AirZip FileSECURE Hierarchy of Entities

The FileSECURE environment supports a hierarchy of entities, designed to provide clear separation of role and function. This paper provides an overview of the hierarchy and key features of each.

FileSECURE Authentication & Policy Server

System Level

This level represents the traditional systems administrators (Administrator in Microsoft Windows or root on Unix/Linux based systems) who are responsible for installing, updating, configuring and starting and topping FileSECURE.

Super User

The Super User is the overall FileSECURE server administrator. Super User is responsible for:

- managing the creation of Organizations
- allocation or reallocation of licenses to Organizations
- secure storage of Organization private keys
- resetting Organization Manager passwords
- backup and restore of the FileSECURE database.

The Super User license is included in the FileSECURE Server license.

Organization

A unique feature of FileSECURE is that each server can support one or more Organizations. Each Organization is cryptographically and logically separate from the other. Designed to operate in an SaaS or On-Demand environment providing service to many companies or groups of users, each Organization has its own manager(s), users, policies and secured files.

Most users operate using a single FileSECURE Organization (representing the company), but a number have chosen to use a separate FileSECURE Organizations for internal (employees) and external (customers, suppliers, partners, subcontractors) users. The advantage of this separation is that:

- external users cannot be accidentally granted access rights to sensitive information meant only for company employees
- internal users can be integrated with the company LDAP/Active Directory server and external users can be separately managed within FileSECURE (if desired)

The disadvantage of separate Organizations is that if a file is needed to be shared with members of both Organizations, the file will need to be secured twice – once for each Organization.

© Copyright 2005-2010 AirZip, Inc. All Rights Reserved.

FileSECURE Clients

Manager

Each Organization may have one or more Managers assigned. When an Organization is created by Super User, a default Manager (the account, “admin”) is created. Super User assigns this Manager to an individual who will have ultimate responsibility for managing users and policies for the Organization. This individual is identified primarily by his or her email address.

Manager can establish policies for the Organization, such as:

- defining the security level (affecting number of password attempts, etc.)
- permitting or denying the creation of temporary Readers or use of offline mode, and the durations of each if permitted.

Manager is also responsible for:

- license allocation within the Organization
- either creating users (or synchronizing them from an LDAP based directory service)
- allocating users to Manager, Publisher, Author, Editor or Reader roles
- permitting Authors to create dynamic Readers
- determining which workstation(s) from which a user may use FileSECURE
- establishing Organization wide Categories (policies)
- managing user groups (if not LDAP integrated)
- enabling or disabling users (if not LDAP integrated)
- resetting user passwords if they become locked out (if not LDAP integrated)

In addition to the mandatory "admin" account, other users can be designated as Manager as well. All Managers are also Authors, Editors and Readers.
For licensing purposes, Managers are not separately licensed. Customers purchase the required number of Authors. Any of these can be designated as a Manager. At least one Author license is required when purchasing FileSECURE, so this provides the mandatory "admin" Manager account.

Author

A FileSECURE Author is a user who owns or controls the content of a file or document and who wishes to restrict access to that content. In securing the content, the Author can decide who has access (Users and/or Groups), when they have access (not before or after a certain date and time), and what rights each User or Group has over the content (View, Print, Copy, Control). An Author can apply predefined policies (called Categories) when securing content, or dynamically add specific Users and Groups as needed.

An Author can change access rights or revoke those rights to secured content to any User or Group as the need arises.

If an Author is defined with the Author-Plus attribute, that Author is then permitted to create dynamic users on an as needed basis. A dynamic user is a Reader that is created for a limited duration (the maximum duration being determined at the Organizational level by a Manager). This is useful where a transient relationship exists between the owner and recipient of secured content. Once a dynamic Reader expires, the user license is returned to the license pool for re-use. All that is needed in order to create a dynamic user is an email address. A dynamic user can be re-

© Copyright 2005-2010 AirZip, Inc. All Rights Reserved.

activated after expiry if needed. (Note: Dynamic users are always created in the FileSECURE internal user database regardless of whether LDAP synchronization is in use or not.)

An Author account is also automatically a Reader (permitting viewing content the Author has secured).

Authors are licensed on a per-user basis.

Editor

FileSECURE Editor was introduced with version 4.3 to provide a secured editing environment during document creation and editing. Previously, FileSECURE was focused solely on the secure distribution of content. This content was created using standard applications and then secured before being distributed to third parties. Because many user's are creating documents on laptops or desktops that are not physically secure, AirZip developed the Editor to permit documents to be secure from the moment they are created.

FileSECURE Editor is integrated into Microsoft Word, Excel and PowerPoint (versions 2003, XP and 2007), the most widely used office applications. When using Editor to create a new Word document, for example, Word will not create a .doc file. Instead, the file will be created as a secure AirZip (.azs) file from the beginning. In fact, all Word temporary and recovery files will also be encrypted to prevent unauthorized backdoor access to the content.

A variety of policies can control FileSECURE Editor functions, and Editors can be assigned to a supervisor Author where the Author controls the policies and rights that can be assigned to files and documents by the Editor.

The Author of a document can assign different Editors to compose or review a secure document, though there can only be a single Editor active at a time. This provides a simple workflow interface that can be integrated with formal workflow systems using FileSECURE Publisher.

Editor's are separately licensed clients, but each Editor is also a Reader.

Reader

FileSECURE Reader is a specialized software program designed to render secured content in a protected environment. This protected environment includes:

- enforcing the permissions granted to the user of the file being viewed. If the user has View only permission, the user is prevented from printing the content, copying it to the clipboard or saving an unsecured copy to disk.
- preventing the user from using the Windows Print Screen function to print a copy of the on-screen content.
- blocking screen capture programs from obtaining a copy of the content. FileSECURE presently blocks in excess of 350 named screen capture programs (several thousand if all the different versions of these are considered), and the list is continually being updated as new utilities are discovered. In addition, the FileSECURE Manager can explicitly permit or block specific screen grabbing applictions.
- preventing remote access programs such as Windows Terminal Services, Windows Remote Desktop, pcAnywhere, VNC, etc. from viewing content

while remotely logged onto a user workstation viewing secured content. These can also be whitelisted by the FileSECURE Manager.
- ensuring any temporary files created when opening or viewing secured content are encrypted. AirZip has recently developed its own virtual machine technology there the file system, Windows registry and IPC (interprocess communications) layer are all encrypted. This substantially increases FileSECURE's security and its ability to secure third party applications..
- applying an Author mandated watermark to content being displayed or printed. The watermark information can include text strings such as "Confidential", "Do Not Copy", the FileSECURE user ID, organization ID and Windows user name of the user viewing the content, the file name, current date/time as well as the workstation's hostname, IP and MAC addresses.

Readers are licensed in packs of 10 users.

Publisher

FileSECURE Publisher is a separately licensed FileSECURE Client that offers an XML driven engine providing access to all of FileSECURE's securing functions. Publisher is primarily targeted at users that need:

- auto securing of files.
- bulk securing or re-securing large quantities of files.
- mass creation of FileSECURE user accounts (if not LDAP integrated).
- integration with third party Document Management Systems, Office Automation Systems, PLM Systems, etc.

Publisher AutoSECURE

AutoSECURE permits automatic securing and (optionally) automatic distribution of files placed in predefined directories/folders by users or scanner devices.

AutoSECURE operates by monitoring one or more directories/folders on a shared file system and is configured using the AutoSECURE Workbench. Each directory can be assigned a different policy. Users who wish to secure content simply drag and drop files into one of the directories and the policy is automatically applied. In addition, the secured files can be automatically emailed to all the users associated with the policy. As an example, separate directories could be defined for Human Resources, Employee Notices, Financial Reports, Draft Marketing Materials, and so on. For each, functional managers could be assigned Read/Print/Copy rights and employees of those departments simply Read only. Any document placed in one of the folders would be secured with the predefined rights and automatically distributed to everyone in each of the departments. Additional directories could be maintained for Managers Only, etc. to further restrict distribution.

A major advantage of AutoSECURE is that the users who are placing content into the securing directories need not even be aware of FileSECURE, and have not need of any FileSECURE Client software. They would only need the Reader software if they were to be the recipient of secured content.

Standard Windows access control methods can be used to permit or deny user access to the auto-securing directories. AutoSECURE Monitor permits monitoring of operations.

Other uses for AutoSECURE include secure backup. As an example, each employee could be allocated a personal directory on a file server (monitored by Publisher) and instructed to copy their local “My Documents” directory to this directory each Friday afternoon. The contents would then be automatically secured. In this case, no distribution to other users is necessary, but the secured files could instead be moved to offline tape or WORM storage. If it were ever necessary to restore a user’s backed up files, they would be restored to disk as secured files and the user could then either unsecure them or access them as secured files. In all cases, access is controlled and audited.

Publisher ScanSECURE

Optical scanners capture content and save the resulting images, PDFs (and/or OCR’d files) to disk using a variety of methods including file transfer protocol (ftp), server message block (smb), etc.

ScanSECURE is a special mode of FileSECURE Publisher that is used in conjunction with scanners to secure images (or OCR content) as it leaves the scanner. Similar in operation to AutoSECURE, ScanSECURE is configured to monitor the directory/folder receiving the output from the scanner. Policies can be automatically applied and the resulting secured content distributed.

In the case of certain high end scanners and Multi-Function Printers (MFPs), FileSECURE can be integrated directly into the front panel of the device allowing the user who scans a document to dynamically select a predefined policy, or User or Group. The resulting file will be secured and distributed accordingly. In addition, the scanner user can enter an ad hoc email address and content rights/permissions for the document to be scanned. FileSECURE will automatically create a dynamic Reader account based on the email address and notify the user that this account has been created. The notification contains a temporary password that much be changed the first time the user logs in to the system.

The information entered into the font panel of the scanner is sent to Publisher as an XML metadata stream. ScanSECURE is programmed to wait for a period of time to receive the metadata instructions. If this is received before the time expires, then the instructions in the metadata are carried out. If not, then the default rules assigned to the directory being monitored are applied.

ScanSECURE is licensed on a per-physical-scanner basis.

Publisher API and Integration

Publisher was developed to provide high level programmatic interfaces to support bulk operations, integration with third party applications such a Document Management, PLM and Workflow systems and the ability to develop web and cloud applications such as WebSECURE.

Publisher provides XML or COM/ActiveX interfaces permitting applications written in C, C++, C#, VB, Java, Perl, Windows Powershell, etc. to interface directly to the securing engine.

Publisher is recommended to run on a machine dedicated to this purpose (i.e. no other FileSECURE usage), and is licensed on a per-instance basis.

AirZip, Inc,
961 Red Tail Lane
Bellingham, WA 98226
USA
tel：+1.360.922.0613
fax: +1.604.630.7101

email: info@airzip.com
http://www.airzip.com

AirZip Asia Ltd.
Level 19, Two International Finance Centre,
8 Finance Street, Central,
Hong Kong, S.A.R.
tel：+852.2251.8466
fax：+852.2251.8467

email：info@airzipasia.com
http://www.airzipasia.com

People’s Republic of China offices:

email：info@airzip.com.cn
http://www.airzip.com.cn

AirZip Beijing Co., Ltd.
Room 5609, 5th Floor, Chenchang Bldg., Zhichun Road
Haidian District
Beijing, 100080
Tel: +86.10.6262.1936-5034

AirZip Shanghai
Huangsheng Building, Room 1609, 399 Jiu Jiang Road
Shanghai 200003
tel：+86.21.6361.7286
fax：+86.21.6361.7285

AirZip Shenzhen
World Finance Center
Unit A, 31/F, Block A
4003 Shennan Road
Luohu District
Shenzhen 518001
tel: +86.755.2598.0171
fax: +86.755.8283.7487