

AirZip[®] FileSECURE[™] Server 3.0

Installation and Configuration Manual **Linux Windows Solaris**

March 2005



Contact AirZip to report problems and/or provide feedback.

Additional help resources or updates may be available by emailing support@airzip.com

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.

© 2003-2005 AirZip, Inc. All Rights Reserved. AirZip and FileSECURE are trademarks of AirZip, Inc.

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 1.51

Table of Contents

1	INTRODUCTION	5
1.1	Who Should Use This Guide	5
1.2	What is AirZip FileSECURE	5
1.3	What's New with Release 3	5
1.4	System Components	6
1.5	System Requirements	6
2	FILESECURE SERVER INSTALLATION	8
2.1	New Installation Steps	8
2.2	Updating an existing FileSECURE Server	8
3	CONFIGURE AND HARDEN YOUR WINDOWS PLATFORM	10
3.1	Hardening a Linux Platform	11
3.2	Hardening a Solaris Platform	11
3.3	Hardening a Windows Platform	11
4	CONFIGURE YOUR DATABASE ENGINE	13
4.1	Install Microsoft SQL Server (if used)	13
4.2	Install the PostgreSQL	14
4.3	Install the Oracle 9i	15
5	INSTALL THE FILESECURE SERVER SOFTWARE	16
6	CONFIGURE THE FILESECURE SERVER DATABASE	22
7	CONFIGURE THE FILESECURE SERVER	23
8	REQUEST AND INSTALL A SIGNED X509 CERTIFICATE	25
9	INSTALL AND CONFIGURE THE SUPER USER UTILITY	27
9.1	Installing the Super User Utility	27
9.2	Configuring your Super User Account	27
9.3	Change your Super User Account Password	29
9.4	Set Email Options	29
10	INSTALL LICENSE ACTIVATION CODES	30
11	CREATE FILESECURE ORGANIZATIONS	31

12 BACK UP AND RESTORE THE FILESECURE SERVER DATABASE 34

Last page of document

34

1 Introduction

1.1 Who Should Use This Guide

This manual provides procedures for installing and configuring required components for AirZip FileSECURE Server Release 3 for both new installations and current installations. The Release 3 FileSECURE Server simplifies this process.

This manual is intended for use by System Administrators or the individual installing FileSECURE Server software. It is recommended that the individual doing the installation be trained and familiar with the operating system to be used. If using Microsoft SQL Server 2000, PostgreSQL, or Oracle 9i, the individual doing the installation should be familiar with the administration of these enterprise database engines.

1.2 What is AirZip FileSECURE

FileSECURE is a very powerful yet easy to use Digital Rights Management based application for sharing confidential and sensitive information without giving up control. AirZip FileSECURE creates and enforces rules that control the use of your information through persistent security technologies. Simply put, if you have any concerns about where your information goes and how it is used, AirZip FileSECURE provides the assurance that your information is accessed only by authorized individuals and in accordance with your security policies.

Users can be authorized for various types of permissions including view only, view and print, and view along with save, copy and paste. The right to use a file can be set to start and expire at specific times. Most importantly, the ability to use a file can be revoked by a central authority at any time. Furthermore, AirZip FileSECURE tracks and can be used to audit the usage of the files including how many times a person has opened the file and what was done once it was opened.

AirZip FileSECURE enforces security policies on electronic information even when the information travels to other organizations and individuals.

1.3 What's New with Release 3

New FileSECURE Features include:

- An improved FileSECURE Server Installer that simplifies installation on Linux, Windows, or Solaris platforms.
- An option for configuration with Oracle 9i.
- A cross platform Embedded Database Engine.
- A FileSECURE Server Control Panel with utilities for managing the FileSECURE Database and self-signing X509 certificates.
- An advanced reporting package that provides fully customizable event reports.
- An ability to reassign all file permissions from one user to another.
- An AirZip AZF File Format that secures a print quality version of any document along with the original document.
- Windows Explorer and Microsoft Office Shortcuts for securing files.
- A FileSECURE PrintSecure feature that secures a print quality version of any printable file from within its associated application!
- Enhanced Compression of scanned documents using AirZip image compression.
- Improved viewing for scanned documents including thumbnail navigation in FileSECURE Reader.
- User-selectable preferences.

- An enhanced AutoSecure and ScanSecure Options that enables XML metadata directives to control automatic securing and send functions.
- An option for opening secured files directly in the native application where you have Copy permissions.
- Faster, more dynamic viewing for scanned documents and images in Reader.

1.4 System Components

AirZip FileSECURE system consists of the following components:

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 specific permissions they have.

The **FileSECURE Super User** is an application used to configure and manage the FileSECURE Server and to set up and manage Organization partitions.

The **FileSECURE Manager** is used by an organizations security officer to configure and manage the FileSECURE service to meet an organization's security and information sharing needs.

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

The **FileSECURE Reader** is an application used to access protected information. The Reader ensures that information is used only in the intended way and only by authorized users.

1.5 System Requirements

The following minimum system requirements are required to install and deploy each component of the FileSECURE solution:

FileSECURE Server	<p>Server Platform Options:</p> <ol style="list-style-type: none"> 1. Linux with kernel version 2.4.9-31; 2. Solaris 8, or 3. Windows 2000; 2003 Server, 2000 Server, or XP <p>The computer used to host the FileSECURE Server should have at least 3 – 5 GB of free space for database growth. The FileSECURE Server components alone take about 40 – 50 MB, not including the database.</p> <p>The speed and client fan-out of the server is dependent on the processing and especially the memory of the server. A 1+ GHz single or multiple CPU machine with at least 0.5GB of RAM is recommended. More RAM is suggested if Oracle, PostgreSQL, or MS SQL Server is co-hosted on the same machine.</p> <p>Database Engine Options:</p> <ol style="list-style-type: none"> 1. FileSECURE Embedded Database where installed on the same computer as the FileSECURE Server, 2. Microsoft SQL Server 2000 SP3 Database (also MSDE 2000 per note below) where installed on the same Windows 2000 Server SP3 or 2003 Server as the FileSECURE Server or a network-connected
--------------------------	--

	<p>Windows 2000 Server and 2003 Server,</p> <p>3. PostgreSQL 7.3.3 Database where installed on the same Linux machine as the FileSECURE Server or a network-connected Linux computer, or</p> <p>4. Oracle 9i Release 2 Database where installed on the same Windows machine as the FileSECURE Server or a network-connected Windows computer.</p> <p>Note: If you previously installed FileSECURE using its embedded Microsoft Desktop Database Engine (MSDE 2000 SP3), you may use the MSSQL option to continue its use where installed on the same Windows XP, 2000 Workstation, 2000 Server, or 2003 Server machine as the FileSECURE Server or a similar network-connected Windows computer.</p> <p>Contact AirZip for compatibility with other configurations. Because there are many possible machine and software configurations, FileSECURE may not function in all configurations even of the above systems.</p>
FileSECURE Super User Utility	Microsoft Windows 2003, XP, 2000, ME, and 98. Installation requires approximately 5 MB of disk space.
FileSECURE Manager	Includes Author and Reader. Microsoft Windows 2003, XP, 2000, ME, and 98. Installation requires approximately 35 MB of disk space.
FileSECURE Author	Includes Reader. Microsoft Windows 2003, XP, 2000, ME, and 98. Installation requires approximately 25 MB of disk space.
FileSECURE Reader	Microsoft Windows 2003, XP, 2000, ME, and 98. Installation requires approximately 15 MB of disk space.

2 FileSECURE Server Installation

2.1 New Installation Steps

Installation and activation of AirZip FileSECURE Server is a ten-step process:

1. Configure and harden your Linux, Windows, or Solaris platform (See Section 3).
2. Install and configure Microsoft SQL Server, Oracle 91, or PostgreSQL database engines for data storage if one of these database engines is to be used (See Section 4).
3. Install the FileSECURE Server software (and the FileSECURE Embedded Database Server if not using one of the forementioned database engines) (See Section 5).
4. Configure the FileSECURE Database engine (See Section 6).
5. Configure the FileSECURE Server using the FileSECURE Server Control Panel and utilities for creating (or updating) the FileSECURE Database (See Section 7).
6. Install a signed X509 Certificate (See Section 8).
7. Install and Configure the Super User Utility (See Section 9).
8. Install License Activation Codes (See Section 10).
9. Create FileSECURE Organization(s) using Super User Utility (See Section 11).
10. Regularly back-up your FileSECURE Database (See Section 12).

2.2 Updating an existing FileSECURE Server

The FileSECURE software installer automatically detects previous versions of the FileSECURE on the Linux, Solaris, or Windows platform. It locates the current system files (filesecure.property, filesecure.keystore, and the Embedded database datafile if used) and reuses these files for the new installation.

Upgrading AirZip FileSECURE Server Release 2.x to Release 3 on Windows is a five-step process:

Step 1: Backup the FileSECURE Server 2 database as a precaution

Step 2: Run the FileSECURE Server 3.x Installer (See Section 5.)

Step 3: Verify the database, server, advanced, and certificate configuration and restart the FileSECURE Server Service (See Sections 6, 7 and 8).

Step 4: Start the FileSECURE Server 3.x Server Service.

Step 5: Remove the FileSECURE Server 2.x software using the following steps:

- Open the Control Panel.
- Select Add/Remove Programs.
- Locate the AirZip FileSECURE Server program.
- Click the Change/Remove button.

Upgrading FileSECURE Server Release 2.x to Release 3 on Linux or Solaris is also a five-step process:

Step 1: Backup the FileSECURE Server 2 database as a precaution.

Step 2: Run the FileSECURE Server 3.x Installer.

Step 3: Copy two files: "fileSecure.keystore" and "fileSecure.properties" from [Release_2_directory]/properties to [Release_3_directory]/previousVersion/properties.

Step 4: Run the Upgrade script to import the previous system files from the command line either

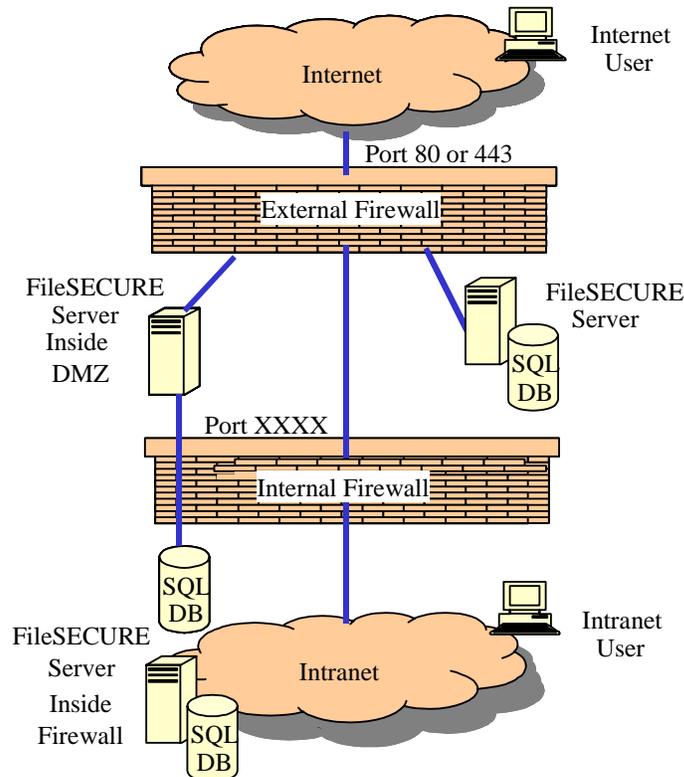
`"/upgradeRelease2.sh" or "sh upgradeRelease2.sh"`

Step 5: Remove the FileSECURE Server 2.x software using the following steps: a. If you have installed it into your system daemon, remove the file `"/etc/init.d/azFS"` (or `"/etc/rc.d/init.d/azFS"`) and symbolic link `"/etc/rc.d/rc3.d/S99azFS"`;

b. Remove the home directory `[Release_2_directory]`.

3 Configure and Harden your Windows platform

The FileSECURE Server should be thought of as a specialized secure web server. As depicted in the diagram below, the FileSECURE Server should always be protected by a firewall. The server should be assigned a Server Name (also know as a Common Name) such as **filesecure.yourcompany.com**. The Server Name (or Common Name) is the full DNS name that is used when navigating to the FileSECURE Server. To support Internet users, the firewall must allow access on the configured port number. Installation on Port 80 or 443 is strongly recommended for the broadest Internet access without complications. FileSECURE Server, when it is installed, uses Port 80 in its default configuration.



Your topology may depend on how many users your system will eventually support, and whether you want to host your SQL Server on a *separate* machine. The FileSECURE Server must be installed on a machine with reliable, fast network access.

The network interface to the SQL server (MS SQL Server, Oracle, or PostgreSQL), if hosted on a separate machine, is especially critical and should be supported on a parallel network card if not located on the same computer.

To configure the Server

1. Install the Server platform.
2. Configure your Firewall to allow or deny access.
3. Configure your DNS Server for correct routing to traffic to the Server Name (Common Name) you have selected for your FileSECURE Server.
4. Ping the server from a sample of targeted client workstations to ensure proper connectivity and DNS addressing.

3.1 Hardening a Linux Platform

Basic Linux Server Hardening Guidelines (Not comprehensive)

- The Linux server should have a designated server security administrator responsible for Procedures, Network, Physical, and OS Security.
- Linux is capable of high-end security; however, the out-of-the-box configurations must be altered to meet the security needs of most businesses with an Internet presence. Essential steps include updating the operating system, disabling unnecessary services, locking down ports, logging, and maintenance. Open source programs allow administrators to automate these processes using Bastille, sudo, logging enhancers such as SWATCH, and antivirus software.
- Consult the articles on Linux Server Hardening available on the Internet such as the one at the following link:
<http://linuxtoday.com/security/2003070900526OSHL5W>
- Implement SSL support
- Maintain latest Virus protection software
- Ensure that regular backups and that media is physically protected from theft or damage and regularly stored off-site.

3.2 Hardening a Solaris Platform

Basic Solaris Server Hardening Guidelines (Not comprehensive)

The Solaris server should have a designated server security administrator responsible for Procedures, Network, Physical, and OS Security.

Other useful documentation, including hardening scripts for Solaris, can be found on the following web sites:

The TITAN project and documentation can be found at
<http://www.fish.com/titan/>

The JASS Web site — <http://www.sun.com/software/security/jass/>

The Solaris Security Toolkit- Quick Start, Alex Noodergraaf and Glenn Brunette, June 2001 —

http://www.sun.com/blueprints/0601/jass_quick_start-v03.pdf

The YASSP page — <http://www.yassp.org>

<http://www.enteract.com/~lspitz/armoring.html>.

3.3 Hardening a Windows Platform

Basic Windows Server Hardening Guidelines (Not comprehensive)

The Windows server should have a designated server security administrator responsible for Procedures, Network, Physical, and OS Security.

Always install the latest service pack and the latest security hot fixes from Microsoft. They fix critical security related problems in the operating system. The latest security hot fixes are available at:

<http://www.microsoft.com/technet/security/current.asp>

Always rename the Administrator account and give it a password with 14

characters in length and make sure that the password contains numbers, punctuation and upper and lower case characters.

Never use the same password for the local and domain administrator passwords.

Avoid, if possible, installing FileSECURE Server on Primary or Backup Domain Controllers (PDC and BDC).

Store backup copy of any encryption certificates and private keys off site as well as on-site (with both in a secure location).

Securing Windows (server and professional version) is a moving target; therefore, review Microsoft's Security website and the SANS guide for Securing Windows 2000.

- Post Installation: Implement SSL support.
- Maintain latest Virus protection software.
- Ensure that regular backups are performed and verified, that media is physically protected from theft or damage, and that Backup media is regularly stored off-site.

4 Configure your Database Engine

FileSECURE Server provides a choice in database engines for storing user and file permission data:

The **FileSECURE Embedded Database** is suited to small workgroup environments up to 100 users, assuming normal usage patterns. It is automatically installed with FileSECURE Server and can be used on any supported platform. It may be used only on the same machine as the FileSECURE Server.

Microsoft SQL Server 2000 is a commercial, enterprise data management platform designed for Windows Servers and is recommended for enterprise installations of FileSECURE. Contact Microsoft to license SQL Server.

Note: If you previously installed FileSECURE and are using its embedded Microsoft Desktop Database Engine (MSDE 2000), use the MSSQL option to continue its use.

PostgreSQL provides a high performance, enterprise data management platform. It is an open source database that may be used with FileSECURE on Linux platforms.

Oracle 9i is likewise a commercial, enterprise data management platform that may be deployed on a wide range of platforms and is recommended for enterprise installations of FileSECURE. Contact Oracle to license.

4.1 Install Microsoft SQL Server (if used)

Follow Microsoft instructions for the installation of SQL Server 2000. Once installed, the following information about the SQL Server will be required to complete the FileSECURE installation:

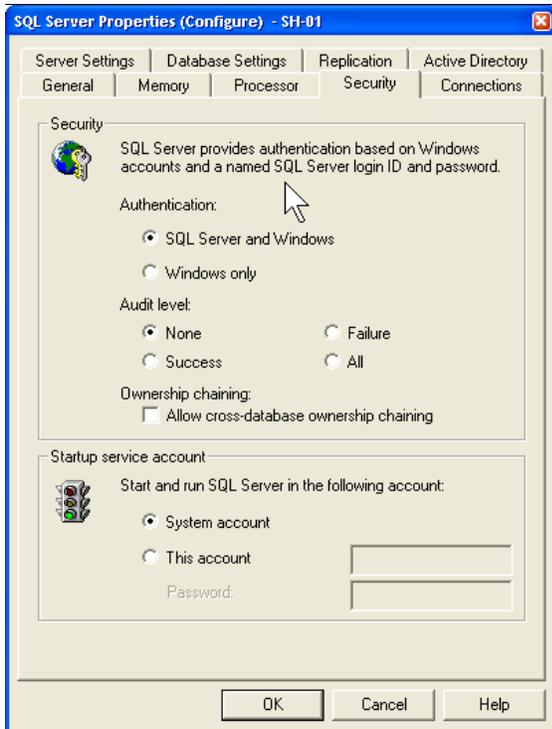
- SQL server login account ID and password.
- The machine name where the SQL server or MSDE database resides.

It is recommended that SQL Server 2000 be installed with Service Pack 3. During the SP3 [installation](#), a screen like this will be shown and it is highly recommended that the SA account be given a password for security reasons before continuing:



Record this password for later use in FileSECURE Server configuration.

Set the authentication level for the SQL Server in the **SQL Server – Security Properties Page** as shown below.



Select **SQL Server and Windows** as the method of authentication for both the full SQL Server (and the MSDE Desktop server if you configure the MSDE database with the full SQL Server tools instead of using the included automatic installer).

4.2 Install the PostgreSQL

Install PostgreSQL referring to the PostgreSQL documentation available at the following link:

<http://www.postgresql.org/docs/pdf/7.3/admin-7.3.2-US.pdf>

or the online book

<http://www.commandprompt.com/ppbook/>

PostgreSQL can be installed on either same machine with FileSECURE Server or another machine.

The basic steps are as follows:

1: Create a LINUX user account to own and manage the PostgreSQL database files. For example,

```
$ su - -c "useradd postgresAdmin"
```

2: [Install PostgreSQL](#) via following 10 steps in Chapter 2 of the online book

<http://www.commandprompt.com/ppbook/>

3: Follow the instruction from the above documents to initialize the database. For example, if you install PostgreSQL in the default directory /usr/local/pgsql, go to /usr/local/pgsql/bin and run

```
initdb -D /usr/local/pgsql/data
```

4. Start the database server using:

```
postmaster -D /usr/local/pgsql/data
```

or

```
pg_ctl -D /usr/local/pgsql/data -l logfile start
```

4.3 Install the Oracle 9i

Install Oracle 9i referring to Oracle documentation available at the following link:

http://download-west.oracle.com/docs/html/A95493_01/toc.htm

Note When installing Oracle 9i, you have an option to choose which character-set to use. This is global to the Oracle installation. It is not possible to allow different database schemas to use different character sets. To enable the broadest support of languages, configure Oracle to use the UTF8 Unicode char-set option if possible.

5 Install the FileSECURE Server Software

Once SQL Server, Oracle 9i, or PostgreSQL is configured or if using the FileSECURE Embedded database, FileSECURE Server installation should take between 5 and 30 minutes.

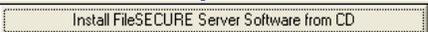
The FileSECURE Server Installer installs the AirZip FileSECURE Server software as well as Tomcat web service, Java Virtual machine to run the server components, SSL libraries to ensure secure communication and other security tools, and Embedded Database (QED) software.

Install CD also contains copies of this manual, user guides, and copies of the client software package.

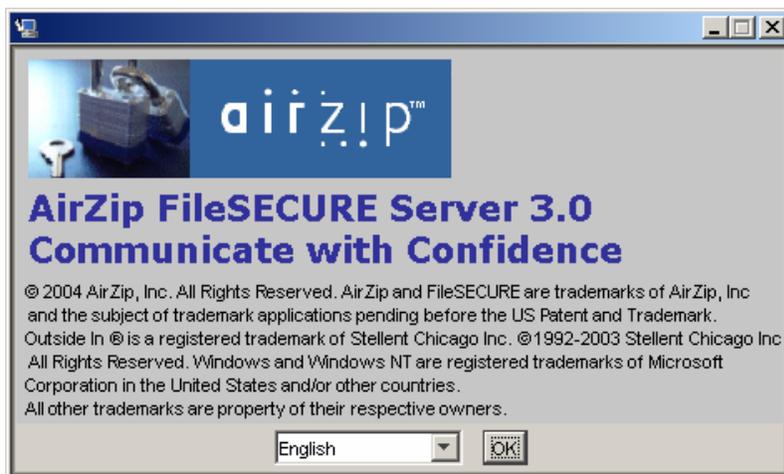
To install the FileSECURE Server for the first time or to upgrade to the latest release, follow these steps:

1. Locate the FileSECURE Server Release 3 Install CD or download all the files on the distribution CD to a **LOCAL directory** on your server or workstation. FileSECURE Server can be installed from a network share.

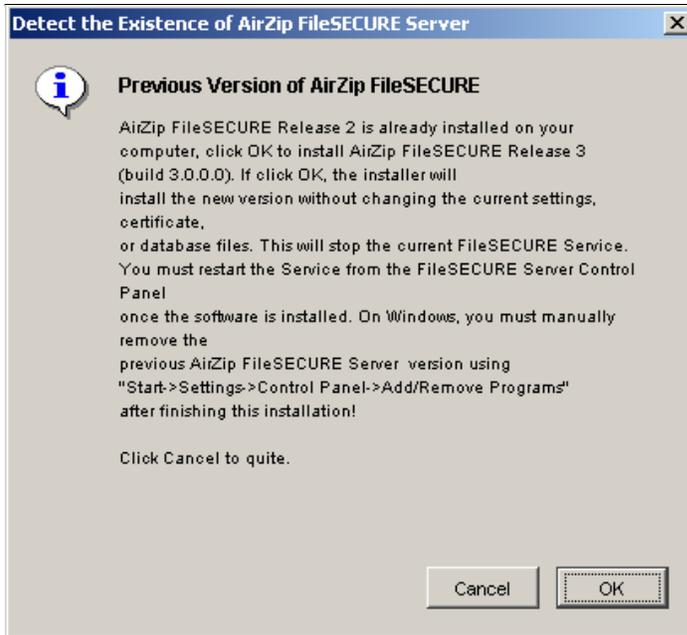
2. Locate and run the FileSECURE Server Installer (AirZipFSInstallOnLinux, AirZipFSInstallOnSolaris, AirZipFSInstallOnWindows). to begin the process of installing the FileSECURE Server Software.

Note: When inserted in Windows machines, the Install CD will open an installation selection application if your CD device is set to allow “AutoPlay”. The installation selection application simplifies access to the content of the CD. Just click  to install the Server software.

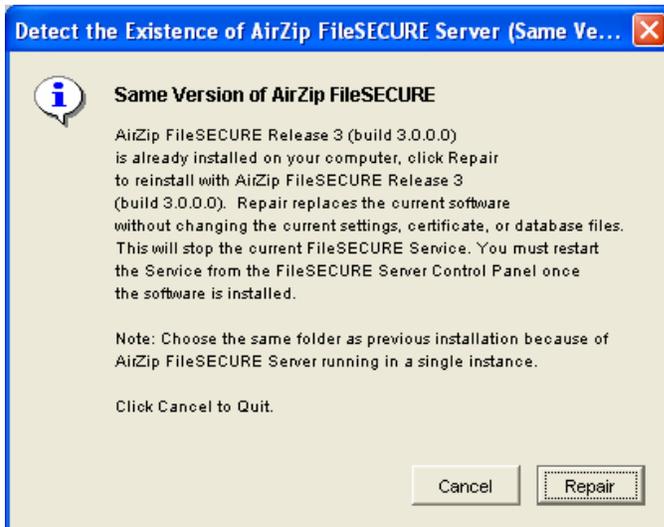
3. At the Welcome screen, select the language for the installer package from the available list and click OK. The language selection determines the language used for the installation process only. The FileSECURE Server Control Panel and Help are provided only in English.



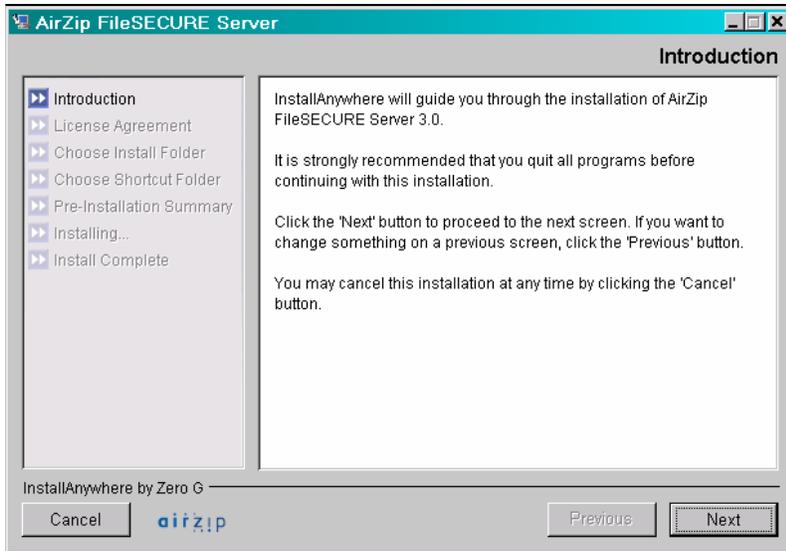
Note: If the following screen appears when executing the Server Installation, it means that a previous version of FileSECURE Server is already installed:



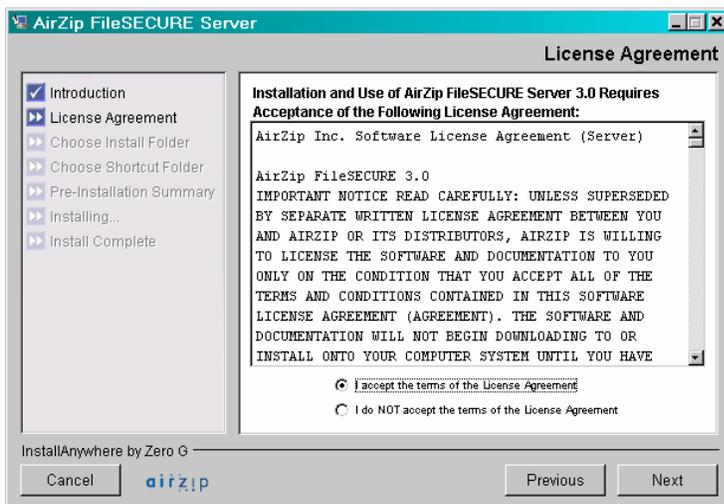
Note: If the following screen appears, click Repair to replace the current FileSECURE Server software with the software on the install disk or Cancel to retain the currently installed software.



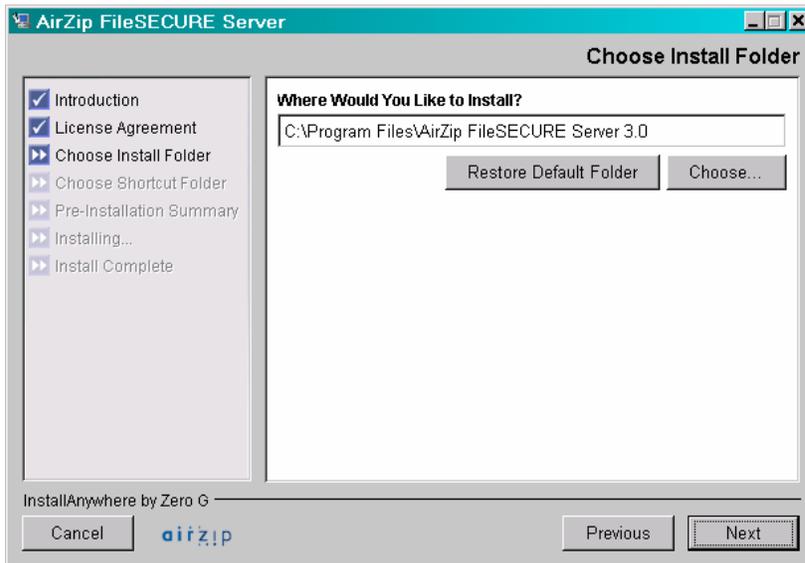
4. At the next screen review the instructions and click Next.



5. Review licensing terms thoroughly before proceeding.

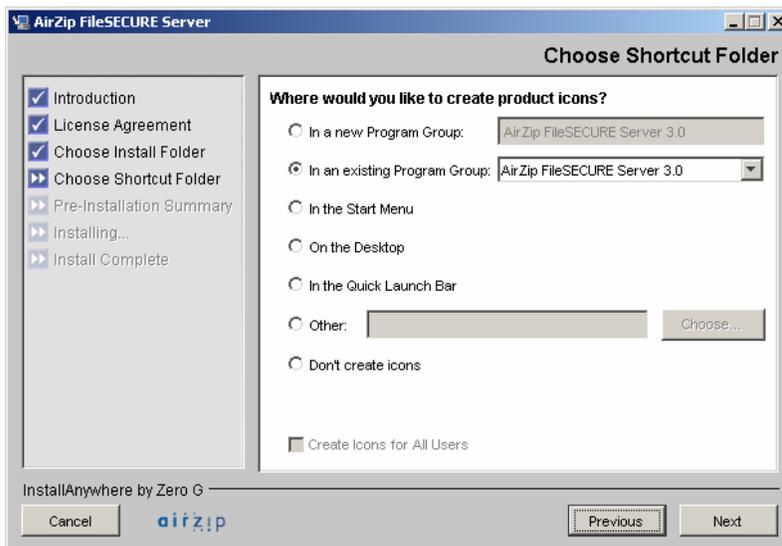


6. If installing on Windows, at the next screen select a target directory for Server Installation. The default installation directory is shown but can be changed to another directory using the “Choose...” button.

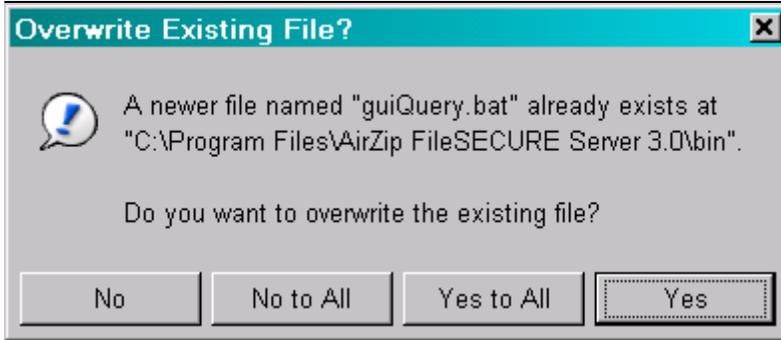


Once the target directory is selected, click the “Next ” button to proceed.

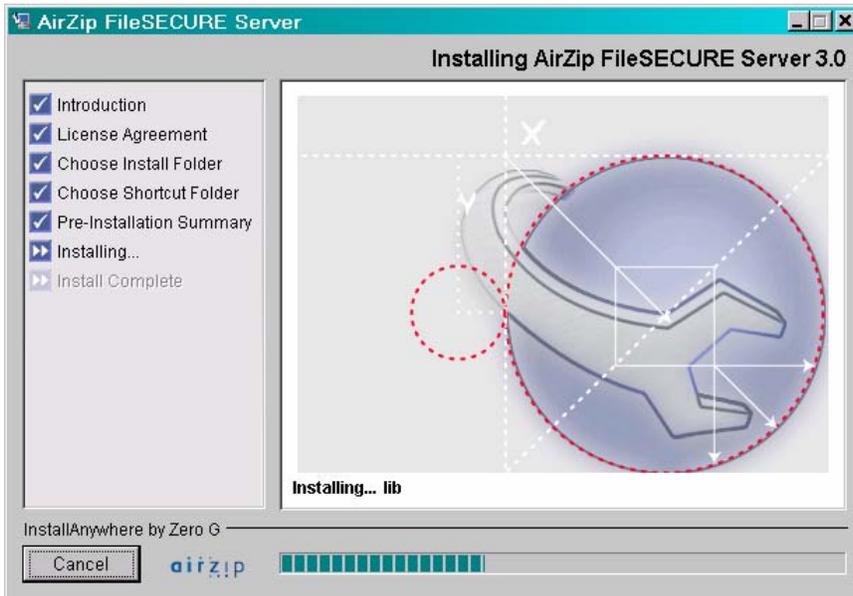
7. If installing on Windows, at the next screen select where you would like to create product icons and click **Next**.



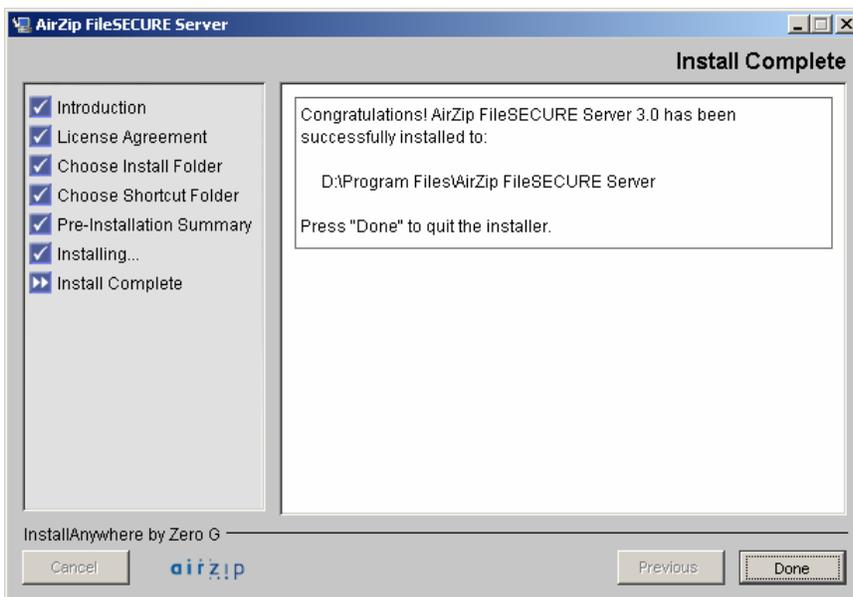
If upgrading to a new version of FileSECURE Server, the installer will ask if you want to overwrite certain current files. You may generally select **Yes to All**. The installer locates and updates critical current files.



8. The following display shows the status of the installation process.



9. When the installer confirms that the installation is complete, click **Done** and proceed with the Server configuration.



10. Proceed to Section 6.

6 Configure the FileSECURE Server Database

To select and configure the FileSECURE Database

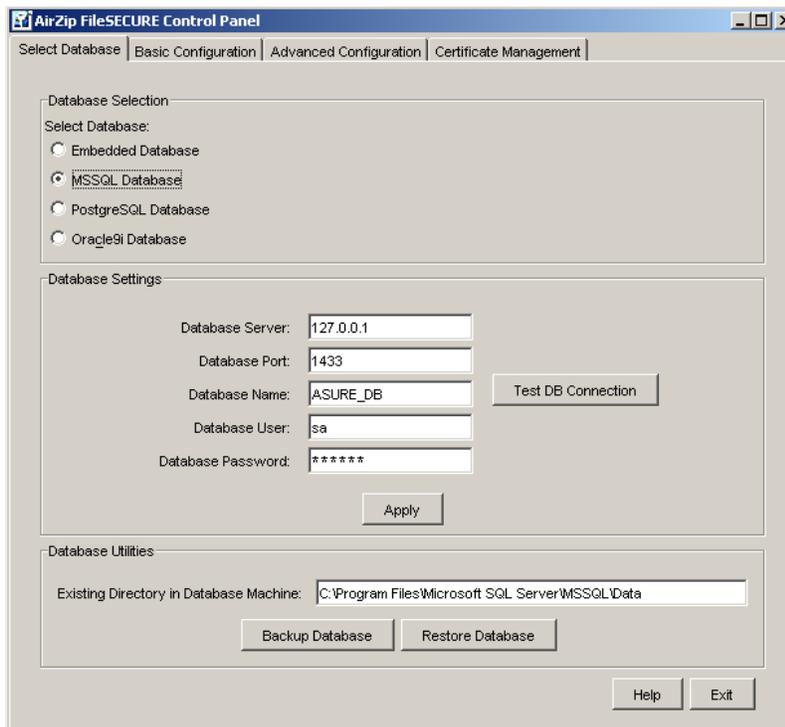
1. Open the FileSECURE Server Control Panel and select the Database tab. To open the Control Panels on Windows, select **Start->Programs->AirZip FileSECURE Server 3.0->AirZip FileSECURE Server Control Panel**



To open the Control Panel on Linux or Solaris, use the follow case sensitive string from command line:

```
./controlPanel.sh or sh controlPanel.sh
```

The Control Panel Select Database tab is shown below



2. Follow the online help instructions to select and configure your database and to run requisite database creation and update scripts. After a new installation you must "create" the FileSECURE database. After upgrading to a new version of FileSECURE Server software release, you must "update" the database to the latest configuration.

If using the Embedded Database or Microsoft SQL Server from a Windows Server, clicking the **Apply** button will automatically create or update the FileSECURE database. **⚠ Note:** Closely follow the online instructions for creating the database the first time when using Microsoft SQL Server.

⚠ Note: If you previously installed FileSECURE and are using its embedded Microsoft Desktop Database Engine (MSDE 2000), use the MSSQL option to continue its use.

Follow the online help instructions to manually run the requisite scripts for PostgreSQL and Oracle 9i database configuration.

Backup and Restore: See section [Back up and Restore the FileSECURE Server Database](#) of this manual for additional details.

7 Configure the FileSECURE Server

To configure the FileSECURE Server

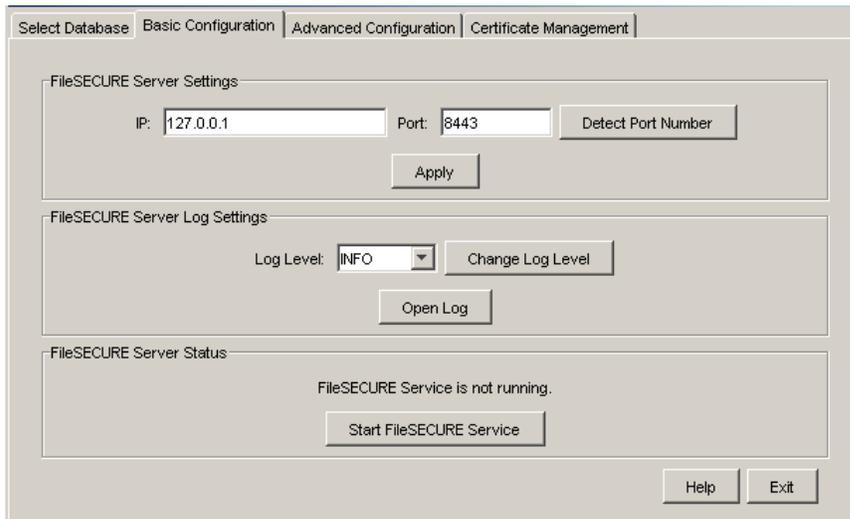
1. Open the FileSECURE Server Control Panel and select the Basic Configuration tab. To open the Control Panels on Windows, select **Start->Programs->AirZip FileSECURE Server->AirZip FileSECURE Server Control Panel**.



To open the Control Panel on Linux or Solaris, use the follow string from command line

`./controlPanel.sh` or `sh controlPanel.sh`

The Control Panel Basic Configuration tab is shown below



2. Follow the online help instructions to configure FileSECURE Server settings, to change log settings, and to start and stop the FileSECURE Server. When FileSECURE Server software is first installed, basic server configuration settings are set to default values. The only configuration setting that must normally be checked is the communication PORT setting. Otherwise, the FileSECURE Server may be started immediately and the other options modified as and when desired.

To set service provider information and to configure an SMTP Server for email notifications Advanced FileSECURE Server Configuration

1. Open the FileSECURE Server Control Panel (as described in Section 7) and select the Advanced Configuration tab shown below.

Select Database | Basic Configuration | **Advanced Configuration** | Certificate Management

Provider Setting

Provider Name:

Provider Phone:

Provider Email:



SMTP Setting

SMTP Server Name:

SMTP User Name:

SMTP User Password:

2. Follow the online help instructions.

8 Request and Install a Signed X509 Certificate

FileSECURE uses the Secure Socket Layer (SSL) protocol to secure the communication between FileSECURE Client and FileSECURE Server. SSL is a security protocol that provides privacy and authentication for network traffic. SSL was developed in the Netscape web browser and has since become a de-facto industry standard.

The use of SSL requires the installation of an X509 Certificate on the FileSECURE Server.

FileSECURE requires that the certificate is

- a) Signed by AirZip, Verisign, Thawte, Baltimore or another Certificate Authority where you have imported its Root and
- b) Matches your server's Internet Server Name – e.g., filesecure.yourcompany.com – that you are using on your server.

An X509 certificate is a public key of a user, in this case the FileSECURE Server, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.

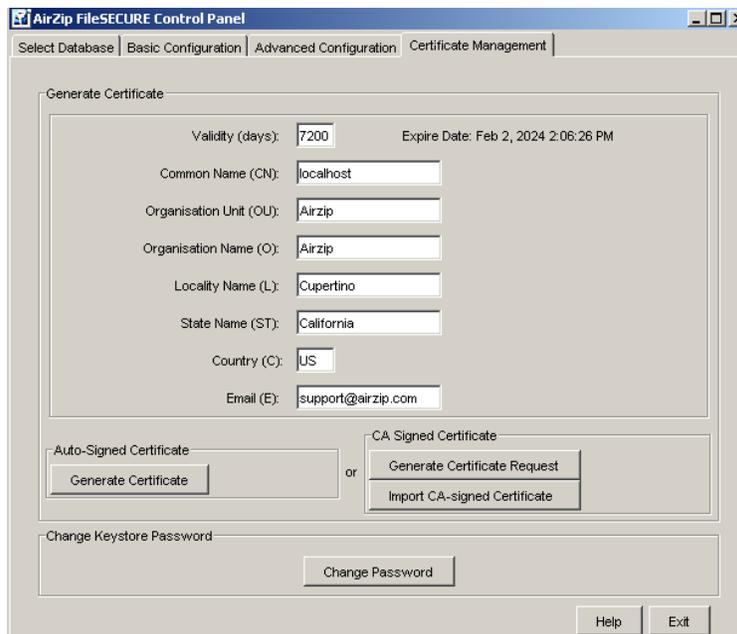
FileSECURE clients validate the Server certificate and will present a warning message each time the user authenticates with the Server if an improper certificate is installed.

To properly secure your FileSECURE Server and avoid repeat user warnings, you must replace the temporary self-signed certificate installed with the FileSECURE Server software with one that is properly signed.

Note: Your certificate is unique to your Server and cannot be moved from machine to machine.

To display the contents of the X509 certificate protecting your FileSECURE Server or to request and install new X509 certificates

1. Open the FileSECURE Server Control Panel (as described in Section 7) and select the **Certificate Management** tab shown below.



When first opened, the top portion of this panel displays the contents of the currently installed X509 certificate including its expiration date, Common Name that it registers, Organization to which it was issued, etc. The FileSECURE Server Installer automatically installs a placeholder X509 Certificate.

2. Follow the procedures provided in the Online Help topic for this control panel tab to

-
- to generate an AirZip auto-signed certificate that is useful for evaluation or other temporary configurations. It is easy but not as secure as a certificate signed by an authorized Certificate Authority, or .
 - alternatively, generate X509 Certificate request that can be sent to an authorized Certificate Authority, then use the control panel to install the signed certificate that is returned. This is the most secure method for protecting your FileSECURE Server.

You may also use this control panel to change the Keystore Password. Your X509 Certificate is stored in a file called a 'keystore'. The keystore is password protected. When FileSECURE Server is initially installed the password for the keystore is set to 'airzip'. You may change the password for your keystore at any time.

9 Install and Configure the Super User Utility

After the FileSECURE Server has been installed, the Super User Utility must be installed on a Windows computer to enter necessary License Activation Codes and to begin to add or manage Organizations. The following provides step-by-step procedures for:

1. Installing the Super User Utility
2. Configuring your Super User Account
3. Changing the Super User password
4. Installing License Activation codes
5. Configuring a new organizational account

9.1 Installing the Super User Utility

To install the Super User Client, follow these steps:

1. Locate the FileSECURE Server Release 3 Install CD.

2. Insert Install CD into the Windows machine on which you want to install the Super User Utility.

Note: When inserted in Windows machines, the Install CD will open an installation selection application if your CD device is set to allow “AutoPlay”. The installation selection application simplifies access to the content of the CD. . If the installation selection program does not start automatically, locate and run the **autorun.exe** program. The **autorun.exe** program is located in the top directory of the CD’s contents.

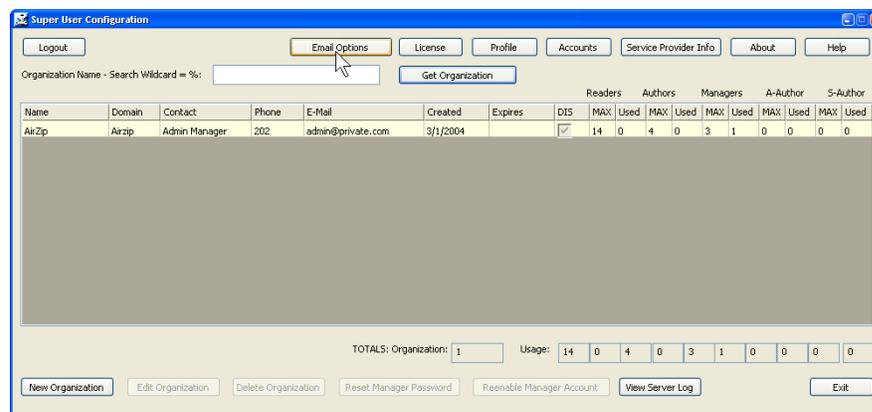
3. Click  to begin the installation process.

4. Answer the typical questions until the install is completed.

Be sure to carefully review the license terms.

When the installation is complete, select **Start > Programs > AirZip FileSECURE > Super User Utility** to run the Super User Utility.

The Super User Utility window will appear as shown.



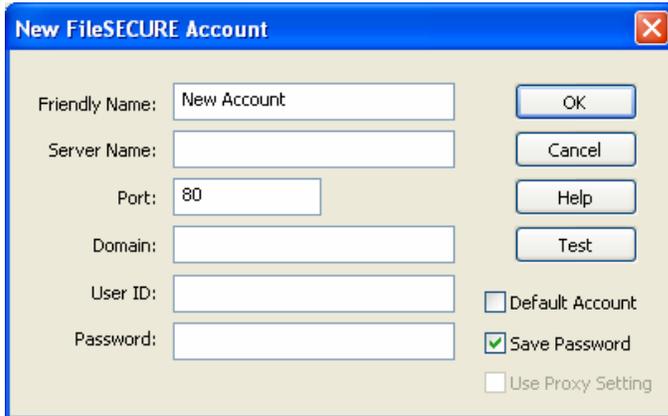
5. Click the  button to access the Help Center to learn how to use the Super User Utility features and capabilities.

9.2 Configuring your Super User Account

Once the Super User Client is installed and started, the next step is to configure your super user account by following these steps:

1. Open the Super User Utility (Start > Programs > AirZip FileSECURE > Super User Utility).

2. Click the  button in the upper left hand corner. You will be presented with the follow dialog:



The dialog box titled "New FileSECURE Account" contains the following fields and controls:

- Friendly Name:
- Server Name:
- Port:
- Domain:
- User ID:
- Password:
- Buttons: OK, Cancel, Help, Test
- Checkboxes: Default Account, Save Password, Use Proxy Setting

3. Fill in the fields as follows:

Friendly Name should be something that will help you recognize that this is the account login that will be used for logging on as the Super User, such as MyServer Super User.

Server Name should be the full DNS name (e.g., filesecure.airzip.com) that user organizations will be using to access your FileSECURE Server to ensure it is operational. If the DNS name has yet to be implemented, an IP address (216.218.133.74) or the “Microsoft Windows Network” machine name on which you have installed the server can be used on an interim basis.

Port is the port number that you used when configuring your server.

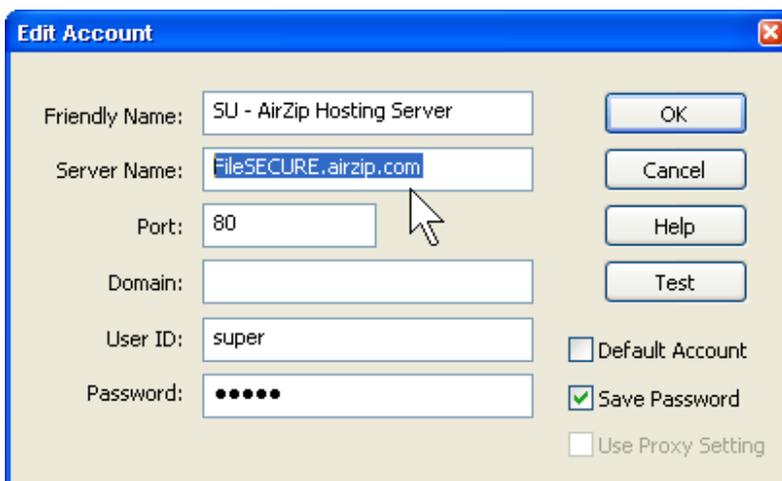
Domain should be left blank for logging on as Super User.

User Id is **super** (case sensitive, all lower case).

Password is **super** (also case sensitive, all lower case).

Note: It is always a good idea to “ping” the selected server’s name and/or address if there is ever a question about visibility or connectability.

When complete, your Login dialog should look something like the following:



The dialog box titled "Edit Account" contains the following fields and controls:

- Friendly Name:
- Server Name:
- Port:
- Domain:
- User ID:
- Password:
- Buttons: OK, Cancel, Help, Test
- Checkboxes: Default Account, Save Password, Use Proxy Setting

IMPORTANT NOTE ON USING OTHER ADDRESSING SCHEMES:

Normally the Organizations that will be using your FileSECURE Server

will do so through a WAN Internet connection using a fully qualified Internet URL or IP address.

If all Organizations on this server will use only LOCAL LAN access, then users may elect to use the actual Microsoft Windows Network machine name to contact the FileSECURE Server.

4. Click the **Test** button to confirm that the information is entered correctly and the account is available. You should see the following messages:



5. Click the **OK** button to logon to the server. You will be returned to the main screen, but the Login to Server button will be replaced with a Logout button if you have logged in successfully.

9.3 Change your Super User Account Password

The first thing you should do when you have logged on successfully is change the Super User password. Follow the procedures below:

1. Click on the **Profile** button at the top middle of the Super User Utility main screen.
2. Select the Change Password checkbox in the lower part of the resulting dialog.
3. Type the new password twice; once in the New Password box and once in the Confirm box. The result should look like this:



4. Click OK to change the password.

9.4 Set Email Options

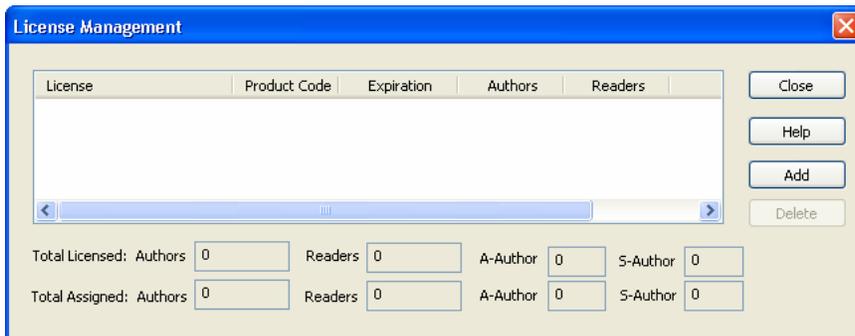
When you add a new Organization or reset a Manager's password, FileSECURE composes an email message addressed to the Organization Manager. The message contains the user's account details and other essential information. The Super User will use your MAPI-compliant emailer to send such messages unless you change your Email Options to automatically use your SMTP Server. Use the Email Options button with its associate Help to enter your SMTP Server information.

10 Install License Activation Codes

AirZip FileSECURE Server software incorporates a software licensing mechanism that allows features and registered user expansion via simple to install license activation codes. When your Server Software is first installed, you may log in using the Super User account but you must install one or more software license activation codes in order to begin configuring new Organizations or using specific features such as Directory Services Synchronization. Typically a license code enables the configuration of a particular number of registered Author and/or Reader Users. Authors include users configured as Managers, AuthorPlus, or Author accounts.

To enter a License Code

1. Open and login to **FileSECURE Super User Utility** (Start > Programs > AirZip FileSECURE > Super User Utility).
2. Click the **License** Button to open the License Management dialog



3. In the License List, click **Add** button.
4. Enter the license code that your AirZip Reseller has provided to you in the Add License dialog and click **Apply**. **Note: The license codes are case insensitive.**
5. The License Management dialog box lists all license codes entered and the associated capabilities enabled. It also displays the total number of licensed and currently configured, registered user accounts available for organizations on this Server.

11 Create FileSECURE Organizations

The FileSECURE Server provides service to multiple independent groups of users, called Organizations. An Organization might be a department in a large company or agency. An Organization might be another company for which you are hosting FileSECURE as a service.

Each Organization has its own Users, its own definition of how its Users are organized into User Groups, its own definition of Security Categories and permissions, its own permissions database, and its own reports. Each Organization is assigned a unique “Domain” name that becomes a part of the credentials that users must have to access their account. Users must know the URL of the FileSECURE Server, their Organization’s Domain name, their User ID, and their password to access their account.

Each Organization has a primary default Manager Account. When you use the Super User Utility to create an Organization, you also create the default Manager Account and normally assign that account to a person within that Organization who will act as its “security officer” in terms of setting up the Security Policies for their Organization as well as controlling User Accounts.

Importantly, users in one Organization do not have access to any information or data about any other Organization. Likewise Super Users do not have access to file or user information for any Organization.

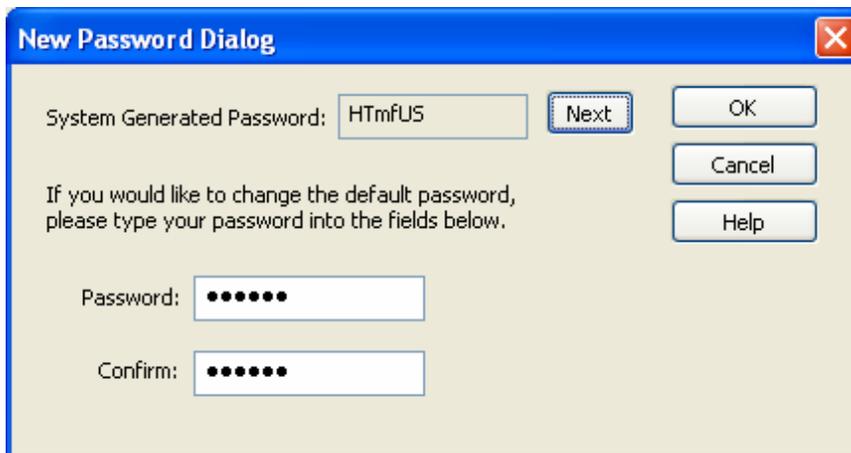
The simplest configuration for FileSECURE Server for a company, institution or agency is to configure just one Organization.

Aside from the Super User, all other FileSECURE Users access the FileSECURE Server using Accounts associated with Organizations. Keep in mind the following concerning Organizations:

1. Super Users can create Organizations, but FileSECURE Managers access and control each Organization separately. You will not be able to use your Super User Account to access or administer Organizations, only the person that you assigned as the default Manager of that Organization and any subsequent user provided a Manager account may add FileSECURE Users and configure the operation of FileSECURE within their Organization.
2. When each Organization is created, an initial default Manager Account is created to access the Organization.
! IMPORTANT: The UserID of the default Manager is always “admin”.
3. Each Organization is completely independent and autonomous, with no access rights between them.

To create your first Organization, do the following:

1. Click the **New Organization** button in the lower left corner of the main screen.
2. The New Organization Password Dialog will be displayed, similar to this:

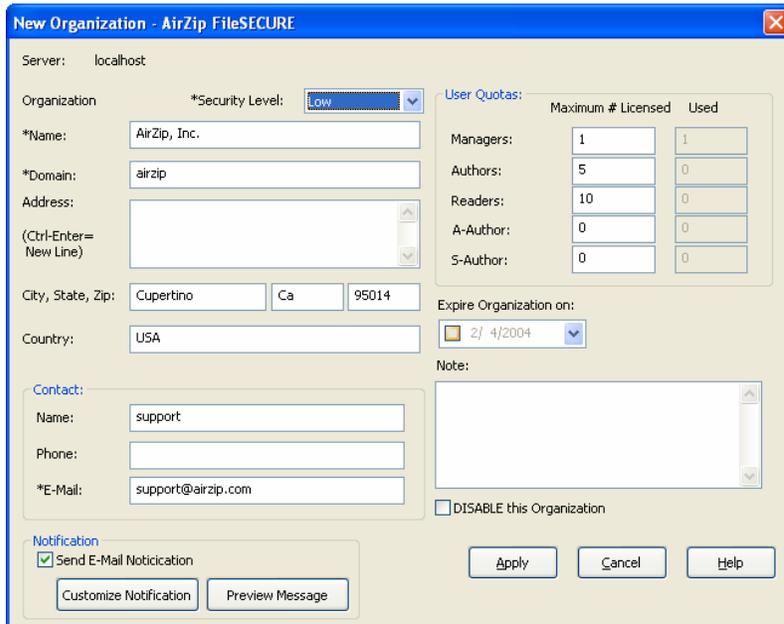


3. This dialog displays a random password for the default Manager Account for the new Organization. You have three options from here:
 - a) Click **Next** to generate another random password.
 - b) Type in your own password in the Password and Confirm boxes.
 - c) Click **OK** to accept the current password.

You may want to write the password down at this point for future reference to possibly assist the new manager in authenticating for the first time.

After accepting the password, the New Organization dialog will be displayed.

4. Refer to the online Help for procedures for properly configuring a FileSECURE Organization. When filled out, it will look something like this:



New Organization - AirZip FileSECURE

Server: localhost

Organization *Security Level: **Low**

*Name: AirZip, Inc.

*Domain: airzip

Address:
 (Ctrl-Enter= New Line)

City, State, Zip: Cupertino Ca 95014

Country: USA

Contact:
 Name: support
 Phone:
 *E-Mail: support@airzip.com

User Quotas:

	Maximum # Licensed	Used
Managers:	1	1
Authors:	5	0
Readers:	10	0
A-Author:	0	0
S-Author:	0	0

Expire Organization on: 2/ 4/2004

Note:

DISABLE this Organization

Notification Send E-Mail Notification

5. Click the **Preview Message** button at the bottom left of the New Organization dialog box to review and possibly customize the email message that will be sent to the new Organization's security administration officer.
6. Click the **Apply** button when you have filled in all the appropriate information. FileSECURE will automatically generate and save to your hard drive the New Organizations Private Recovery Key. **NOTE: Ensure that Recovery Keys are stored for safekeeping with a reliable key escrow agent.**
7. When the private key dialog box appears, note the name of the key, which can be found in the same directory as the Super User application on your computer. As soon as you have noted the name of the Private Key, click **OK**.

⚠ PRECAUTION: These private keys are provided primarily for disaster recovery in the highly unlikely event that a FileSECURE Server should ever lose its normal security protecting keys. This key is generated ONLY when an Organization is created and is ONLY useful for the created organization's protected files.



❗ **The PRIVATE KEY should be copied to dependable removable media and physically stored under lock and key for safe long-term insurance.**

❗ **The PRIVATE KEY file should then be REMOVED from the hard disk of the Super User's computer AFTER the key has been copied and verified.**

8. The Super User Utility will now bring up an email message addressed to the manager of the new organization. Edit this message as appropriate and send it to complete the creation of a new organization/ domain and an administrator account for that organization/domain.

The Super User application will inform you that the account has been created successfully.

The email notification message instructs the users assigned as the default Manager to download the Manager software (which also includes FileSECURE Author and Reader) from AirZip standard FileSECURE client download sites.

Manager software is on the following site:

<http://www.airzip.com/FileSECUREManager3.htm>

When the Manager creates other users, they likewise receive email messages detailing their account information and instructing them to download and install the software from the following sites:

<http://www.airzip.com/FileSECUREAuthor3.htm>

<http://www.airzip.com/FileSECURERead3.htm>

AirZip FileSECURE download sites provide quick start guides for each client.

12 Back up and Restore the FileSECURE Server Database

FileSECURE becomes a critical enterprise application containing data of extreme importance. FileSECURE Server stores only information related to users and file permissions. The growth in database size is linearly dependent on the number of users and their level of activity. Regular database back up is strongly recommended.

Note: Use extreme caution when restoring a database to a previous backup, as all transactions between the time the backup was generated and the current time will be lost and will not be recoverable unless another “current” backup is made first.

To Backup and Restore FileSECURE Embedded or MSQL 2000 Database

1. In the Database Utilities area of the FileSECURE Server Control Panel, click the **Backup Database** button to generate a backup of the current contents of the FileSECURE data tables.
2. Select the location for the back up copy of the database and click Ok.

To restore the FileSECURE Server Embedded Database

1. Select the location of the most recent database back up file
2. Click the **Restore Database** button.

To Backup and Restore databases created on PostgreSQL

- Use PostgreSQL backup utilities.

To Backup and Restore databases created on Oracle

- Use Oracle backup utilities.

Last page of document