FileAssurity Central Administrator

Administrator's guide and system overview

Contents

Introduction ... 3
Files contained on the CD ... 6
Steps to Follow ... 7
Setting up the Master Database ... 9
General Database Operation ... 10
Overview of Administrator roles ... 12
Installing & initializing Central Administrator ... 14
  Installing Keystore Backup Service ... 14
  Installing Central Manager ... 15
Logging on to the system ... 40
Central Administrator Application (the Master Keystore) ... 41
  Menu Options ... 42
  Tabs ... 44
Administrator generation functions ... 46
Keystore policy ... 48
  Export private keys ... 49
  Import private keys ... 49
  Hidden keys ... 50
  Key generation ... 50
  User information recovery key ... 50
  Keys cannot be deleted ... 51
  Use encryption ... 51
  Update keystore after (n) days (n) hours ... 51
  Keystore password change ... 52
  Use Signing ... 52
  Keys not allowed to sign with (Group keys) ... 53
Re-issuing user keystores ... 56
Information Recovery ... 57
Enter file recovery mode ... 58
Installation of the client software ... 62
Client keystore automatic backup ... 63
Managing multiple Master Keystores ... 65
Trust models ... 67
  Concepts of trust in digital signatures ... 67
  The Central Administration Trust model ... 69
FAQs ... 71

Introduction

FileAssurity Central Administration provides you, as the Administrator, and your management, with the ability to set up and administer a simple Public Key Infrastructure (PKI) system. It doesn't require you to become an expert in technical mechanisms or to implement military grade security in order to administer the system.

But it does mean that you have to use the same levels of care, or better, that you already use when setting up user accounts on your networks, or on applications systems, or when authorizing employees to sign documents on behalf of your organization.

This guide has been written to give you (and relevant senior management) an appreciation of the requirements that have to be met when setting up this type of system and administering and running it on a day-to-day basis.

There is a separate document, "FileAssurity Central Administrator – Administrator's guide and system overview", which provides a structured approach to planning and installing the service in your organization and provides you with an outline plan to follow as you prepare for and implement Central Administration.

Of course, in all projects of these types, the size of the project matters. If you are a small organization (or you are implementing for a small number of users) then you will be able to generate and administer all the users manually without any undue inconvenience.

Do remember that your security project simply may never need to scale immediately to millions, and to plan and implement a service for that would not be appropriate. Also, you may not be trying to implement using the PKI capabilities of FileAssurity OpenPGP to implement a PKI service that also covers all your access control and applications security environments.

However, if you are planning to implement a service rapidly for many hundreds, or even thousands of users, it is going to require a great deal more management, automation and planning. This has relatively little to do with the FileAssurity products and much more to do with the difficulties of administering large, and perhaps complex user structures and delivering them in a sensible timescale.

You will perform a number of vital functions when administering a Central Administration PKI based security service, including:

- creating and issuing user keystores;
- specifying the policy applicable to the user(s);
- with authorization, recovering encrypted files;

- recovering user keystore passwords;
- renewing a user's key life;
- altering the policy applying to a user's keystore;
- revoking users.

By the very nature of the control these functions provide over user capabilities, you must remember that you are administering a sophisticated security system that may be relied upon as a high security mechanism by your users, and that the security of both individual users, and the system, is your responsibility. Whilst ArticSoft have provided a service that can be implemented securely, if you do not take proper steps to provide both database security and backup and recovery, you risk allowing your secure service to be compromised.

Before setting the system up you should read the remainder of this guide. In many areas, particularly that of Policy, you are likely to have to discuss some of the issues involved with management in order to make sure that you will implement appropriate Policy for users, both in terms of the controls applied to users and their ability to access the Master Database that controls user authorization and revocation.

The guide is organized into sections, starting with the initializing of the system, the Administrator (you) and Authorizing Administrators, and then considering the controls available to you and how those should be selected and applied for live running.

Management need to be aware of operational and potential regulatory issues around the areas of Information Recovery and how it is performed and supervised, and may need to approve other policies outside the scope of this guide.

The available Policies that you can enforce are described and discussed, and, where relevant, recommendations are given for policy settings that are generally appropriate.

Recognizing that in some enterprises you may have to administer users in groups rather than as individuals, a section is given on operating Central Administration with more than one Master Keystore, which is discussed as a means of facilitating overall administration.

Finally, because there has been much debate generated by the IT industry over a concept called 'Trust Models' which may be applied to systems publishing certificates or tokens, a section has been included outlining the methods by which it is often proposed that users may establish 'Trust' in digitally signed information that they receive from other people. This section is intended to help you understand what kinds of 'Trust' a digital signature encryption service may be capable of providing, and the responsibility of users to also check and verify that the information they receive is plausible, even when digitally signed.

A short reading list is given at the end of the guide to provide you with additional references if you wish to have more detailed information than is given in this guide. The guide is not supposed to be a definitive reference on the many technical methods and techniques that the ArticSoft products deliver. It is intended to help you develop an appreciation for the management decisions that you are responsible for making (together with your colleagues) and the options that are available that others (either in management or representing IS technical skills) may have to decide when implementing an overall solution.

Files contained on the CD

FileAssurityCentralManager.exe
Central Manager program and Master Database keystore updater program Tomcat and database configuration services for Administration

FileAssurity_OpenPGP_Managed.exe
FileAssurity Managed Client for normal PC users of the service (clients)

Switches.txt
A file containing instructions on the file settings which, if it is present preset when the client software is initially installed on a user's computer system, are used to customize the installation for that user.

Batchkeystore.csv
Contains a description of the fields that must be present in a batch keystore issue file and examples of suitable records.

Documentation

FACMv2B.doc
This administration manual.

Steps needed when setting up FACM.doc
Administrator's guide and system overview

FAOPGP_Release2_Manual (Folder)
The client manual for Managed Client users. This is almost identical to the user manual for FileAssurity OpenPGP. It can be displayed by clicking on the file 'index.htm'

Steps to Follow

When setting up the Central Administration system there are several steps you need to follow. This section outlines these steps which are explained in more detail later in this manual.

1) Install and setup an SQL compliant database
This is the database that Central Administrator will communicate with and where the users keystores will be held. Currently the MSSQL and MySQL databases are supported

2) Install the Central Administrator software
You must generate an initial system before you are able to deploy keystore licenses

3) Register and license the Central Administrator software
You will need to perform this step before you can start generating user keystores as the license file contains the information on the number of keystores you can generate. You can license a system that you have used for evaluation purposes or create a new system

4) Generate keys
You will need to generate any group keys for users that they ought to have present in their keystores by default, or create keys for specific groups of users so that they can share common information, if you do not wish to import them

5) Import keys
You may want to import various public keys that will be used by users to encrypt files for others

6) Apply policy rules
So you can control what users can do with their keystores and keys. When you are setting up groups you will have a separate policy per group

7) Generate keystores in either manual or batch mode
Once you have generated and/or imported keys and set policy rules you will need to generate keystores for users

8) Backup keystores
You will want to save specific keystores that are relevant for groups of users so that you can import them into the system at a later date (e.g. when a new user joins that group).

9) Distribute keystores
Once you have generated a keystore it will be stored in the database. When the user installs the client software the correct keystore will be retrieved from the database based

on their username. So distribution is an automatic process that is handled by the installation of the client software.

10) Install the client software

You may either install the client software on behalf of users or let them run the installation themselves. A file called 'switches.txt' supplies the installation process with the necessary information to connect to the database. If this is found in the installation folder then the client software will automatically configure itself and connect to the database. If it is not found (say when a user wants to operate from home on their home PC or travelling when using a laptop) then the user will be prompted for this information.

Setting up the Master Database

Before you install Central Administrator you need to provide an SQL compliant database for Central Manager to load keystores to and for Managed Clients to download and upload to. The two types of SQL compliant databases supported by ArticSoft are MSSQL and MySQL.

ArticSoft do not provide database software or database management and administration tools and services. These will be supplied by the manufacturer of the database service that you have selected.

The database administrator is responsible for setting up the database that is going to be used. The database can be given any name that is appropriate for the organization. Where the Master Database is being run offline and then copied over to one or more locations for live running, the names of the copied database(s) need not be the same as the Master Database, and users can be configured to connect to specific databases in their setup parameters. Users must also be connected to the database updater service and the parameter for that is included here (please see a later chapter).

The database location (IP address) should be one that is unlikely to change during the life of Central Administration. Whilst the Central Manager application has been provide with the functionality to be able to change that information, you would have to separately update all clients whose keystores have already been generated. We recommend that you make this an IP address which you are not expecting to have to change.

Where you have decided that the Central Administrator is going to be used offline (in other words the Master Database that they administer is on a stand alone machine and is not connected to the network for users to access) then you can need to organize that the IP address used is the same as the live address (or that you connect as localhost).

When configuring the database, as opposed to configuring the users accessing the database, you will need to set up user names and passwords. The master database user, often called 'root' (the master database user with the ability to carry out any action in the database) should have a password set that is at least 12 characters long. If available, you should switch on the feature in the database service that requires all passwords to be encrypted. This prevents a simple attack where a hacker reads the password file and uses it to control the contents of the database. (A hacker cannot use the keystores in the database without obtaining their passwords, which are never stored, so private keys are not at risk if the information is read, but the hacker could delete information making your system impossible to use.)

A specific user identity and password will be set up by the Central Manager program during system generation to use in order to write records to the Master Database. It should be remembered that the person who initially connects the Central Manager program to the Master Database will have to know both the master user identity and password (or a user identity that can create databases and users) and the Administration and client user passwords.

Once a Master Database has been configured you are then ready to run the Central Manager program to create the Master Passwords for the system.

NOTE : Keystores and their passwords are always held in the database encrypted so they are never exposed to an attacker.

General Database Operation

You will need to operate a database backup and recovery system to preserve user keystores against loss or accidental corruption. A backup should be taken each time that the Master Database is updated by the Central Manager, and on a regular schedule to cover user updates to their own keystores.

If the Master Database is being run offline the backups can be taken after each update has been carried out. If the Master Database is being run online there may be operational reasons for scheduling a backup at a different time, and this should be agreed with the database systems Administrators, but you should be aware that there is a risk of losing keystores generated and issued before a backup is next taken.

Because the sensitive information held in the database is encrypted it is not necessary to control read access to the database, although good practice is to allocate a user name and password to read only access to the 'facm' database. This is simply to reduce the likelihood of an outsider being able to access this information. The username and password can be long because they are normally hidden from the user.

Information is written to the database by two users, the Central Administrator, who updates information there on behalf of the management of the organization, and the Tomcat updater. Tomcat is a process that runs continuously in the server(s) hosting Master Databases. It 'listens' on the port defined during setup for user requests for keystore backups. (A user may, at any time, ask that their keystore be backed up on the Master Database. If the contents of the user's keystore changes during a session they will be prompted to take a backup when they come to logoff.) If a backup request is received, Tomcat will check the claimed user identity and identifying parameters for the keystore being offered against cryptographic controls in the database. If these match then Tomcat will store and update the user keystore. If they do not match then the request will be refused.

Access control to write to the ‘keystores’ and ‘backup’ tables must therefore be more carefully controlled than is necessary for read access. The Central Manager and the Tomcat updater programs need to have write access to the ‘keystores’ table. This must be configured in at the time of systems generation. That user name and password should be very long (more than 12 character positions) to prevent hacking attacks against the updater system.

Overview of Administrator roles

Central Manager has been pre-set to implement a number of controls to prevent unauthorized access to security critical features of the system. These features are the ability to:

- generate and change user keystores;
- recover user passwords;
- recover the Central Administrator password;
- recover information encrypted by any user.

To control these functions, three separate Administrators are required for the operation of the system.

The first Administrator is responsible for the day to day operations of generating user keystores, changing the policies that apply to keystores and changing the end date of an issued user key.

This Administrator runs the Central Manager program when it is first initialized, and subsequently carries out the day to day operational tasks administering users, and is the role to whom this manual applies.

The Administrator will need to know information about the location (IP address) and master user of the Master Database from their database administrator if they did not create the database service themselves.

When the Administrator first runs the Central Manager program they must decide whether the Master (or root) Key for the system will be generated automatically by the program or if they are going to import a key pair that they have acquired from another source. The Administrator will then be asked to enter a password to protect access to the keystore generation processes of Central Administration and the Master Keystore.

As soon as that has taken place, Central Manager program will request that two more Administrators enter passwords. These passwords must be at least 10 characters long, and cannot be changed once they have been entered.

These additional Administrators are required to authorize the following actions:

- recover the Administrator password;
- recover a file or secure text that has been created by one of the users.

The people setting up the system must decide who should carry out the roles of the Administrators. Normally the day to day Administrator would be part of the IS

department, or a member of the Chief Security Officer's staff responsible for user administration, but it could be anyone with adequate training, provided that proper supervision in the taking of backups and in the operation of the system is applied.

The selection of the two authorizing Administrators is a matter of internal convenience. Since a user does not have to change the password to their keystores there will be a low requirement to re-set user passwords, and keystores can always be re-issued under their original passwords without any need for separate supervision, so the frequency of needing these Administrators to be present should be low.

Since these Administrator passwords are long, and cannot be changed, it is recommended that they are written down and kept in a secure place, such as a fire safe. In this way, anyone with appropriate authority may be able to use them without there having to be specific, named individuals. This could therefore be two members of senior management, a senior member of the HR and IS functions, internal counsel and another senior manager, a partner of the firm, and so on.

However, due regard should be given to any internal or regulatory requirements that must be observed where the decryption of information that is personal or private may take place. It is beyond the scope of this guide to consider the impact of privacy legislation, human rights legislation, and the authority to intercept communications. Organizations wishing to implement this service should ensure that they have a published policy advising all their employees of the use of the encryption service and the possibility of monitoring or recovering of information. They should also consider any responsibilities they may have if subject to warrants for the disclosure of encrypted information.

Installing & initializing Central Administrator

The Central Administration application allows you to create a Master Keystore, and to populate the Master Database (that you have previously created) with keystores that have been generated for the users of the managed FileAssurity service.

We recommend that you operate the Central Administration service on a computer that is operated as a stand-alone machine, not connected to a network or to a communications service. The files on this machine should always have a backup that is stored in a fireproof safe, preferably off site, and, when not in use, the machine should itself be stored in a fire safe so that the applications program and the Master Keystore and Database are protected at all times.

If the Master Keystores and Database are lost, for whatever reason, it is impossible to re-create them, even if you used an external key pair as the root keys, and you will have to set up an entirely new system to administer your users. Losing the Master Keystores means you will not be able to recover any of the information that was encrypted by users because there will be no access to the information recovery keys The implications of having to re-create an entire infrastructure are significant in terms of cost, timescales, difficulty of deployment and complexity of setting up new 'trusted' relationships with others. **Taking regular backups is strongly recommended!**

As a comparison, it is similar to having to re-create all the commercial relationships of your organization with its customers and business partners in a single day, without any documentation to start from. Not impossible, but difficult and expensive, and potentially embarrassing.

Installing Keystore Backup Service

The Tomcat keystore backup service is configured and installed on the Administrator's computer during system initialization. The installation wizard can also be used to install the Tomcat service on another server if that is required.

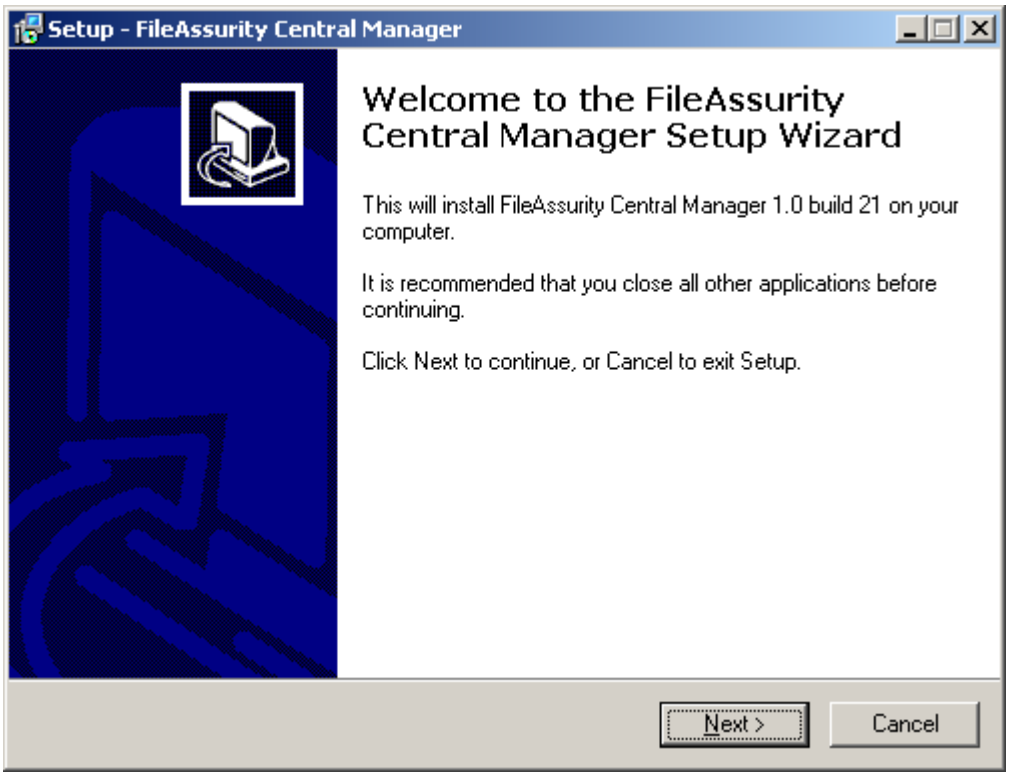
FileAssurity Managed Clients have the ability to have their keystores protected by being backed up on the Master Database when online. At any time when a Managed Client can connect to the Master Database the user can request that the current version of their keystore is uploaded so that it is protected by the organization's disaster recovery and business resumption planning service(s).

This can also be very useful for a user working on more than one computer system (perhaps with a desktop at the office and a laptop when out of the office) needs to be sure

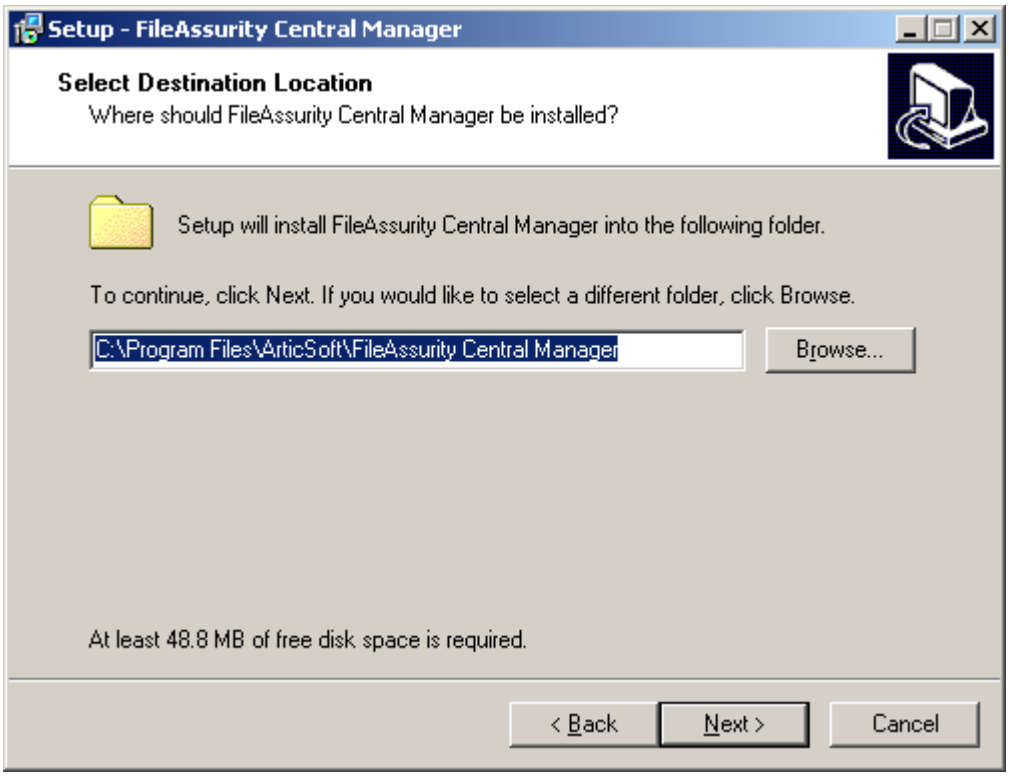
that the keystore they logon to is going to be the latest version. Whenever the keystore contents change the user will be asked to backup their keystore when logging off.

Installing Central Manager

Double-clicking on the file 'FileAssurityCentralManager.exe' will start the Central Administrator installation process.

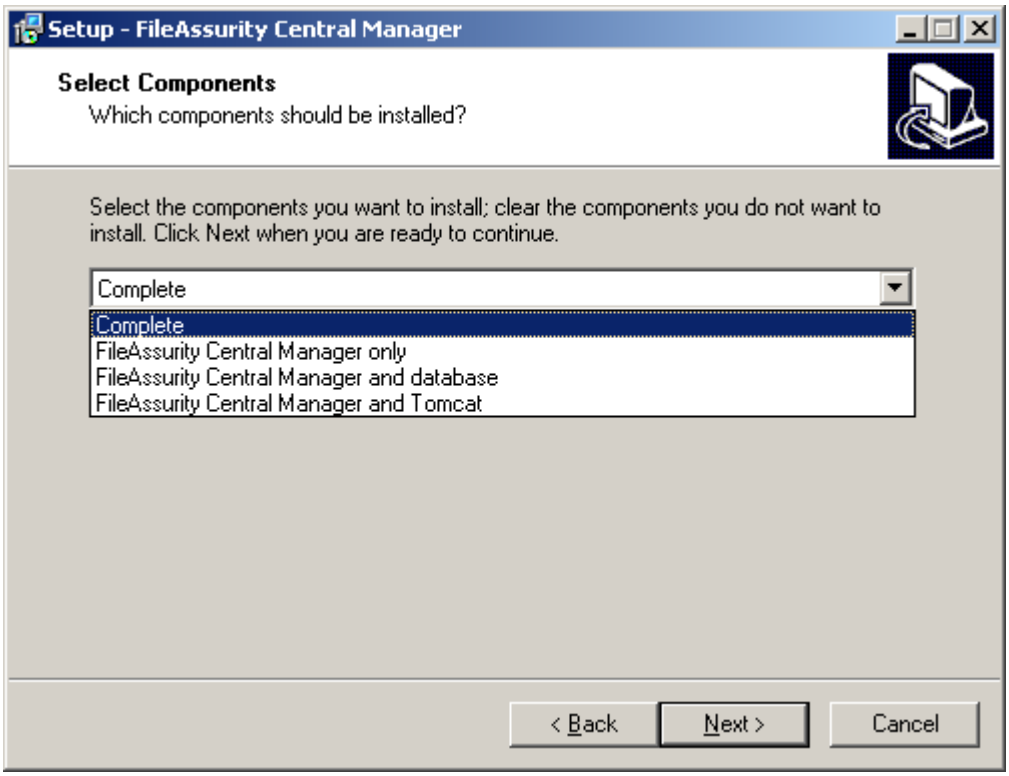


Once you have accepted the license agreement you will be asked where you want the files to be installed.



If you choose another location please remember that Master Keystores will be located in the folder that you have chosen rather than within the Windows 'Program Files' area.

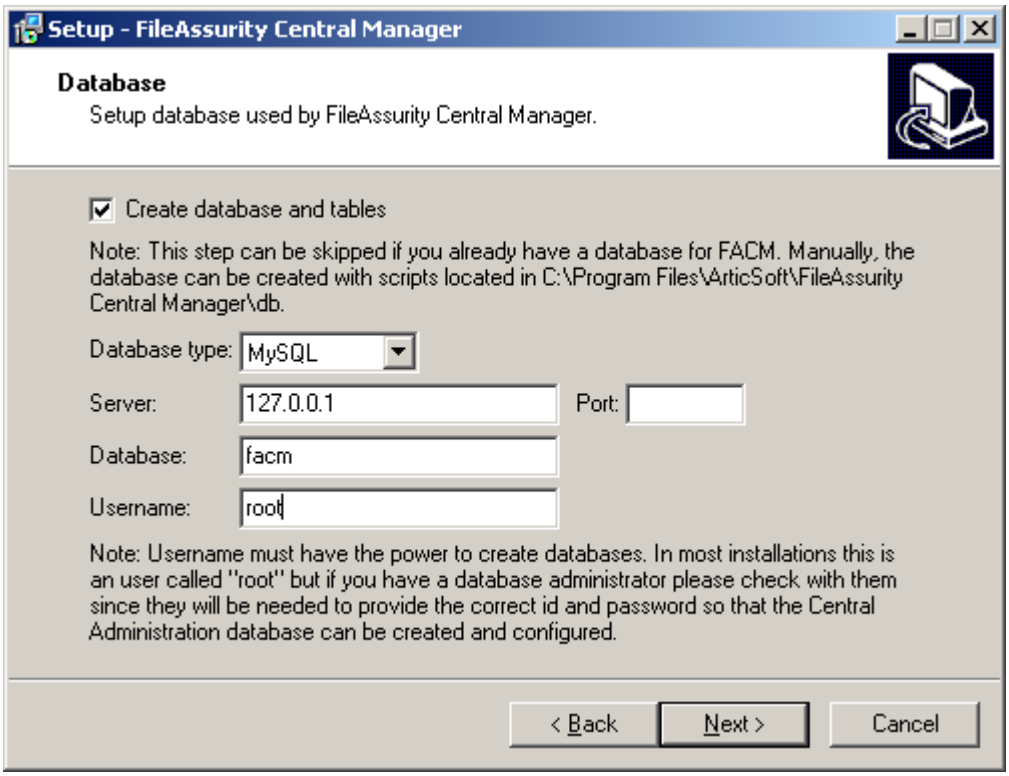
You may now choose the type of installation that you are performing.



. In this example we are going to select a 'Complete' installation, which installs the Central Manager program, defines and configures the database and its users and configures the Tomcat updater service.

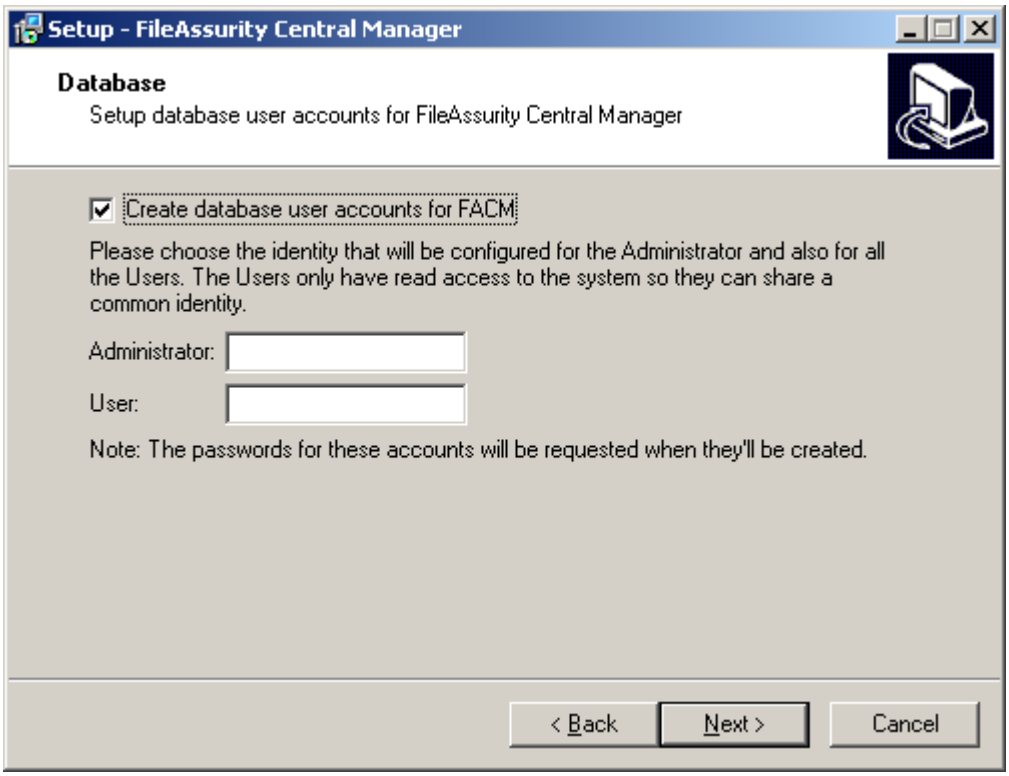
The next screen allows you to define the database and tables that are to be used. Obviously this is not selected when you are simply re-installing Central Manager or where you will install Central Manager and Tomcat only. If this is the first installation then you will fill in the relevant information in the boxes to meet your own installation requirements. We have shown some typical parameters as an example but you must check those for your own installation.

The IP address shown is not likely to be one that you can make publicly available, although it may be suitable internally. The default port number that Tomcat will use for listening on is 8080 if you do not enter a number here. If you are running internal firewalls you will want to check that this port number will be allowed to be used. When the Managed Client contacts the database it uses port 80 and communicates with TCP/IP on all occasions. Since the critical information being transferred is fully encrypted there is no compromise to the system if an attacker is able to observe the transfers.



Please remember that the database name can be anything that you wish, and does not have to use the name shown. If you are not the database administrator for the database server at the IP address you have defined, please check with them for a suitable username and password to allow you to create the database and users. You may use the values that we show in this and the following panels without serious risk of compromise provided that you have followed our recommendations concerning the use of passwords within the system.

Again, if you are installing for the first time you will need to complete the next panel:



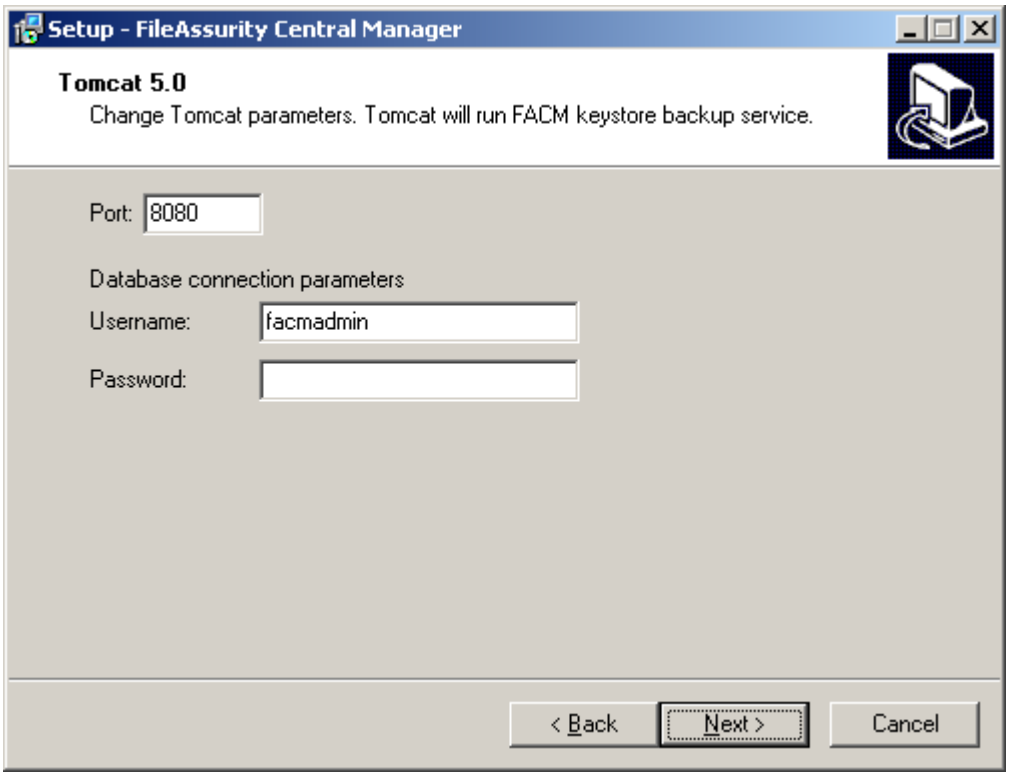
The usernames being set in this panel are those for the users of the Master Database.

The Administrator username is the one that Central Manager and Tomcat will use to write records to the Master Database. It should be long and complex, using upper and lower case and special characters and numbers so that it would be difficult for an attacker to find, guess, or try to locate using a brute force attack. It is never used by anyone except the programs running, so it does not have to be easy for people to remember!

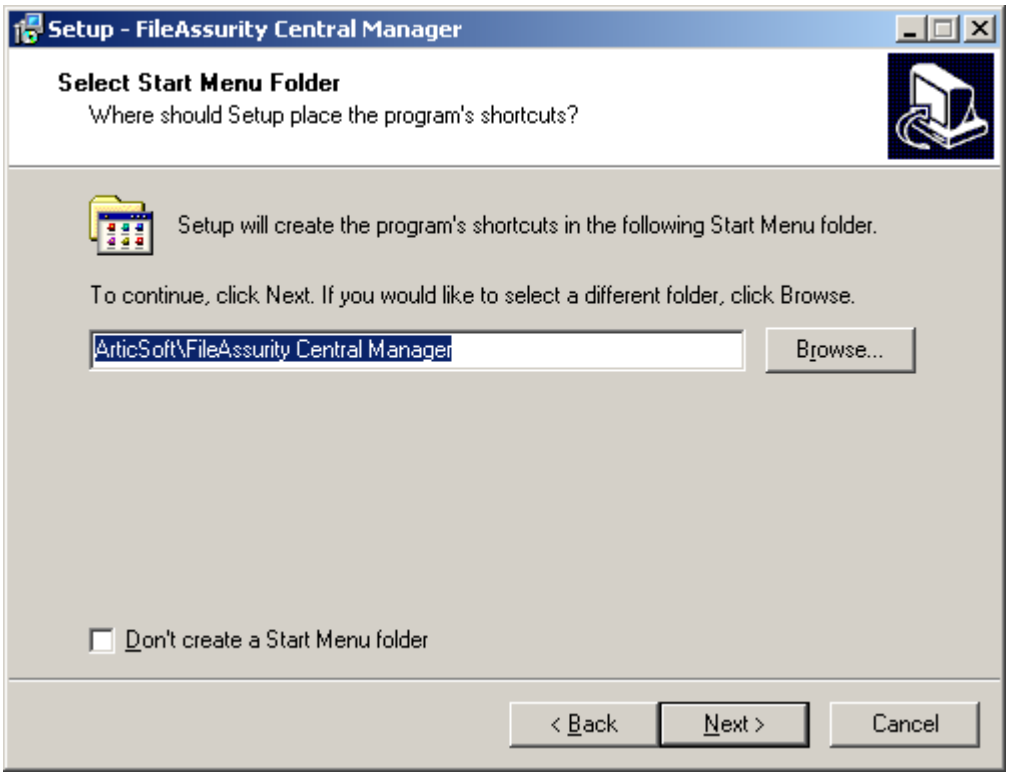
The User username is the one that all Managed Clients will use in order to read their records from the Master Database. It may be shorter to make it easier to remember because roaming users may have to enter it when working with a new computer system.

On the next screen you need to confirm the Tomcat operating parameters. These are the parameters that will be configured into the Tomcat installation, and they should match the parameters that you enter for inclusion into the Managed Client programs.

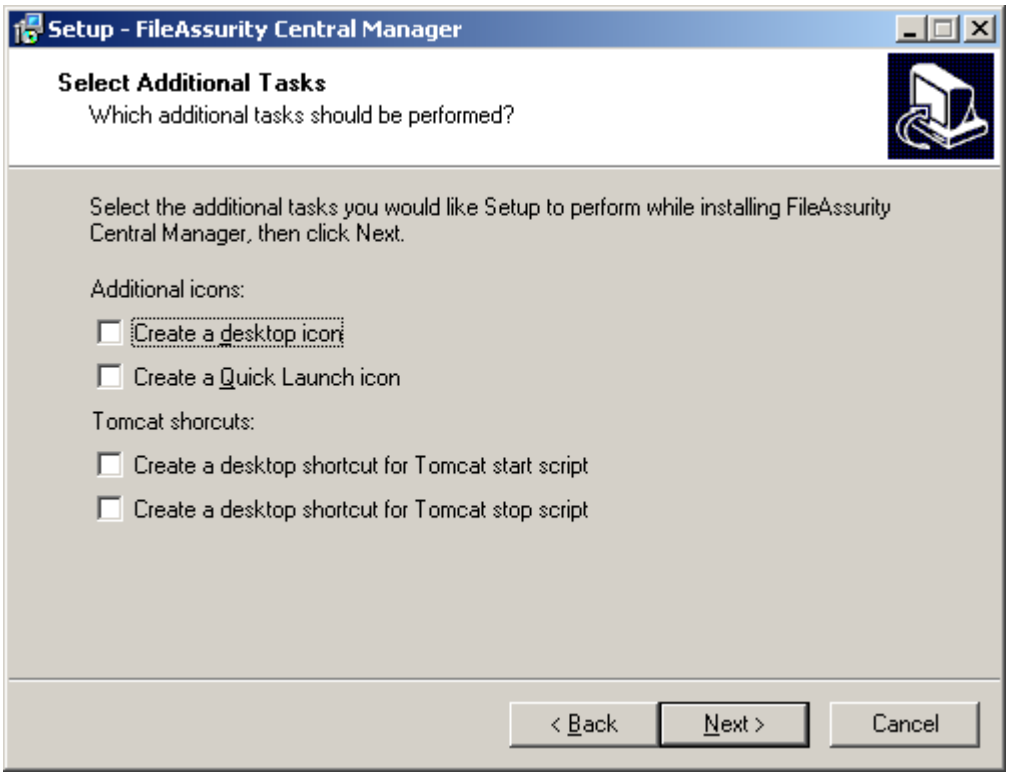
Please note that you should fill in the Username that you chose earlier for the database and the password for that username rather than the parameter that we show on the example panel:



You will now be asked if you wish to setup a Start Menu folder for inclusion in your Windows system.

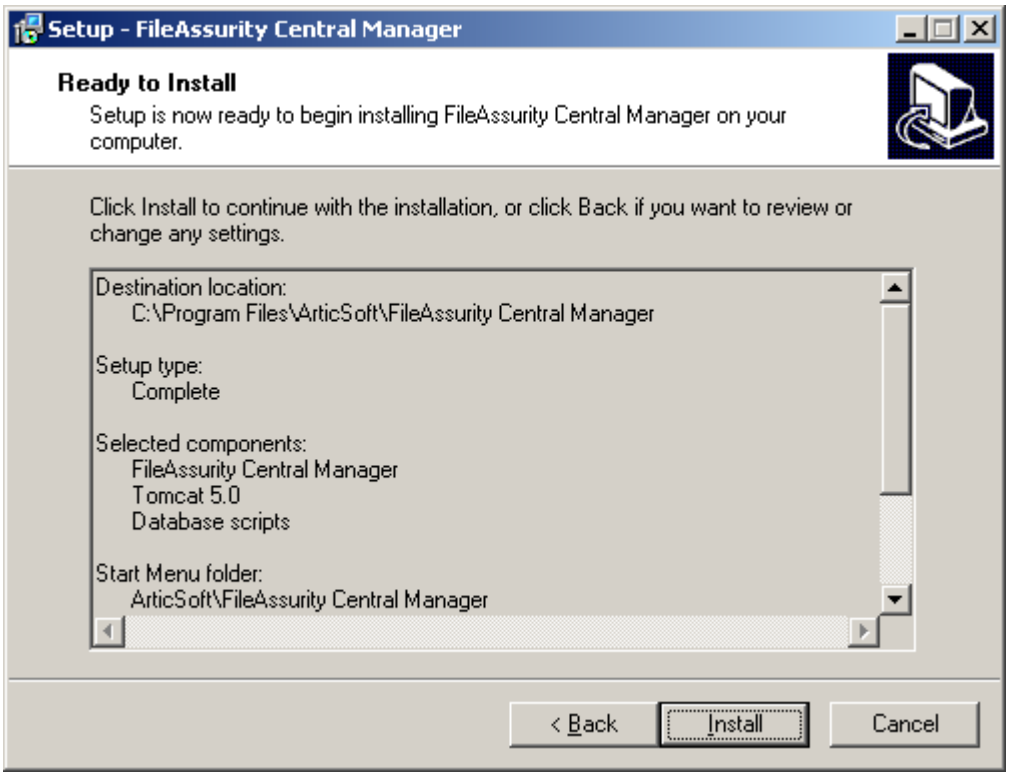


We are still configuring the Central Manager program and now need to decide if the program should be able to be run from a desktop link or from an icon in the system tray. Also, you may wish to be able to start and stop Tomcat (if it is to be run from the PC you are installing on) from desktop links. Please note that you should include Tomcat in your Startup activities on the computer on which it will run operationally so that it will be automatically be deployed whenever that system is started rather than having to wait for operator intervention to make the updater system available.

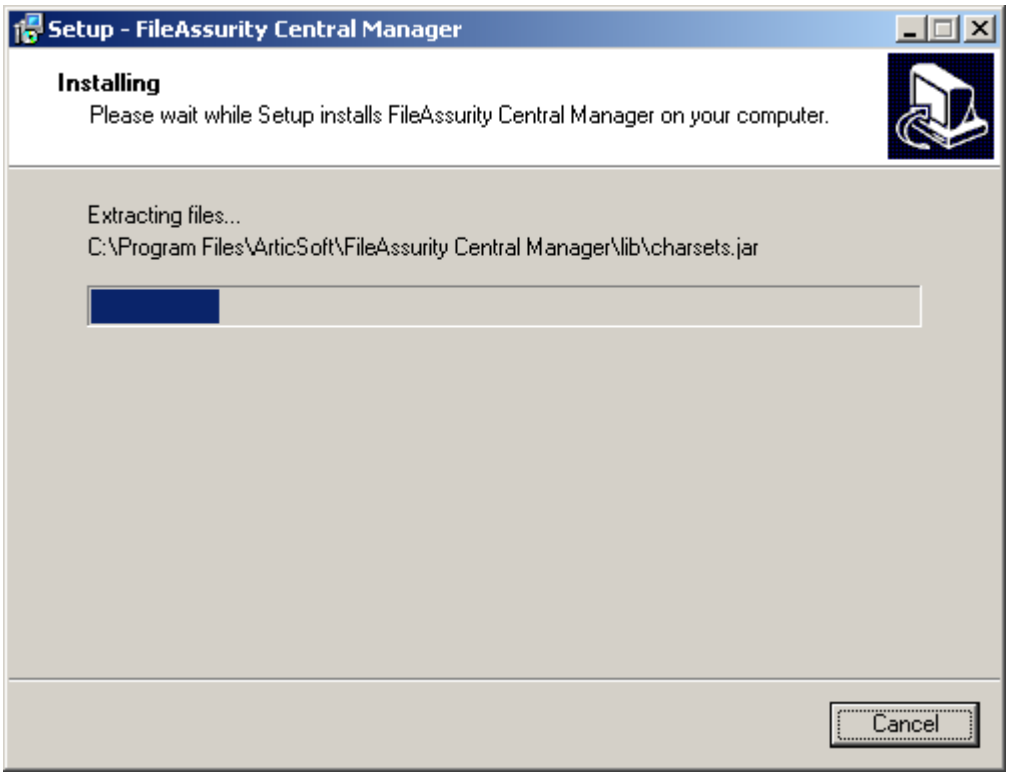


The boxes you check in this panel will depend upon which approaches suit your operational convenience.

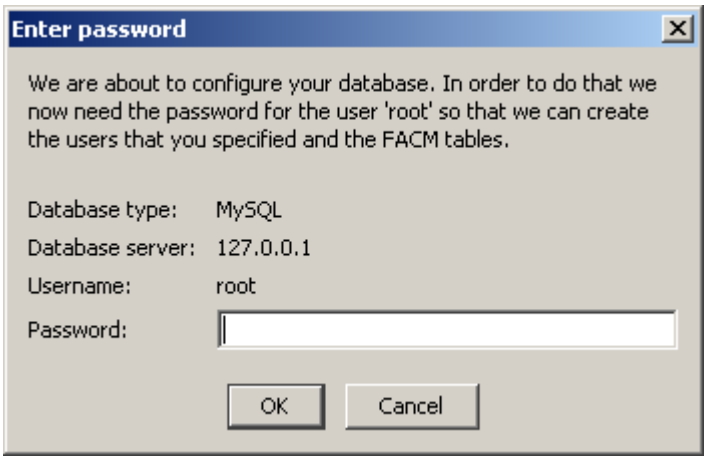
You are now shown a summary of the parameters and commands that you have created so that you can, if you wish, check them, and if any are seen to be wrong you can go back through the system to correct them.



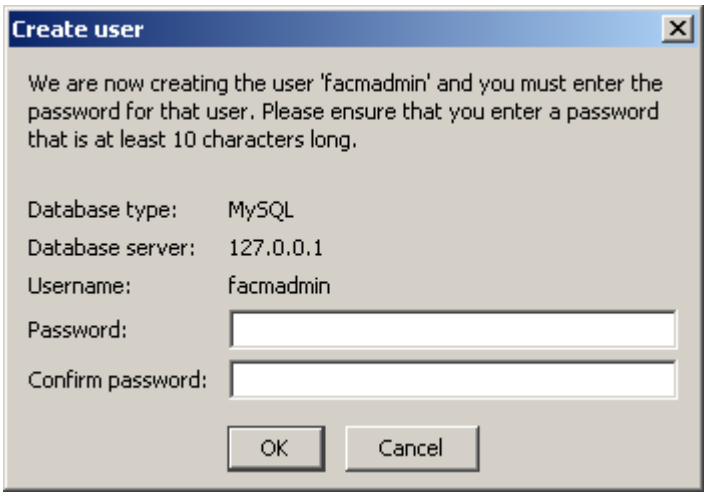
Once you have pressed Install you will see the flowing screen as the components that were selected are installed:

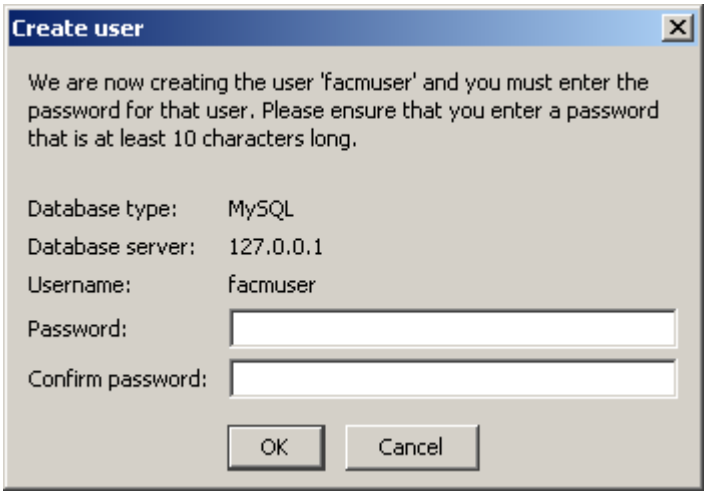


Once the required components have been installed the configuration of the database (if required) takes place:

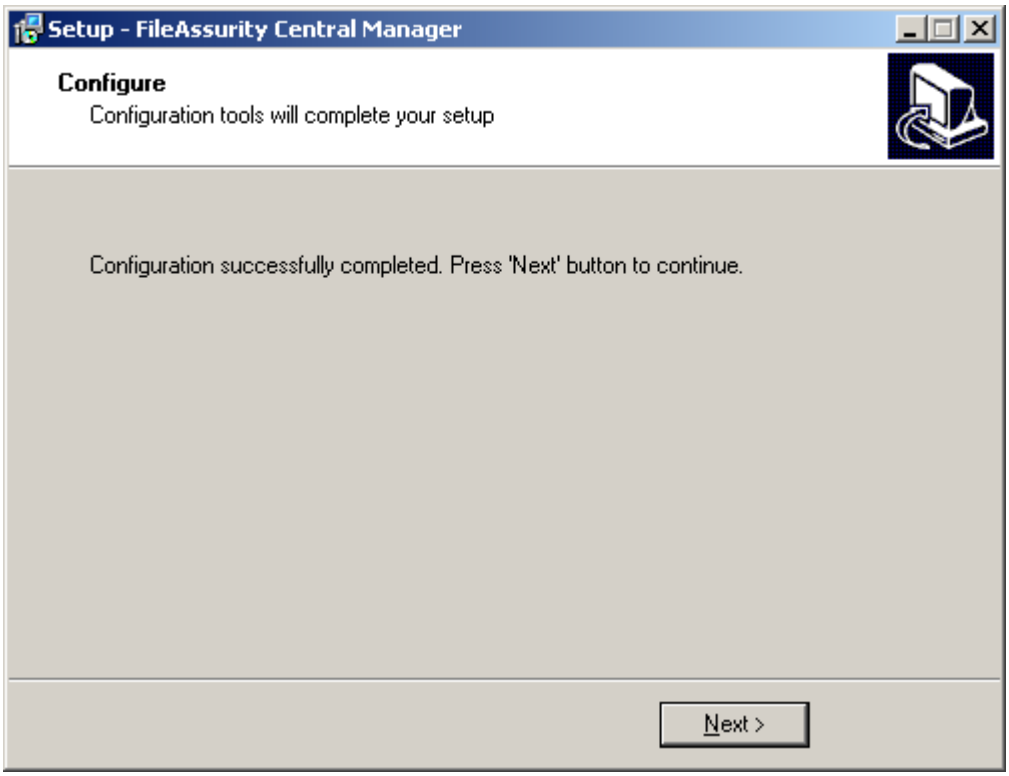


Here we are assuming that the master user 'root' is the Username that you are working with, and that you will enter the correct password for that username. If you entered a different username earlier you will see that name instead. On completing this screen the database will be created and the tables configured. The usernames and passwords for the database are set up in the following panels.

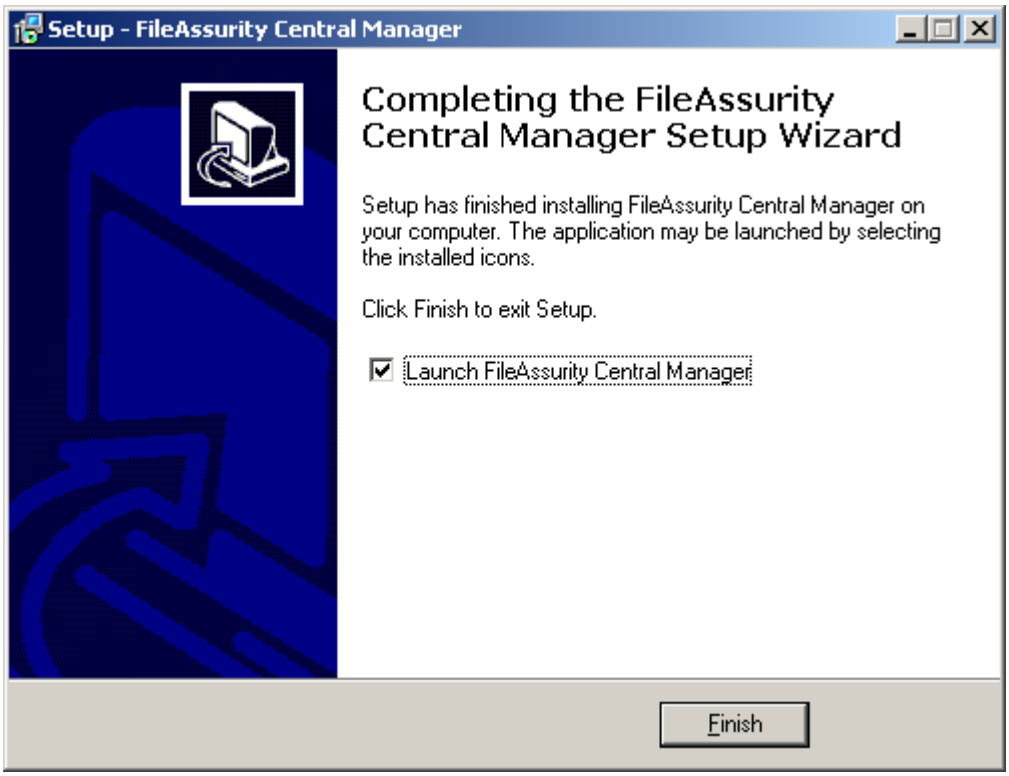




The passwords for the Administrator, and then for the User are there then configured into the database, and the database service made available for use.

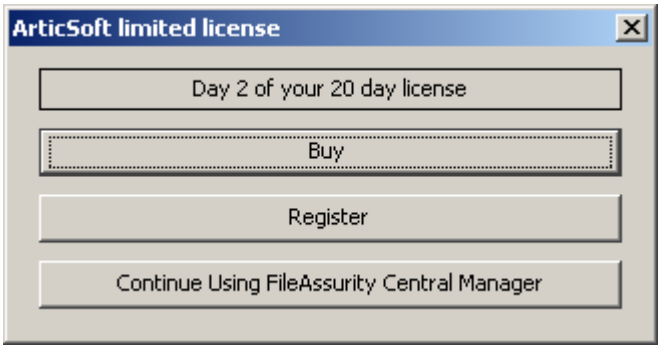


You have now completed the setup process and on pressing next you will see the following panel:



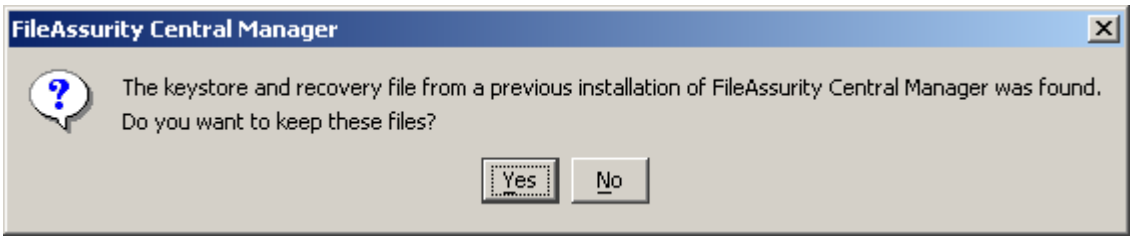
Press the

button to launch Central Administrator. The following dialog is displayed if you have not yet purchased or registered the Central Manager application:

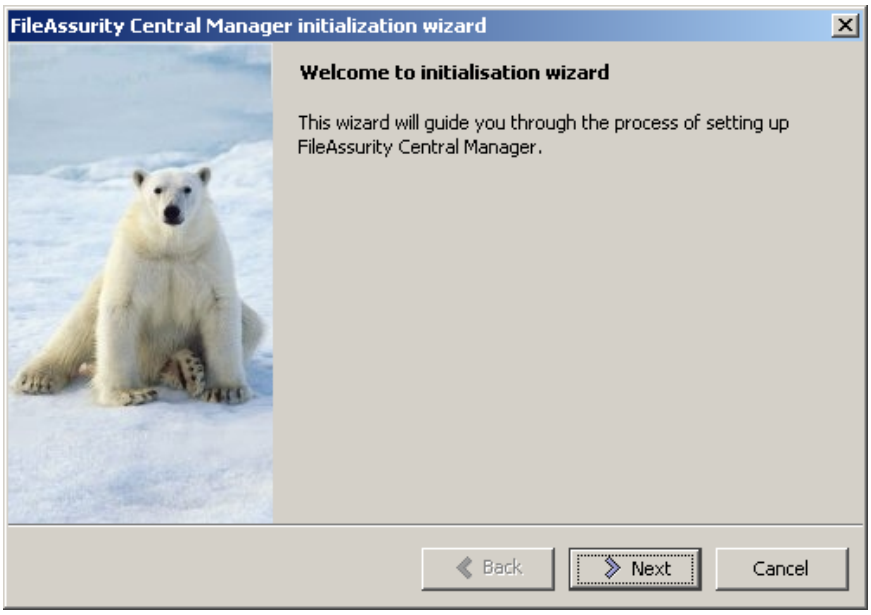


If you have already received registration codes you can click on the Register button in order to register online with the ArticSoft software registration service. Please note that you MUST go online to the ArticSoft website to register Central Manager.

If you are reinstalling Central Manager rather than installing a new copy you will see the following message:

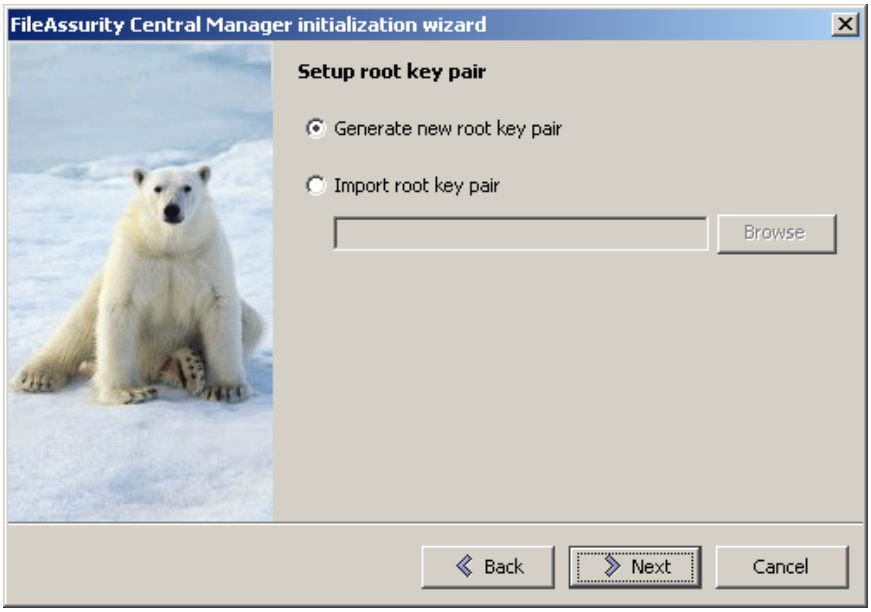


In the event of a re-installation you should answer Yes if you need to continue to work with previous Master Keystores. Please note that if you answer No at this point then the previous active keystore will be deleted and a new one introduced. This will also mean that you will not be able to access any other previously created Master Keystores because they are keyed to the system that is initialized by the system set up process that is entered. This panel is not displayed if Central Manager has not been implemented on this PC before. If you press No (or if there are no previous installations) the following panel is displayed:



On pressing the

button the following dialog is displayed prompting you to either import or generate a root key :



The root key is used to digitally sign all of the ArticSoft keystores. The root key is inserted into all user keystores and can be used to verify all internal users. You have the option of generating the Master Administration key and certificate, or importing it from an external source if that is preferred.

The choice is important because all the user keys that are subsequently generated will be digitally signed with this key, which will also be included in the Trusted Authorities list for all users.

This means that all the keys generated by the Administrator are automatically recognized by all the user clients of the system. (Please also see the section later of 'trust models.')

Importing a Root key pair

If you choose to import an X.509 standard key/certificate then it should be set to be a Root Authority or should be a Certification Authority that links back to one of the normal Trusted Authorities. If it is neither then the import will be rejected.

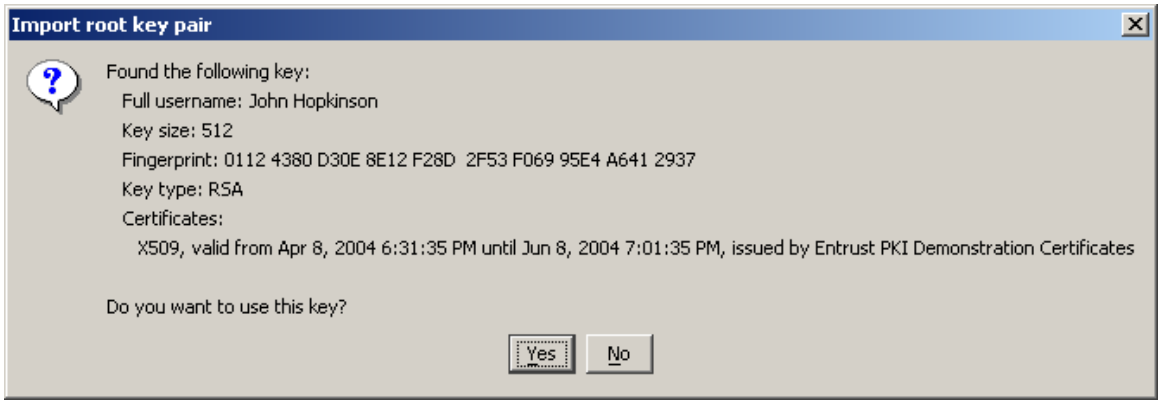
It is also essential to make sure that the signature size is a minimum or 1024 bits in length, and ideally at least 2048 bits. Ideally it should also have a life of at least 10 years. This is because it is unwise to select a key that has a shorter signature size than those created and used by default in both the Central Manager program and the Managed Clients, which are 2048 bits. Further, when that root key comes to the end of its allocated life, all the keys that it has signed will also fail. Replacing that key with a different key at

some later time is currently not possible, although it may be possible for the authority that supplied the key to extend its life. Central Manager has the ability to go on extending indefinitely the life of keys that it has created, including the root key for the system if Central Manager generated that key itself.

Note that you can only import key files of type .p12. This is because Central Administrator uses the X.509 hierarchical key structure capability rather than the OpenPGP 'web of trust' capability to check issued keys back to the root for the system. Central Manager will not attempt to resolve loops in certification chains or resolve OpenPGP chains nested more than once.

Importing a Root key pair

If you decide to import a root key pair you will be asked to browse to locate the file (.p12), and when you have selected it you will be asked for the password to release the private key. You will then be shown the critical parts of the keys being imported:

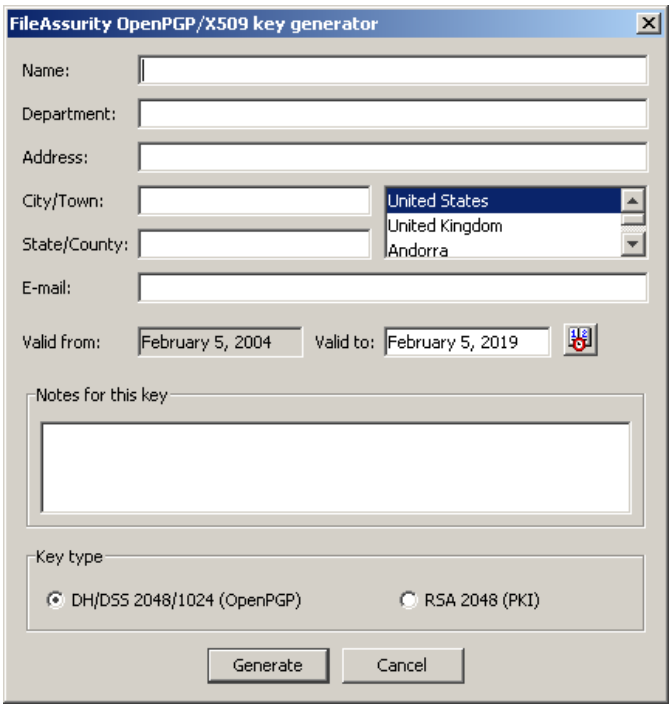


and asked to confirm that this really is the key that you wish to use as the root key for your installation. If it is correct press Yes.

Generating a Root key pair

Key Manager provides you with the ability to generate self-signed multi-purpose RSA 2048 and DH/DSS 2048/1024 bit keys. Although shorter key lengths are available compliant with international standards, Key Manager is pre-set to provide the maximum strength keys currently available. Keys generated using Key Manager are x.509 v3 compliant. Please note that the root key pair cannot be exported from the system, although the public key/certificate can be exported from the list of Trusted Authorities.

Note also that the information entered into the certificate will form the default entry for all subsequent keys generated. If you decide that you will generate a new root key pair the following dialog will be displayed:



All the fields (apart from notes) must be completed. And must contain at least one none-space character. You cannot enter The information you enter here is used in the key generation process and will be available to others when the key is distributed.

Name
Enter a 'friendly name' that is used to identify the owner or user of the key to you or other people. For example, 'ACME Corporation'.

Department
Enter your department name (for example, 'IS').

Address
Enter your organizations name (for example, ACME).

City/Town
Enter the City/Town where you or your organization resides.

State/County
Enter your State/County where you or your organization resides.

Country
Select your country from the pull-down list box.

E-mail
Enter your e-mail address. For example, 'administrator@acme.com'.

Valid From
This field is automatically filled in by Key Manager and is the date the key is created. This field cannot be modified.

Valid To
The date on which this key will cease to be valid. The system will prompt you with a date fifteen years ahead, which you can alter by entering a new date directly in the field or using the button to select a date from the calendar.

Note: The default life of a key pair generated by Central Manager is 15 years, but you are able to alter this to the period of time that your organization feels appropriate to their own commercial requirements. This is not likely to be less than 10 years both because the key length is considered suitable for that length of time, and because a significant amount of work can be created if you were to try and change the life of the key , say, every year or two.

Notes for this key
You can enter any additional information you want associated with this key. This information is purely for you to help you identify the signing/encryption key. For example, you may want to enter what you intend to use the key for. You can edit these notes at any time once the key has been added to your keystore. The information you enter here is never exported with the key.

Key Type
We do not make any specific recommendation for the choice of key type for your system. There are arguments in favour of either approach. You should note that the DSS signature key length of 1024 is used in DH/DSS because the standard issued by the US National Institute for Science and Technology did not allow a longer signature key, whilst RSA supports a 2048 bit key for both signature and encryption. **If you choose DH/DSS you will not be able to export keys in the .p12 or .p7b formats which are particular to the X.509 certificate standard.**

- DH/DSS - this generates a 2048/1024 bit key
- RSA - this generates a 2048 bit key

Once you have filled in all of the fields, press Generate. A message dialog informs you that a key is being generated. This key will be displayed in the 'Trusted Authorities' tab in Central Administrator and will be present in every user's keystore.

NOTE: All the above fields must be filled in because the international standard requires valid content. You will not generate keys very often so please take the time to enter

information correctly. If you have generated a key with incorrect information in it, delete it using Key Manager and generate a new one. You are able to override the requirement not to use special (strictly not the characters A-Z, a-z, 0-9 and space) characters, but if you do so you must be aware that certificate information you generate does not comply with international standards and may not be recognized or accepted by the user of other systems that strictly enforce the standard, although they will be accepted by ArticSoft products. **ArticSoft cannot accept any responsibility for difficulties caused with interoperability where you have not followed the standard.**

The key generation process creates unique keys based on information supplied by you and random numbers generated by FAOPGP. Therefore, whilst you can generate a key for exactly the same user information as a previous key but it will actually have a different key value and hence be a unique key. Central Manager makes a check that you do not attempt to generate a key pair with the same user identity and e-mail address, and will reject the request.

Generating the information recovery key pair

Once the decision has been made to either generate a key pair or import a key pair, the Master (root) Key for the system is set up and an Information Recovery key pair is also generated. This key pair is always hidden. It cannot be exported and the Administrator is not able to use it directly for any purpose. With approval from both recovery Administrators the key can be made available through the information recovery feature of Central Manager.

It is not possible to import an Information Recovery key pair because if you could do this then you could also bypass all the administrative controls that prevent an Administrator from being able to gain access to any encrypted information without supervision.

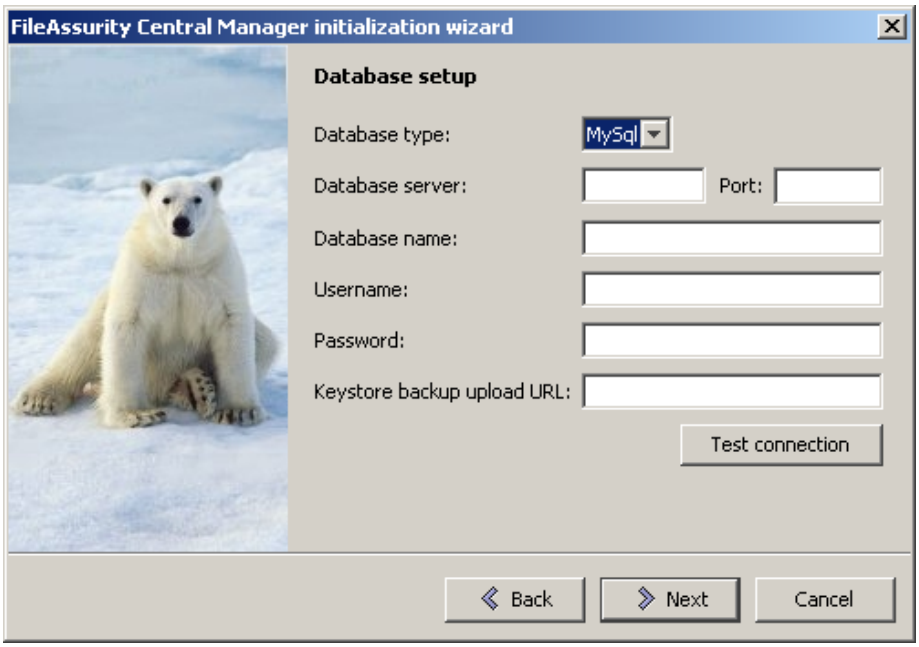
Please note that your system will be identified to ArticSoft using a secure hash combination of your root key and recovery key, so that all dealings with you will be unique, and no other system, even if it uses the same root key, will be considered identical.

Once the information recovery key pair have been generated the following dialog is displayed prompting you to protect the Administrator Keystore with a password:

The password must be at least 8 characters long. **NOTE :** This password cannot be changed once it has been entered so you will need to make sure it is adequately protected. This is because it is also recoverable using the two other Administrator passwords.

On pressing the

button the Administrator must then connect to the Master Database in order to start the Administration service. The following dialog is displayed:



In the example above we have not shown default names and settings. These will depend upon choices that you have already made when configuring the system. Your chosen settings should be shown on the panel. You should press the Test connection button to make sure that Central Manager is connecting correctly to the specified database. If you receive a message that you cannot contact the database please check the parameters very carefully to ensure that they are correct. **If you cannot prove the connection you should not try to continue the installation. Please be sure to take screen prints of any messages here before contacting ArticSoft support. They will not be able to resolve issues at this stage without full documentation of the problem.**

Database type
The Master Database may be any database service that is SQL compliant, upon request through ArticSoft sales. Currently MySQL and MS SQL are supported. Where examples are given of commands to set up or to administer a database it is anticipated that you (or the IS technical staffs supporting you) have an appropriate level of technical understanding of the requirements needed to select, install, implement and operate an appropriate database package, and to be able to create the access information and structure needed such that all users of the managed clients are able to access a copy of that database in compliance with policy rules that have been set by you or another Administrator.

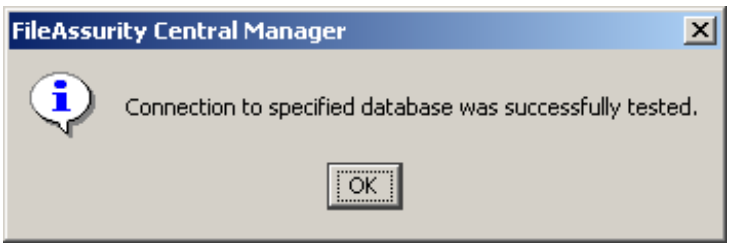
Database name
You can enter any name to identify the database that Central Administrator will talk to.

Username
Enter the user name that the Administrator uses to connect to the database. This should be the name of an Administrator that has read access to the whole database and write access to the keystores table.

Password
Enter the password for the Administrator

Keystore backup upload URL
This is the location where users upload their keystores to. This could be the same as the original database or for security reasons the original may be off-line. For the Central Administrator running with the Master Database on their local computer this could take the form, http://localhost:8080/updater/KeystoreUpload. Otherwise it should be the IP address of the Master Database and the port number that you have set to connect through. The values 'updater/KeystoreUpload' are not configurable.

Once all of the fields have been filled in above, press the Test connection button to validate the entries. If all of the fields have been correctly validated and connection to the database is successful then the following dialog will be displayed:



IMPORTANT NOTE :
The information that is input at generation can be changed. This initializing information is used by Central Manager when configuring client keystores. It is possible to change it at a later stage, however if you do that you may have to reprocess all the keystores issued prior to the change if you are doing this to migrate all users to connect to a new IP address or use a new port, or connect using a new username and/or password.

You should therefore try to choose a database address that will not have to be changed, and that the user name and password used by the Central Manager program unlikely to need change. Once the Central Manager program has connected to the database these parameters become part of the system and are held in the control files for the system.

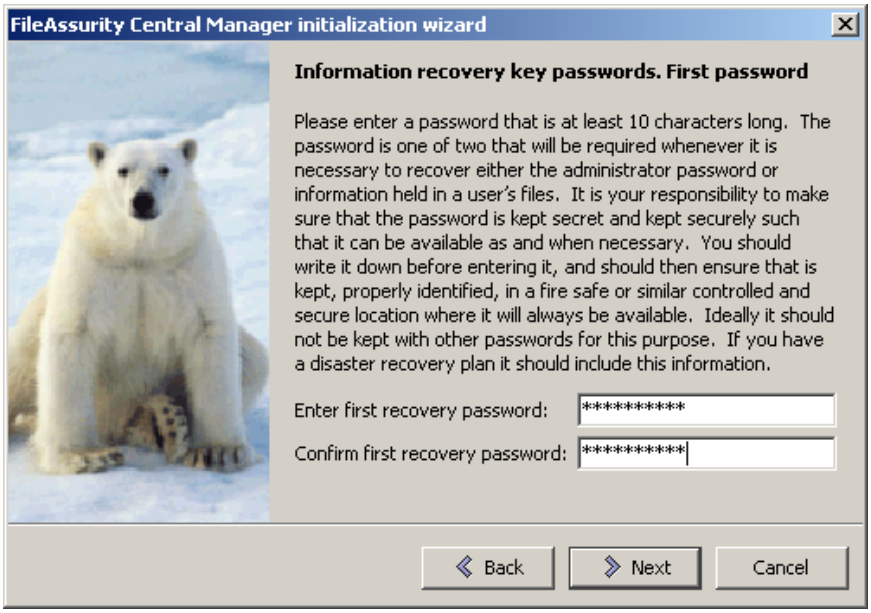
Once the Master Database has been successfully contacted two additional administrators must register passwords in order to be able to use the information recovery service (this allows these two administrators to authorize the decryption of any information that has

been encrypted by a user). Files and protected text may only be recovered if the two administrators authorize the use of that facility when Central Administrator is started (when logging onto the system).

IMPORTANT NOTE : Once entered these passwords cannot be changed and so they must be carefully protected. The passwords screens contain specific advice to the administrators over the care and protection of their passwords .

On pressing the

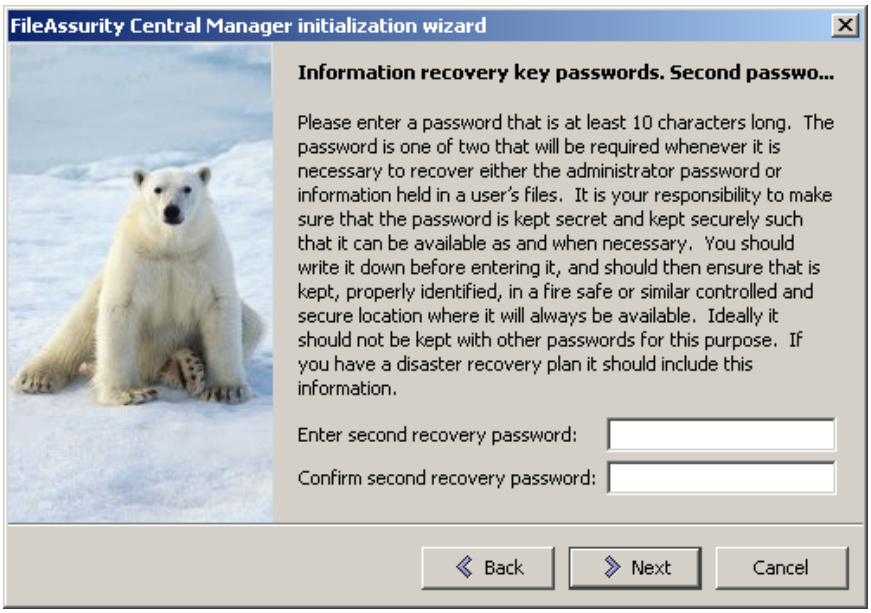
button the following dialog is displayed:



The first Administrator designated to provide the information recovery service should enter a password and confirm this password in the dialog above.

On pressing the

button the following dialog is displayed:

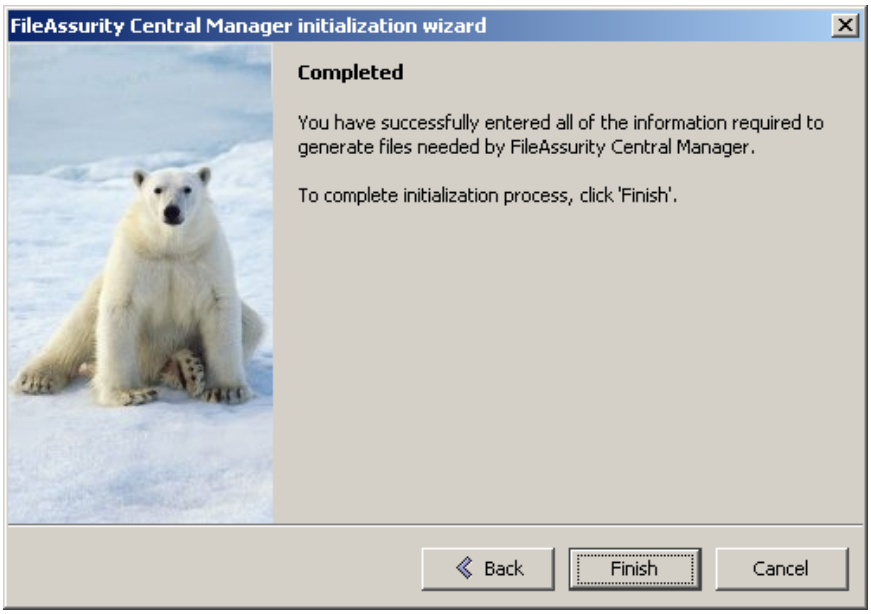


The second Administrator designated to provide the information recovery service should enter a password and confirm this password in the dialog above.

Whilst one administrator can be used to input both passwords, for security reasons we advise that two separate administrators are used in the information recovery process. This should help prevent any potential abuse of the system as two people have to be involved in order to recover encrypted information.

On pressing the

button the following dialog is displayed:

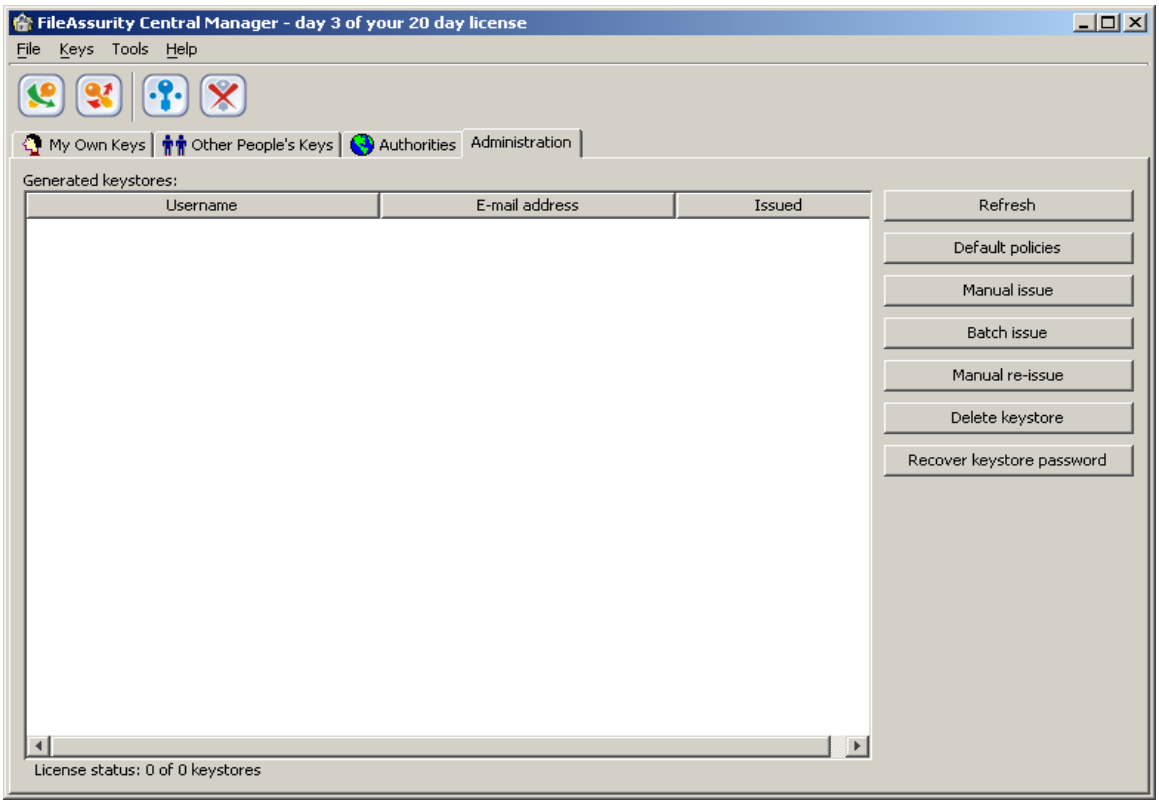


To complete the configuration of FileAssurity Central Administrator press the Finish button. You will now be asked to logon to the system.

Logging on to the system

To use the Central Administration application logon to the Administrator's keystore.

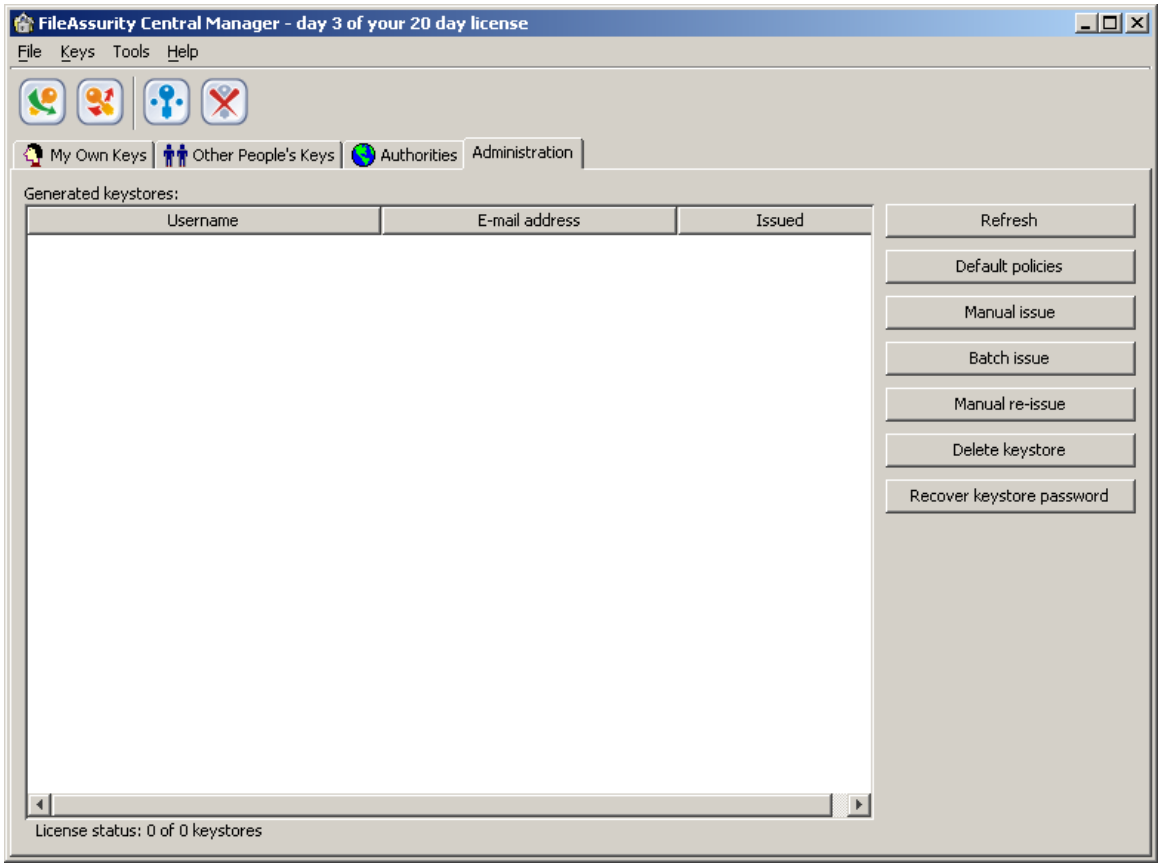
Enter the password for the Administrator keystore and press the Login button. (We will deal with the Information recovery logon in a later section.)



You are now ready to generate keys, set policy rules and issue keystores.

Central Administrator Application (the Master Keystore)

You are in charge of the Master Keystore. This has a similar appearance to a client keystore. In it you can create key pairs, import keys and key pairs. However, you cannot use this keystore for handling files, folders and secure text. The contents of the active Master Keystore are completely reproduced in the keystores that you generate for users.



You will need to generate and/or import keys for users. These keys will form the basis of their keystores and will enable them to encrypt files for themselves and others. In the Master Keystore, keys that are generated or keys that have been imported by you that contain a private key will be displayed in the 'My Own Keys' tab. These keys can be used to digitally sign files (if this policy has been permitted) and to encrypt files that only they can decrypt. Keys that are imported into the system and do not contain a private key will be displayed in the 'Other People's Keys' tab and can only be used to encrypt files

for others. Keys that are displayed in the 'Trusted Authorities' tab are root keys that are used to validate certificates.

Everything that is present in the Master Keystore is created in the Managed Client user keystore when it is generated. So if you include a key pair in the Master Keystore it will be present in all the user keystores generated whilst it is present. Please note that you may change Master Keystores to handle organizational or department default keystore/policy settings – see later.

This can be a very useful way of ensuring that keys will always be present in user keystores. Users can therefore send or receive protected information without having to import keys from outside. It is also the way in which you can include Trusted Authorities in keystores so that the digital signatures verified by them can be recognized by your users whilst it would not be recognized by the list carried in most browsers.

It is very important, therefore to make sure when generating keystores for users, that the Master Keystore contains the keys that you intend to distribute to the users whose keystores are being generated.

The Master Keystore must be included in any backups because it is essential to the operation of the Central Administrator program and the generation service cannot be operated without the Master Keystore.

If you create key pairs for inclusion in the generated keystores you should consider exporting those key pairs and storing them on a backup such as CD-ROM so that they can always be recovered in the event of a disaster.

Menu Options

File

Send License Request
You will need to register your implementation of Central Administrator with the ArticSoft online registration service. This will license you to issue a maximum number of keystores within your organization. Once registration has been completed you do not need to connect to the ArticSoft registration service again. Selecting this option creates a zip file containing information that is bound to the certificate of the Administrator root key. Once you have chosen a filename, your email application will be opened and the zip file attached to a mail message ready to be sent to accounts@articsoft.com

Add License
Prompts you for a .key file via a Windows browse dialog. This is the file accounts@articsoft.com has sent you. Once this file has been successfully imported, the Central Administration program informs you at the bottom of the dialog how many keystores you have available to issue.

Exit
Closes the Key Manager application.

Keys

Import Keys
Adds keys to the keystore. These may be keys belonging to users or keys provided by other people. You may import keys stored in the file formats .asc, .pgp, .gpg, .p12, .pfx, .p7b, .cer, . pkr. It does not matter what tab is selected in Key Manager as Central Administrator automatically works out where to store the key depending on the type of key file being imported.

Export Keys
Exports keys from the keystore. You can also right-click on a key to export it. You may want to generate and then export keys in order to form a key list (a list of keys available for import into other user's keystores).

Generate Key
Generates a personal protection key pair (encryption and signing key) for a user. This is exactly the same process as generating a root key except that this is now for the user.

Delete Key
Removes keys from the keystore. Highlight a key and then select this option. A dialog will be displayed asking you to confirm that you wish to delete the key before deletion takes place because this action cannot be reversed. You should always backup the keystore before deleting keys.

IMPORTANT NOTE: All Central Administration keystores are accessed using the Administrator password. They do not change between Master Keystores and you do not have a different password for each keystore. When you have Restored a keystore to become the Master Keystore, the filename of that keystore is displayed at the bottom of the panel whilst it remains active.

Help

Displays the help file (this manual) and version information.

Tabs

My Own Keys
This tab lists additional protection (encryption and signing) keys in the Master Keystore that will be added to a generated keystore besides the key pair generated automatically by the system when a user keystore is generated. A user keystore always contains all the keys that were present in the keystore in use by the Central Administrator at the time of generation. (Please also remember that a user keystore will also inherit the Policy that was in effect at the time the keystore is generated.) Key pairs will be included in this tab where, for policy reasons, a user should be able to use the key pair for digital signing or for automatic decryption. Those choices are determined by policy settings

Other People's Keys
This tab lists other peoples keys that are being included in the Master Keystore. These will have been included to ensure that users can encrypt files for specific users, organizational groups, or external enterprises. Policy rules may determine that the user cannot delete such keys. This may be relevant where the keys are for internal groups, and users should be prevented from being unable to use them.

Authorities
This tab contains industry recognized Certification Authorities (CAs) that vouch for the validity of keys used to sign files and the Administrator root key. The CA performs checks on the owner of the key to ensure they are who they say they are.
FAOPGP uses the information in this tab as part of the file validation process. Providing a person is using a key that has been validated by a CA, FileAssurity products will transparently verify the files. Users do not need to add any keys to their keystores for this to occur. The Authorities tab will also contain the root key for your installation (whether it was generated or imported at system generation time). If, as Central Administrator, you choose to delete Authorities, then they will not be included in user keystores. That must be a matter of judgment. You should read the section on Trust models, and consider carefully what you are attempting to prove with the technical mechanisms as part of your business process before deleting Trusted Authorities.

Administration
This tab shows keystores that have been previously generated for users and enables the administrator to generate user keystores, re-issue user keystores, set policy rules and recover user keystore passwords.

Main Display Area

The main display area displays the default names of the keys in your keystore and their associated email addresses. The email address is used by FAOPGP when sending files securely by email. The names shown are 'friendly names' that should help you identify the source of the key. You can change names by double-clicking on the appropriate key name, editing it and pressing 'Enter'. You would normally only make changes when the name is not helpful. A flashing cursor is displayed in the selected field to let you know you are in EDIT mode.

NOTE: Whilst you can change the name associated with a key this is unique to your keystore - this information is never exported with the key - the original name assigned during key generation is always used because that is the one actually on the certificate.

A ✓ is displayed next to the key name if the key has been successfully validated.

Notes
You can enter any information you find useful in this section. This information is purely for your own purposes, to help you identify keys, or to store additional information associated with them. For example, you may want to enter what you use this key for or for storing additional information about the owner of the key (such as their address or phone number). The notes section is not used by FAOPGP for any purpose and notes are not exported with keys.

Editing Notes
You can edit notes at any time by highlighting the appropriate key and selecting [Edit]

Saving Notes
Select [Save] in order to save the changes you have made.

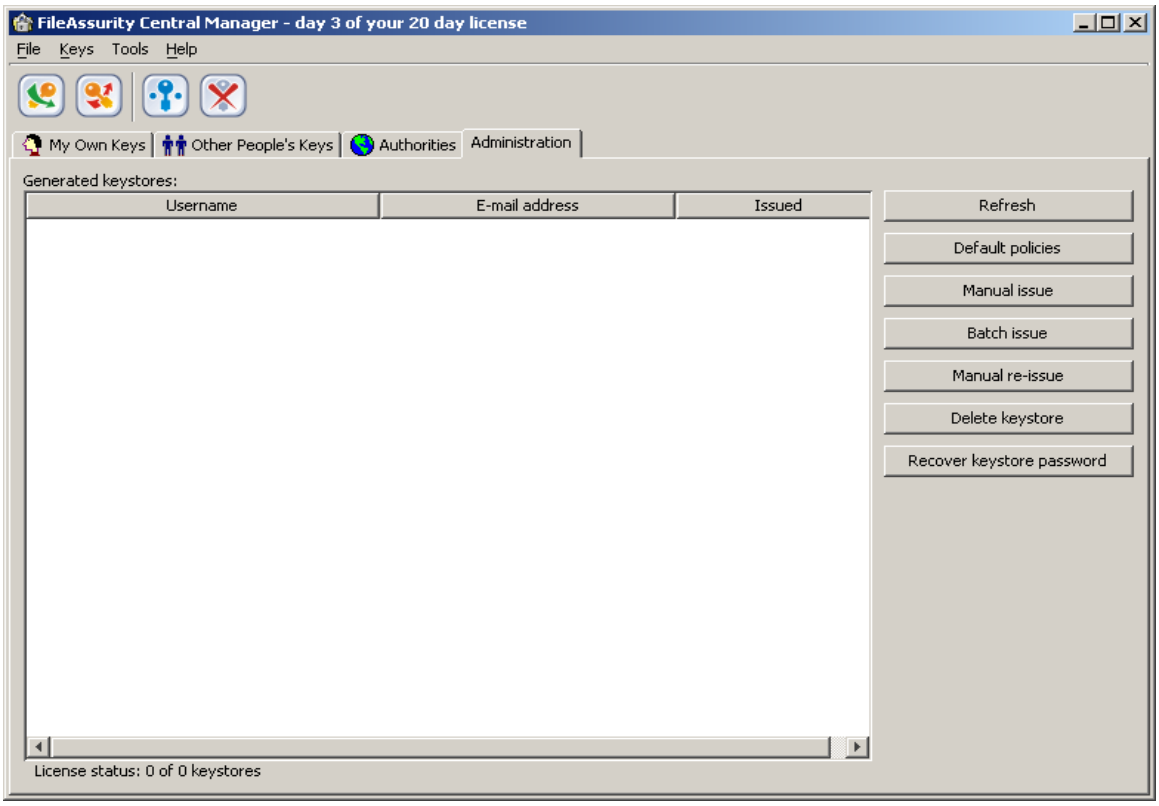
Cancelling Changes
Select [Cancel] in order to cancel any changes you have made.

Key Information
Information displayed at the bottom of the dialog tells you what certificates certify the key you have selected. If you have generated a key in FAOPGP, then certificate types of both X509 and PGP format will be displayed.

Advanced Press this button to view additional key information associated with the key you have selected (highlighted).

Administrator generation functions

The Administrator has a number of capabilities in keystore administration and these are accessible via the 'Administration' tab.



The screen above shows that the Administrator is able to make enquiries of the Master Database and select individual keystores located there for update.

Refresh

- allows the Administrator to update his view of the content of the Master Database.

Default policies

- allows the Administrator to set the default policy settings for the Master Keystore from which other keystores are generated or updated.

  Policies are explained in depth later in this document.

Manual issue

- this command allows the Administrator to issue a single keystore. When using this command the Administrator has to complete all the details for each keystore that is going to be generated.

Batch issue

- this capability allows the Administrator to generate and issue keystores in bulk by reading information from a .csv file. If you select this option then you will be asked to browse to a .csv format file containing the parameters for the user keystores that you wish to generate. The file will be verified in realtime. If an error in the input file is found you will be notified on-screen, and you will have to correct all errors found in the input file before it will be processed. The format of the input for the batch file is described in the file batchkeystore.csv which is included on the installation CD-ROM. Please note that you can only specify the user keystore password using batch generation. This mode is NOT supported by manual issue. Also, batch generation does not allow for the e-mail distribution of passwords and database details. If the system generates passwords you will have to set up a process to extract them for forwarding to the user. The information that you need will be contained in the audit log generated by the batch issue process.

Manual re-issue

- this command allows the Administrator to change the end validity date of the default certificate in the user's keystore and to change the policy rules associated with that keystore. It may also be used to add key pairs to user keystores. **Be aware that if you are updating policy, then the policy that will be used is the policy for the currently active Master Keystore. If the Master Keystore has been loaded from backup, then its filename will be displayed at the very bottom of this panel. Further, any keys that are present in the Master Keystore currently in use will be added to the user keystore when policy is being updated.**

Delete keystore

- this command allows the Administrator to remove (revoke) a user keystore. The delete function asks for confirmation that the correct keystore has been deleted. **TAKE CARE USING THE DELETE FUNCTION AS DELETED KEYSTORES CANNOT BE RECOVERED. IF IN DOUBT MAKE SURE YOU HAVE A BACKUP COPY OF THAT DATABASE ENTRY**.

Recover keystore password

- user keystore passwords can be recovered using this feature
- highlight a user keystore and then press this button

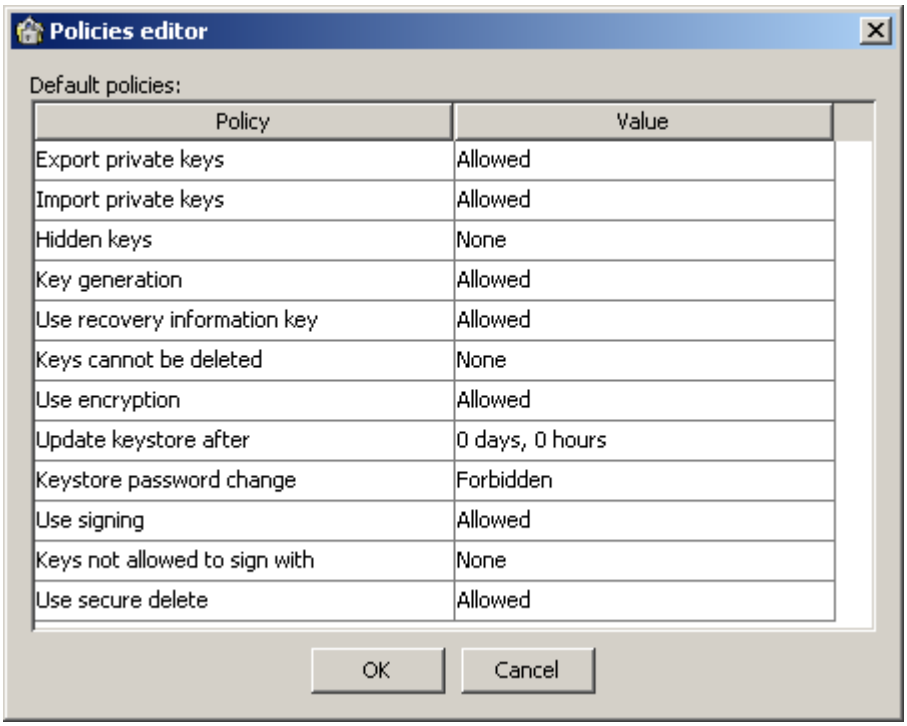
- when this option is selected the user keystore password is displayed on the screen and is not made available in any other way

Keystore policy

Keystore Policy is used to determine controls that can be applied to users in a managed environment. Like the Master Keystore, the current Policy settings are applied to user keystores being generated.

It is therefore important to understand the interaction between the contents of the Master Keystore and Policy. It is also essential that the Administrator check on current policy settings before generating user keystores. **This is particularly critical before setting off a batch generation of keystores. If the policy settings in force in the Master Keystore are inappropriate there may be a significant amount of work involved trying to rectify any errors.**

The policy options available to the Administrator are:



Policy	Value
Export private keys	Allowed
Import private keys	Allowed
Hidden keys	None
Key generation	Allowed
Use recovery information key	Allowed
Keys cannot be deleted	None
Use encryption	Allowed
Update keystore after	0 days, 0 hours
Keystore password change	Forbidden
Use signing	Allowed
Keys not allowed to sign with	None
Use secure delete	Allowed

Policy settings are applied to the contents of the user keystore as it is generated from the Master Keystore.

The policies that can be applied are of two types.

The first are policies applied to individual keys in the Master Keystore. The second are applied to the capabilities of the user using the keystore that has been generated.

Policy settings may be changed retrospectively by the Administrator applying new values to individual keystores. However, the Administrator cannot remove keys that are already installed in user keystores. This is a management control. If you have already issued a key or key pair to a user you cannot remove it. Similarly, if the user has the authority to import keys then it would not be correct for the Administrator to remove keys. So Administrators are not able to remove keys from users once they have been issued.

The Policy settings available for the Administrator to enforce are described in more detail as follows:

Export private keys

- used to ensure that a user cannot compromise their private key by stopping their ability to export it.
- it would be selected when you do not want the user to be able to transfer their private keys to another system. If a user can export their private key they may be able to use it in another application such as another OpenPGP compliant product, where they could continue to be able to use a key that the Administrator has issued.
- normally this should be set to Forbidden, but the Administrator may have users for which this should be Allowed. This might be because the user needs to have these keys present on both a laptop and a desktop computer.

Import private keys

- ensures that users cannot import identities from other sources for possible private use in this system,
- this policy allows the Administrator to prevent a user from importing key pairs from another source. If a user is able to do this they can import keys from any other source and use them, perhaps for topics that the organization would not approve or would not be considered compatible with use of the product in the conduct of their employment. At the same time there may be senior members of the organization that would have such a requirement and that would have to be respected.
- the recommended normal setting for this policy is Forbidden.

Hidden keys

- allows the Central Administrator to prevent a user from being aware of the presence of keys (either a key pair or a public key/certificate) that are loaded in their keystore. The Central Administrator may have generated or imported keys which may be used to communicate with Groups (please see later for a review of the issues to consider when dealing with Group keys). Where users are recipients of Group information the Group keys may be hidden to prevent them being able to send information to the Group. This works because users are not able to select this key to 'encrypt for' when protecting files or message text.
- the Central Administrator should select this option where there are keys that the user does not require to be aware of, but which enable the user to have access to files which are logically the common property of a group (say, all communications to the Finance department in general).
- if keys are hidden then they cannot be deleted by the user, so if a key is hidden it is not necessary to specify that it cannot be deleted (see later).
- the information recovery key is always hidden when present.
- you can select the appropriate key(s) from the pull-down list box.

Key generation

- allows the Central Administrator to stop a user from generating their own key pairs. This may be necessary if the Administrator does not wish a user to be able to generate a cryptographic identity other than the one that the Administrator has generated.
- this control must also be seen in the context of information recovery (see later) and import of private keys (see earlier).
- the Administrator would normally Forbid this capability because the Managed Client should not require it.

User information recovery key

- allows the Central Administrator to perform Information Recovery for this user or not.
- this policy would normally be set to Allow for all users, but there may be some senior members of the organization that do not wish the Administrators to be able to recover files secured by them (members of the board perhaps).
- This policy should normally be set to Allow.

Keys cannot be deleted

- allows the Administrator to prevent a user from deleting keys that the Administrator has loaded into the keystore. This may include keys of Trusted Authorities or other keys that the Administrator has decided to include in the user keystore such as keys being used as 'group' keys. It is not necessary to mark the key generated for the user as not to be deleted because that is done automatically for you.
- please note that keys that have been defined as hidden by policy do not need to be defined as 'cannot be deleted' because the user cannot find them in order to delete them.
- you can select the appropriate key(s) from the pull-down list box.

Use encryption

- allows the Administrator to define if users are able to encrypt information.
- this may be important where it is essential for junior staff to be able to receive encrypted information from others (either externally or internally) but they are only able to digitally sign information themselves.
- this can be used in conjunction with the recovery key, since if the user cannot encrypt then there is no need to impose the overhead of a recovery key for their keystore.

Update keystore after (n) days (n) hours

- this puts in place the frequency with which the user must connect with the keystore database. The effect of this is to require the user to contact the Master Database and verify their keystore is still listed before they can use the application. (This feature creates the ability to have online user revocation by deleting the user keystore. Revocation becomes effective as soon as the user next has to connect to the Master Database.)
- a value of zero means that the keystore must be verified every time that the user logs on. A value greater than zero sets the time interval before verification must take place.
- this means that where you have users who are off-site for periods of time (sales staff, senior management) you can set periods of time appropriate to their connectivity to the central system, as a means of checking that they are still approved users.
- this is also a form of revocation control. If a user attempts to logon and the program cannot connect to the Master Database then it will not allow the user to operate FileAssurity OpenPGP until they can connect to the Master

Database. Users can therefore be suspended temporarily or permanently by removing their keystore records from the Master Database. This can be done by the database Administrator or the Central Administrator.

Keystore password change

- allows the Central Administrator to Forbid the user from changing the keystore password. There are several implications when setting this policy entry.
- if the user is able to change the keystore password then there is no way that the Central Administrator will be able to change policy or refresh the certificate of the user unless the user changes their password to the one assigned on generation.
- whilst the user can upload their keystore to the Master Database the Administrator cannot actually administer the keystore, unless the user discloses what their password is.
- normally, therefore, this field would be set to forbidden unless there is a reason why the user should be able to change their keystore password.

Use Signing

This policy applies to ALL of the keys in a user's keystore and can be used to prevent a user selecting any of their own keys for digitally signing information. If set to 'Forbidden' then the user can only use the keys in their keystore for encryption.

NOTE : If you only want users to be prevented from signing with specific keys then you can do this via the 'Keys not allowed to sign with' policy.

Digital signatures may be used in some circumstances to imply that a document signed with a digital signature has legal authenticity. Where that digital signature can be linked back to your organization it might be implied that a document has the authority of your organization. It is possible that you may wish to prevent some of the users of the service you are providing from being able to apply a digital signature to any file, text or document, and you would use this policy setting so that they could receive encrypted information but could never apply a digital signature to information.

Keys not allowed to sign with (Group keys)

This policy can be used by the Administrator to create key pairs that can only be used for encryption by the users. This may be a convenient method for creating keys that allow all those who have access to them to be able to read information encrypted using that key. This is referred to as using Group keys. You can select the appropriate key(s) from the pull-down list box.

Consider that an organization may contain a number of different groups or departments that need secure communications internally, such as: accounts, production, senior managers, and so on.

Further, when people external to the organization wish to communicate securely with it they may have no single individual as the point of contact. The may also wish to address themselves to a function or Group inside the organization and are content that any approved individual within that function is able to read their message and respond to it.

Conventional public key systems require that individuals communicate with individuals. However it is possible to issue members of defined Groups with a Group key pair so that they are able to encrypt information for any member of the Group and also decrypt anything for the Group.

Naturally this is achieved by following a convention in Central Administration that the Managed Clients are restricted in the way that they can use the public key system. You could achieve the same effect by issuing all members of the same group with a key pair from the Master Keystore, but it would be illogical to allow any member of the Group to use that key pair for digitally signing information since it would not be possible to know which individual had actually signed it.

Therefore the ability to restrict the use of a key pair to be used by a Group by forbidding use for digital signature allows the Administrator the flexibility to create a situation where internal information may be shared readily, and where, by making Group public keys and certificates available to those outside the organization, they can facilitate communications with external individuals and organizations.

The Administrator should remember to set the identity of the key pair to the Group name and the e-mail address associated with it to an appropriate generic e-mail address for the organization: e.g. sales@articsoft.com, accounts@articsoft.com, support@articsoft.com.

Please note that if you have used the 'hidden' policy on a key pair being used for a group then the user cannot encrypt information for the group. Information can be decrypted

without the user being aware of the presence of the key pair. Use 'keys not to sign with' where the user has to have the ability to share information with other members of their group.

Use Secure Delete

If set to 'forbidden', this policy will prevent users from using the secure delete facility in the FileAssurity OpenPGP client and thus preventing them from securely deleting files beyond recovery.

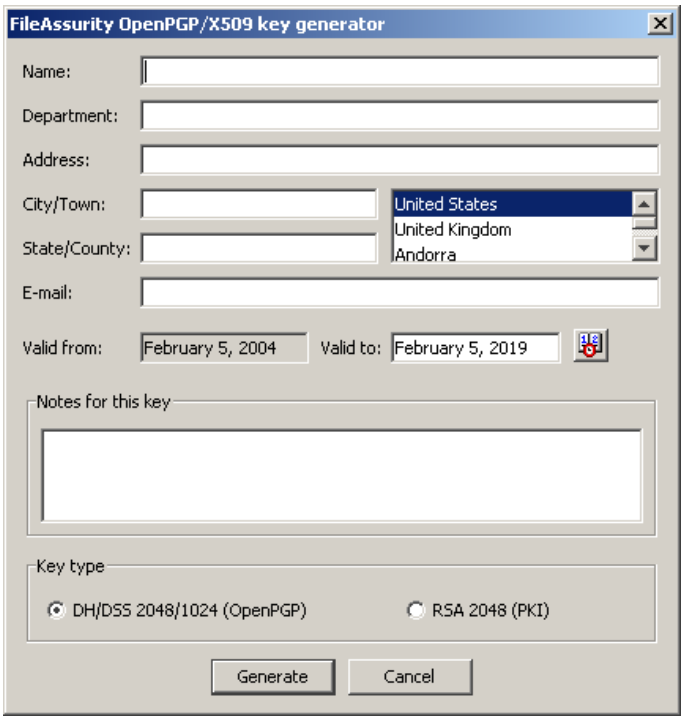
Generating user keystores

Once you have populated user keystores with the necessary keys and applied the necessary policy rules you will need to issue the user keystores. This has the effect of adding them to the SQL database.

Keystores can be generated in either manual (a single keystore) or batch mode (multiple keystores). If you have a lot of users batch mode is the quickest method of operation, as information is taken from a .csv file rather than you having to manually enter it each time. In both modes, the keystore generation process automatically generates a unique password for each user keystore.

Manual Issue

If manual issue is selected then the following dialog is displayed :



The fields apart from Name will be automatically taken from your system root certificate and put in as default entries. If you fill in the required User name and alter the other fields (make sure to change the e-mail address) if required you can then generate the user keystore.

Once the Generate button has been pressed the system asks if you want to email the password it has generated for this keystore to the user. If you select 'Yes' your default email application is opened with a message containing the password - the email address entered above is automatically filled in so all you have to do is press the 'send' button. If you select 'No' you will have to communicate the password by another means using a manual system.

Batch Issue

If you select this option you are prompted for the name of the .csv file that contains the information that is needed for each user keystore, including the fields to be completed for an X.509 format certificate. When generating keystores in batch mode all fields are required and no default settings are taken from the system root certificate.

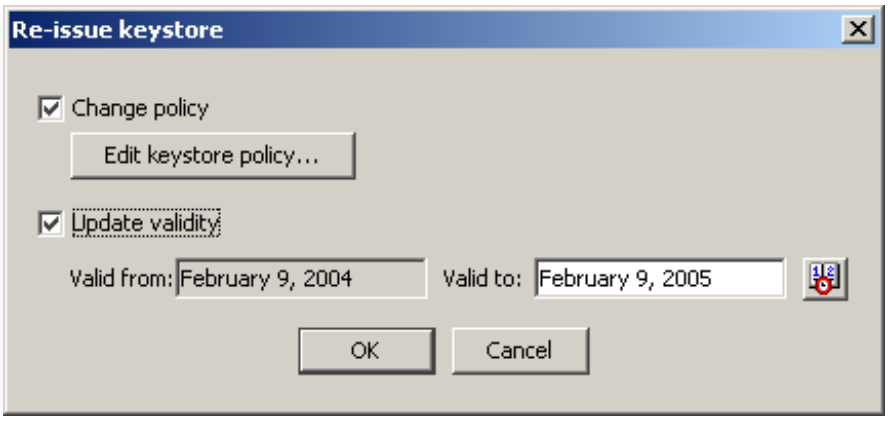
An example file format, batchkeystore.csv, is provided on the CD.

Once you have selected your .csv file, another browse dialog is displayed prompting you for the location of the report log. Processing begins immediately after you have saved the report log file. The report log also displays the passwords for the user keystores.

IMPORTANT NOTE :
The user identity and their e-mail address used in the key generation process are also used as the username and email when the record is in the Master Database. These cannot be changed. The username is also be used when implementing the client user because that is used by the client program FileAssurity OpenPGP to locate the correct keystore to download onto the client desktop.

Re-issuing user keystores

This feature enables you to change user's keystore policies and to update the validity date of a key. The validity period for a key/certificate and policy rules can be altered on a keystore by keystore basis. It is not possible to delete keys from a user's keystore during a re-issue, although it is possible to add keys to a user keystore, and to change policy. Currently this feature is not available for batch processing.



Change policy
You may want to change policy rules for a user if new policies are required to be enforced throughout your organization.

Check the 'Change policy' check box and then press the Edit keystore policy button.

You will now be shown the default policy field CURRENTLY IN FORCE IN CENTRAL MANAGER – NOT THAT ORIGINALLY IN FORCE WHEN THE KEYSTORE WAS CREATED. If you are using backup/restore keystore in order to have default keystore/policy settings for specific groups of users please check carefully that you have the appropriate Master Keystore loaded before making changes to policy.

Please also remember that ANY keys present in the Master Keystore that were not present when the user keystore was originally generated will automatically be added to the user keystore if you approve a change of policy.

Helpful Hint : This option can also be used to check the policy rules that are currently in place for an existing users keystore. By selecting 'Edit keystore policy' you will be shown the current policy applied to that user.

Update validity
You may want to change the key validity date because you originally chose a short time period (depending upon the attitude of the organization to security controls this may have be anything from 99 years to 3 months) and you now need to extend the key life. It may be operationally inconvenient to issue users with new personal keys, and much simpler to allow them to continue to use 'old' keys that are already being used to protect files and other information that they have stored on their computer systems and on backups.

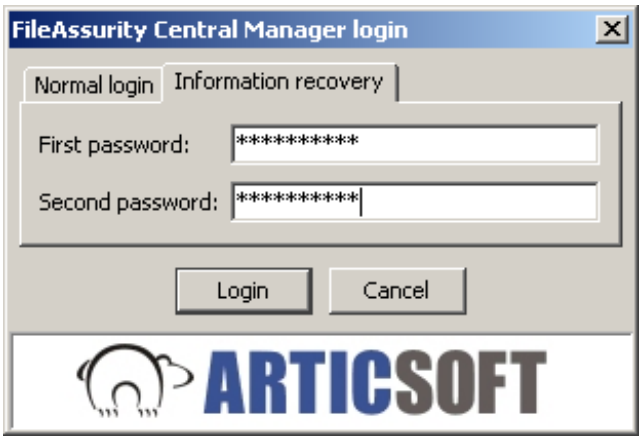
Check the 'Update validity' check box to choose a new valid to date.

Once a key/certificate has expired it can be used for signature verification and decryption, but CANNOT be used to digitally sign or encrypt information.

Information Recovery

The information recovery feature of Central Manager enables the two administrators to recover the main Administrator password (the password that accesses the Master Keystore) and to perform recovery of encrypted files and secure text. It does not directly lead into other Administrator functions although, having recovered the Administrator password, the two administrators could then log on as the Administrator.

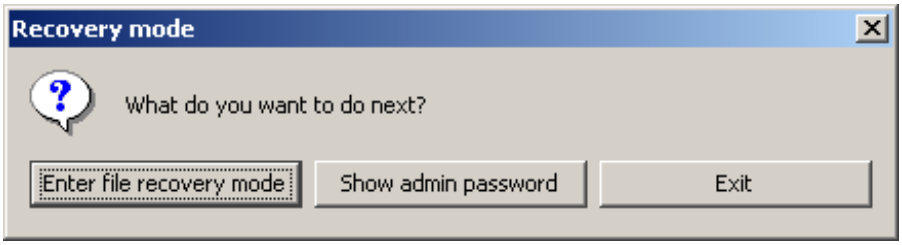
To enter the information recovery mode, the two administrators must logon to the Master Keystore. On the logon box select the 'Information recovery' tab. The following dialog is displayed:



Enter the password for the Administrator keystore and press the

button.

After you have successfully logged on a choice has to be made over the mode of operation. The modes are as follows:



Show admin password
If the recovery of the Administrator's password is selected then it is revealed and the system returns to the logon screen. The password is displayed on the screen and is not made available in any other way.

Enter file recovery mode

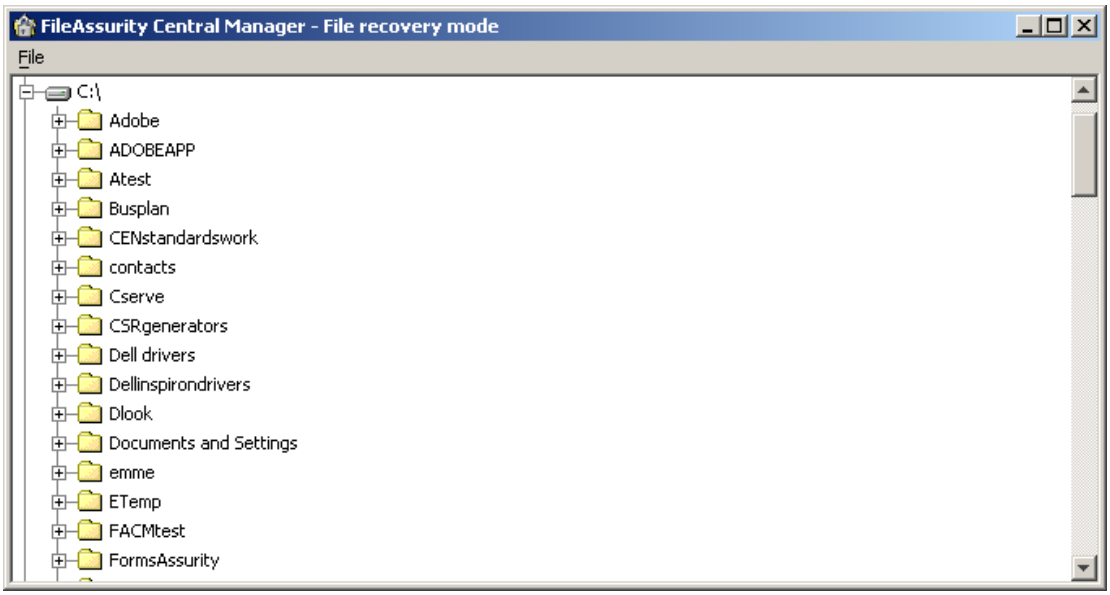
This mode is used when it is necessary for management to obtain information that has been protected by one of the users of the service. This may be necessary for a number of reasons:

- a user is not available and an important piece of information is on their system that management require before their expected return;
- a user has left the organization and it is necessary to recover information that they were in control of;

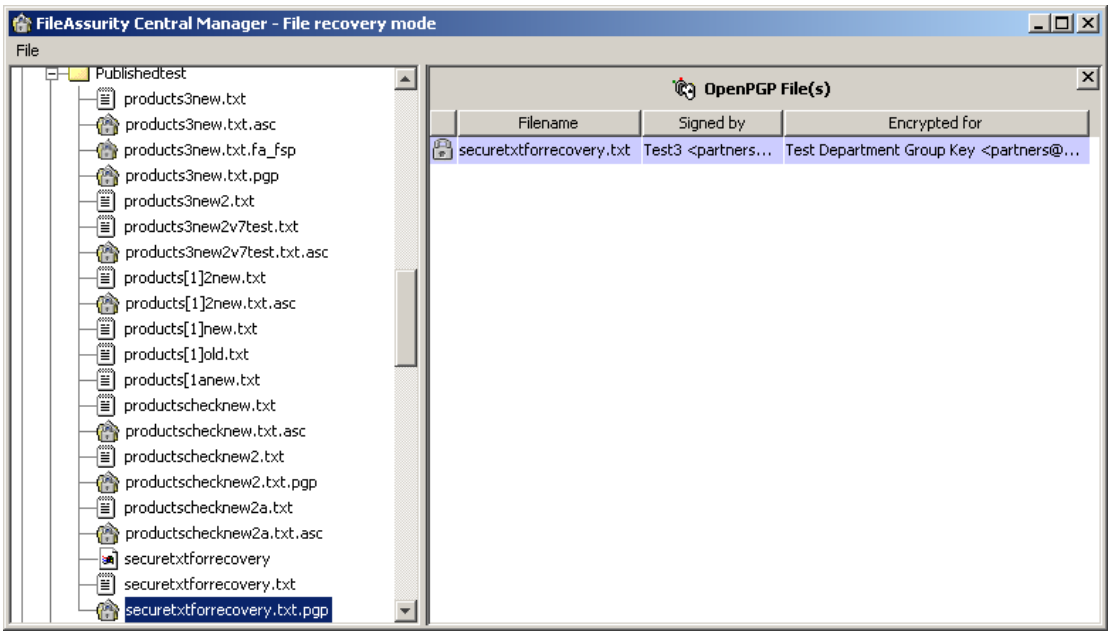
- management has genuine concerns that activities are taking place that are contrary to the organizations stated policies (perhaps including breaking national laws) and that it is essential to investigate those concerns to prove the correctness of the situation.

Entering this mode displays a directory tree where you can select the files or secure text to be recovered.

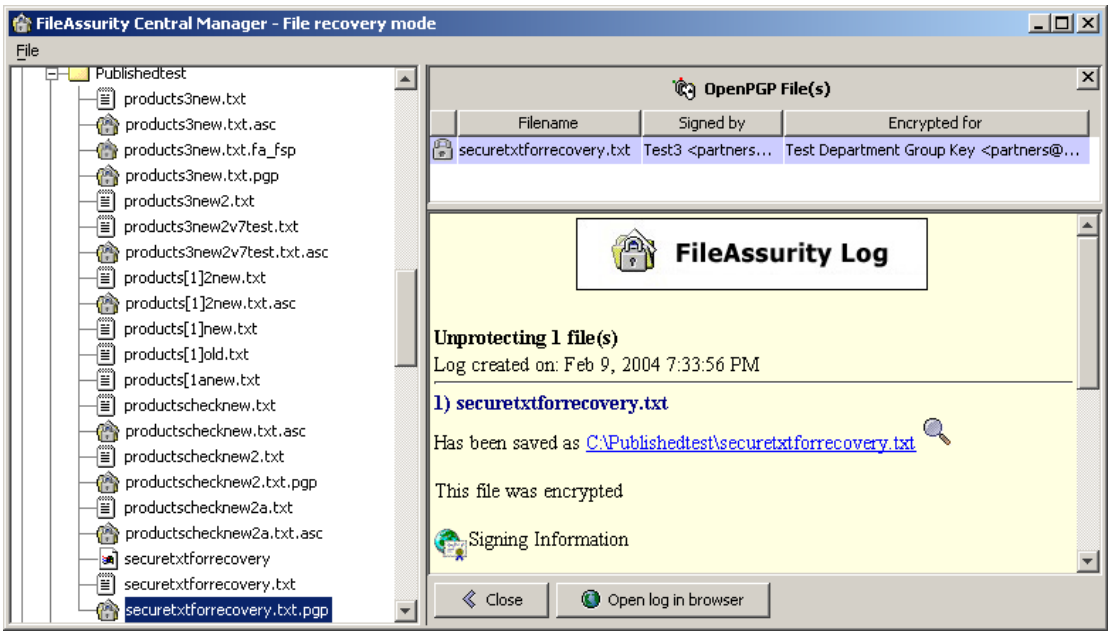
NOTE: **If you want to recover secure text this must be pasted into a file and saved with a .txt.asc extension. This will ensure that a file with a .txt extension is created when it is automatically decrypted by the Central Administration program, which you can then read using any text editor (such as Notepad or WordPad). This has to be done because the information recovery system cannot process secure text directly since it is working with files rather than the system clipboard.**



Once you have selected the protected file double-click on it to display the security details associated with the file in the right-hand pane.



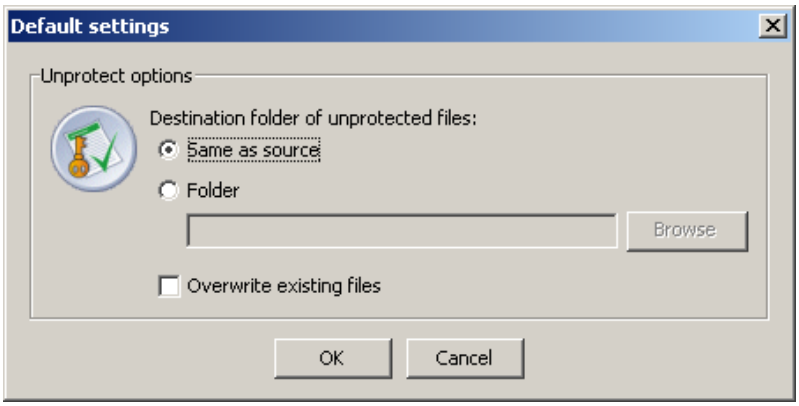
Double-click on the file in the right-hand pane to decrypt it. The following dialog is displayed:



Do check the decryption information, particularly if the file was digitally signed to check if you actually know the source of the file. You can either click on the link to open the recovered file or browse and open it using Windows Explorer.

Changing the location of recovered files

If you want to change the location where recovered files are saved to, select the 'Default Settings' options from the File menu. The following dialog is displayed prompting you for the location to save the unprotected file :



Destination Folder of Unprotected Files

- **Same as source**. Unprotected files are stored in the same location as the protected files that you are currently working with. This is called the "Source" folder. For example, if the protected file is located in c:\mydocuments then the unprotected file will also be stored in c:\mydocuments. The destination folder will change depending on where the protected files are located.

- **Folder**. You can choose a folder via the Browse button where unprotected files will always be stored. The destination folder will remain the same no matter where the protected files are located.

Overwrite Existing Files

- Box unchecked - if the original (unprotected) files already exist with the same name in the destination folder you will be prompted as to whether you want to overwrite them or not.

- Box checked - unprotected files that already exist with the same name in the destination folder will automatically be overwritten and no warning will be given.

NOTE : The file recovery mode remains in force until this tree view dialog is closed down. You cannot run Central Manager in both Administrator and File Recovery mode at the same time.

Installation of the client software

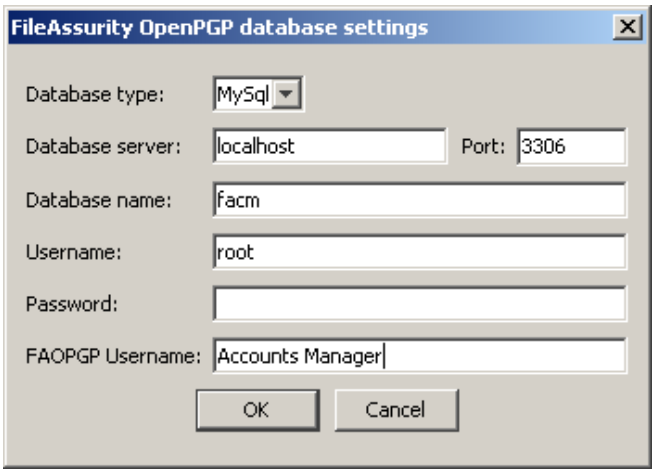
FileAssurity OpenPGP centrally managed client is identical to the standalone client (non-centrally managed version) except that it contains the necessary code to enable it to talk to the central database.

Installation procedures should be followed as detailed in the FileAssurity OpenPGP manual. The only difference during the install process is that the centrally managed client takes installation parameters from a file in order to talk to the database. If this file is not present it will prompt the user for this information.

When the user client first connects to the database (this happens during installation) it needs to prime the database (populate the database with the necessary information to enable the FileAssurity OpenPGP client software to connect to the database). A file called switches.txt is provided as an example of the parameters required and can be modified accordingly. Information contained in this file is as follows:

- Address of database server
- Port that it is on
- Name of the database
- User name that you are logging onto the database as (same for all clients)
- Password for the database (same for all clients)
- FileAssurity OpenPGP user name for that particular client (that specified by the administrator when the record was created in the database)

Switches.txt needs to be present during installation and must be copied to the folder where you are running the installation of the software from. If it is not found during installation of the client the following dialog is displayed prompting the user to enter the necessary information that the client software requires in order to connect to the database:



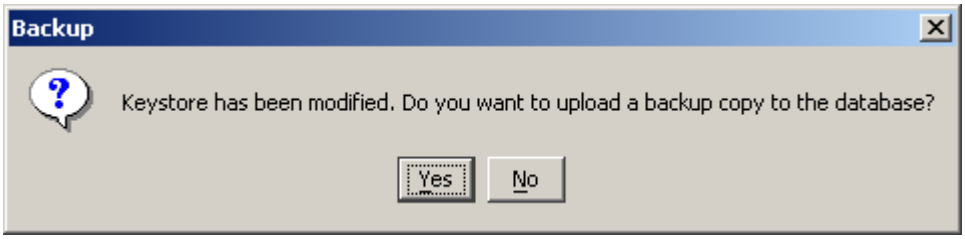
Client keystore automatic backup

Users have the ability to cause their current keystore to be uploaded to the Master Database if they wish at any time. Further, if the keystore is altered during a session, when the user comes to logoff they will be asked if they wish to update the entry in the Master Database. (It may not be possible to update the entry. This could be because it is not possible to contact the Master Database at the time the update is requested – perhaps the user is working offline or they are not able to find an access route to the Master Database.)

An updater program is constantly running that will verify if the keystore being sent for update is actually from the correct user. If it is then the update will run, otherwise it will not.

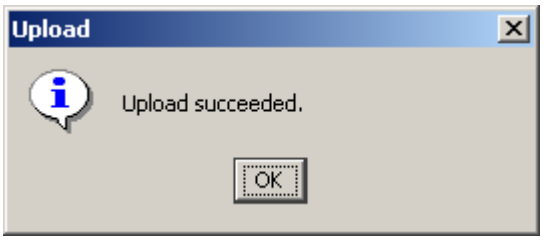
The Administrator can update Keystores that have been backed up. But it must be remembered that users cannot change their issued keystore passwords if this service is to be used.

When a user changes any information in their keystore, when they next logoff the following dialog is displayed :



This dialog allows the user to specify the location of the database. Normally this will be a default set by the system, and included with the keystore details on download.

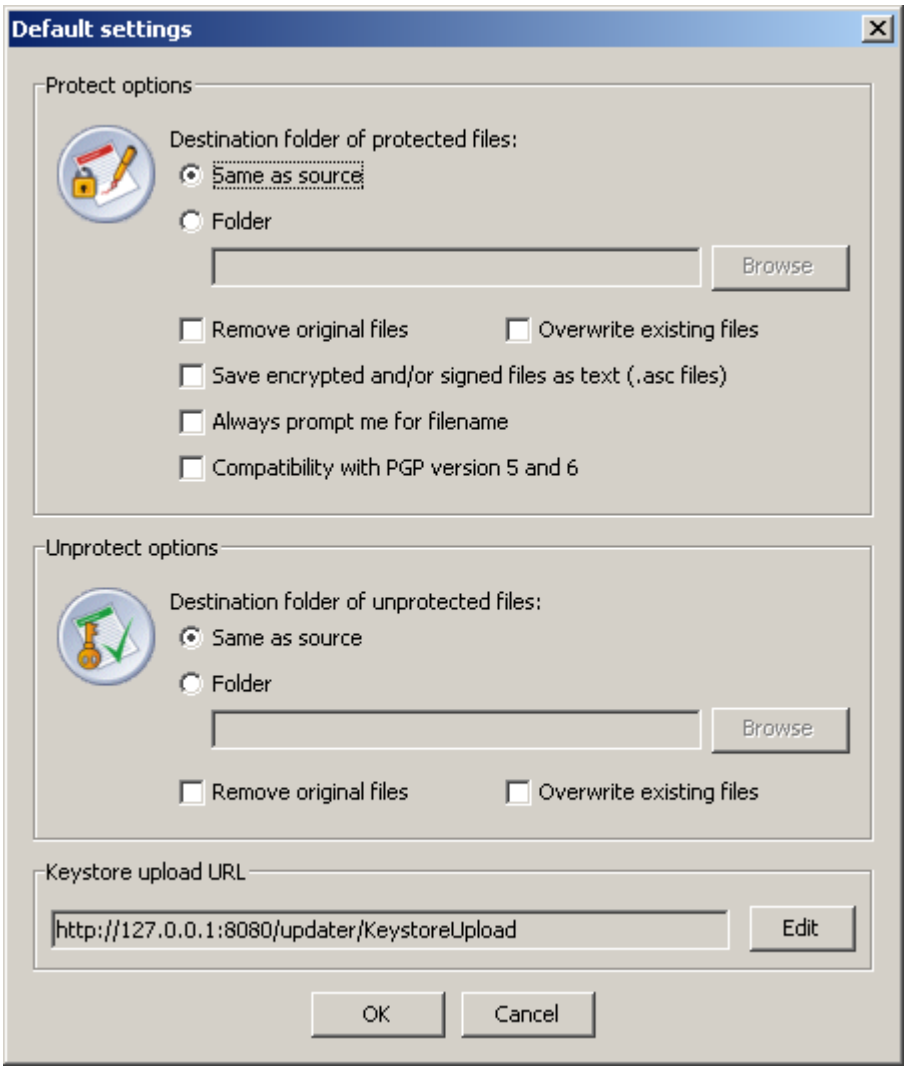
If the update is successful the following message will be displayed:



If the update attempt fails they will be offered the opportunity to try again (it wouldn't be the first time that you could not get to the desired web site at the first attempt). The user

can also request an upload at any time by selecting Key Manager > Tools > Upload keystore backup and the same dialog will run.

In the event that a user has to change the Master Database they are using (perhaps an operational change of address has taken place) they are able to change the default address for the upload by using the Default settings screen accessible by right clicking on the icon in the systems tray. The keystore upload parameter is shown at the bottom of the panel.



Clicking on the Edit button opens the line for amendments. Please note that these amendments will be saved on the client PC for future use.

Managing multiple Master Keystores

In a small organization the Administrator should be able to manage, create and issue all the keys that are necessary for the users on an ad-hoc basis. Where keys are to be shared between users it may be simply a matter of the Administrator generating key pairs that are to be shared, exporting them and then deleting them from the Master Keystore. By exporting these keys to a single folder or to several folders the Adminstrator can quickly build up a 'keys list' of available keys for different individual users and communities of users.

That way, whenever the Administrator is generating a keystore for a particular user they can look through the available keys list and import any required to the Master Keystore before generating the user keystore. As soon as the user keystore has been generated the Administrator can then delete those keys from the Master Keystore and import those needed for the next user.

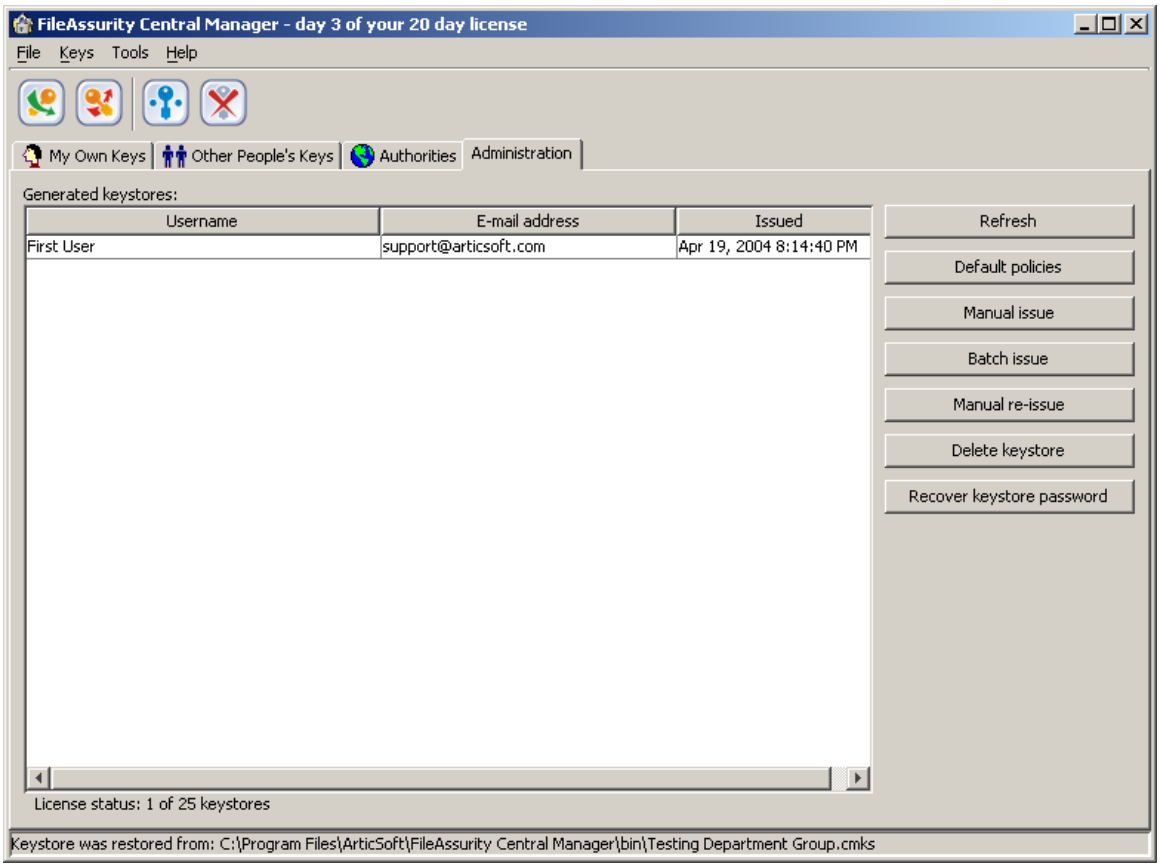
In a larger system it is impractical to keep manually adding and deleting keys from the Master Keystore for single or batches of users.

Setting up multiple Master Keystores

In this case it makes sense to have more than one Master Keystore, and to organize the Master Keystores into groups consistent with the way in which the organization issues group keys (if you have chosen to do that). You can use the backup and restore keystore facility to backup specific keystores and give them specific names reflecting their operational use. A Master Keystore contains both the keys for the keystore and the applicable policy for that keystore, so that these remain consistent. You can name keystores after departments, roles or tiers of management, or all of them, depending upon what is operationally most suitable to you.

When the Administrator wishes to set up a Master Keystore for a specific Group they can use the current Master Keystore to create the Master keystore of keys and policies that is required. Once the new Master Keystore is finalized it can be saved using the Tools > Backup keystore feature. The backup panel allows the Administrator to give the Master Keystore a specific name.

Once a Master Keystore has been backed up it can always be reloaded. Whenever you reload a Master Keystore from backup the full filename of the Master Keystore is shown at the bottom of the Administration panel, and remains displayed, even after reloads. An example screen showing this is as follows:



If it is necessary to add keys to a Master Keystore for a Group, or to change policy for the Group, then it is only necessary to change the Master Keystore for that Group.

You are responsible for ensuring that backups of the Master Keystores are properly maintained. If a Master Keystore is destroyed (disk failure or overwriting) it will be impossible to recreate.

Please be aware that because Master Keystores are keyed to the Administrator password it is vital that you choose a 'good' password to protect them. Whilst we recommend a minimum of 8 characters, you should make the password as long as is operationally convenient and should make full use of upper and lower case and special characters. (The same advice is appropriate for the selection of the two other Administrator passwords.)

Trust models

Concepts of trust in digital signatures

You will read in literature from various sources about the subject of trust models. Many of these discussions are technical and complex. Unfortunately that means that trust models may be artificially difficult to understand or implement. This section of the manual has been produced to try and simplify for the Administrator the nub of the issues that are in debate, and to propose a simple way of dealing with what can, if not controlled, become an unduly difficult and expensive problem to try and solve.

Underlying the question of a 'trust model' is the question, "Why should you 'trust' a digital signature that you receive, and what should you 'trust' it for?"

If you, as an Administrator, have issued keys to individuals, you can be confident that only those individuals use those keys, and are able to revoke (stop) users from using those keys, then you may be able to feel confident that you are in control of the overall situation and can be confident about the validity of those keys (and users). Therefore you, and all your users, can feel confident that the user identity (and e-mail address) can be reliably associated with any document digitally signed by that user.

If you are going to rely upon keys that you did not issue and do not control you obviously have a more difficult problem. You can either rely upon what someone else 'tells you,' either because you know them personally, or because that is a published 'policy' that you have implemented. (After all, you may know that they are using the same ArticSoft control system as you, and can be confident that there are no revocation problems with keys issued by them, so there is no reason not to trust the digital signatures issued by those organizations.) But you are still just relying upon the link between the claimed user identity and an e-mail address.

This is a very important concept. You (and all the users that you administer) are relying on the 'trust' that the user identity and the e-mail address (which cannot be separated) are valid. You will make other decisions as to what you, as a business, will do as a result of receiving information from someone that you are confident you can identify. There are many other business mechanisms that will impact upon the decision making process. These may include credit control, who decide if the person or business is or is not a customer, or a customer in good standing that you should respond to, or blacklisted and should receive no service. These are measures of 'trust' that are generally beyond the ability of PKI type services to deliver. For a more erudite discussion as to the capabilities of PKI based systems we recommend that you consult the web pages of Peter Guttman,

the New Zealand cryptologist, who has researched the subject in significant detail. An Internet search on his name will usually provide a link to his home page.

Although some of the trust models that are published may seem to be attractive, in a purely technical context, there are many difficulties that the Administrator needs to consider. The most important of these is the business context that has to be reflected in the technical architecture that the Administrator is implementing. Others include issues of verification and revocation. Both are considered to be technically difficult.

Generally, in an enterprise, the sales and purchase ledger systems are what really determines 'trust' (or perhaps much more accurately, lack of trust) relationships with customers and suppliers, and not a cryptographic architecture. Business processes are dynamic rather than static. They reflect current relationships rather than those embedded in public certificates, which cannot normally be changed during their lifetime, or on the linking of one Trusted Authority (or Certification Authority) to another. Your business will be constantly changing its view of the 'trust' it places in an individual or an organization, depending upon a 'mixed basket' of measures. Some of those will be purely financial, others will be based upon the personal views of sales management, credit control, directors and officers, and so on. Essentially, none of them can be turned into a simple model where one size fits all.

The internal decision making process by which some actions are approved and some are refused is not yet subject to a single model that can fit all occasions and all requirements. Indeed, the practical problem faced by most so called trust management systems is that they are incredibly limited in what they actually deliver, and the very specific occasions on which their model is appropriate.

When it comes to the concept of trust management, perhaps the only critical points that can be delivered with the currently available technologies are some improved confidence that you know where a piece of information has come from, and that the information is likely to be reliable, at least for the purpose of passing it forwards to another part of your business process. Trying to provide all the possible attributes that your internal business processes might require, before they can function properly, may be theoretically possible with today's PKI based technologies, but to date it has proved too complex, difficult and expensive to achieve. The problems are magnified significantly if one attempts to go beyond the (ever changing) boundaries of the enterprise, where organizations that operate significantly different internal 'trust' models have to interoperate. If every organization on the planet worked with exactly the same 'trust' model, and could express that in terms of information contained in a static certificate, then increasing the 'trust' reliance beyond that of a identity might prove feasible. It is beyond the scope of this guide to suggest to the Administrator what may or may not be feasible within their own organization, but these notes may serve as pointers as to the issues that are involved if one wishes to try and expand the 'trust' verification that is carried out by FileAssurity products.

The Central Administration Trust model

Central Manager has been designed to work with both the OpenPGP trust structure and the X.509 trust structure.

When key pairs are generated by Central Manager or by Managed Clients (when that has been authorized) they are always created with both an OpenPGP and an X.509 certificate.

When keys or key pairs are imported:

- if they are from an OpenPGP source a check is made to see if signed certificates are present with the imported key, and if there are, a check is made to see if any of the signer's certificates are already in the user's keystore. Any that are present are highlighted on screen at the time of import so that the user is made aware of any 'trust' relationships that already exist.
- If they are from an X.509 source, a check is made for a chain of certificates leading back to the issuing root authority. (If the certificate is self-signed there is no chain to check.) If certificates are missing from the chain the key(s) cannot be imported by the user. The root Authority for a certificate that is not self-signed must therefore be present in the user keystore.

Central Manager is provided with a list of generally accepted Trust Authorities as published by Microsoft and Netscape, together with other appropriate and nationally recognized bodies. The Administrator is able to delete any root Authorities that are not to be made available to users, and is also able to add in root Authorities to user keystores.

The Administrator's public key (generated or imported at initial setup) is always included in all user keystores and cannot be deleted. It provides the root Authority for the Central Administration service.

Thus the Trust Model used in Central Administration allows for both the 'web of trust' model where individual users can choose to accept and trust specific certificates, a hierarchical trust model where certificates can be trusted because they link back to a root Authority, and a managed trust model where certificates link back to an authority that the Administrator has imposed on the keystore.

Because there are few compatibilities between the OpenPGP certificates and the X.509 certificates, no processing is carried out on policy fields where these are contained in the certificates.

The users of FileAssurity OpenPGP can accept and work with keys and certificates from both sources because they are making the final decision about the correctness of the information that they receive. FileAssurity checks that digital signatures are correct, that there is a certificate chain in their keystore, and that the dates are currently valid. Once

the automatic checks have been made, the user must still make the normal commercial decisions that they would make in any other event before proceeding. This is because FileAssurity OpenPGP is only handling the technical components of the security infrastructure and can have no understanding of the meaning of the information it is being used to protect.

Since the user is checking the information that they receive there should be adequate supervision to determine if the information corresponds to its apparent source, is complete and is plausible.

FAQs

What would a typical user keystore contain ?

1. if the administrator generated every key

   The keystore will contain all the key pairs that were in the administrator's keystore when the user keystore was generated. It will also contain the policies that the administrator preset for the user about the use of keys, encryption and other services. If it is allowed, the keystore may also have keys that the user has imported so that they can send encrypted information to others.

2. if the user is allowed to generate their own keypair(s)

   The keystore will contain all the keys and policies as in case 1 above, and also any key pairs that the user has either generated or imported for their own use.

Does the client computer have buttons grayed out if that facility is not allowed?
No. The user gets a message telling them that functionality has been disabled.

What happens if the user cannot connect to the database?
Keystore policy determines how often the user must connect to the keystore database. If you can't connect to the database when required you will be unable to use the system – if you can't logon to the keystore you can't encrypt or decrypt files, etc.

How do you re-issue a new password on a user keystore?
You can't change the user keystore password. If a password has to be changed you will have to set the user up with a new keystore.

How can I define a user's password
You can't manually, the system automatically generates one. You can specify a password when working in batch mode, but if you choose to do that then you take full responsibility for the quality of the passwords that your users are working with.

How can I found out how many keystore licenses I have available?
If you go to the Administration tab in Central Manager you can see at the bottom left of the dialog how many licenses have been issued and how many are available in total.

How do I remove a user from the system?
If you want to remove them permanently you must ask the Database Administrator to remove their record from the database. Do remember that if the database is recovered from backup it is possible that deleted users may become available again! You must always be careful when databases have been recovered to check if user keystores have

been accidentally lost. This is critical in encryption services. If a user keystore has been lost it may be necessary to use the information recovery capability to recover information that the user has encrypted and now cannot access.

If you want to temporarily remove a user from the system you may ask the database administrator to temporarily change their user name so that they are unable to retrieve their keystore record.

What is the Master Keystore file called and where is it located?
The currently active Master Keystore is a file called facm.cmks and can be found in C:/program files/ArticSoft/FileAssurity Central Manager/bin/facm.cmks. If you have created Master Keystores in support of group keys then you will see in that folder a number of other keystores with an extension of .cmks.

How do I add a key to a user keystore?
You need to make sure that the user is not using their keystore. Then you add the key that is needed to your keystore and be sure to delete any keys in the Master Keystore that the user should not have access to. Then update the policy in their keystore by making the key hidden and then not hidden. Update policy and the key should be added to the user keystore.

I am just about to update policy on a keystore. How do I know what the default Master Keystore policy should look like before making the change?
Before you update policy you should make sure that you understand that you have the proper authority (this should be given to you by your Human Resources a.k.a. Personnel function or by an appropriate line manager or authorized officer of the company) to make a change to the policy for a user. The source of authority will tell you if they are now members of a new group, or should simply have a new key made available to them. In the case of a new group, then you should first ensure that you have restored the Master Keystore for that group. In the case of adding a new key then you should verify which group they are currently a member of and restore the appropriate Master Keystore for that group. Once you have done that you can make whatever are the approved changes in policy or available keys. Do remember that you cannot remove keys from the user's keystore. If a user is moving from one department to another and should not have access to any old information then you must delete their old keystore and issue a new one using the Master Keystore for the new department, together with its default policy options, unless the authority requires you to vary the standard policy.

I want to change the IP address of my database. How do I do it?
You can change the database and user/password setting using Tools> Database settings to do that. Do remember that this will only affect user keystores that you generate from this point on. It will not update all the current keystore users. So if you change these settings you will need to contact all current keystore users (or reprocess their keystores) to introduce the new setting.

Reading list

These texts are not referred to directly in the guide, however, they may be useful pointers where the reader would like to gain a more detailed understanding of some of the topics that are dealt with in the guide.

A PKI (Public Key Infrastructure) can be highly complex, complicated and expensive to implement, and the reader should consider recommendations in the reference works on PKI with some caution unless they identify an implementation that specifically matches the business requirement that is being solved or supported. The PKI referred to in this guide is limited to providing a secure method for digitally signing, encrypting and sending or receiving information from individuals or groups for whom you or your users have reasonable knowledge. It is not intended to be the method for automatically processing information that inherently makes or brings legal and enforceable commitments.

We do not specifically recommend any books to the reader, and different readers may find different levels of book more appropriate to their personal requirements. We have tried to indicate where a book is more likely to be technically detailed by prefacing it with an asterisk (*).

Sams Teach Yourself MySQL in 24 Hours (Sams Teach Yourself)
Julie Meloni

Apache, Mysql, and Php Weekend Crash Course
SCHAFER
John Wiley & Sons Inc
Paperback - 24 October, 2003

Sams Teach Yourself Microsoft Sql Server 2000 in 21 Days (Sams Teach Yourself)
Richard Waymire, Rick Sawtell
Sams
Paperback - 19 November, 2002

Sql for Dummies
Allen G. Taylor
John Wiley & Sons Inc
Paperback - 5 August, 2003

* **Learning SQL: A Step-by-step Guide Using Access**
Richard Earp
Addison Wesley
Paperback - 1 February, 2003

* **Managing & Using MySQL**
Randy Jay Yarger, et al

O'Reilly UK
Paperback - 10 May, 2002

* **SQL Server 2000 System Administration (MCSE Training Kit)**
Carl Rabeler
Microsoft Press International
Paperback - 23 May, 2003

* **PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues**
Kapil Raina
John Wiley & Sons, Inc.

* **Understanding PKI: Concepts, Standards, and Deployment Considerations**
Carlisle Adams, Steve LLoyd -- (Paperback - 15 November, 2002)

* **Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure (Networking Council S.)**
Russ Housley, Tim Polk
John Wiley & Sons Inc

* General information on PKI may be found at www.pkiforum.com, http://www.pkilaw.com/, http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf, http://www.dcoce.ox.ac.uk/background/, . Other information is available from the ArticSoft web site at www.articsoft.com.