



AirZip[®] FileSECURE[™] 4.0

Installation and Configuration Manual
Windows · Unix/Linux · Mac OS X

August 2005



(c) 2002-2005 AirZip, Inc. All rights reserved. AirZip, the AirZip logo, FileSECURE AutoSECURE, emailSECURE and ScanSECURE are either registered trademarks or trademarks of AirZip, Inc. in the USA and other countries.

Contact your Authorized AirZip Reseller 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.

The product includes software developed by the Apache Software Foundation (<http://www.apache.org>).

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 4.0

Table of Contents

1	INTRODUCTION	1
1.1	Who Should Use This Guide	1
1.2	What is AirZip FileSECURE	1
1.3	What's New in Release 4	1
1.4	System Components	2
1.5	System Requirements	2
2	FILESECURE SERVER INSTALLATION OVERVIEW	5
2.1	Steps for a New Installation	5
2.2	Steps for Updating an Existing Installation	5
3	INSTALLING THE SERVER DATABASE	6
3.1	Installing Microsoft SQL Server	6
3.2	Installing PostgreSQL	7
3.3	Installing Oracle 9i	7
4	INSTALLING FILESECURE SERVER	8
4.1	Installing or Upgrading FileSECURE Server	8
5	INSTALLING A SERVER LICENSE	13
5.1	License Management	13
5.2	Requesting a License Key	13
5.3	EVALUATION, TEMPORARY and PERMANENT Licenses:	14
5.4	Installing a License Key	14
6	CONFIGURING THE SERVER DATABASE	15
6.1	Configuring the Server Database	15
6.2	Database Backup and Restore	15
7	CONFIGURING FILESECURE SERVER	17
7.1	Basic Configuration	17
7.2	Configuring the Communication Port	17
7.3	Configuring the Server Log Level	18
7.4	Starting and Stopping FileSECURE Server	18
7.5	Changing the provider settings	18

8	REQUESTING AND INSTALLING A CERTIFICATE	20
8.1	Generating a self-signed certificate	21
8.2	Generating a X509 Certificate Request	21
8.3	Installing a CA-Signed Certificate	22
8.4	Changing the Keystore Password	22
8.5	Restoring a Previous Certificate	22
9	INSTALLING AND CONFIGURING SUPER USER UTILITY	24
9.1	Installing the Super User Utility	24
9.2	Configuring the Super User Account	24
9.3	Changing the Super User Account Password	25
9.4	Configuring Email Settings	26
10	CREATING ORGANIZATIONS	27

1 Introduction

1.1 Who Should Use This Guide

This manual provides procedures for installing and configuring required components for AirZip FileSECURE Server Release 4. Both new installations and updating existing installations are covered. This manual is intended for use by system administrators installing AirZip FileSECURE Server.

1.2 What is AirZip FileSECURE

AirZip FileSECURE is a powerful yet easy to use Digital Rights Management solution 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. 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 in Release 4

New Server Features

- Licensing mechanism enhanced to enable FileSECURE to be effectively used in an ASP (hosted) environment.
- Support added for hardware encryption devices certified by the State Commission of Cryptography Administration of the People's Republic of China.
- Support for proxies and firewalls enhanced.
- Embedded database performance improved.
- CA-signed or AirZip-signed certificate now required for server authentication.
- Control Panel and Database Manager user interfaces improved.
- LDAP performance and synchronization reliability enhanced.
- Support added for the following LDAP servers:
 - Novell eDirectory/NDS
 - IBM SecureWay Directory Server
 - IBM Directory Server
 - IBM Tivoli Directory Server
- Additional server platforms now supported:
 - Apple Mac OS X 10.4 (Tiger)
 - HP-UX 11.11 (PA-RISC) and 11.23 (Itanium)

- IBM AIX 5.1 or later
- Linux (RedHat AS3 and SuSE SLES9) on x86 and POWER
- SGI Altix with ProPack 4
- Sun Solaris 10
- Server internal security enhanced.
- Numerous bug fixes and minor updates implemented.

New Super User Features

- Generated Private Keys can now be saved in a user specified location and are named with the related organization name for easy identification.

New Manager Features

- Improved support for LDAP servers.

New Author Features

- Support for Visio 2002 and 2003 and Outlook 2000-2003. Documents can now be secured from within Visio and both the email body and attachments can be secured from within Outlook.
- Full integration with the RICOH Ridoc Documentation Management System.

New Reader Features

- Viewing support enhanced to view up to 370 different file formats.
- Screen capture blocking improved to block a wider range of screen capture programs to ensure higher security for documents. Sessions run through VNC, VMWARE, Windows Terminal Services and PC Anywhere are prohibited from viewing documents.

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 organization's 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. Microsoft Windows XP, 2000, or 2003 2. Apple Mac OS X 10.4 (Tiger) 3. HP-UX 11.11 (PA-RISC) or 11.23 (Itanium) 4. IBM AIX 5.1 or later 5. Linux (RedHat AS3 or SuSE SLES9) on x86 or POWER 6. SGI Altix with ProPack 7. Solaris 8 or later <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 50 – 60 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 Windows 2000 Server and 2003 Server, 3. PostgreSQL 7.3.3 Database where installed on the same Linux machine as the FileSECURE Server or a network-connected Linux computer, or 4. Oracle 9i Release 2 Database where installed on the same Windows machine as the FileSECURE Server or a network-connected Windows computer. <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	<p>Microsoft Windows 2003, XP SP1/SP2, 2000 Pro/Server, ME, NT4.0 SP6, and 98. Installation requires approximately 5 MB of disk space.</p>

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 Overview

This chapter provides an overview of the steps required to install or update FileSECURE Server. Please be aware that FileSECURE Server must be installed on properly secured server. General system security is not covered in this manual; however, it is necessary to ensure that your server and network are appropriately secured.

2.1 Steps for a New Installation

1. Install and configure Microsoft SQL Server, Oracle9i, or PostgreSQL database engines for data storage if one of these database engines is to be used (See Section 3).
2. Install the FileSECURE Server software (See Section 4).
3. Request and install a license key (See Section 5).
4. Configure the server database (See Section 6).
5. Configure FileSECURE Server using the FileSECURE Control Panel (See Section 7).
6. Request and install a signed X509 Certificate (See Section 8).
7. Install and Configure the Super User (See Section 9).
8. Create FileSECURE Organization(s) using Super User (See Section 10).
9. Regularly backup your FileSECURE Database (See Section 6).

2.2 Steps for Updating an Existing Installation

The FileSECURE Server software installer automatically detects previous versions of FileSECURE Server. It locates the current system files (fileSecure.properties, fileSecure.keystore, and the embedded database files, if used) and reuses these files for the new installation. Existing databases from a previous version are automatically updated when the FileSECURE Server 4 service is started.

1. Backup the FileSECURE Server 2/3 system files (fileSecure.properties, fileSecure.keystore, and the embedded database files, if used) as a precaution.
2. Run the FileSECURE Server 4 installer (See Section 4).
3. Request and install a new license key (See Section 5).
4. Verify the database, basic, advanced, and certificate configurations, and restart the FileSECURE Server service (See Sections 6, 7, and 8).
5. Remove remaining FileSECURE Server 2/3 directories and files (if desired). Note that the previous version will be uninstalled by the FileSECURE Server 4 installer, but certain data files will not be removed by the uninstall process.

3 Installing the Server Database

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.

The following enterprise databases are supported:

- **Microsoft SQL Server 2000**
- **PostgreSQL 7.3.3** on Linux
- **Oracle 9i**

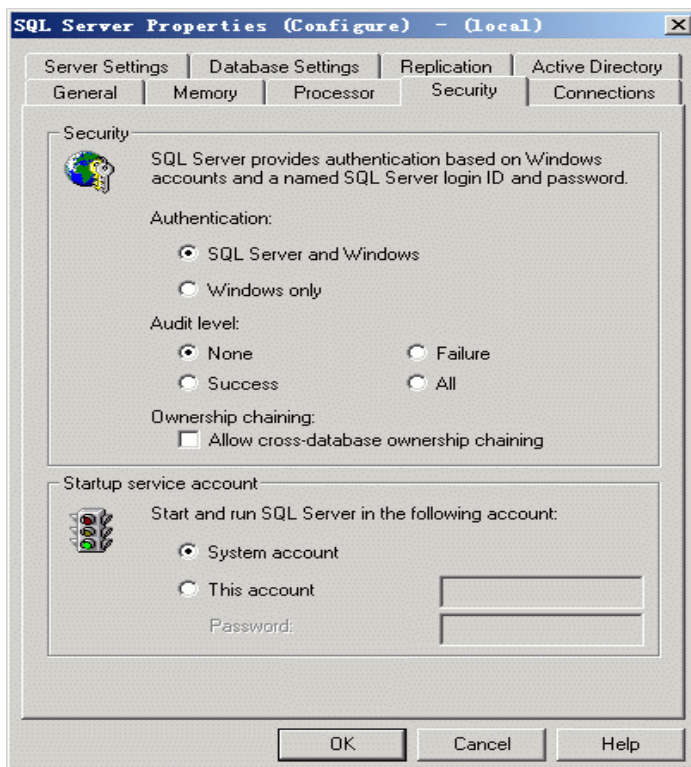
3.1 Installing Microsoft SQL Server

Follow Microsoft instructions for the installation of SQL Server 2000. It is recommended that SQL Server 2000 be installed with at least Service Pack 3. Once installed, the following information about 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.

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).

3.2 Installing PostgreSQL

PostgreSQL can be installed on either the same machine as 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.

3. Initialize the database. For example, if you install PostgreSQL in the default directory /usr/local/pgsql, change directory to /usr/local/pgsql/bin and execute the following command:

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

4. Start the database server using:

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

or

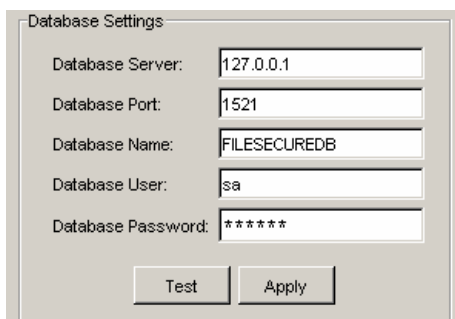
```
$ pg_ctl -D /usr/local/pgsql/data -l logfile start
```

3.3 Installing Oracle 9i

Install Oracle 9i referring to Oracle documentation. 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.

To create the FileSECURE database after installing FileSECURE Server software on the target platform, use the Oracle tool SQL*Plus Worksheet to create a new database schema in Oracle. You may use any name for the scheme. ASUREDB or FILESECUREDB is recommended.

The Oracle SID automatically defaults to the database name portion of the global database name. When you create a database, you are not able to use the underscore character “_” in the SID. If an Oracle SID is “FILESECUREDB” for the FileSECURE Server database, then “FILESECUREDB” should be used for Database Name in the FileSECURE Control Panel Database Settings as shown below:



Database Settings

Database Server: 127.0.0.1

Database Port: 1521

Database Name: FILESECUREDB

Database User: sa

Database Password: *****

Test Apply

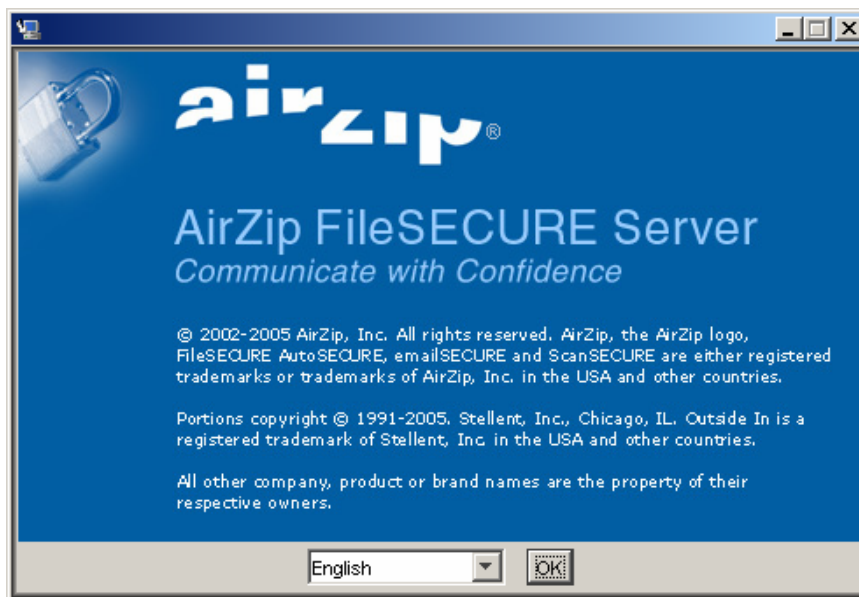
4 Installing FileSECURE Server

Once SQL Server, Oracle 9i, or PostgreSQL is configured (if not using the FileSECURE embedded database), the FileSECURE Server installation should take between 5 and 30 minutes.

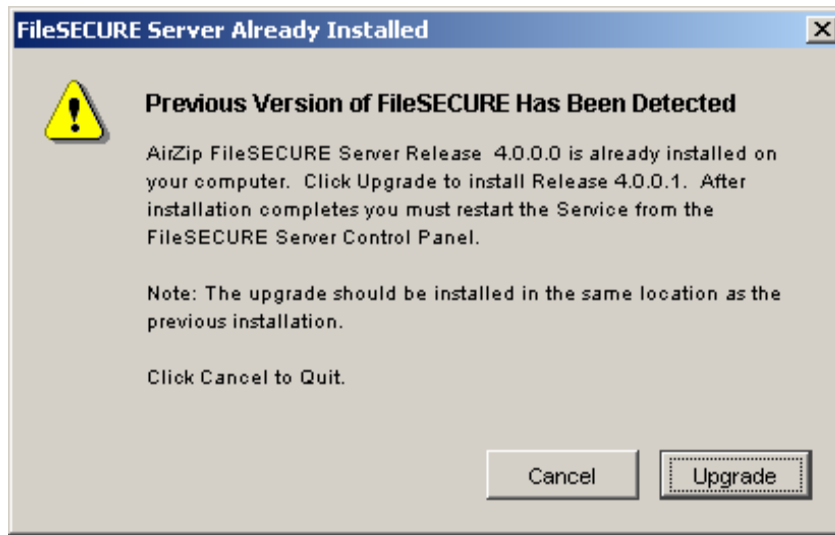
The FileSECURE Install CD also contains copies of this manual, user guides, and software installers for the FileSECURE client programs.

4.1 Installing or Upgrading FileSECURE Server

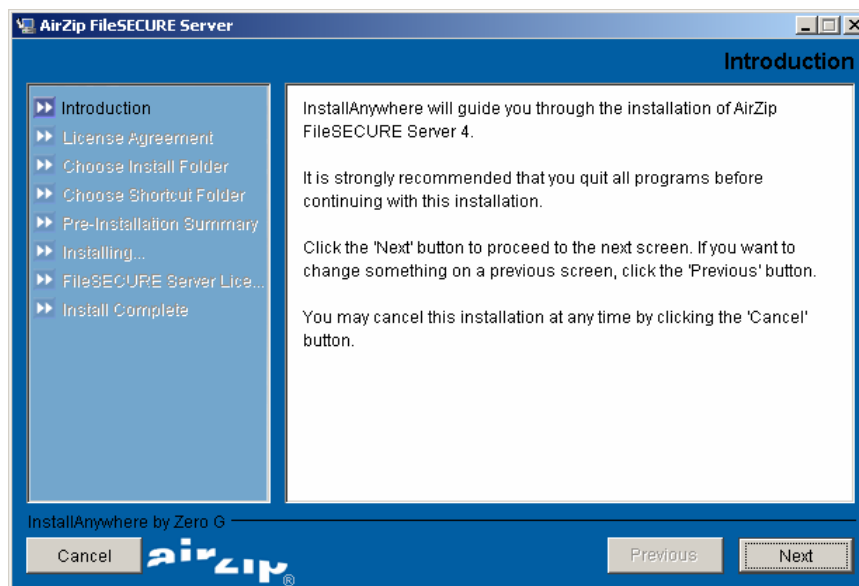
1. Locate the FileSECURE Server Release 4 Install CD or download the installer files to a local directory on your server or workstation. FileSECURE Server can also be installed from a network share.
2. Locate and run the FileSECURE Server installer (FileSECUREServerInstall) to begin the installation process.
3. At the Welcome screen, select the language for the installer package from the available list and press **OK**. The language selection determines the language used for the installation process only. The FileSECURE Server Control Panel and Help are provided in English only.



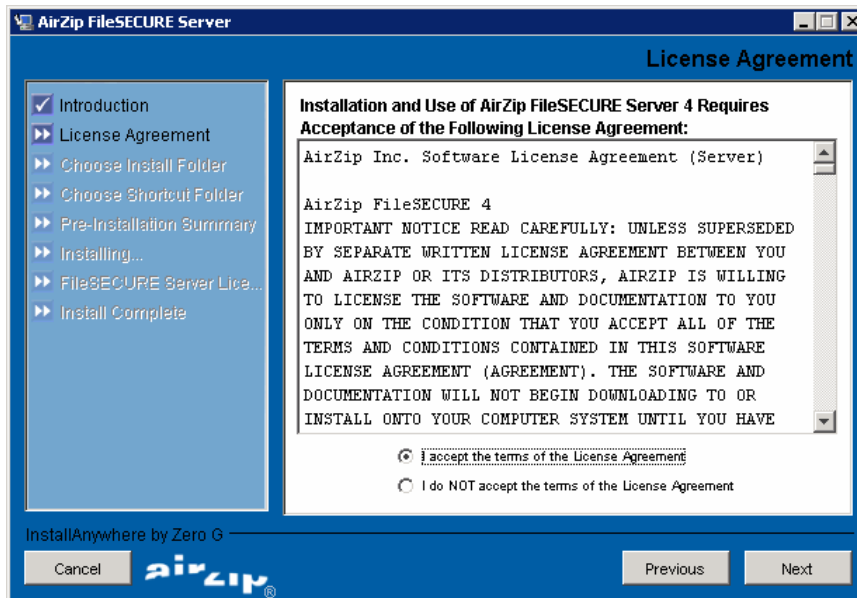
If the following screen appears when executing the Server Installation, it means that a previous version of FileSECURE Server is already installed. Click **Upgrade** to upgrade the previous installation.



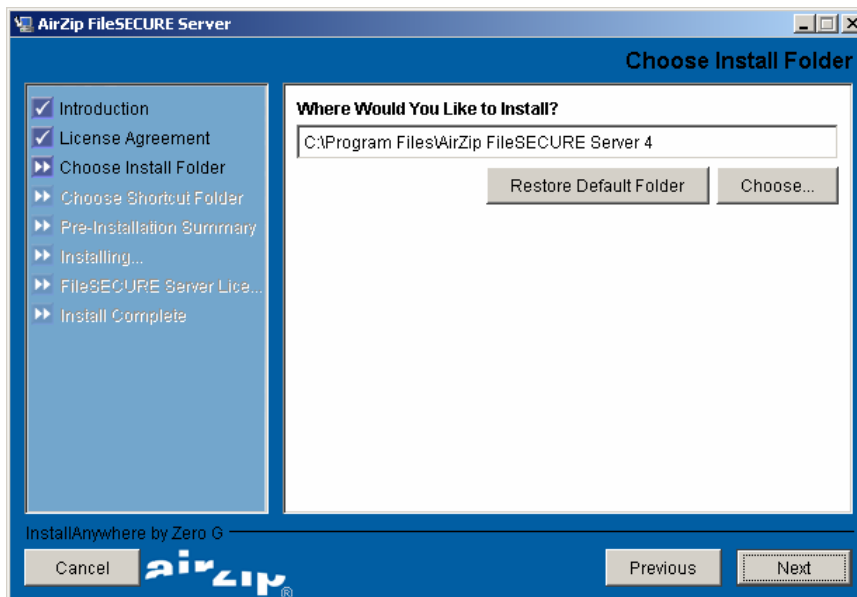
4. At the next screen review the instructions and press **Next**.



5. Review licensing terms before proceeding.



6. Select the target directory for Server installation. The default installation directory is shown but can be changed to another directory by using the “**Choose...**” button.

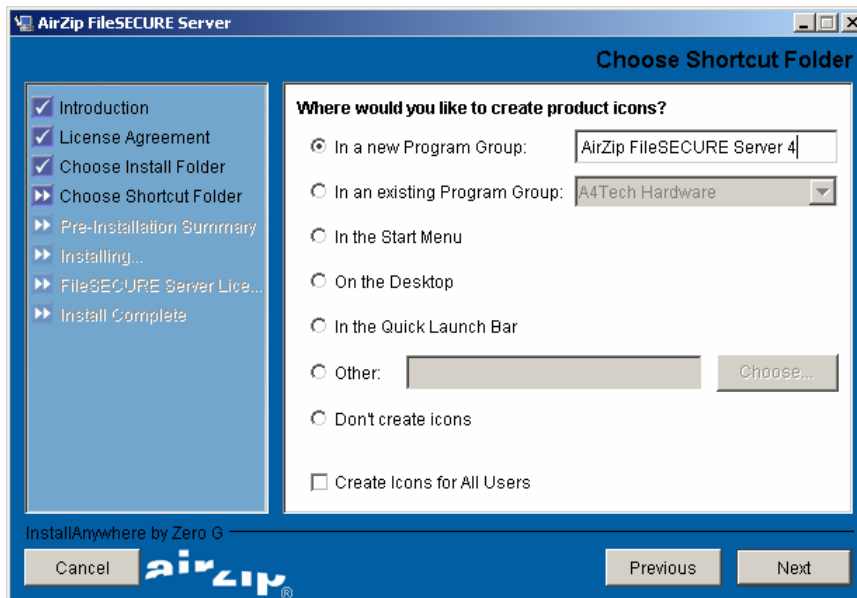


The default installations directories are as follows:

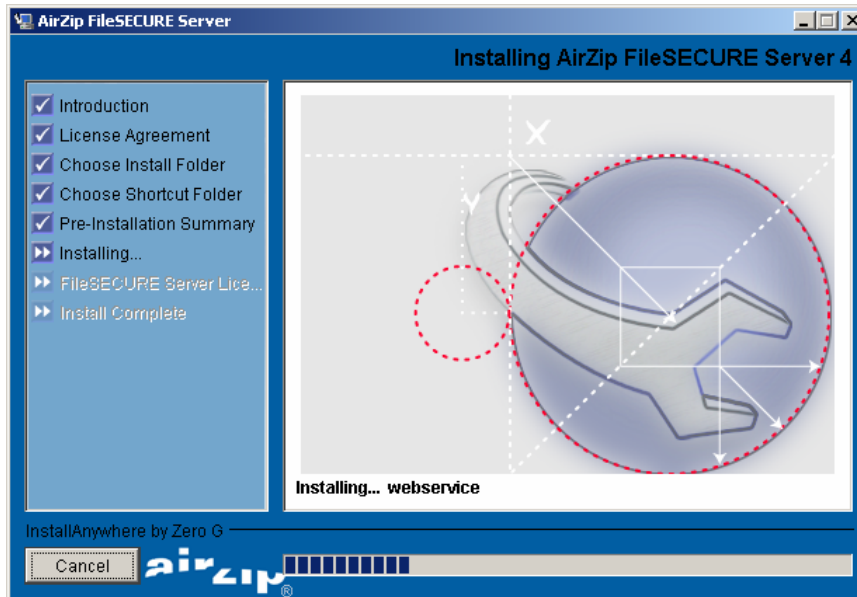
- **Windows:** C:\Program Files\AirZip\FileSECURE Server 4
- **Unix/Linux:** /opt/airzipfss4/
- **Mac OS X:** /Applications/AirZipFileSECUREServer4/

Once the target directory is selected, press **Next** to proceed.

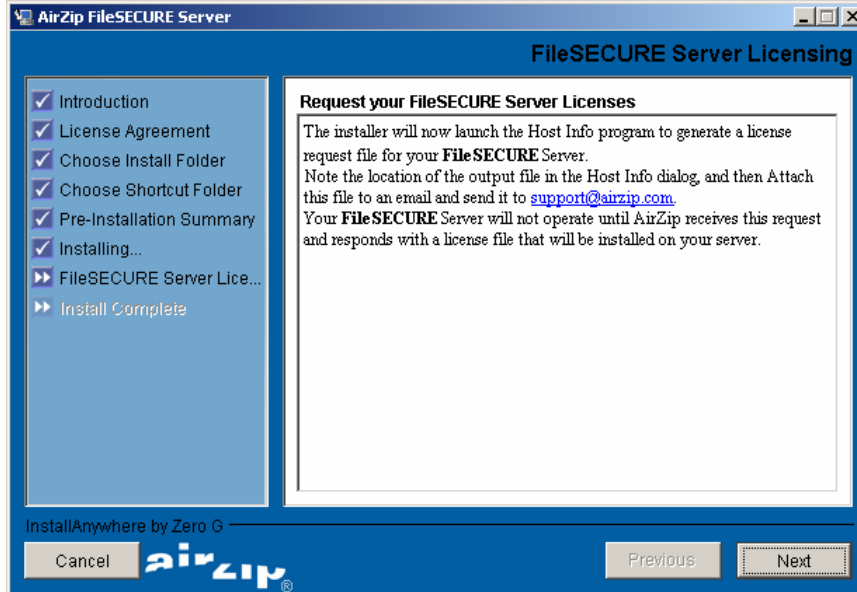
7. If installing on Windows, at the next screen select where you would like to create product icons and press **Next**.



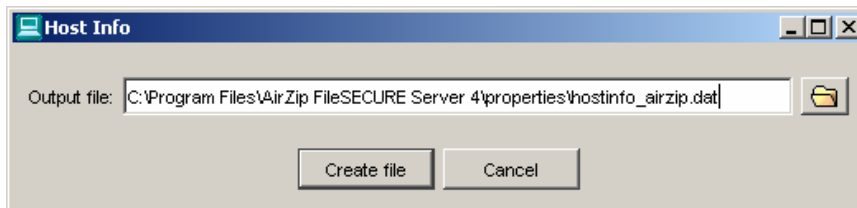
8. The following display shows the progress of the installation process.



9. Generate the host information file to request your license key.

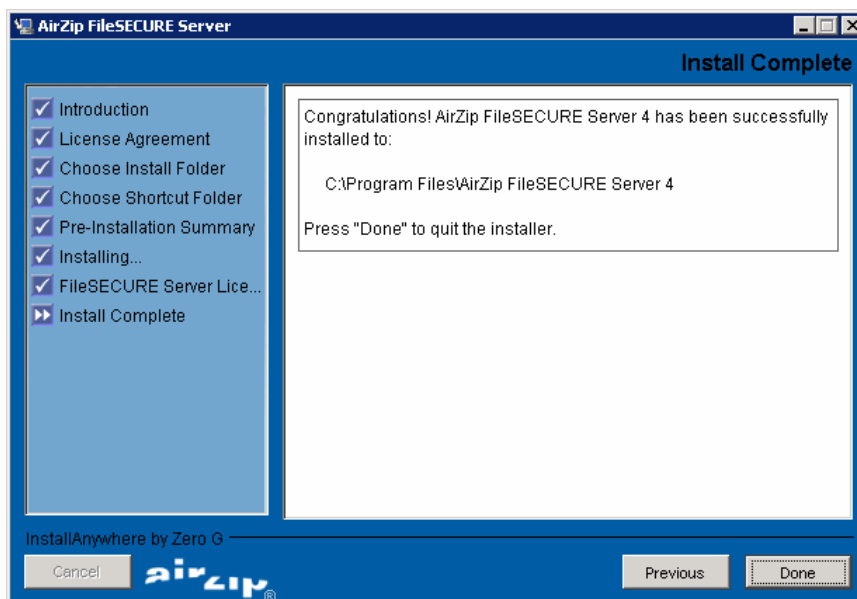


The following dialog will appear:



Select the directory to save the file to and then press **Create file**. Press **Next** to proceed to the final installer screen.

10. Press **Done** to complete the installation



5 Installing a Server License

5.1 License Management

AirZip FileSECURE Server incorporates a software licensing mechanism that:

- a) locks the software to a specific machine, and
- b) controls the availability of specific features via a license key file.

Before you can run FileSECURE you must first install a valid license key.

You will need to submit a license request to AirZip, receive a license key file, and install this license key file before you may start the FileSECURE Server. The license key contains information such as the maximum permitted number of Organizations, Authors, and Readers. It also determines which features may be enabled, such as LDAP integration and the use of an enterprise database engine.

5.2 Requesting a License Key

If you chose not to generate a license key request during the installation, it can be done manually afterwards.

1. Run the **hostinfo** program to generate the required host information. hostinfo is accessible from the Start menu in Windows, or by locating the appropriate executable file on Unix/Linux or Mac OS X:
 - **Windows:** Program Files > AirZip FileSECURE Server 4 > Host Info
 - **Unix/Linux:** /opt/airzipfss4/bin/hostinfo
 - **Mac OS X:** /Applications/AirZipFileSECUREServer4/bin/hostinfo
2. The default filename is named according to the hostname of the system you are running on and follows this scheme: **hostinfo_your-machine-name.dat**. The default location for this file is the **properties** directory of the server installation. Select a location to save the file and press the **Create File** button.
3. Email the following information to support@airzip.com:
 - a) Your name;
 - b) Company name;
 - c) Company mailing address;
 - d) Your telephone number;
 - e) Your email address;
 - f) Your Proof of Entitlement ID that came with your software (not required for evaluation licenses);
 - g) Host information file generated by the hostinfo program.
4. Once your request has been processed, you will receive your license key as a binary attachment to an email message from support@airzip.com.

Note: License key requests and license keys themselves are both binary files. If transferring these files between systems, please be sure to transfer them as “binary” and not “ASCII”.

5.3 EVALUATION, TEMPORARY and PERMANENT Licenses:

Evaluation Licenses are issued to allow customer to evaluate the product. These licenses allow full use of the product until they expire. They are valid for 15-30 days from date of issue, and may be renewed upon special request.

Temporary Licenses are issued to customers who have ordered the product but have not yet paid for it. These licenses are valid for 60 days from the date of issue. AirZip's terms of payment are Net 30 days from date of invoice.

Permanent Licenses are issued once the software has been paid for. (AirZip's licensing system is tied to its billing system, and permanent licenses cannot be issued until payment has been received). A permanent license does not expire (unless the customer has purchased a fixed term license).

5.4 Installing a License Key

Once you have received your license key, it must be installed.

1. Stop the FileSECURE service if it is running.
 - Press **Stop Server** in the **Basic Configuration** tab of the FileSECURE Control Panel.
2. Copy the license file you received from AirZip to:
 - **Windows:** C:\Program Files\AirZip\FileSECURE Server 4 \properties
 - **Unix/Linux:** /opt/airzipfss4/properties
 - **Mac OS X:** /Applications/AirZipFileSECUREServer4/properties

Note: The license key file naming scheme is: **fs_license_your-machine-name.key**. AirZip will supply you with an appropriately named license key file. Ensure that you do not rename this file when transferring it to the **properties** directory.

3. Restart the FileSECURE service.
 - Press **Start Server** in the **Basic Configuration** tab of the FileSECURE Control Panel.

Note: If your license expires, you will no longer be able to run FileSECURE. Contact AirZip for a replacement license. As soon as a valid license is installed, FileSECURE will again be fully operational.

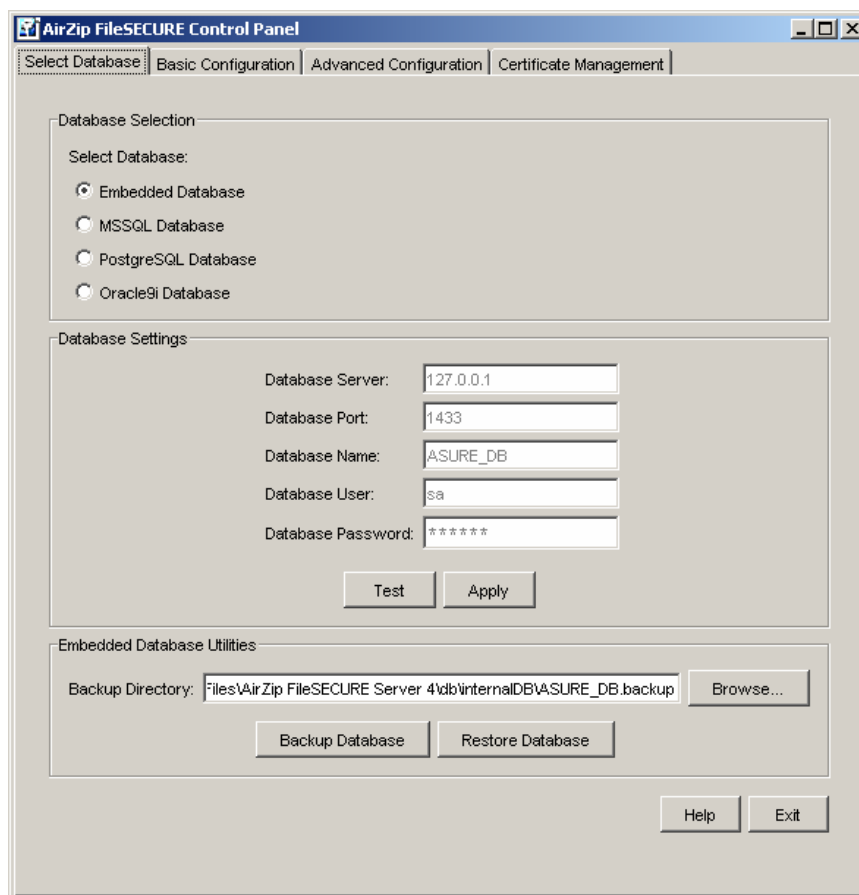
6 Configuring the Server Database

6.1 Configuring the Server Database

1. Open FileSECURE Control Panel and select the **Select Database** tab. FileSECURE Control Panel is accessible from the Start menu in Windows, or by locating the appropriate executable file on Unix/Linux or Mac OS X:

- **Windows:** Program Files > AirZip FileSECURE Server 4 > FileSECURE Control Panel
- **Unix/Linux:** /opt/airzipfss4/bin/fscontrol
- **Mac OS X:** /Applications/AirZipFileSECUREServer4/bin/fscontrol

The Control Panel Select Database tab is shown below:



2. Select and configure your database. Enter the appropriate values in the Database Settings area and press **Test** to verify your settings. Once they are verified, press **Apply** to automatically initialize or update the FileSECURE database.

6.2 Database Backup and Restore

To backup the FileSECURE embedded database:

1. Stop the FileSECURE server if it is running.

2. Select a directory for the backup files in the Embedded Database Utilities area of the FileSECURE Control Panel.
3. Press the **Backup Database** button to generate a backup of the current contents of the data tables.

To restore the FileSECURE embedded database:

1. Stop the FileSECURE server if it is running.
2. Select the directory containing the most recent database backup files in the Embedded Database Utilities area of the FileSECURE Control Panel.
3. Press the **Restore Database** button to restore the database.

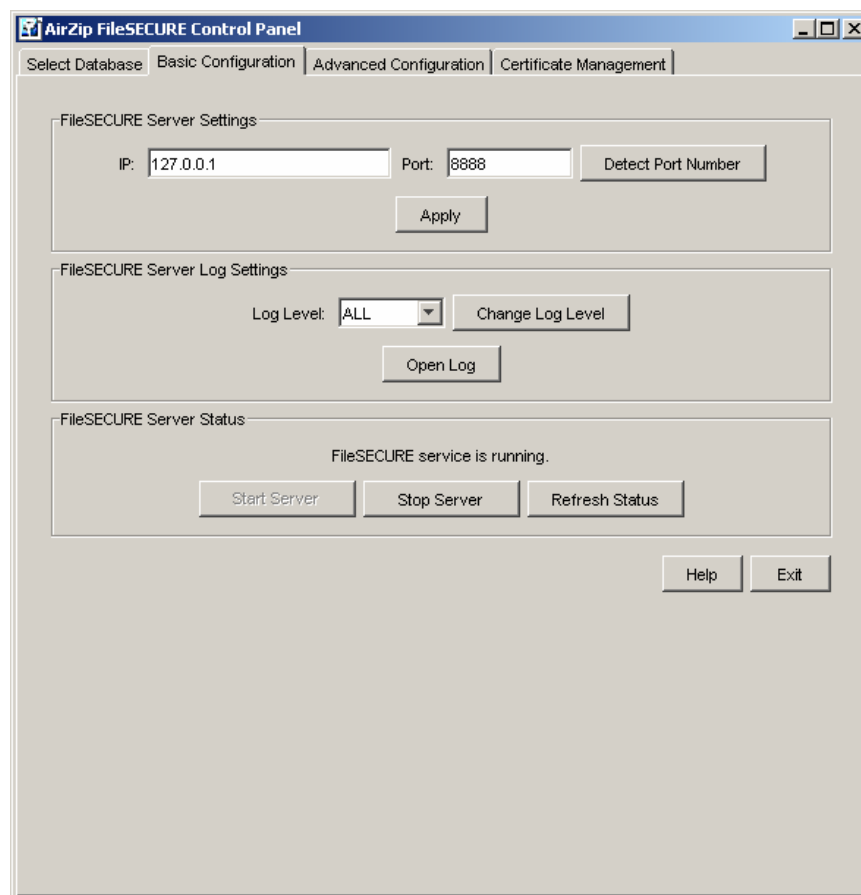
To backup and restore databases created on MS SQL Server, PostgreSQL, or Oracle 9i, use the database vendor's backup utilities.

7 Configuring FileSECURE Server

7.1 Basic Configuration

1. Open FileSECURE Control Panel and select the **Basic Configuration** tab. FileSECURE Control Panel is accessible from the Start menu in Windows, or by locating the appropriate executable file on Unix/Linux or Mac OS X:
 - **Windows:** Program Files > AirZip FileSECURE Server 4 > FileSECURE Control Panel
 - **Unix/Linux:** /opt/airzipfss4/bin/fscontrol
 - **Mac OS X:** /Applications/AirZipFileSECUREServer4/bin/fscontrol

The Control Panel Basic Configuration tab is shown below:



When FileSECURE Server is first installed, the basic server configuration settings are set to default values. These settings only need to be modified under special circumstances, such as when you are already running another service on the default FileSECURE Server port.

7.2 Configuring the Communication Port

1. Select a port number. 443 is the recommended default. SSL is used on all selected port settings.

2. Press **Detect Port Number** to check if the port is free.
3. Click **Apply** to save the settings.

7.3 Configuring the Server Log Level

1. Select the required level from the **Log Level** drop down box.
2. Press **Change Log Level** to save the setting.

The following table explains the logging levels:

Level	Description
Off	No messages are logged
Severe	Only severe errors are logged
Warning	Severe errors and warnings are logged
Info	Severe errors, warnings, and informational messages are logged
Config	
Fine	
Finer	
Finest	
All	Messages from all levels are logged

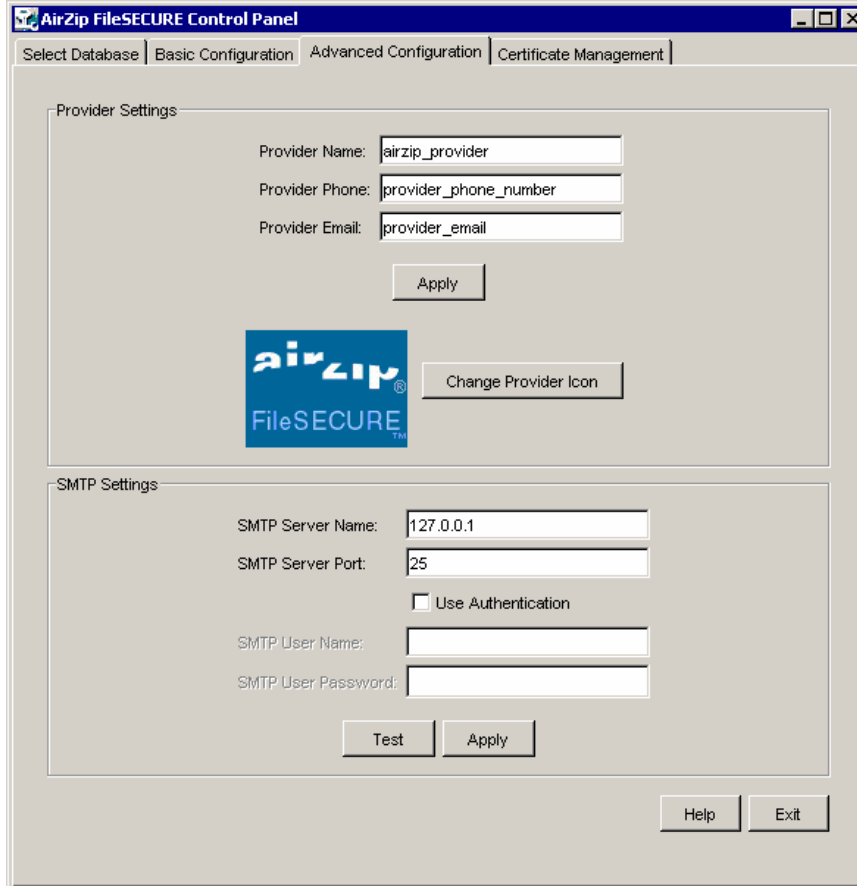
7.4 Starting and Stopping FileSECURE Server

1. Press either the **Start Server** or **Stop Server** button as required.
2. Press the **Refresh Status** button to ensure that the Control Panel is displaying the correct server status.

7.5 Changing the provider settings

To set service provider information use the Advanced Configuration Tab.

1. Open the FileSECURE Control Panel and select the Advanced Configuration tab shown below.



2. Enter values for the following provider fields:
 - **Provider Name** which is the company's name.
 - **Provider Phone** which is the phone number of the person to contact for server support.
 - **Provider Email** which is the email address of the person to contact for server support.
3. The provider icon is a logo image that identifies your company. The image dimensions should be 110x80 pixels, and the image file format should be GIF, JPG, or PNG. To change the provider icon:
 - Press **Change Provider Icon** to browse for an image.
 - Press **Choose** to select the new provider icon image.

8 Requesting and Installing a Certificate

FileSECURE uses the Secure Sockets Layer (SSL) protocol to secure communications between the FileSECURE client programs and the FileSECURE Server.

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

FileSECURE requires that the certificate:

1. Is signed by AirZip, VeriSign, Thawte, Baltimore or another certificate authority where you have imported its Root Certificate.
2. 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 encryption with the private key of the certification authority which issued it.

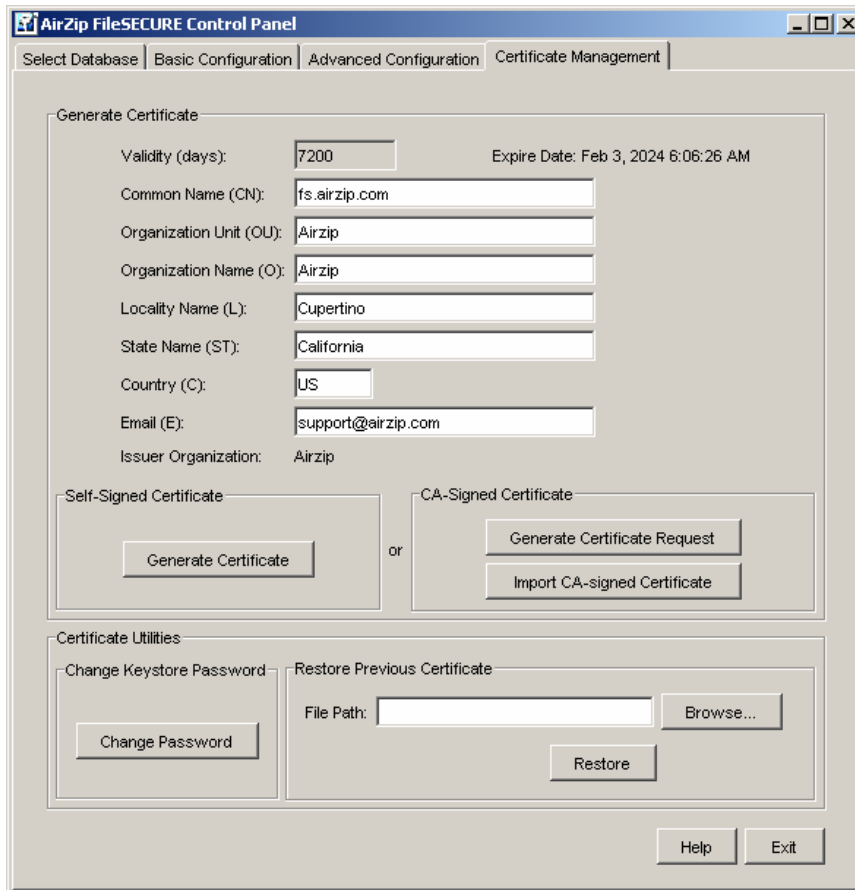
The FileSECURE client programs validate the Server certificate and will present a warning message each time the user logs in to the Server if an improper certificate is installed.

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 signed by a certificate authority.

Note: Your certificate is unique to your server system 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 (server hostname), and the organization to which it was issued. The FileSECURE Server automatically installs a self-signed placeholder X509 Certificate.

8.1 Generating a self-signed certificate

To generate a self-signed certificate that is useful for evaluation or other temporary configurations.

1. Enter your server's hostname in the **Common Name** field.
2. Press **Generate Certificate**.
3. Press **Yes** to generate the certificate.
4. Press **OK**.

8.2 Generating a X509 Certificate Request

Complete the following steps in order to generate a X509 certificate request that can be sent to an authorized certificate authority:

1. Enter the following information in the appropriate fields at the top of the panel :
 - In the **Common Name** field enter the server hostname that will be used by the FileSECURE client programs to access your server. If your server is to be accessible from the Internet, you will need to have assigned it a server name such as **filesecure.yourcompany.com** through your ISP. If installing FileSECURE on a server

with only local access, assign it a suitable machine name such as filesecureserver. While you can use an IP address, it is not recommended to do so. The server name will be registered within the X509 certificate that protects your site.

- The name of the **organization** providing the FileSECURE service (for example, your company name).
 - The name of the **organization unit** providing the FileSECURE service (for example, Finance, Engineering, or Health Services).
 - The **town or city** where the organization providing the FileSECURE service is located. Do not abbreviate.
 - The **state or province** where the organization providing the FileSECURE service is located. Do not abbreviate.
 - The **two-letter country code** where the organization providing the FileSECURE service is located (for example, US, UK, CN, or JP).
 - The internet **email address** of the person requesting the certificate (for example: jane_doe@mycompany.com). The certificate authority will return the certificate to this address.
2. In the CA-Signed Certificate area, press the **Generate Certificate Request** button.
 3. In the dialog box that follows, select the location where the Certificate Request is to be saved.

8.3 Installing a CA-Signed Certificate

Once you have received your CA Signed Certificate, you need to install it. The procedure is as follows:

1. Stop the FileSECURE Server. This is done by selecting the **Basic Configuration** tab in the FileSECURE Control Panel and pressing the **Stop Server** button.
2. Save your newly signed certificate to a known location.
3. Press the Import CA-signed Certificate button.
4. In the dialog box, locate the signed certificate file, for example *signed.crt*.
5. Press **Import**.
6. Start the FileSECURE Server. This is done by selecting the **Basic Configuration** tab in the FileSECURE Control Panel and pressing the **Start Server** button.

8.4 Changing 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*. To change the password for the keystore:

1. Press the **Change Password** button
2. In the following dialog enter the old password (by default it is *airzip*) and enter the new password twice to confirm the change.
3. Press **OK** to change the password.

8.5 Restoring a Previous Certificate

If you want to replace the current certificate with another one that you previously requested:

1. Press the **Browse** button in the **Restore Previous Certificate** area.

2. Select a saved **fileSecure.keystore** file.
3. Press the **Restore** button.

9 Installing and Configuring Super User Utility

After the FileSECURE Server has been installed, the Super User must be installed on a Windows system to add and manage Organizations. The following provides step-by-step procedures for:

1. Installing the Super User
2. Configuring your Super User Account
3. Changing the Super User password
4. Configuring a new organizational account

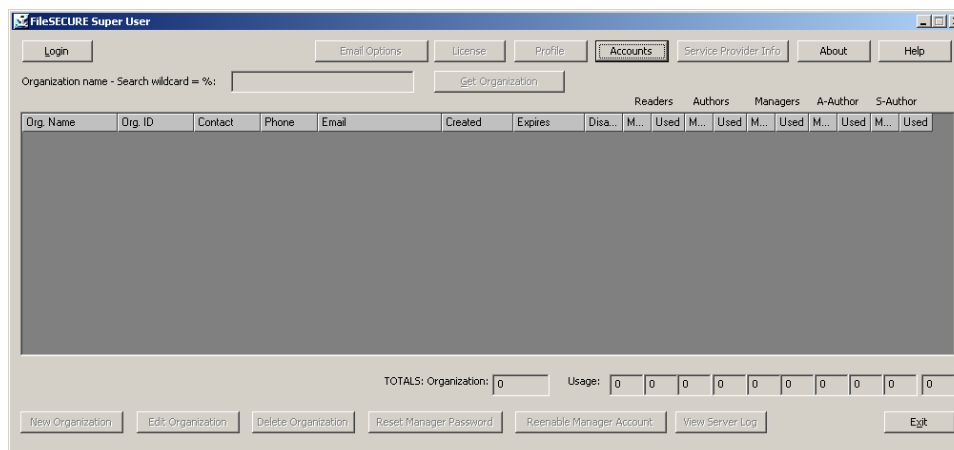
Super User and Manager users may not save their account passwords, in order to ensure a high level of security for your system.

9.1 Installing the Super User Utility

To install the Super User Client, follow these steps:

1. Locate the FileSECURE Server Release 4 Install CD.
2. Insert the CD into the Windows system on which you want to install the Super User.
3. Select the **Install the Super User Utility** option from the installation menu that is displayed.
4. Complete the installation by following the steps in the installer wizard.

When the installation is complete, select **Start > Programs > AirZip FileSECURE > Super User** to run the Super User. The Super User window will appear as shown.

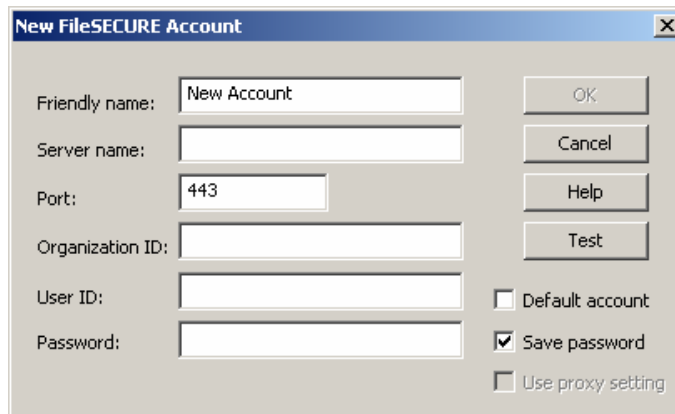


5. Press the Help button to access the Help Center to learn how to use the Super User features and capabilities.

9.2 Configuring the 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 (Start > Programs > AirZip FileSECURE > Super User).
2. Press the **Login** button in the upper left hand corner. You will be presented with the follow dialog:



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 in 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. If the DNS name has yet to be implemented, an IP address (216.218.133.74) or the local network machine name on which you have installed the server can be used on an interim basis.

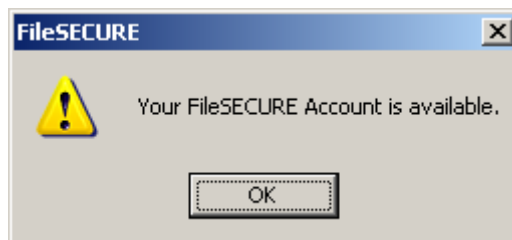
Port is the port number that you used when configuring your server.

Organization ID should be left blank for logging on as Super User.

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

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

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



5. Press the **OK** button to login to the server. You will be returned to the main screen, and the Login button will be replaced with a Logout button if you have logged in successfully.

9.3 Changing the 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. Press the **Profile** button at the top middle of the Super User 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:

The 'Change User Profile' dialog box contains the following fields and controls:

- First name:
- Last name:
- * Email address:
- Change password
- New password:
- Confirm:
- Buttons: OK, Cancel, Help

4. Press **OK** to change the password.

9.4 Configuring Email Settings

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 default MAPI-compliant email program to send such messages unless you change your email options to use your SMTP Server. Use the Email Options button with its associated Help to enter your SMTP Server information.

The 'Email Options' dialog box contains the following fields and controls:

- Email information
- Email mode:
- SMTP server:
- SMTP port:
- Authentication
- SMTP user:
- SMTP password:
- Buttons: Test, OK, Cancel, Help

10 Creating 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 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.

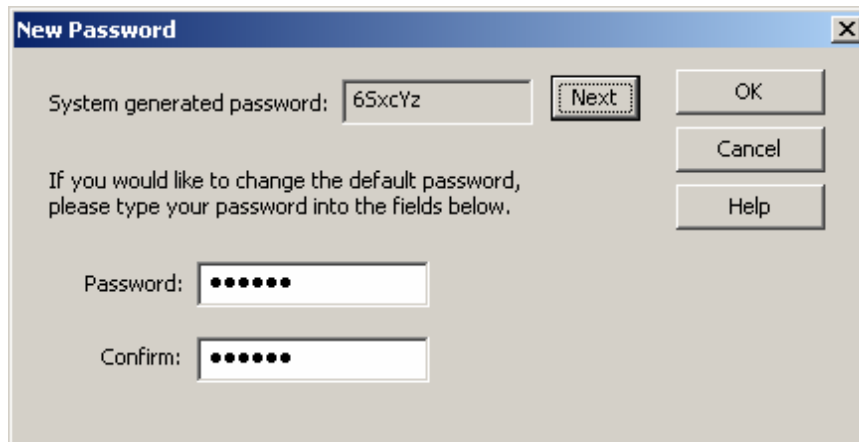
The simplest configuration for FileSECURE Server for a company, institution or agency is to configure just one Organization.

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. The User ID 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:



New Password

System generated password: 65xcYz

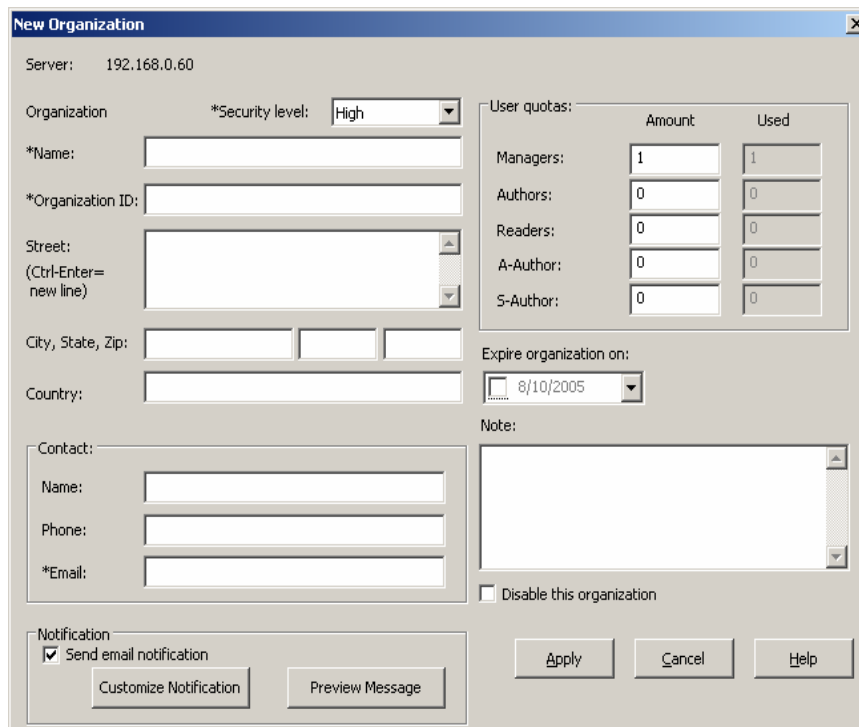
If you would like to change the default password, please type your password into the fields below.

Password:

Confirm:

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

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



New Organization

Server: 192.168.0.60

Organization *Security level: High

*Name:

*Organization ID:

Street: (Ctrl-Enter=new line)

City, State, Zip:

Country:

Contact:

Name:

Phone:

*Email:

Notification

Send email notification

User quotas:

	Amount	Used
Managers:	<input type="text" value="1"/>	<input type="text" value="1"/>
Authors:	<input type="text" value="0"/>	<input type="text" value="0"/>
Readers:	<input type="text" value="0"/>	<input type="text" value="0"/>
A-Author:	<input type="text" value="0"/>	<input type="text" value="0"/>
S-Author:	<input type="text" value="0"/>	<input type="text" value="0"/>

Expire organization on:

Note:

Disable this organization

The following describes each field (Fields marked with an asterisk are required to create a new organization.)

Organization:

- **Security Level:** The level can be set to *High*, *Medium* or *Low*.

- **Name:** The name of the organization.
- **Organization ID:** The name used by the server to identify the organization. **Note:** The organization ID is case sensitive.
- **Street, City State, Zip, Country:** The address of this organization.

Contact:

- **Name:** The name of the manager of the organization
- **Phone:** The telephone number of the manager of the organization
- **Email:** The email address of the manager of the organization

User quotas:

- In this **Amount** column, assign the maximum number of clients desired to the organization. Once the users have been created and logged in, the number in use will be shown in the **Use** column.

Expires On:

- Set this if you want the organization to be active for a specific period of time.

Note:

- This can be used to add reminders or other information about the organization.

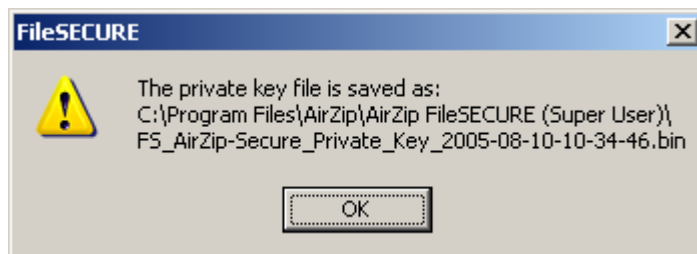
4. Press the **Preview Message** button at the bottom left of the New Organization dialog box to review and possibly customize the email message that will be sent to the new organization's security administration officer.
5. Press the **Apply** button when you have filled in all the appropriate information. FileSECURE will automatically generate a Recovery Private Key for the new Organization. You may select the directory to store the key in. It is recommended that you store this key directly to a removable media device, such as a USB storage device, which should later be stored in a physically secure location.

PRECAUTION: Ensure that the Organization's private key is stored for safekeeping with a reliable key escrow agent.

The private key is provided primarily for disaster recovery in the unlikely event that a FileSECURE Server should crash and lose the keys for one or more documents. This key is generated only when an Organization is created and is only useful for decrypting the Organization's secured files.

The private key should be stored on dependable removable media and physically stored under lock and key for safe long-term insurance.

6. When the private key dialog box appears, note the filename and location of the key, and press **OK**.



7. The Super User 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 and an administrator account for that organization.

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 the standard AirZip FileSECURE client download sites.

The Manager software is available on the following site:

<http://www.airzip.com/FileSECUREManager4.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/FileSECUREAuthor4.htm>

<http://www.airzip.com/FileSECUREReader4.htm>

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