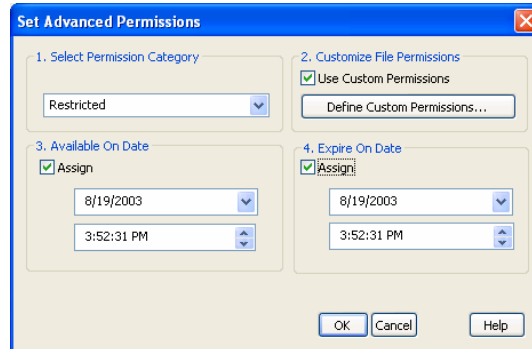
To protect a file or a group of files, you open **FileSECURE Author**, **select** the drive and folder that you want to work with, select the files that you want to protect, and click the **Secure**  button



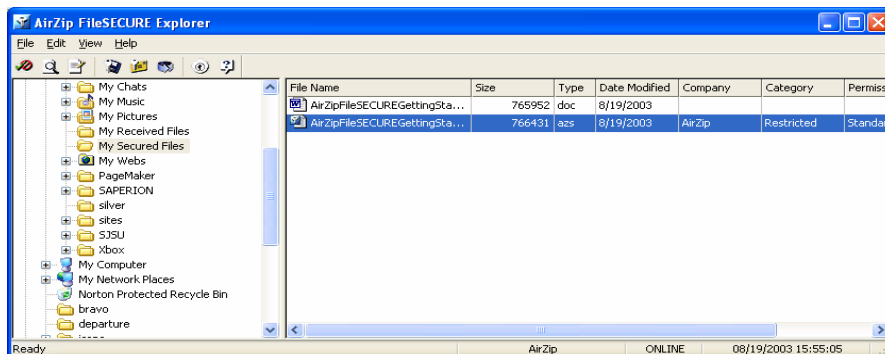
You then select a Security Category using the drop down list of Security Categories provided by your system administrator.



Alternatively you can click **Advanced >>>** button to set Custom Permissions for specific users, Available data and time, or Expiration date and time, if appropriate.



All selected files will be secured with the specified permissions. Secured files will appear as FileSECURE (.azs) files in the same folder as the original file.

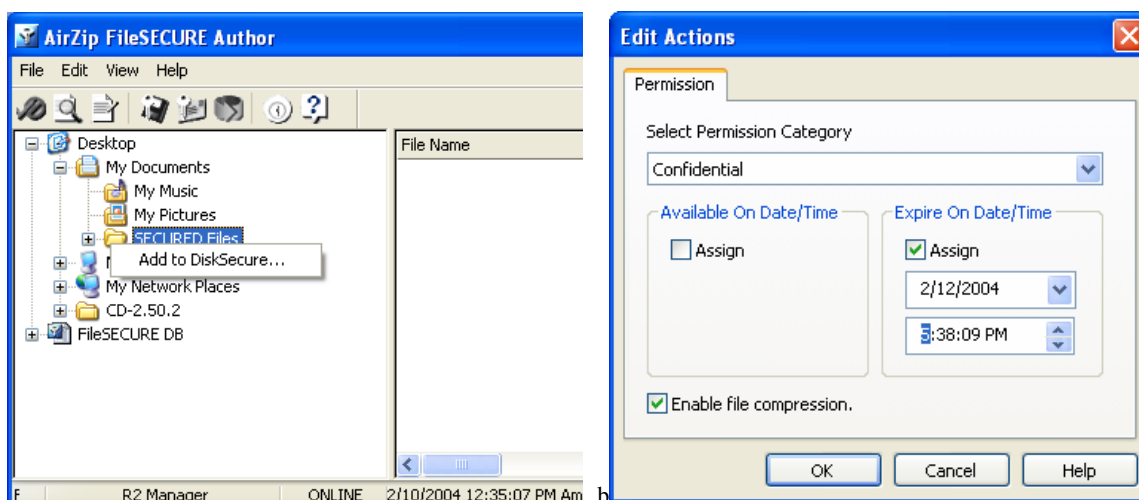


Use **Online Help** to learn more about setting permissions, the Available On and Expire On date and time, and the document shred function.

5 Using DiskSecure

DiskSecure enables you to configure specific folders (directories) on your local disk drive for storing sensitive data. Each time you move a file to a folder (directory) configured with **DiskSecure**, **FileSECURE** secures the file with specified permissions and shreds the original vulnerable file. **DiskSecure** may be used with only one **FileSECURE** account on a particular computer.

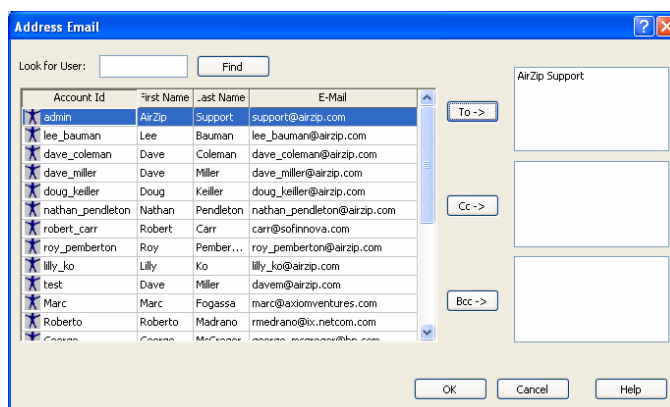
After enabling **DiskSecure**, you configure **DiskSecure** by right-clicking on the folder you want to secure in **Author** and specifying a set of permissions to be applied as shown below.



6 Emailing secured and unsecured files

FileSECURE lets you email protected and unprotect documents using your default E-mailer right from the **FileSECURE Author**. Email is sent via your Outlook, Outlook Express, Lotus Notes, or other similar MAPI-compliant email packages.

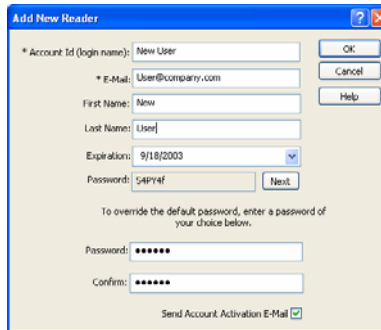
To send a secured file or to secure and send a file to other **FileSECURE** users, you select the file or files to be sent from within the AirZip **FileSECURE Author**, click the **Send** button, and address the message using Select User dialog box that appears.



Add new Reader to User list

If authorized by your administrator, you may add new Readers to the **FileSECURE** User list at any time. A **Reader** is a **FileSECURE** User to whom you may send or otherwise make available secured information. All you need is an email address!


To add a new Reader, use the menu bar **File > Users** function, click the **New Reader** button and enter the appropriate information in the New Reader dialog box.



FileSECURE will create an email to the new Reader from your email account providing them procedures for downloading necessary software and activating their account.

7 Tracking files


FileSECURE tracks who uses each protected file and what action they take with the file. If you are the file owner (typically the person who originally protected the file) you can obtain a Tracking Report on one or more files in one of two ways:

To obtain a tracking report for one or more protected (.azs) files, select the file or files within the [FileSECURE Author](#) or in the [FileSECURE DB](#) and click the **Track**  button.


Account Id	First Name	Last Name	Denied	View	Prnt	Copy	Ctrl	Last Access
N.A.			4	0	0	0	0	2003-07-28 18:00:29
lee_bauman	Lee	Bauman	3	4	0	1	0	2003-08-13 12:18:31
dave_coleman	Dave	Coleman	0	20	0	0	1	2003-08-12 11:27:44
robert_carr	Robert	Carr	0	1	0	0	0	2003-07-31 21:54:20
lilly_ko	Lilly	Ko	4	3	0	0	0	2003-08-08 09:12:58
Natalie	Natalie	Alexander	0	3	0	0	1	2003-07-29 01:16:41

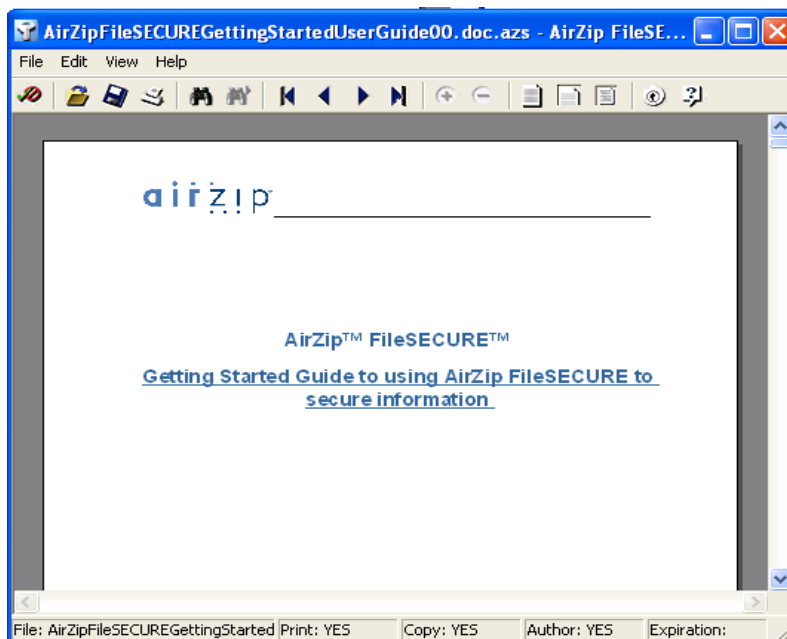
Use **Online Help** to learn more about obtaining the Tracking Report for a particular interval, sorting the Report, and changing document permissions.

8 Controlling Permissions on files you have distributed

To change the permissions assigned to a file or group of files, select the file or files requiring permission changes, click the **Secure**  button, and modify the **Security Category**, or select and modify the **Custom Permissions** as described above.

9 Using secured files

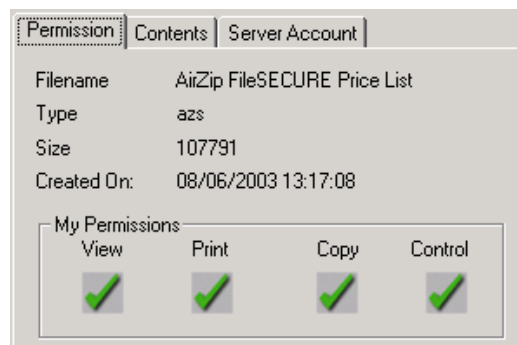
With FileSECURE, secured files are opened using the [FileSECURE Reader](#). You can open FileSECURE (.azs) files in Reader using the Author View  function or by opening the file in the usual ways.



Note that the FileSECURE Reader disables the use of certain Windows functions such as print screen functions and the use of print screen utilities.

When accessing FileSECURE files on websites, the FileSECURE Reader will open directly within Microsoft Windows Internet Explorer. FileSECURE Reader menu features integrate within those of Internet Explorer. Taskbar functions and context menus work the same.

To determine what permissions you have for a file, use the “**File > Properties**” menu item on the Reader or Author or click the **Properties** button on the taskbar. The Permissions Property window such as that at the right will display your permissions along with information about the file contents and the FileSECURE Server protecting it.



The FileSECURE Reader allows you to view the contents of many types of files with good fidelity, even though you may not have the application that was used to create the file. The FileSECURE Reader enables the viewing of many different types of files including:

- Microsoft Word for Windows Versions through 2002
- Microsoft PowerPoint for Windows Versions 3.0 through 2002
- Microsoft Excel Windows Versions 2.2 through 2002
- Adobe Portable Document Format Versions through 5.0
- Text files including html pages and several Unicode, Macintosh, Japanese (ShiftJIS, EUC, JIS, Chinese (Big5,GB) Korean (Hangul), and Cyrillic (ANSI 1251, KO18-R)
- Image files including .jpg, .jpe, .jpeg, .gif, .png, .tif, .tiff, and .bmp files

Use **Online Help** to learn about file viewing modes and controls available on the Context Menu. These modes and controls vary by file type. The Context Menu is opened by clicking the right mouse button anywhere in the FileSECURE Reader view window.

10 Working offline

FileSECURE will allow you to view secured files on your hard drive with FileSECURE Reader while offline, provided:

- Your FileSECURE Service is arranged to allow off line use.
- You have saved the associated Account ID and Password.

- You have been off line no longer than the offline viewing interval configured by the FileSECURE Service Administrator (normally a few days).

11 Getting Support

Contact your Authorized AirZip Reseller or Service Provider to report problems and/or provide feedback.

Additional help resources or updates may be available by emailing support@airzip.com or visiting www.airzip.com/TechSupport.

AirZip Inc. reserves the right to make changes to this document and to the product described herein without notice. The software described in this manual is furnished under the terms and conditions of the AirZip Software License Agreement and may be used or copied only in accordance with the terms of the agreement.

For information about your legal rights concerning the use of the FileSECURE, please refer to the AirZip Software License agreement.

© 2003-2004 AirZip, Inc. All Rights Reserved. AirZip and FileSECURE are trademarks of AirZip, Inc and the subject of trademark applications pending before the US Patent and Trademark.

Outside In ® is a registered trademark of Stellent Chicago Inc. © 1992-2003 Stellent Chicago Inc. All Rights Reserved. Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Revision 02

Document 1010-0211

Last Page of Guide