AirZip® FileSECURE™ 4 Manager User Guide

Table of Contents

1   Welcome to AirZip® FileSECURE™ Manager

1.1   What this guide provides

Section 2 of the Guide contains procedures for determining how to use FileSECURE to protect your organization's information, including "how to steps" for the following:

Determining what information needs to be protected

This first step involves creating a list of the information that you want to protect.

Deciding who needs to protect information and who needs to use information

Once you have a list of information that must be protected, this next step involves categorizing users into Authors and Readers. "Authors" are those users who require the full FileSECURE capabilities of securing information as well as using protected information. "Readers" are those users who are consumers of information and do not need the ability, to protect information.

Deciding how to use User Groups and Security Categories to enforce security policies

Each Security Category defines a set of access Permissions for particular Users or User Groups for a particular type of information.

Decide what Security Settings to use

The Service Settings determine how passwords are distributed, how quickly users are disabled as a result of entering incorrect passwords, and whether or not users can use protected information while off line.

Section 3 of the Guide provides procedures for using **FileSECURE Manager** to configure and manage your FileSECURE Service. FileSECURE Manager provides tools to:

Add, modify, or disable FileSECURE Users

Using FileSECURE Manager, you determine who is authorized to use the service to protect information and who may use the service to access information.

Add, modify, or delete User Groups and Security Categories

FileSECURE Manager allows you to configure Security Categories that enforce your organization's security policies. Each Security Category provides specific access permissions to specific User Groups.

Adjust your Organization's Security Settings

Section 4 of the Guide describes how to update your service account information.

Section 5 of the Guide describes how to use the Usage report to manage FileSECURE on an ongoing basis. FileSECURE Manager provides easy access to your Service Usage Report detailing how your organization is using the AirZip FileSECURE service.

Section 6 of the Guide discusses file recovery in the unlikely event of a total FileSECURE Server failure.

1.2   System Requirements

System Component	Minimum System Requirements
FileSECURE Manager (includes FileSECURE Author and Reader)	Microsoft Windows XP, 2000, ME, and 98. Installation requires approximately 37 MB of disk space.
FileSECURE Author (includes FileSECURE Reader)	Microsoft Windows XP, 2000, ME, and 98. Installation requires approximately 35 MB of disk space.

FileSECURE Reader	Microsoft Windows XP, 2000, ME, and 98. Installation requires approximately 15 MB of disk space.

2 Determining how to use FileSECURE

The first step in implementing FileSECURE to protect your organization's information is to make basic decisions regarding the following:

1. What information needs to be protected?

2. Who needs to protect information and who will have access to the information once protected?

3. How best to configure User Groups and Security Categories to effectively enforce security policies around each type of information?

4. Decide how "secure" you want FileSECURE to be and thus how easy it will be to use?

2.1   Determine what information needs to be protected

Protecting information is of great importance to virtually every organization in every industry and government entity. Here are a few examples.

Begin by making a list of information by department or organization that must be protected as a priority. This will help you to decide who needs the ability to protect information and who needs the ability to use protected information. It will also help you decide how best to set up User Groups and Security Categories in a way that best enforces your security policies.

An example list is shown below.

Department or Organization	Information requires protection
Executives Management	Operating plans, Budgets, Mergers and Acquisitions correspondence
Legal	Patent submissions, Contracts, Litigation
Marketing	Competitive Info, Customer lists
Research and Development	Product Specifications, Schedules
Human Resources	Human Resources Departments, Personnel records, Organization charts
Security	Investigation results
Manufacturing	Bid requests, specifications,
Healthcare & Insurance	Patient records, Insurance claims, test results
Geographical Information Services	Aerial photos, maps
Government Agencies	Records and files, Inter-agency communications, vendor orders
Military	Bid specifications, material orders
Financial Institutions	Account profiles, Transaction details, Manufacturers

Example list of Information to be protected

2.2   Determine if information can be protected

FileSECURE can be used to protect any file, but only those file types that are directly supported by the FileSECURE Reader or that can be printed may be viewed. Importantly, users need not have the original application that created the file on your computer to view or print the file.

FileSECURE Reader supports many but not display files exactly as the application would though files saved in the new AirZip AZF file format will contain a print quality version of the file. After securing and before distributing secured files, Authors should open protected files in the Reader to verify their usability.

The popular file types listed below are supported by the Reader in both AZS (Original file only) or in AZF (print quality) format:

Type of File	File Extensions
Microsoft Word for Windows Versions through 2003	.doc
Microsoft PowerPoint for Windows Versions 3.0 through 2003	.ppt
Microsoft Excel Windows Versions 2.2 through 2003	.xls
Adobe Portable Document Format Versions through 1.5	.pdf
Hypertext Markup Language Web pages - Limited Note: Graphics embedded in HTML pages are not displayed unless they are in the same directory as the HTML file.	.htm, .html
Text files including several Unicode, Macintosh, Japanese (ShiftJIS, EUC, JIS, Chinese (Big5,GB) Korean (Hangul), and Cyrillic (ANSID 1251, KO18-R)	.txt
Image files	.jpg, .jpe, .jpeg, .gif, .png, .tif, .tiff, .bmp

2.3   Decide who needs to protect and use information

Once you have a list of information by department or organization that must be protected, the next step is to identify users as either Authors or Readers. There are now three types of Authors: Author, Author-Plus, A-Author (S-Author).

Manager	A user provided a Manager account may change the FileSECURE Service configurations, configure users, user groups, and security categories. They also have Author-Plus permissions.
Author-Plus	A user provided an Author-Plus account may protect files, access protected files, and add new Readers.
Author	A user provided an Author account may protect files as well as access protected files but may not add new Readers.
Reader	A user provided Reader account may access secured files but do not need the ability to secure files themselves.
A-Author (S-Author)	A user provided an A-Author account may use the FileSECURE Author's AutoSecure option to automatically secure files in specific directories on shared drives. (S-Author is a special version of A-Author).

When configuring FileSECURE, you configure Authors as having **Authors permissions** and Readers as having **Readers Permission**. Author-Plus users can themselves add Readers to the system.

As you will eventually want to organize users into User Groups, it is a good idea to begin to organize Authors and Readers into sets of Users who require access to specific information with specific access permissions. User Groups work in conjunction with Security Categories to enforce security policies. Examples of possibly meaningful User Groups are:

Executives	Users who need access to the organization's most sensitive and important information.
Researchers	Users needing access to the organization's research reports
Contractors	Users outside the company who need temporary access to information
Finance	Users who need access to critical financial reports and studies
Partners	Users who need access to certain types of confidential information
Physicians	Users who need ready access to patient records or client test results

Note: Users may be members of more than one User Group.

User Groups can be created, modified, and deleted as needs change.

For each Author or Reader to be added to the system you will need only their name and email address.

Author Group _____

First Name	Last name	Email Address

Author Group _____

First Name	Last name	Email Address

Reader Group _____

First Name	Last name	Email Address

2.4   Decide how to use User Groups and Categories to enforce security

AirZip FileSECURE Security Categories are similar to security classification labels such as Confidential or Restricted commonly assigned to documents within an organization to denote how such documents need be secured. FileSECURE Security Categories are much more flexible and can be tailored for specific types of information. Each Security Category defines a set of access Permissions for particular Users or User Groups.

User Groups and Security Categories may be configured in many ways to protect, track and control information. Below are examples of applying security categories and User Groups to enable secured sharing of different types of files:

Sharing financial information with management

To share sensitive monthly financial results with key members of your management team, you may configure a Financial Results Category that allows the Finance Results Team to prepare and share such information only with Executives and Managers. The Financial Results Category may allow the Finance Results Team and Executives complete access to the information while allowing Managers only view access. Only the Results Team may reclassify the information for broader distribution.

Financial Results Category	View	Print	Copy	Control
Finance Results Team	✓	✓	✓	✓
Executives	✓	✓		
Managers	✓			

Sharing employee files

To protect employee files, you may want to configure an Employee Records Category that lets Human Resources make information available to Managers who can then share the information with particular Employees by setting custom permissions.

Employee Records Category	View	Print	Copy	Control
Human Resources Records	✓	✓	✓	✓
Managers	✓	✓	✓	

Sharing information with partners

To share sensitive or confidential information with established partners, you may want to configure a Partners Category that lets Marketing prepare and share information such as pricing proposals or new product specifications with partner. In this case, Marketing can view, print, edit and control permissions for the information, which the Partners could only view the information. It may also be useful to allow Executives to have ready access to the information as well.

Partners Category	View	Print	Copy	Control
Executives	✓	✓	✓	
Marketing	✓	✓	✓	✓
Partners	✓			

Sharing information with contractors

To share sensitive or confidential information with a particular contractor, you may want to configure a ContractorA Category that lets Research prepare and share confidential information with ContractorA while ensuring that the information cannot go further.

Contractor Category	View	Print	Copy	Control
Research	✓	✓	✓	✓
ContractorA	✓			

Sharing patient information with consulting physicians

To share confidential patient records with Consulting Physicians, you may want to configure a Patient Records Category that lets Physicians share records and allow them to be conveniently used but with strong tracking. In this case, Physicians view, print, and even edit but their actions are tracked.

Patient Records Category	View	Print	Copy	Control
Physicians	✓	✓	✓	✓
Consulting_Physicians	✓	✓	✓	

You may also use FileSECURE to protect personal files.

Protecting personal files

To product personal files, you may want to configure a Private Files Category that lets a particular User, in this case UserA, secure their files so that only they have access to them. This can be used to protect against loss should a notebook computer be lost or stolen. UserA may share these files with others by simply modifying the Security Category. Other Users may select this Category for files to be shared only with UserA.

Private Files Category	View	Print	Copy	Control
Private (UserA)	✓	✓	✓	✓

Many other configurations are possible.

It is important to make Security Categories understandable enough that they make the use as simple as possible. Author may always define Custom Permissions for special circumstances.

You may want to list the Security Categories in the form shown below.

Category_____	View	Print	Copy	Control
User Group_____				
User Group_____				
User Group_____				
User Group_____				

Category_____	View	Print	Copy	Control
User Group_____				
User Group_____				
User Group_____				
User Group_____				

2.5   Decide which Security Level to use

FileSECURE provides two ways to control security and ease of use. One is a Security Level setting and the other is the Offline Use Duration.

FileSECURE provides three Security Levels: Low, Medium, and High:

Low encourages the wide use of FileSECURE**.**	User accounts are not blocked after any number of consecutive Login failures. Authors and Readers may request the FileSECURE Server to reset their passwords and email a new password before logging into the server. Authors and Readers are allowed to save their passwords for automatic login.
Medium tightens FileSECURE security.	User accounts are disabled after ten consecutive Login failures. A System Administrator must intervene to reactivate the account. Authors and Readers are allowed to save their passwords for automatic login.
High further tightens FileSECURE security.	User accounts are disabled after six consecutive Login failures. A System Administrator must intervene to reactivate the account. Authors and Readers are not allowed to save their passwords and must enter them each time they log into their account.

You may also specify the Key Cache Duration to determine the length of time users have for offline file use before having to reconnect to the FileSECURE service.

---

3   Implementing FileSECURE

Following the above planning steps, you are ready to implement FileSECURE for your organization. Implementing FileSECURE is done using FileSECURE Manager, which is a very simple to use application. This section describes how to:

1. Download and install FileSECURE Manager

2. Start FileSECURE Manager.

3. Authenticate with the FileSECURE service.

4. Select security settings that match your security and ease of use goals.

5. Configure User accounts including Authors, Readers, and Managers (those who will assist you with managing the FileSECURE Service).

6. Configure User Groups to define meaningful sets of users for the purposes of applying security policies.

7. Configure Security Categories that enable users to quickly secure information in a manner consistent with your organization's security policies.

3.1   Download the FileSECURE Software

To download and install the FileSECURE Manager, Author, and Reader, go to

http://www.airzip.com/FileSECUREManager4.htm

and download the FileSECURE Manager software. It includes Author and Reader in one convenient download.

Note: the download pages most users will use are as follows:

http://www.airzip.com/FileSECUREAuthor4.htm for the AirZip FileSECURE Author and Reader

and

http://www.airzip.com/FileSECUREReader4.htm for the AirZip FileSECURE Reader only

3.2   Starting FileSECURE Manager

Open FileSECURE Manager from the start menu by selecting **Start > Programs > AirZip FileSECURE> Manager**. The Manager will appear as shown below.
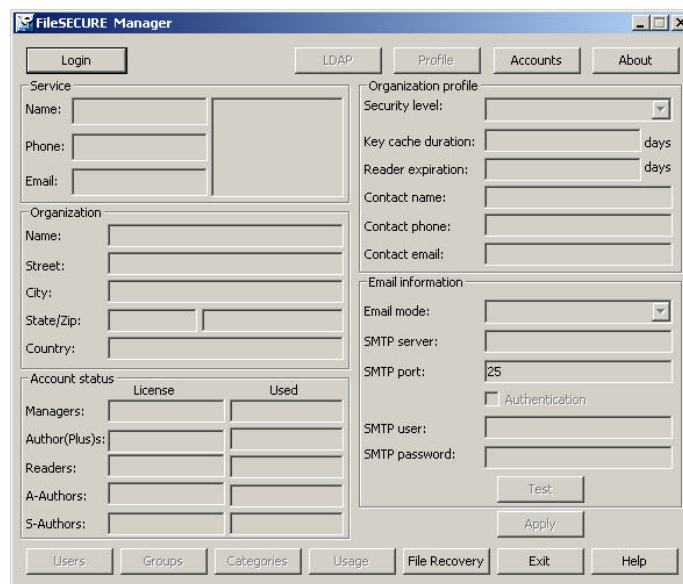
Likewise**,** AirZip FileSECURE Author may be opened from the start menu by selecting **Start > Programs > AirZip FileSECURE> Author**. The Author will appear as shown below.
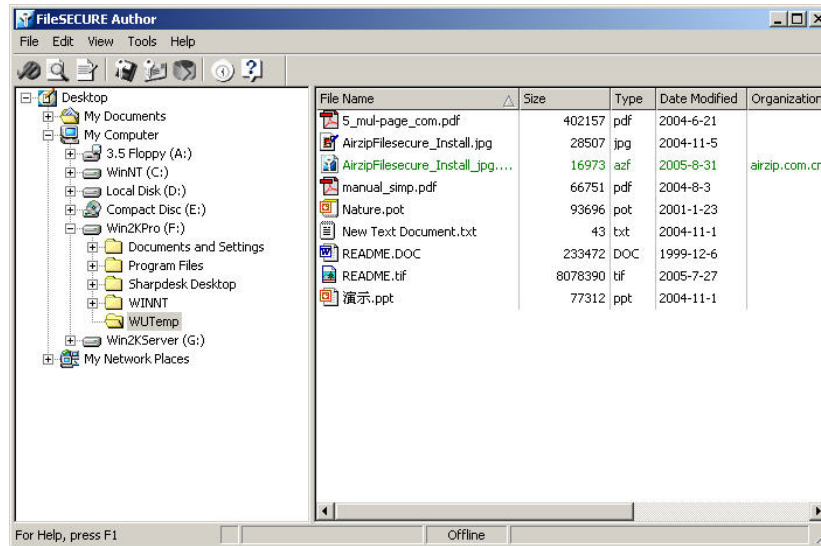
And**,** AirZip FileSECURE Reader may be opened from the start menu by selecting **Start > Programs > AirZip FileSECURE> Reader**. The Reader will appear as shown below.
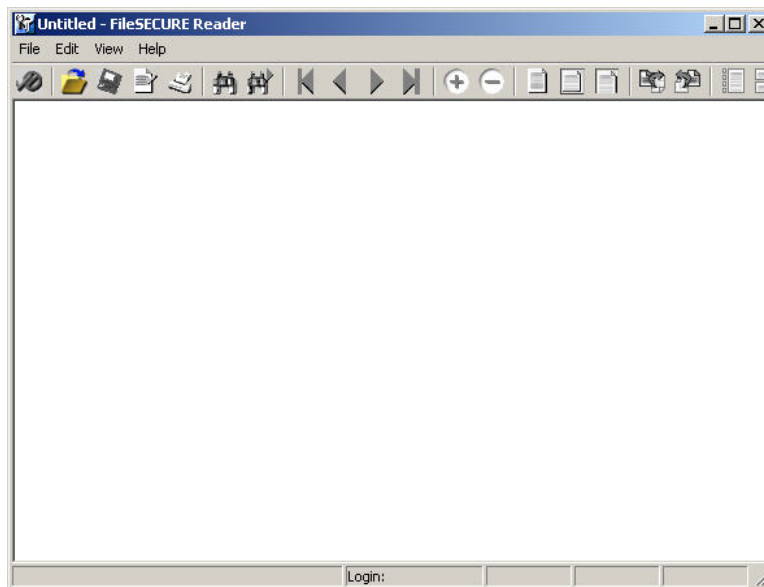

3.3   Authenticating with the FileSECURE Server

You must authenticate with a FileSECURE Server and Organization to use the AirZip FileSECURE Manager. FileSECURE Servers store user account, file encryption keys, and file permissions; Organization ID is the name of an organization that uses a particular Server.

To log onto and use FileSECURE Manager, you will need a *Server Name*, *Port Number*, *Organization ID*, *User ID* and *Password*. Your *User ID* may be your email address or a user name. Contact your system administrator if you have not received your *User ID* and *Password*.

After entering the account information, press the **Test** button to verify your account. If your account information is entered correctly, the test will show that the Server and Account are available. If the test is successful, the **OK** button

will be enabled and you will be able to save your account information. A manager may not save their account password even if their organization security level is **Medium** or **Low**.

The first time that you logon you will 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. Once you have authenticated with a server where you have a **Manager** Account, the Manager screen will appear as below.
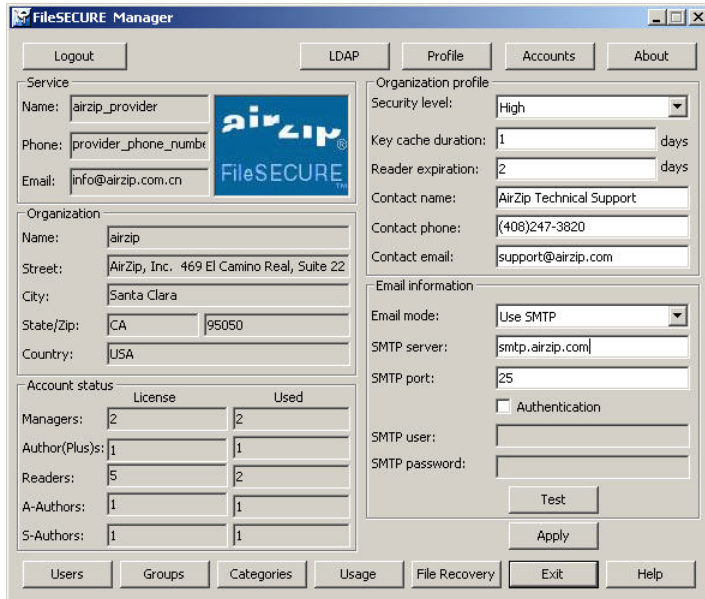
3.4   Setting up User Accounts

There are five basic types of AirZip FileSECURE user accounts:

Manager	A user provided a Manager account may change the FileSECURE Service configurations, configure users, user groups, and security categories. They also have Author-Plus permissions.
Author-Plus	A user provided an Author-Plus account may protect files, access protected files, and add new Readers.
Author	A user provided an Author account may protect files as well as access protected files but may not add new Readers.
Reader	A user provided Reader account may access secured files but do not need the ability to secure files themselves.
A-Author (S-Author)	A user provided an A-Author account may use the FileSECURE Author's AutoSecure option to automatically secure files in specific directories on shared drives. (S-Author is a special version of A-Author).

To configure a User account, you need the following information about the user:

User ID	The User ID may be the User ID that the person uses to log into their computer or the User's email address.
First name	The user's given name.

Last name	The user's surname.
E-mail Address	The user's email address
Type of User	Whether the user is to be an Administrator, Author-Plus, Author, or Reader.

To configure Users, click the **Users** button on the AirZip FileSECURE Manager window.

Use the **Online Help** to learn more about viewing User Accounts, adding New User Accounts, editing User Account, sorting User Accounts, and disabling User Accounts.

Note: User accounts are not deleted but only disabled so that information about User access to files continues to be available.

3.5   Setting up User Groups

User Groups define a set of Users who require access to specific information with specific access permissions. User Groups work in conjunction with file Security Categories as described previously. Again, examples of possibly meaningful User Groups are:

Executives	users who need access to the organization's most sensitive and important information.
Researchers	users needing access to the organization's research reports
Contractors	users outside the company who need temporary access to information
Finance	members of the organization who need access to critical financial reports and studies
Partners	users who need access to certain types of confidential information
Physicians	users who need ready access to patient records or client test results

The same User may belong to multiple User Groups. User Groups can be created, modified, and deleted as needs change.

To add, delete, or modify User Groups, click the **Groups** button on the AirZip FileSECURE Manager window.

Use the **Online Help** function to learn more about viewing User Groups, adding User Groups, deleting User Groups, and renaming a User Group

3.6   Setting up Security Categories

AirZip FileSECURE Security Categories are similar to a security labels such as Confidential or Restricted commonly assigned to documents within an organization in order to denote how such documents need be secured. Unlike security classifications, FileSECURE Security Categories combine with User Group definitions to enforce security policies for particular types of files. Each Security Category defines a set of access Permissions for particular Users or User Groups.

Security Categories can be created, modified, and deleted as needs change.

To add, delete, or modify Security Categories, click the **Categories** button on the AirZip FileSECURE Manager window.

Use the **Online Help** function to learn more about viewing current Security Categories, adding a new Category, modifying Category Permissions, and Deleting a Category.

3.7 Setting your Organization's Security Level

To change the security level

1. Open the Manager.
2. Locate the System Security Level field on the main Manager window.
3. Select the new Security Level using the pull down menu.
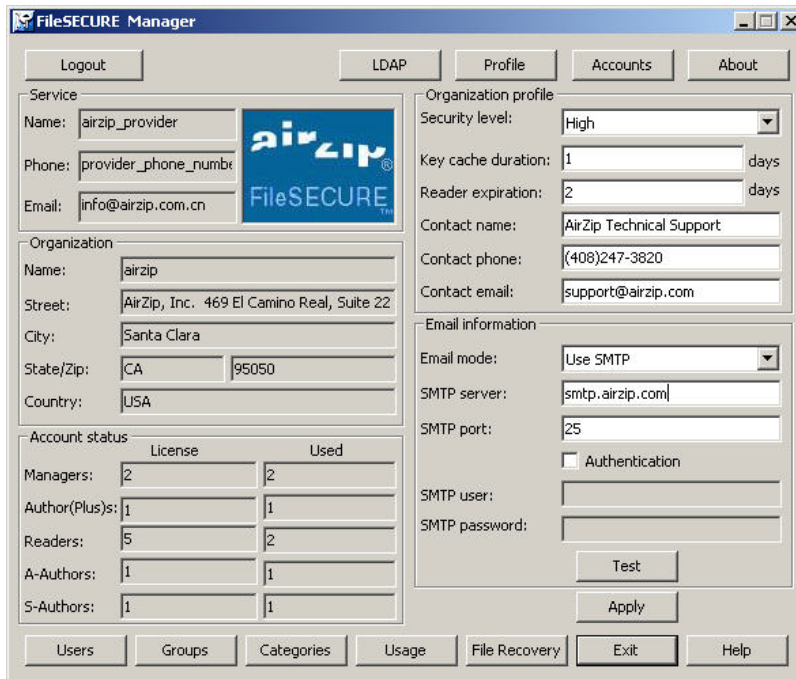4. Click the **Apply** button.

To change the Key Cache Duration

1. Open the Manager.
2. Locate the Key Cache Duration field on the main Manager window.
3. Enter duration in Minutes.
4. Click the **Apply** button.

4 Updating Your Service Account Information

The AirZip FileSECURE Manager allows you to quickly view and modify important information about your FileSECURE Service as well as to configure the FileSECURE Service to meet your organization's needs.

When you open and log on to Manager, the Manager window presents the important information about your AirZip FileSECURE Service including:

- The name and address of your organization as configured on the FileSECURE Server.
- The name and Internet address of the FileSECURE Server.
- Security Level Setting currently in use.
- The name and contact information for your primary company contact.
- The name and contact information of your service provider.
- The number of Administrators, Clients, and Read Only users that you have licensed as well as the number currently configured.

The contact information that appears in the AirZip FileSECURE Manager window should be the person most familiar with your organization's needs. This information enables your service provider or other users of Manager to easily contact you should there be a need to do so.

To update your account contact information if the name, telephone number, or email address of your primary system administrator change:

- Locate the Organization Contact information on the lower right hand side of the main Manager window.
- Click in the field that requires updating and enter the new information.
- Click the **Apply** button to effect all changes.

To update your organization information, contact your service provider.

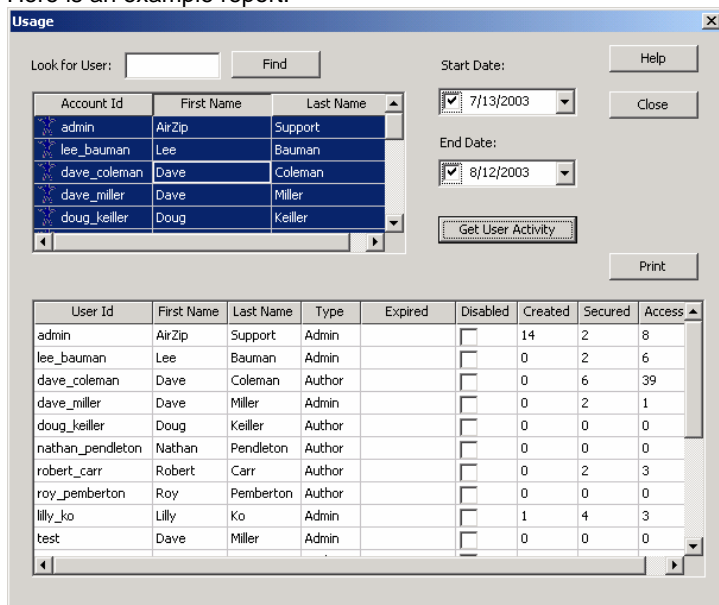---

5 Managing FileSECURE on an ongoing basis

One of the most important tools that you have for determining how AirZip FileSECURE is being used is Usage Reporting. Basic Usage Reporting is intended to help you answer the following questions:

- Is the system being properly used?

- Who is and is not using AirZip FileSECURE?

- Is the system protecting the organization's information?

If the optional Reporting package is equipped on your Server, you may generate and customize reports providing even greater event detail to help you met business and legal requirements. To view the basic Usage or Advanced Event Reports

- From the FileSECURE Manager window, click the **Usage** button.

Here is an example report:

You can Sort the report by clicking on the column labels and you can also print the report. You can also obtain a report for a specified interval of time. Use **Online Help** to learn how.

6 Directory Synchronization

The AirZip FileSECURE Directory Synchronization enables your organization to manage FileSECURE User and Group definitions using your Directory Server such as Microsoft Active Directory and its associated Administration tools.

When Directory Synchronization is activated for your Organization, the contents of your Directory Service determine:

- the list of users who may use FileSECURE

- the type of account to be assigned to each user: Manager, Author-Plus, Author, Reader, and so on.

- the list of Groups that are defined within FileSECURE along with user membership within each Group.

- the User ID, Password, and email address configured for each user

You continue to use FileSECURE Manager to configure

- Security Categories permissions

- other FileSECURE service options

 Note: When Directory Synchronization is activated, FileSECURE Author-Plus, A-Authors, and S-Authors users no longer have the ability to add or expire FileSECURE Readers. All user administration is done via the Directory Service.

FileSECURE Author-Plus and Authors maintain the ability to

- control file Permissions based on Security Categories

- assign file Permission based on User and Group definitions

- conveniently send secured files to any FileSECURE User

FileSECURE Users authenticate as they do today when launching FileSECURE Manager, Author, or Reader but utilize the User ID and Password defined for them in the Directory Service. FileSECURE verifies the User ID and Password with the Directory Service before allowing FileSECURE Manager, Author, or Reader to be used.

In summary, FileSECURE Directory Synchronization enables:

- User and user role (Manager, Author, Reader, etc.) to be based on Directory Service entries.

- Group definitions to be based on Directory Service.

- FileSECURE sign on based on User ID and Password configured in the Directory Service.

- Automated Directory Synchronization with convenient scheduling options.

- Simple configuration of Directory Synchronization.

The FileSECURE Directory Synchronization can be used with the following Directory Services:

- Microsoft Active Directory™

- Sun One Directory Server

- IBM Lotus Domino 5

- Novell eDirectory/NDS

- IBM SecureWay Directory Server

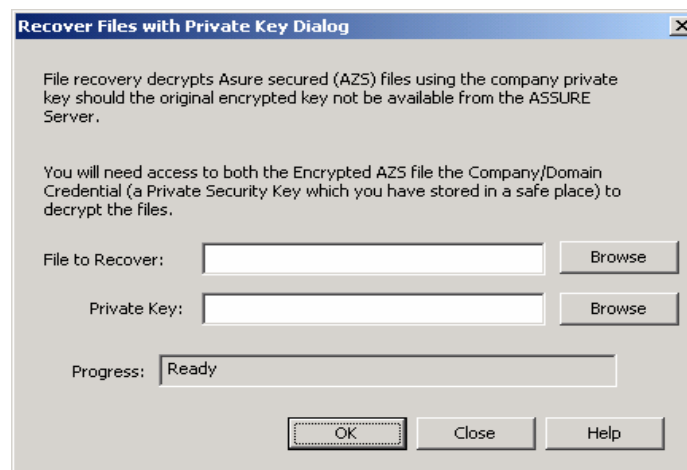- IBM Directory Server

- IBM Tivoli Directory Server

7 File Recovery in emergencies

To ensure that AirZip FileSECURE protected files may be recovered even in the event of a sever system failure where back up measures also fail, a special public-private file recovery key pair is generated with each new organizational account. The Private File Recover Key is provided to the account owner or escrowed for safe keeping. The Public File Recovery Key is used in the securing process in a way that makes every FileSECURE protected file recoverable as long as you have both the protected file and the private file recovery key.

Should you ever have to recover a file you must have

- A copy of the protected (.azs / .azf) file.

- The Private File Recover Key for the organization whose user protected the file

- An Administrator Account on any active AirZip FileSECURE server.

Below is the File Recovery Dialog box you will see when you click the **File Recovery** button.

8 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.**

Last Page of Guide

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.

Revision 4.0