Reviewer's guide to FileAssurity OpenPGP Central Administrator

Introduction

This guide has been developed to help you set up the Central Administrator system for issuing and controlling FileAssurity keystores. Following the guide you should be able to generate a Central Administration service, set user policies and issue user keystores in under 30 minutes (including setting up and configuring the database).

Central Administrator has been developed to allow the enterprise administrator to control the use of encryption and digital signature services by the users in their organization, and to be able to recover encrypted information (under proper authority) when that is necessary.

Prerequisites

Before you can run a test on the system you must have accessible to you either an MSSQL database server or a MySQL database server. You must be able to have temporary use of a user name and password that will allow you to create a database on that server, and you must know the IP address of the server.

For test (non-commercial) purposes you may find it easiest to set up a MySQL database on the computer you are carrying out the test on. If you do not already have an evaluation copy of the MySQL database it can be downloaded from http://dev.mysql.com/downloads/mysql/4.1.html (correct at the time of preparing this guide, but subject to change). You may also need to install the Connector/ODBC package if you have not already loaded a copy. This can be downloaded from http://dev.mysql.com/doc/connector/odbc/en/faq_toc.html#Downloads. The installs are self-explanatory. You may find it easier to install the Connector before the database. Additional information on running the database and the connector are given in the MySQL documents and on their website.

The Central Administrator program will need to be able to access the server to create its database where user keystores created by the administrator or backed up by the user will be kept.

If you are using a test version of the MySQL database, the master default identity is 'root' and it has no password. The URI for the database can be found by right clicking on the traffic light icon in the system tray, selecting 'show me.' You will find it listed under local IP address on the Environment panel. You must close the panel using the "Hide me" button so that the server continues running.

Once the database and connection software (if needed) have been installed you are ready to install Central Manager.

You have two installation programs to run:

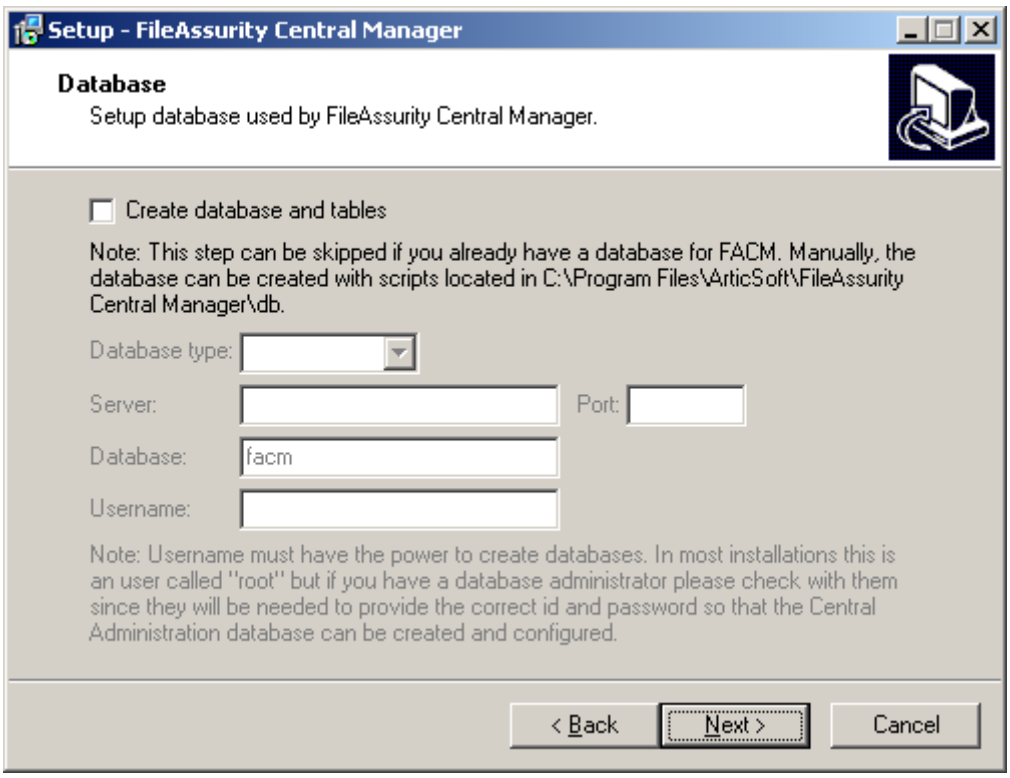
E:/Programs/FACM20.exe
E:/Programs/FileAssurity_OpenPGP_Full_Managed.exe

The first of these installs the Central Administration program, configures the database and installs the keystore uploader service.

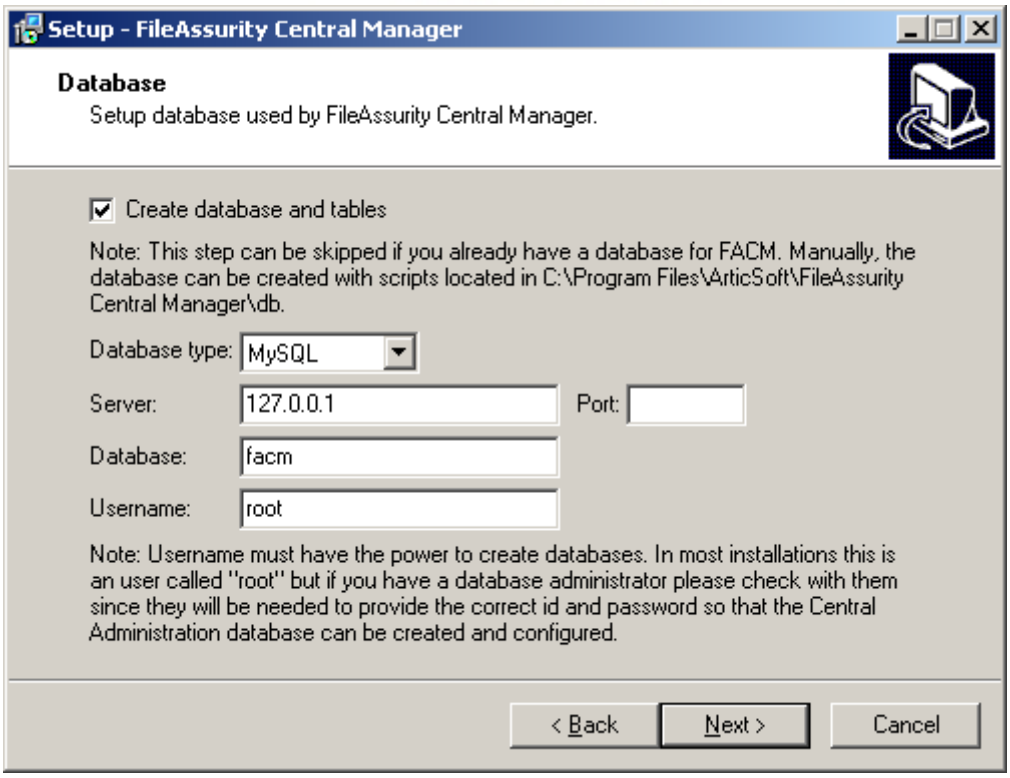
The second installs the client program that ordinary uses will have installed on their computers. For normal users, clients may be installed on any desktop or laptop computer provided it is able to gain access to the database to download its keystore.

Central Manager Installation

If you now install FACM20.exe and either click to accept or to go to the Next panel, accepting the default settings at each step, you will come to this configuration panel:

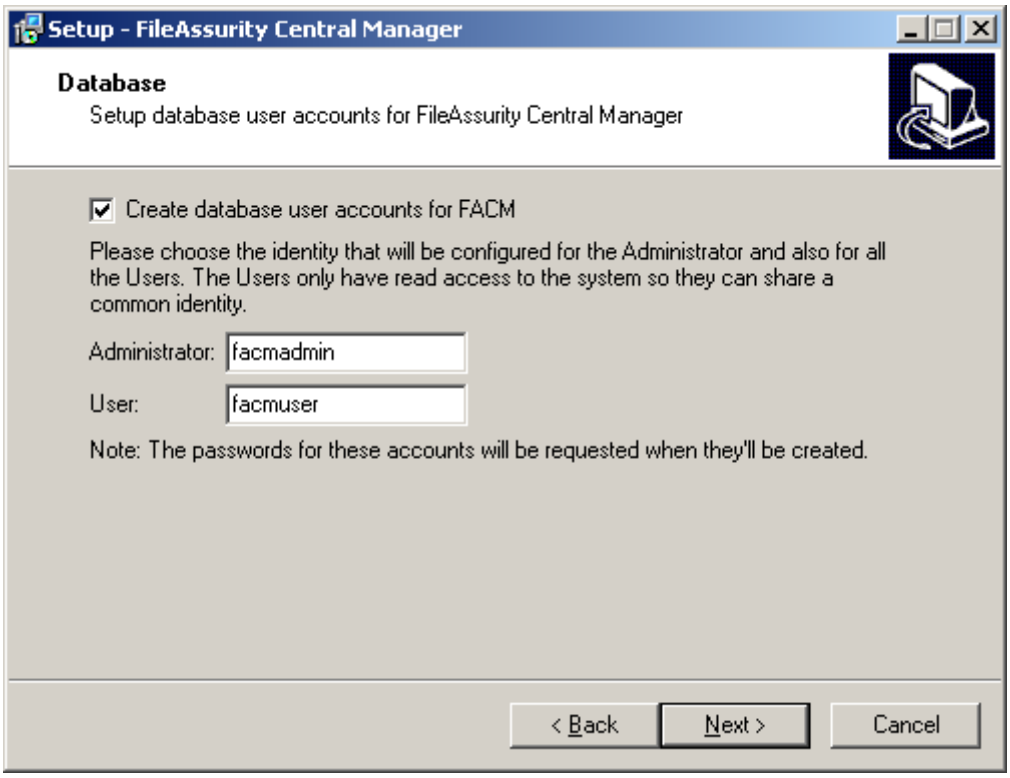


You should fill it in as follows (assuming that you are using the MySQL test database for evaluation purposes):

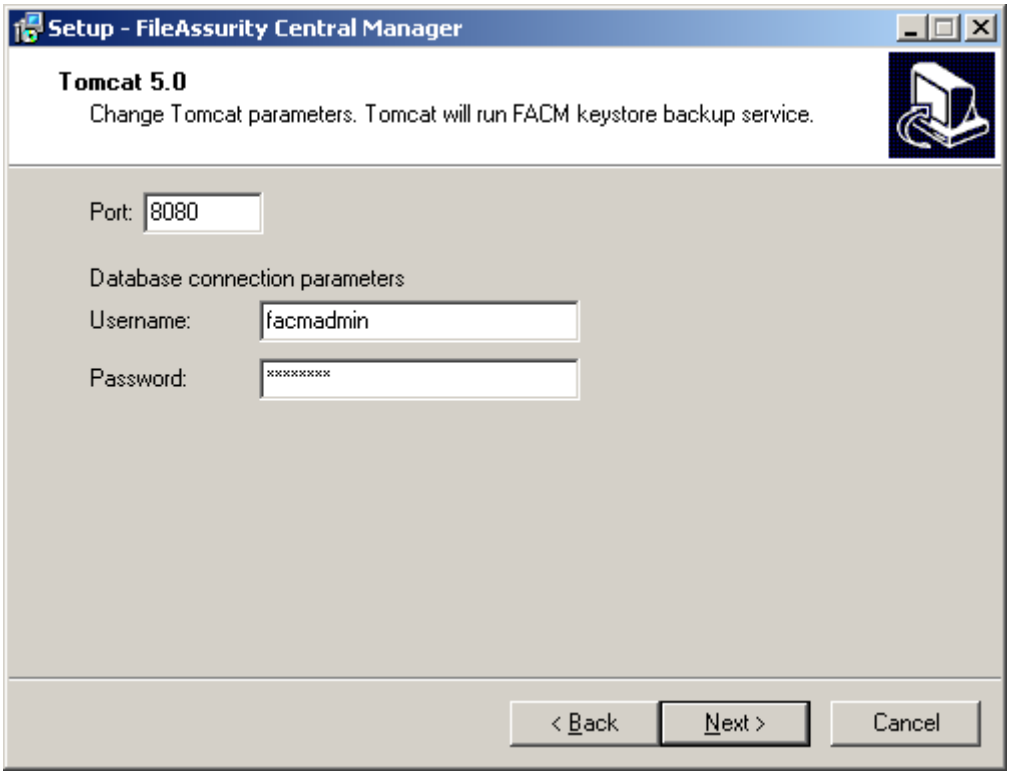


Please note that you replace the server IP address with the one found in the MySQL control panel.

The next panel that you meet is used to configure the usernames for the users of the database facm. Again, please fill in the panel as shown:

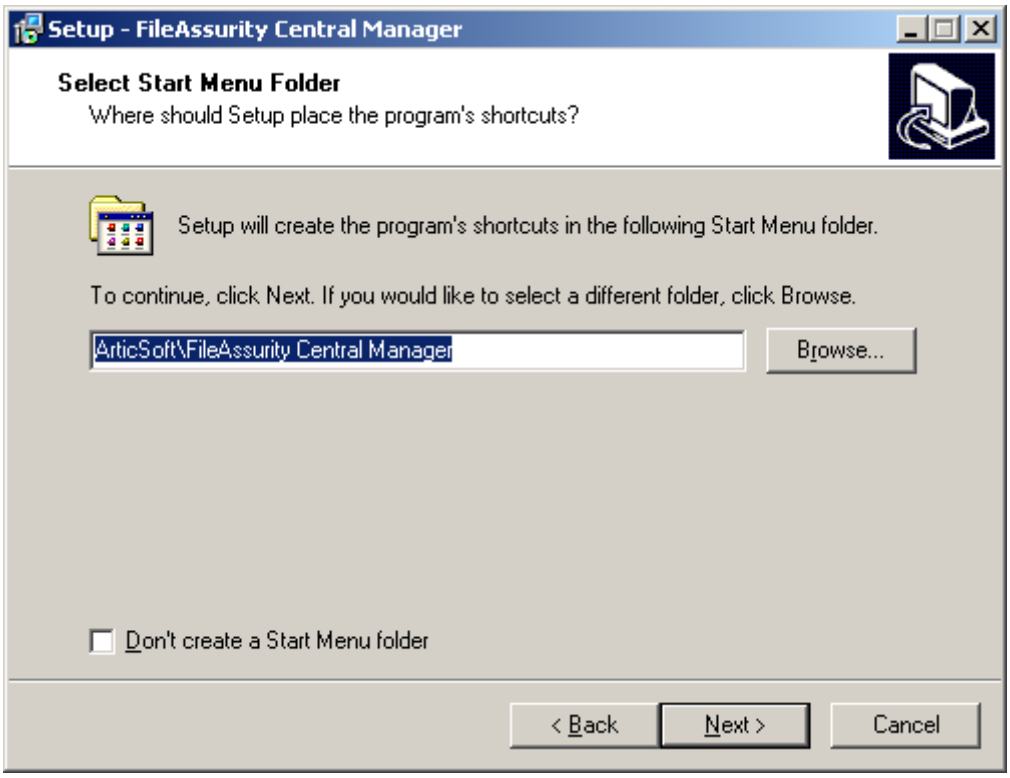


The next panel deals with the setup details for Tomcat. Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. It is used in our implementation to listen for upload requests for user keystores, to verify the source and correctness of the keystore that is proposed for update, and where approved, update the user keystore in the database.

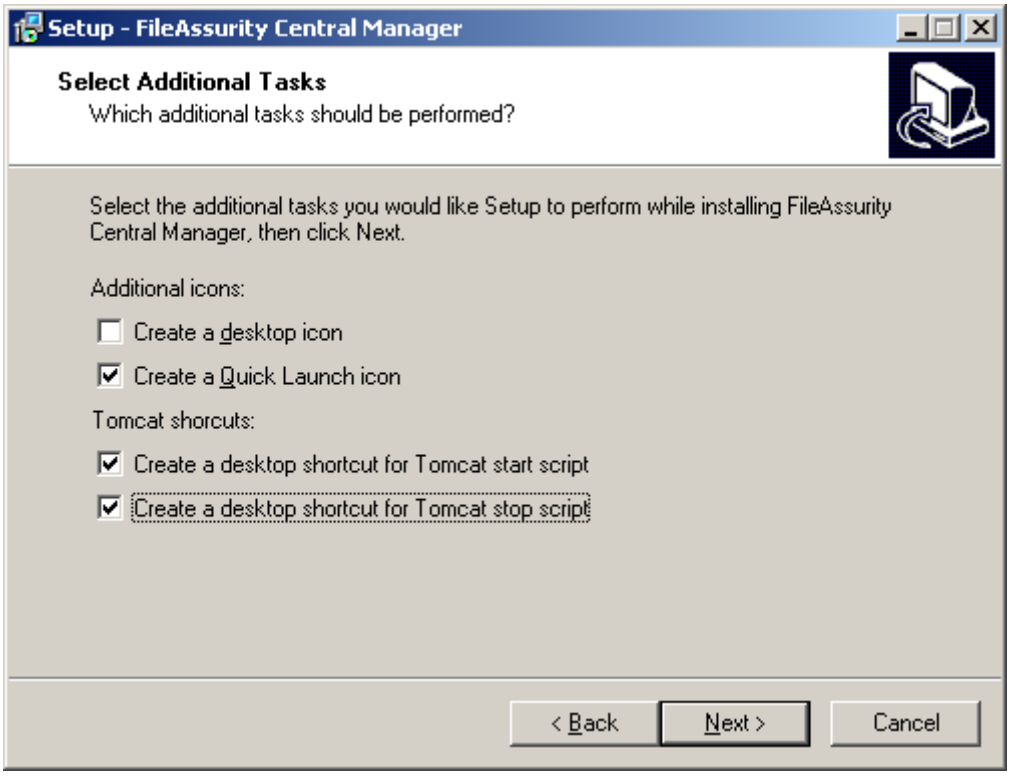


Again, fill in the username. Since this is just a testing system, enter a password that is easy to remember, such as 11111111. IMPORTANT NOTE: please remember that in a production environment you must choose a good, long and complicated username and password for this because it cannot be easily changed once it has been implemented.

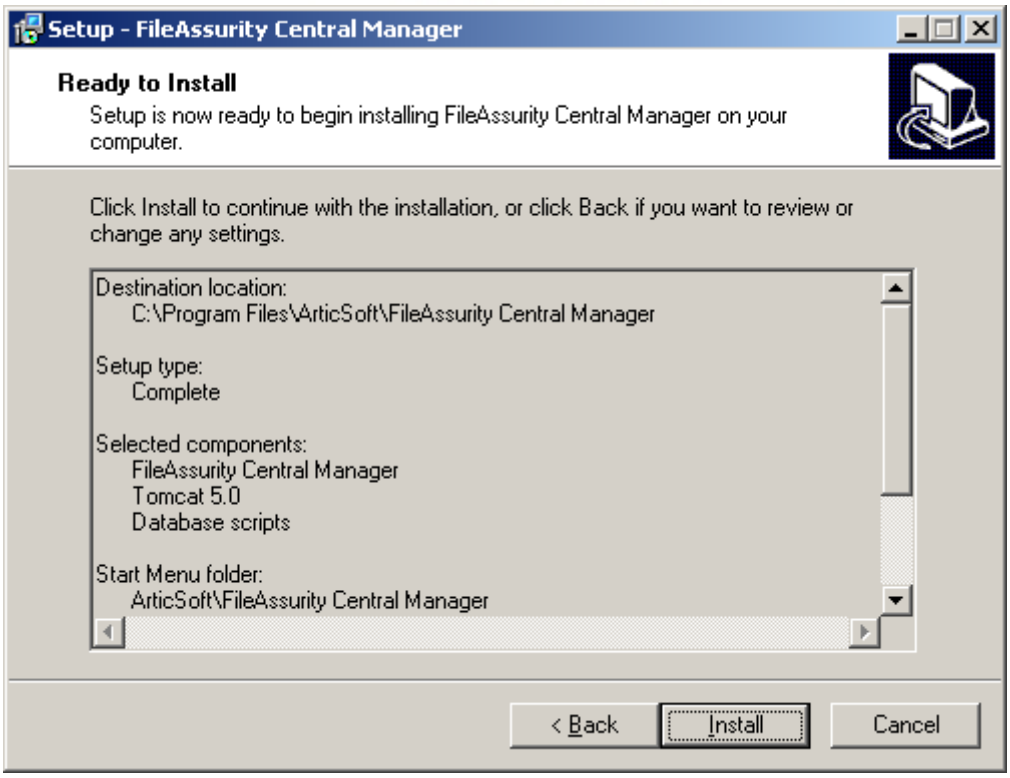
The next panel should be approved without change.



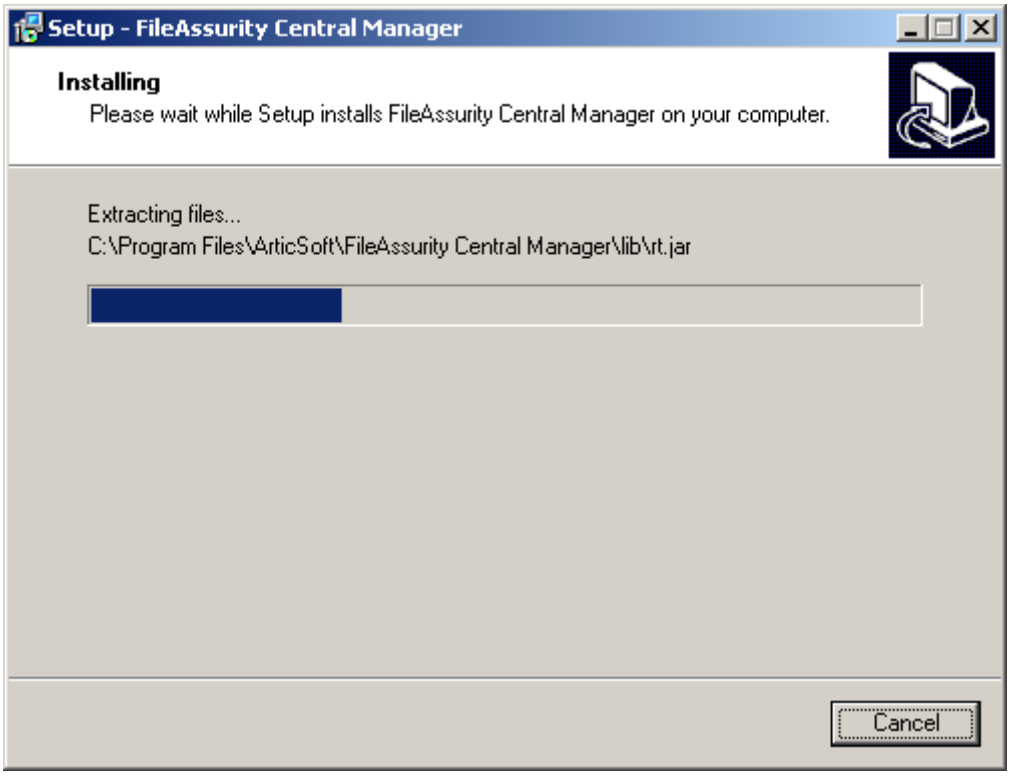
Although it is a matter of taste, you may find the next set of selections convenient when testing. In a production environment you would probably choose to have Tomcat start at system startup rather than be run manually.



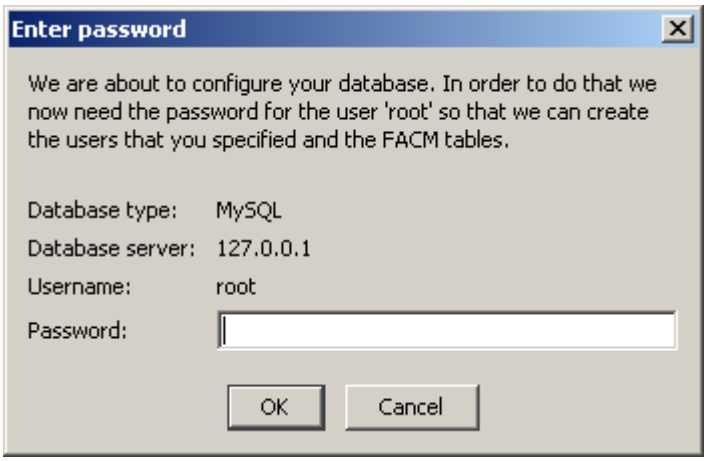
The next panel is a summary of the overall requests that have been made:



ON pressing Install the applications programs and libraries are installed:

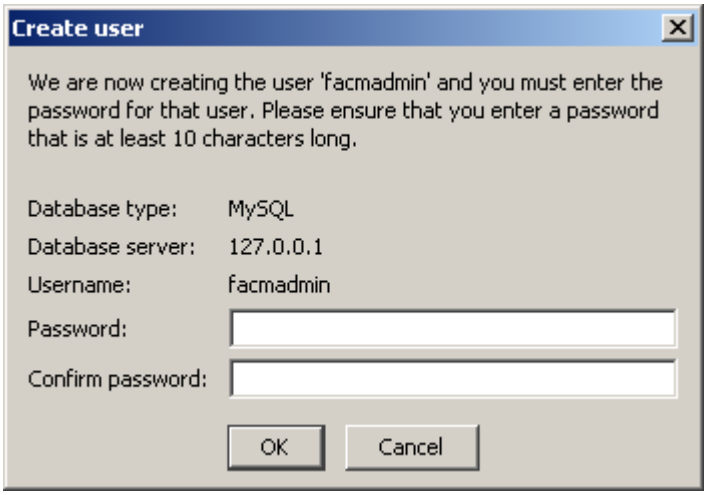


This finishes very quickly and you then enter the database configuration step:



If you are using an evaluation copy of MySQL for this test then you can click on OK which will give a 'null' password. Otherwise you must enter here the correct password for the user shown.

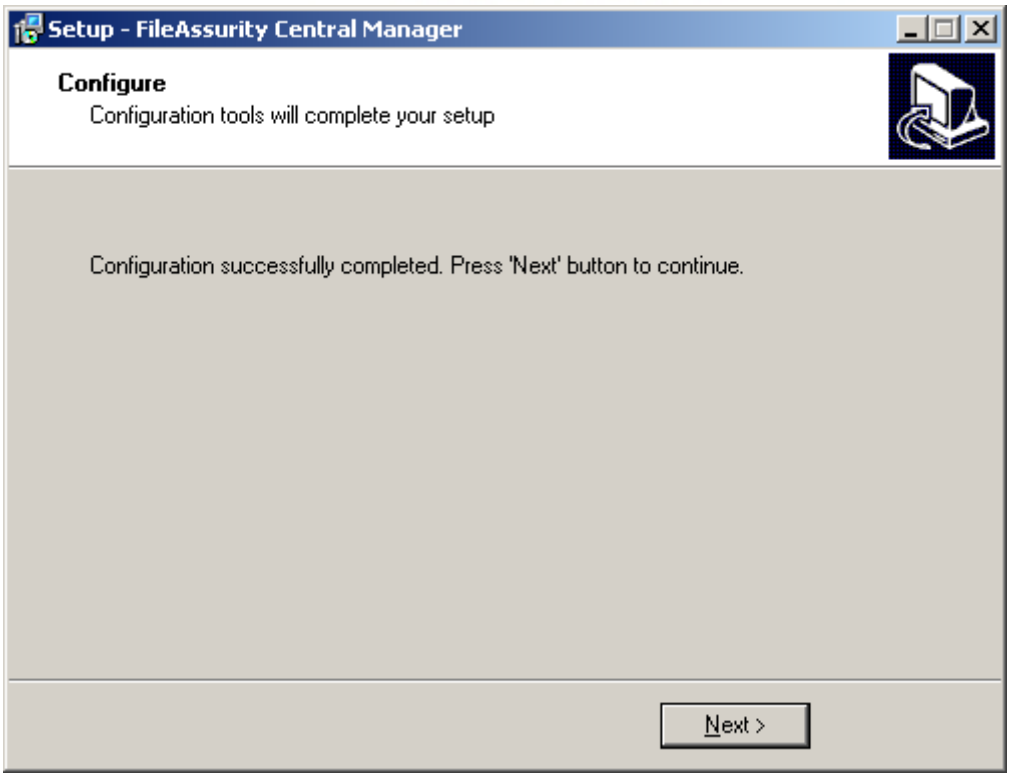
Please note that if you are running a software firewall you need to give permission to the configuration program javaw.exe to access the Internet so that it is able to establish a link with the database using the IP address that you gave earlier. The next panel you see will look like this:



Remember to use the same password here as you used when configuring Tomcat.

At the next panel you are configuring the access for users. This username and password only grant read access to the database, and have to be generally known to all the mobile (roaming) client users of the system. They are not really 'secrets' but are there to slow down would-be hackers. The information stored in the database is either publicly known (such as usernames or e-mail addresses) or is heavily encrypted and as such will not be of any value to an attacker.

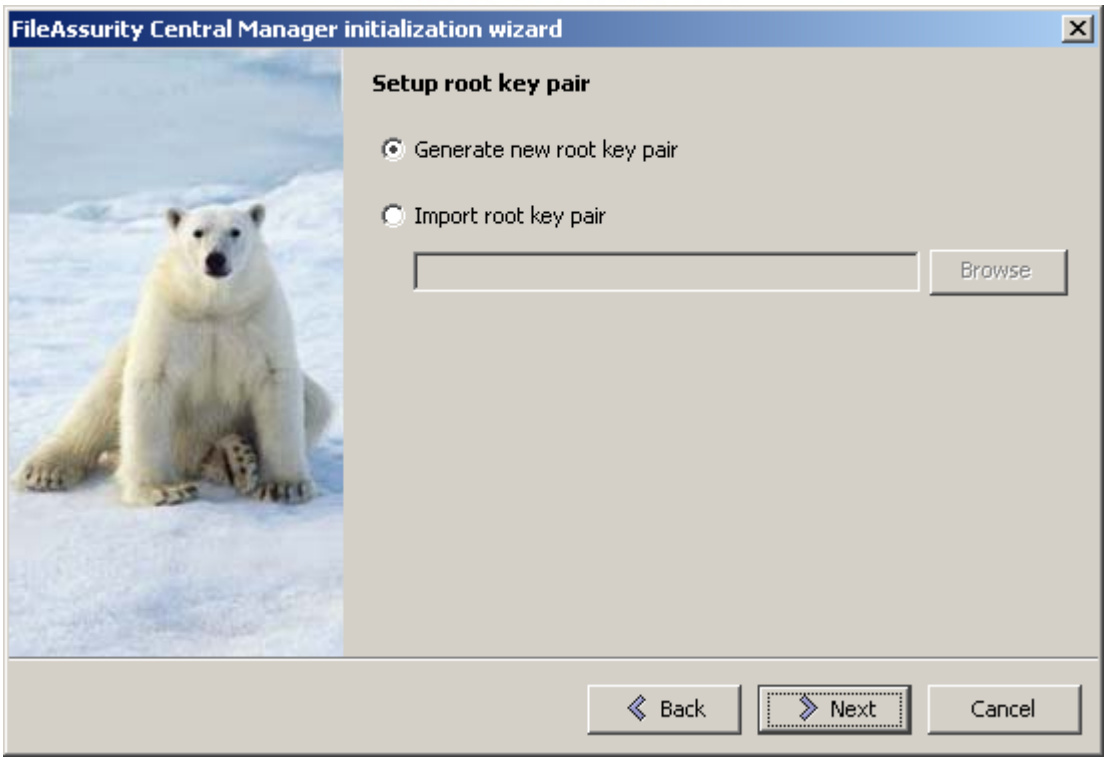
You now see the following panel:



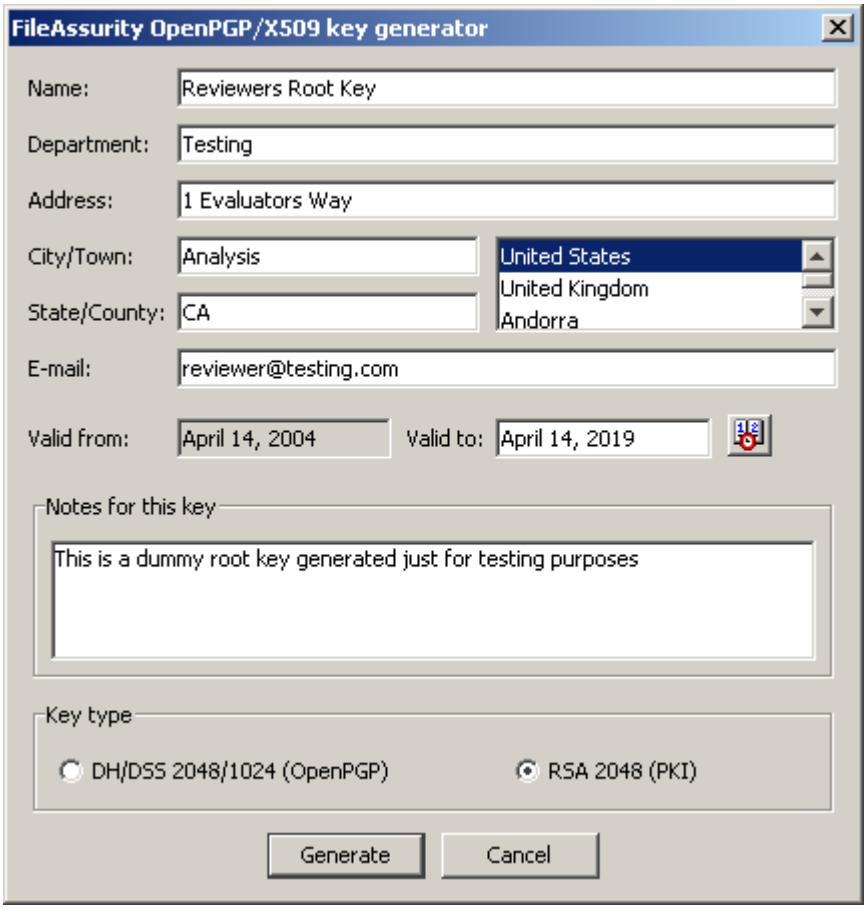
and you are ready to start creating your Certification Authority.

When the Central Manager program starts running you will see a screen showing a limited license for evaluation purposes. If you need to have this period extended you should contact ArticSoft Sales at sales@articsoft.com.

Once the program is running you will start to configure the Certification Authority. The first step is to generate or import the root key pair – that is the key that will be used to digitally sign all the keys issued by the Authority, and link them back to the Authority. For the purpose of the review we will generate a key pair in the following panel:



Clicking on next will bring up the following panel which asks you for information to fill in an X.509 style certificate. A completed panel could look like this:

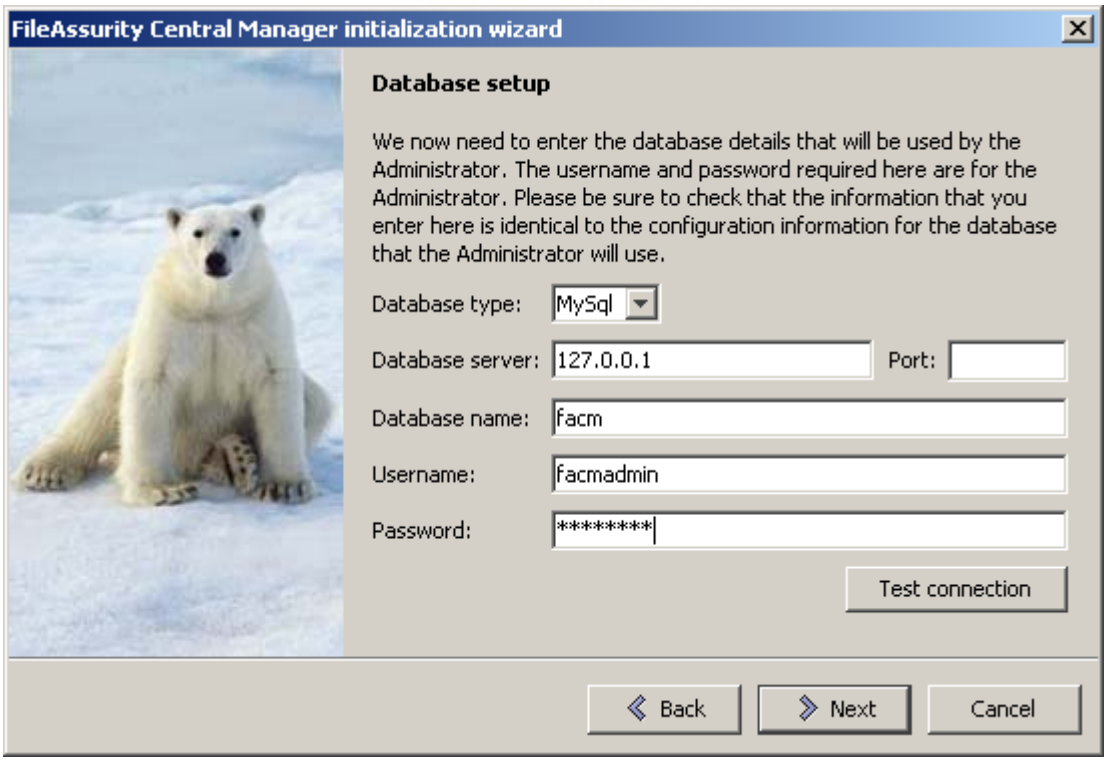


This will generate an RSA based key pair, the certificate of which will be present in all the keystores that are issued (and cannot be deleted by the user).

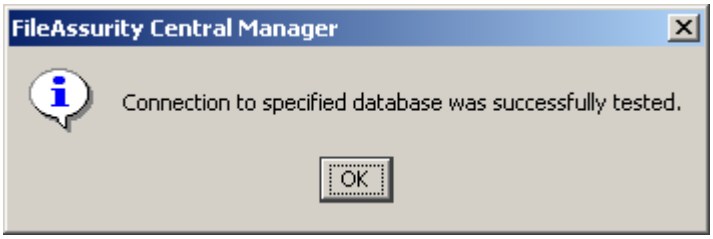
At the same time as the root key pair is being generated, an Information Recovery key pair is also generated. This key pair is kept hidden inside the CA keystore. It cannot be exported by the Administrators. The public certificate of that key pair is stored in every keystore, again hidden, so that it will be seamlessly added to the key list for everything that the user encrypts if the Policy Information recovery has been left enabled!

Once the key pairs have been generated you will be asked to create the Administrator's password. This has to be a minimum of 8 characters long. Since this is a test system you may want to make life easy and use 11111111, but in practice you would choose something very much more difficult to hack.

The Central Manager application now checks the setup parameters that will be used by the Administrator to connect to the database. This is done because in an operational environment you may choose to copy the Administrator's database into another location for operational and security reasons, so the parameters used earlier would be operational, but the ones entered here are for the Administrator to use when running the Manager program. Since this is a test environment the information is going to be identical to that entered earlier.

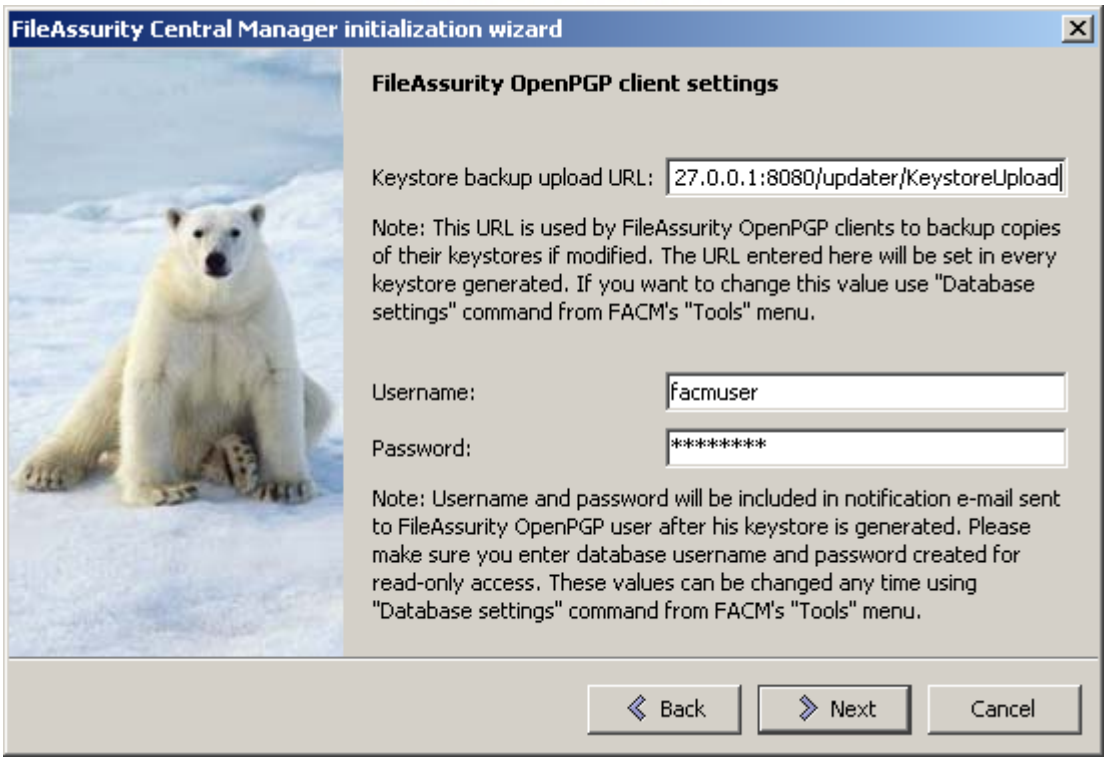


At this point you should check that the Manager program is able to connect to the database through the server. If you click on the Test connection button the program will try to contact the database. Unless you have made a spelling mistake when typing in the parameters you should get the following message:



Pressing on next brings you to the following panel:

In this panel you are specifying the location that all the clients will try to connect to in order to upload (backup) their keystores if there are any changes.



The backup URL is difficult to read in this example. It is actually:

http://127.0.0.1:8080/updater/KeystoreUpload

This is built up as follows:

First is the IP address of the database server that users will have to connect to to access their keystores.

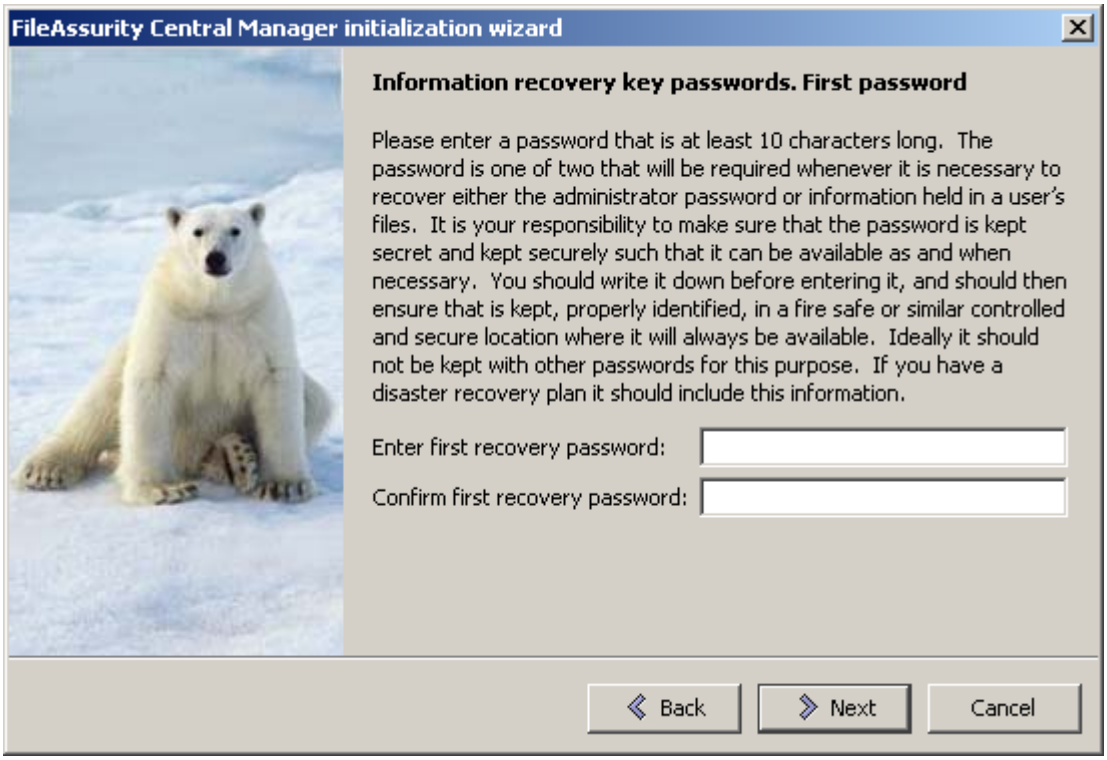
Second, following the colon, is the port they will use to connect to the Tomcat updater program (you will recall earlier that Port 8080 was selected in the Tomcat parameters). Obviously, in an operational environment, you may wish to choose a different port to suit firewall requirements. But this is a test system so the default will work perfectly well.

Updater/KeystoreUpload is the page that the TCP/IP connection requested will look for (just like looking for a web page on the Internet).

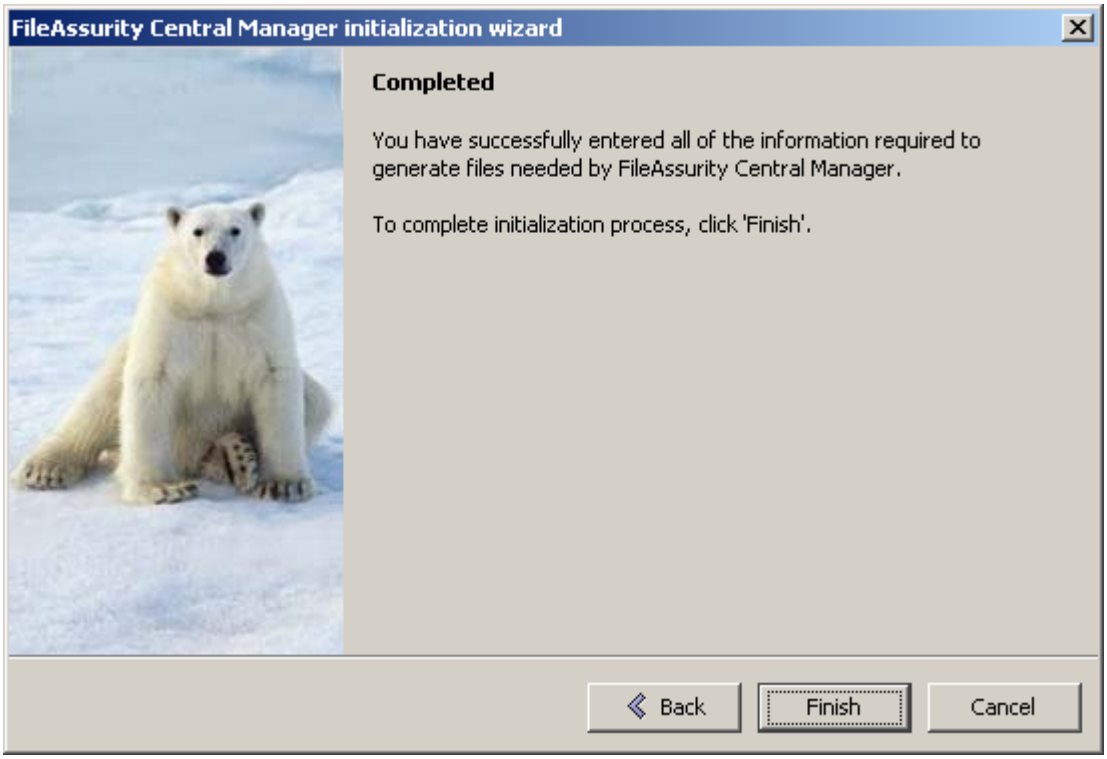
Username and password are needed to grant read access to database records.

Please check the values you have entered carefully before pressing Next.

You now have to enter the information recovery administrator passwords. There are two of these, each of which must be at least 10 characters long. These are used so that one person cannot have complete control over the Administration of the system Because this is a test you may find a password of 1111111111 to be easy to remember. In an operational environment two Administrators would have to be present, each one entering a password.



Having filled in both panels you should now see the following panel:

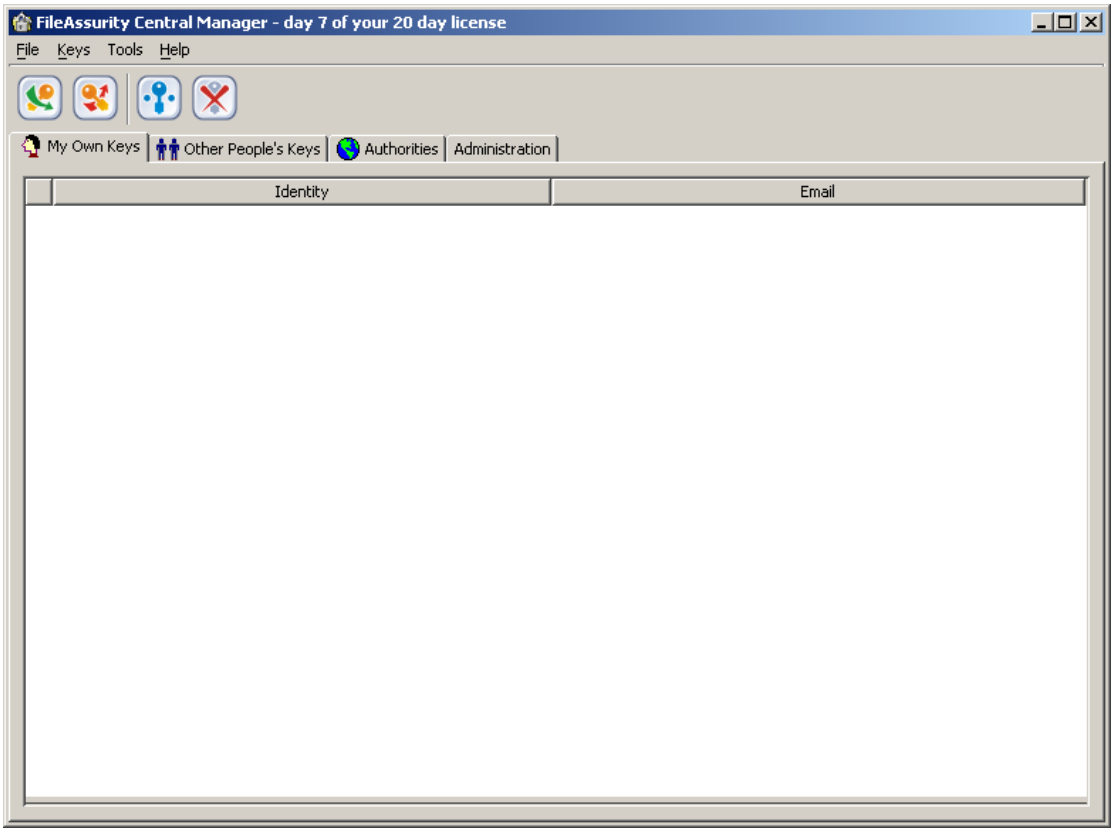


Once you press Finish the Master Keystore will be fully created and saved together with the access passwords and master system keys and control files, and you are ready to start on user keystore generation.

If you decide to continue, you will now be asked to logon to the current master keystore. As you can see, because the system has just been initialized there is no logon history.

You can see that the standard logon has two options: Normal login and Information recovery. Since there are no user files to perform information recovery on we will use Normal login.

Enter the password you selected earlier for the normal administrator. You will then see the following panel:



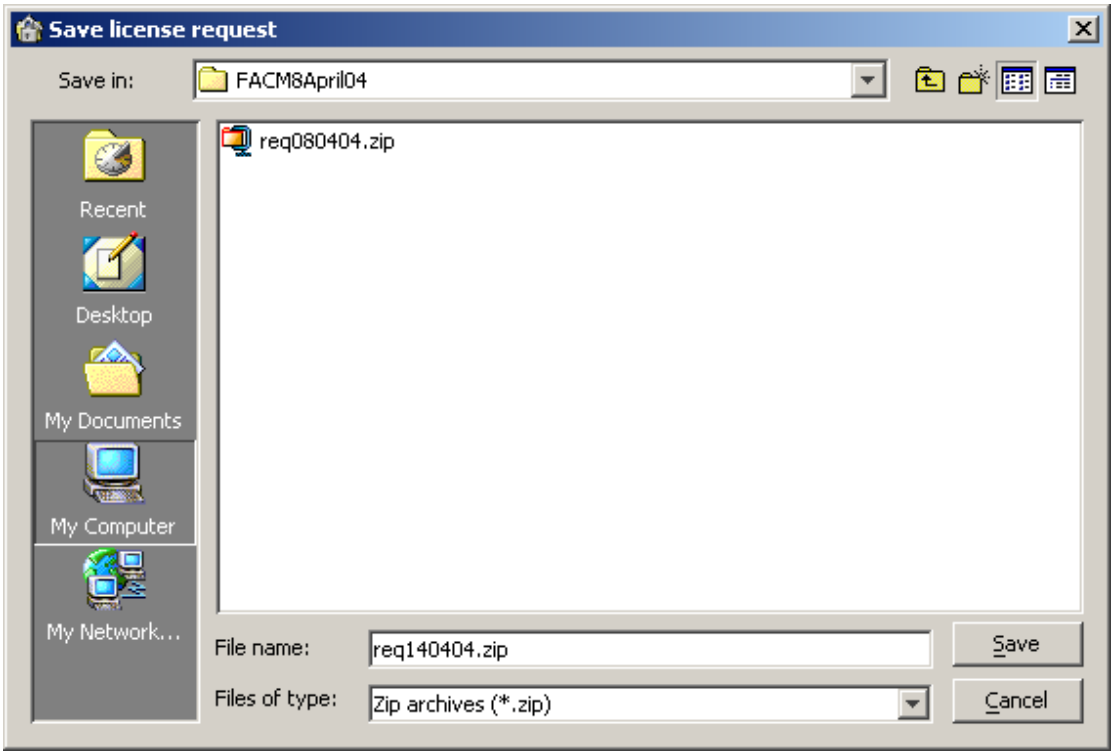
As you can see, this is an empty keystore.

The master keystore is used as the base from which user keystores are built. Anything that is present in the active master keystore, whether it is keys, authorities or policy, will be reproduced in user keystores generated whilst the active master keystore is in force. You may delete Trusted Authorities from the Authorities tab (except for the root key structure and the ArticSoft root key) and you may add other Authorities to the list if you wish. To delete Authorities, click on the Authorities tab, select a key in the list and press the delete key. Please note when adding Authorities that you can only import a certificate into the Authorities list if it has the X.509 Certificate Authority bit set. If it does not then it will import to the Other user's keys location.

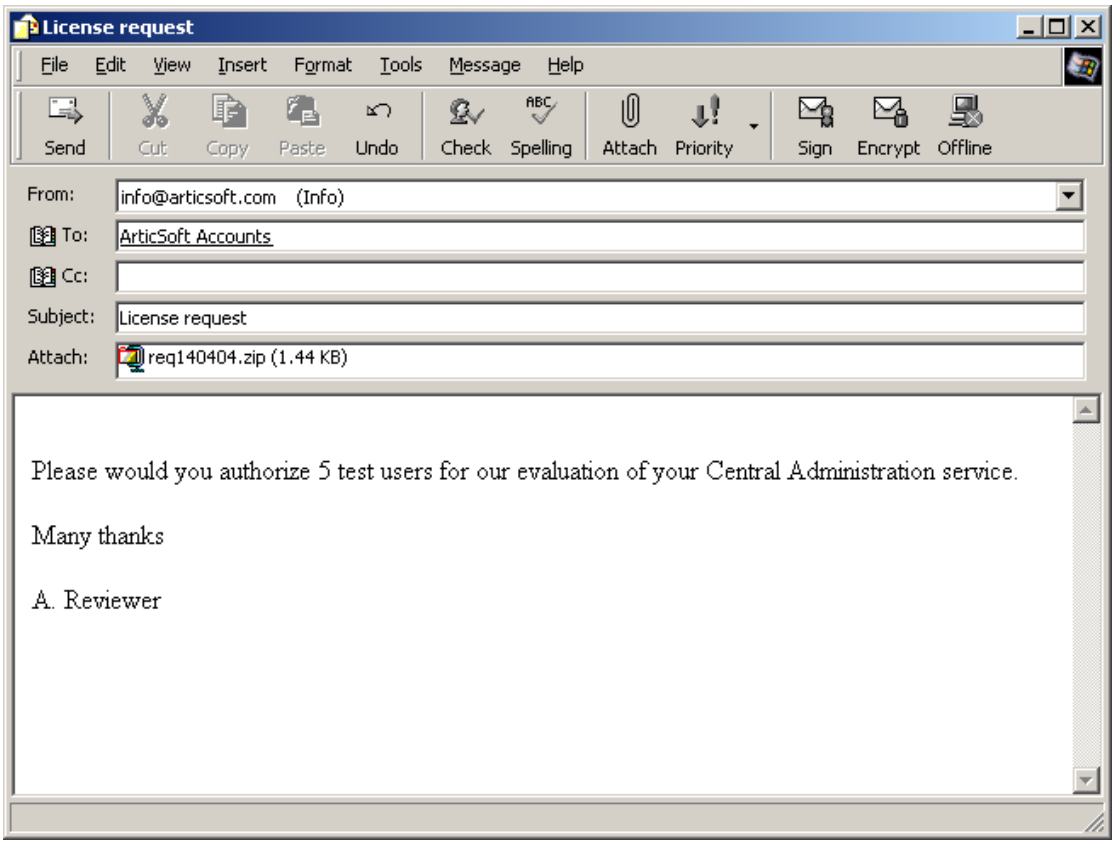
The first thing that you need to do having generated your system, is to request some user keystore licenses.

This cannot be done any earlier because licenses are linked to your Authority, and you have only just generated it.

To request licenses click on the File and the Send license request tabs. This will generate a file containing your installation public details that uniquely identify your installation from any other. You will be asked to save the request file to disk (in an operational environment you would want to save it for future use). Having specified a disk location the file will be saved there, as in the following panel:



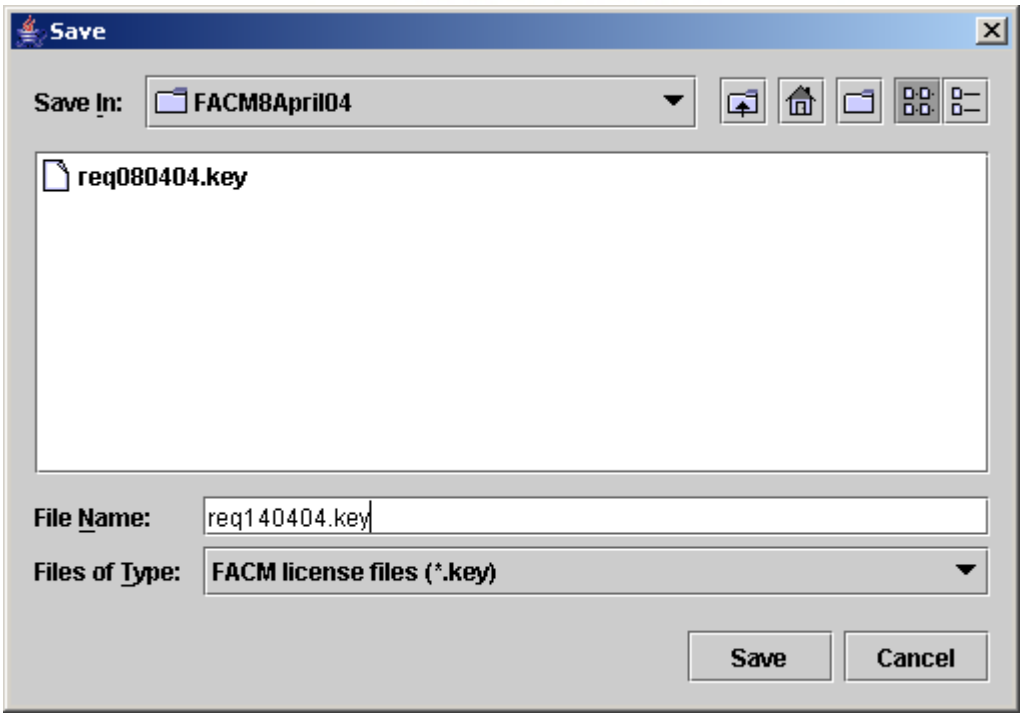
and then your default MAPI client will be loaded primed to send your license request to ArticSoft for fulfillment, as in the following panel:



Of course, in an operational environment it may be preferable to send the request from a different location, machine or person, but since this is a test system you can send the request off to ArticSoft for processing.

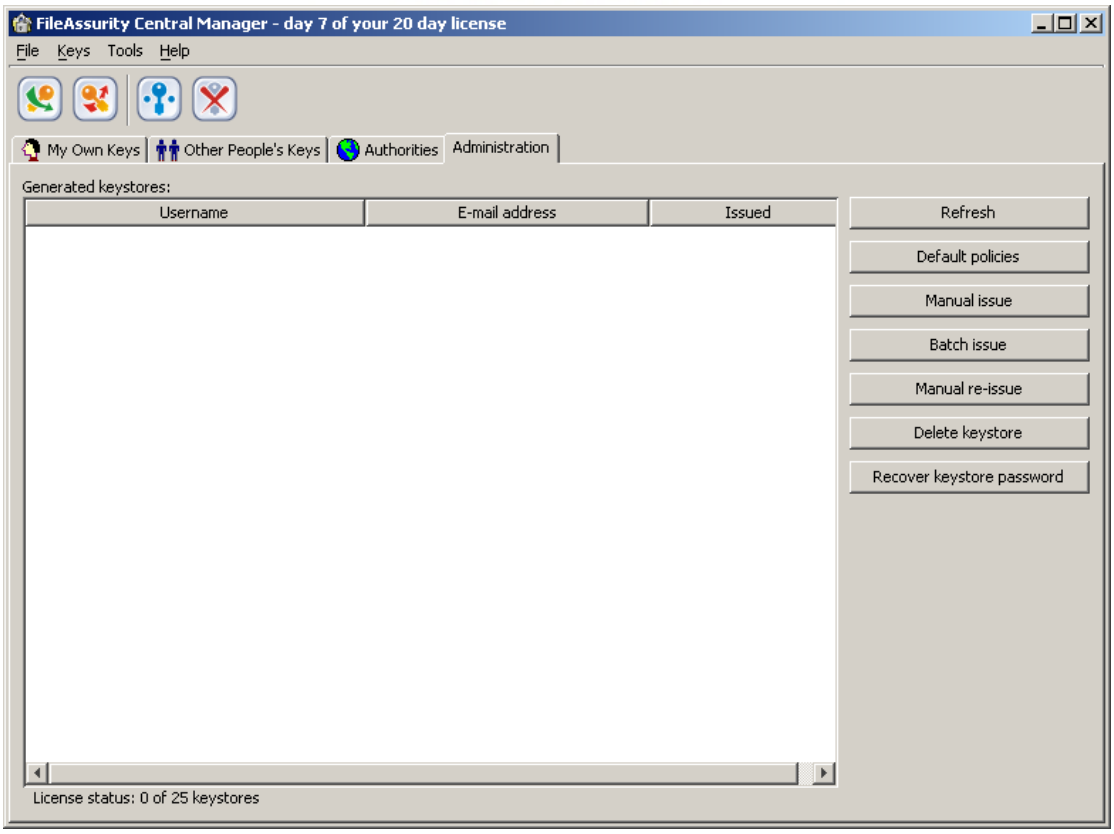
ArticSoft will send you back, by e-mail, a grant of license for a number of client keystore copies. This should happen by return, but may take a little longer at times.

The ArticSoft grant of licenses will be returned as a file with a .key extension, and may look like the following:



When you receive this file through the e-mail you load it into the FACM program by selecting File > Add license and then navigating to the .key file you have received. If you are using one of the Microsoft mail clients you may find it helpful to save the attached .key file to one of your own folders rather than go searching for it in the Microsoft controlled e-mail folder structure.

When you have received the license file and imported it, if you click on the Administration tab you will see the following:



Here you can see that ArticSoft granted 25 keystore licenses for your evaluation.

You have now obtained keystore licenses and are all set to generate user keystores.

But first you have to decide on the policies that are going to be applied to users for whom you are going to generate keystores.

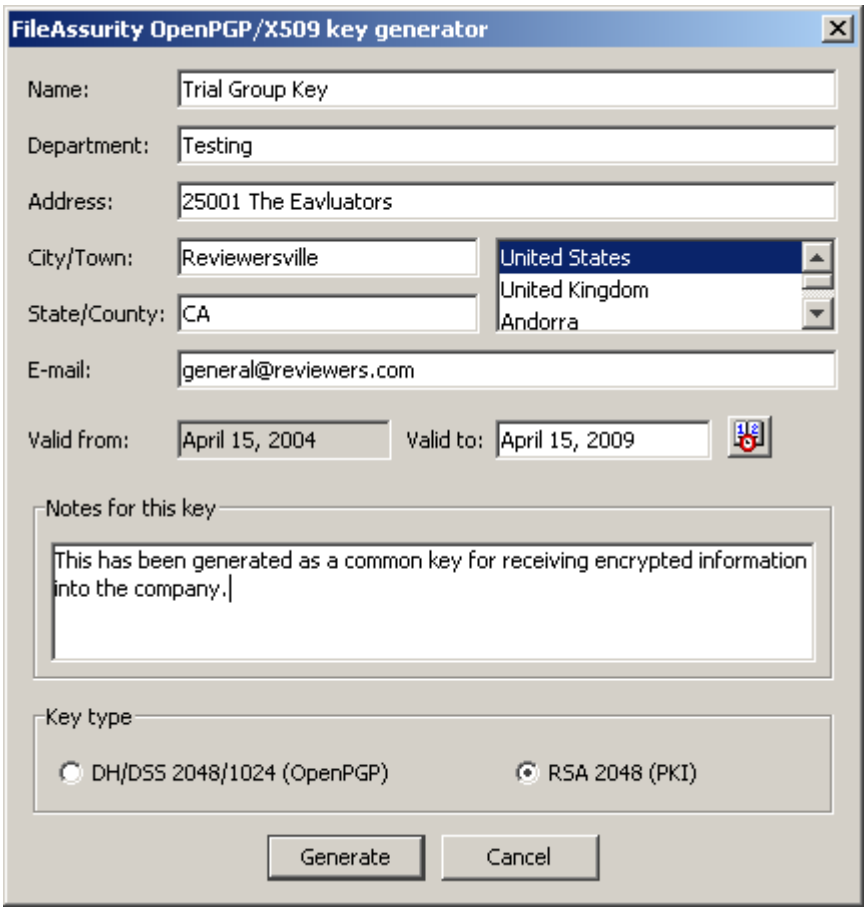
In this first example we are going to look at the simplest case, where you, as the Administrator, are distributing keys for users in a small enterprise.

There are a number of policy requirements that you, as the administrator, are required to enforce. These might be:

1. All the users work as individuals.
2. However, they want people communicating with them to be able to have a single point of reference – a 'company' key which guarantees that anyone outside can be sure that only one of the members of the company can deal with the information that is being sent, as well as being able to communicate with specific individuals.
3. Also, they want to be able to recover information sent by any member of the company.
4. They do not want members of the company to be able to generate or import their own identity keys.

The first item is a public key/certificate of common reference.

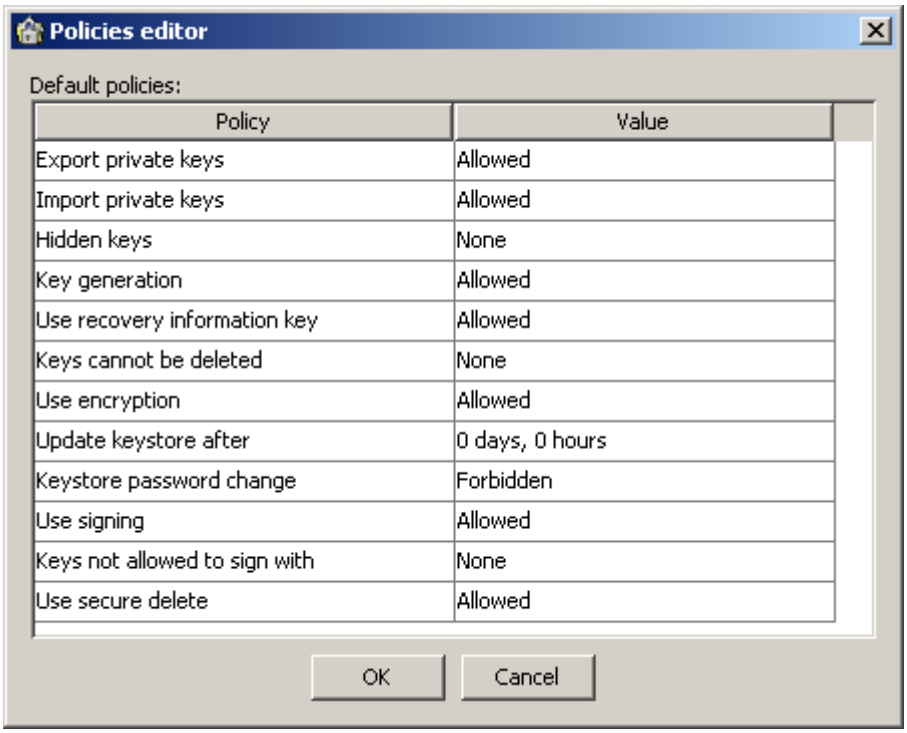
To create this you need to click on the Generate keys icon ;
That will open up an X.509 template which you will need to complete for the key that will be used as the common identity for all members of the company. When you have finished it may look something like this:



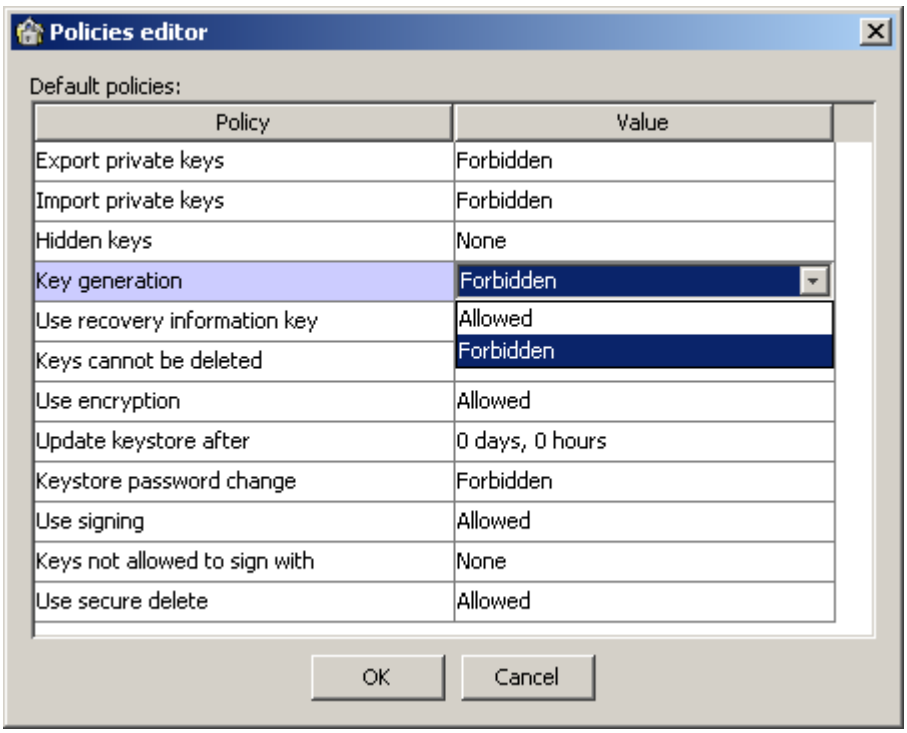
This key will now appear in the My own keys tab in the master keystore. It will be available for all the users who have keystores generated with that keystore present.

So now we need to go and set up the policy table so that company policy is enforced.

The default policy table is found by going to the Administration tab and clicking on default policies. When the program is first loaded the default policies are as follows:



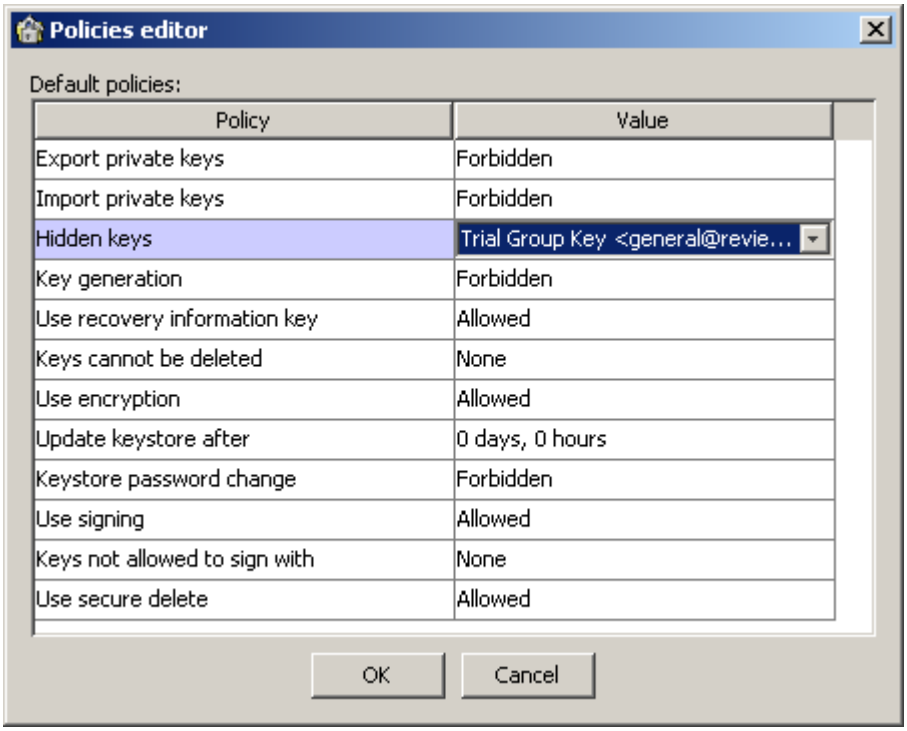
Since the policy is not to allow users to export private keys, import private keys or generate keys these fields need to be changed, as follows:



Since we have a common key between many users there are other policy settings to apply. We do not want the user to be able to delete the key pair, and we don't want them to be able to use it for a digital signature (that would make no sense because you would not actually know who had digitally signed something when everyone has that key). You could choose to make the key pair 'hidden' because that way the user

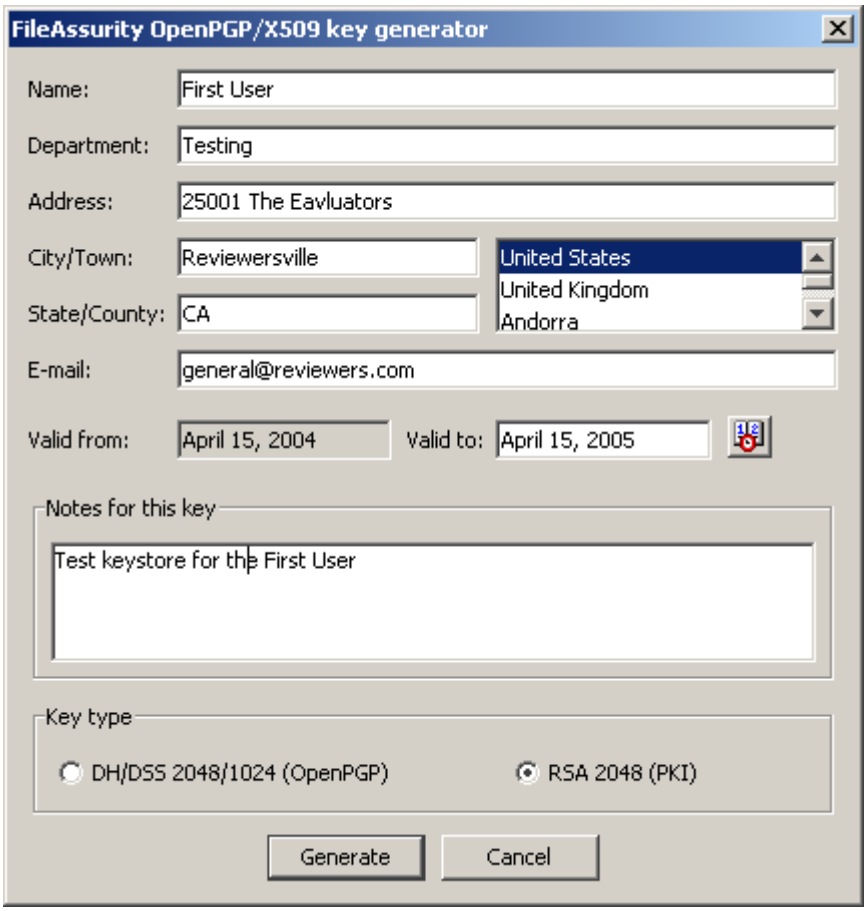
could not select the key for use, but the FileAssurity OpenPGP client would automatically decrypt files encrypted for that key without user intervention. (Please note that if the key is hidden, then, as a separate exercise the Administrator would need to export the public key/certificate and make it publicly available so that outside users would know which key/certificate they needed to use in order to guarantee communication with the company.)

This would give you a policy panel that would look as follows:



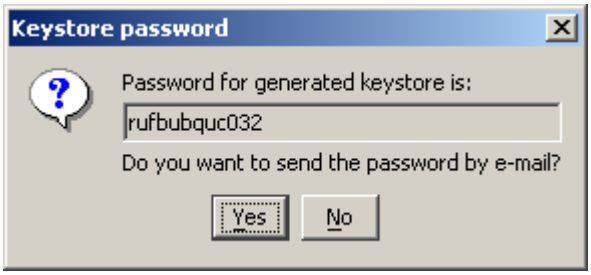
So having set up the agreed policy you are now ready to generate your first user keystore. For the test system we will do this manually. In a live environment, where you might need to generate large numbers of keystores when setting up a service, you can choose to generate keystores in batch mode using a .csv format file (this means that you can extract usernames and e-mail addresses from existing systems rapidly and easily and provide them for automated keystore generation and notification if you wish).

To generate a keystore manually you click on OK to accept the policy and then click on Manual issue in order to generate a user keystore. This opens up a new panel as follows:



Once the keystore has been generated you receive confirmation together with a system generated password which can be sent by e-mail to the correct user (at the e-mail address specified in the certificate that you have just created) or you can send it to them by another method (post, telephone) if you prefer. The text for the e-mail message can be customized.

The system response you will receive looks like this:

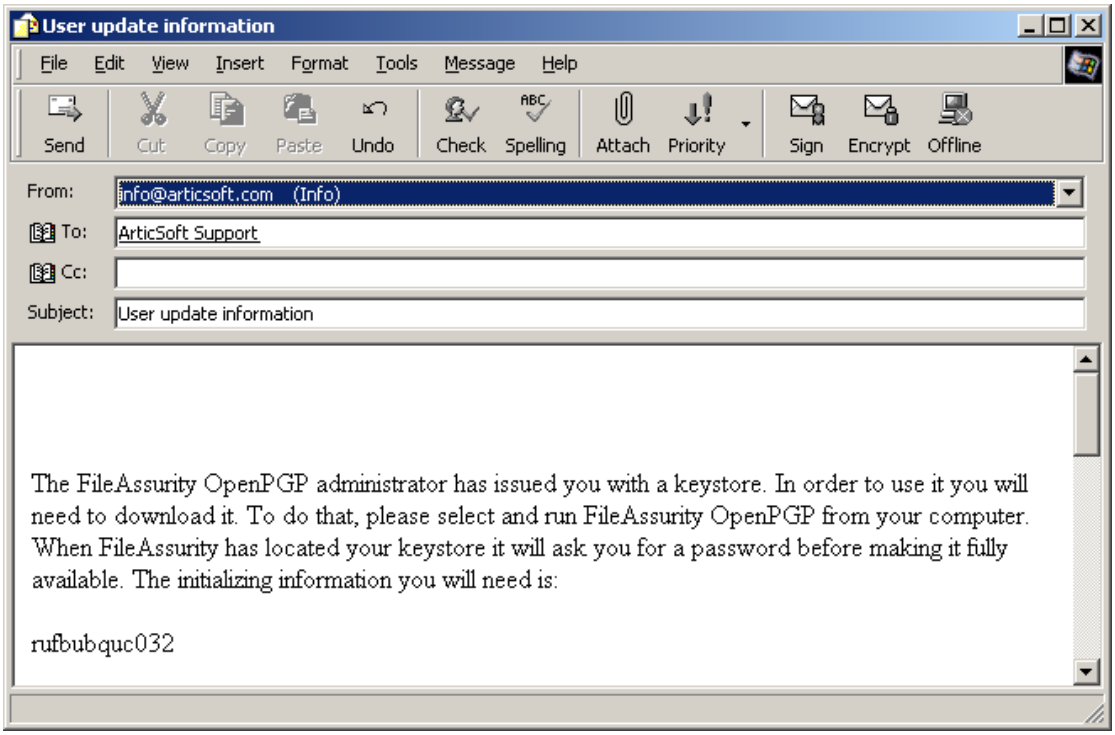


System generated passwords take the following form:

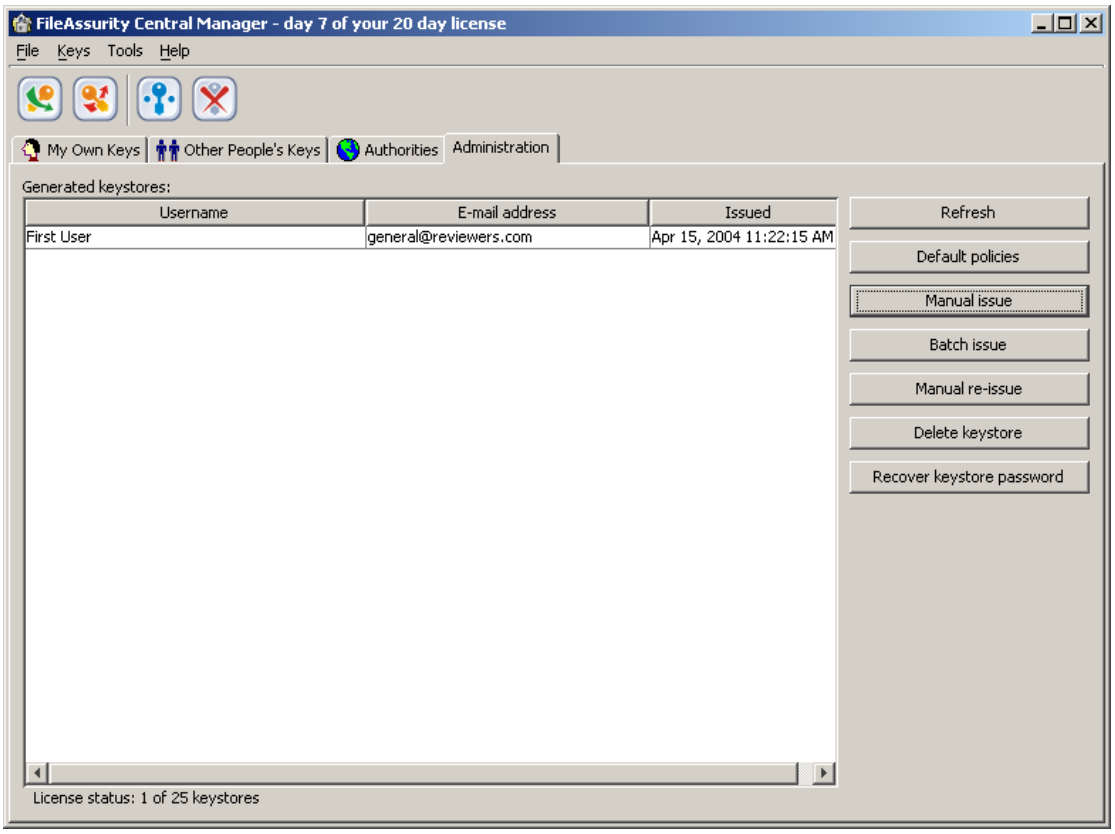
CVC CVC CVC nnn

Where C is a consonant, V is a vowel and n is a numeric digit. Although the password is 12 characters long, it is much easier to remember in this form than random characters, which are typically impossible for people to remember.

If you wish to select the 'send password by e-mail option, Central Manager will pass customizable text to your default MAPI client. A sample form looks like this:



Once the keystore is generated it is loaded directly into the database and appears on the list of issued keystores as shown on the panel below:



You can see on the bottom line of the panel the number of keystores you are licensed for and the number you have issued.

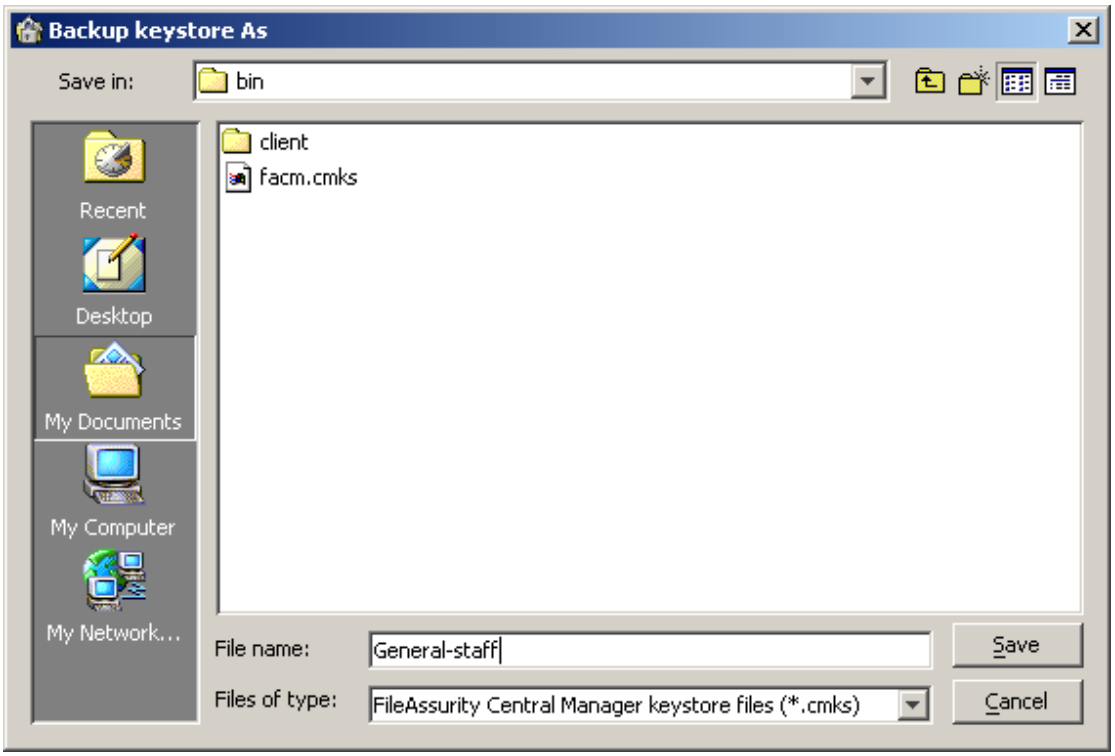
You can now go on and generate keystores for other users by just clicking on the Manual issue button and filling in their username and the correct e-mail address.

So now you have seen keystore generation for a simple enterprise structure.

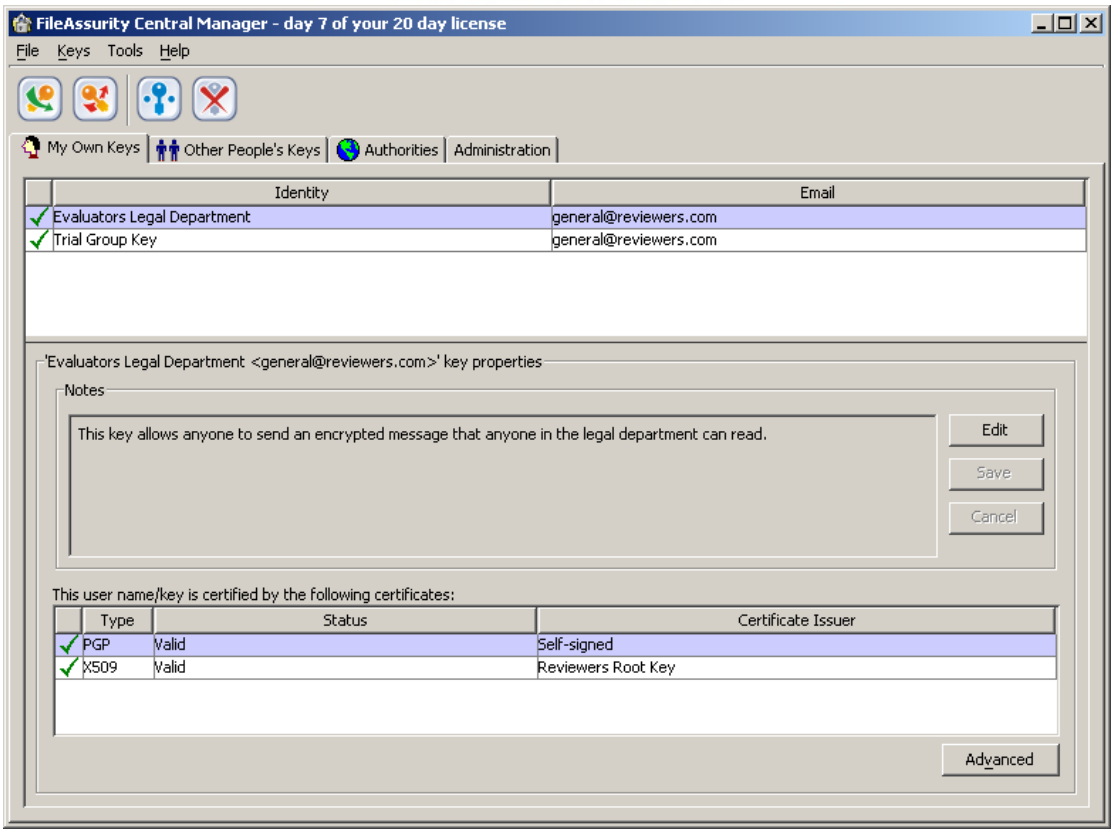
But suppose that you have a more complex structure, where you need to have keys that can be used by the whole business, but also ones that can be used by specific departments or functions, as well as individuals having keys?

You can do this by making use of the master keystore backup and recovery feature. Click on Tools and then backup keystore. You are now able to give the master keystore a specific name and save it, and the policies that were applied with that keystore. This means that later, when you need to issue keys to another user from the same department, you can load the correct departmental keystore, and the appropriate policies will be loaded as well. Let's step through the process for doing this.

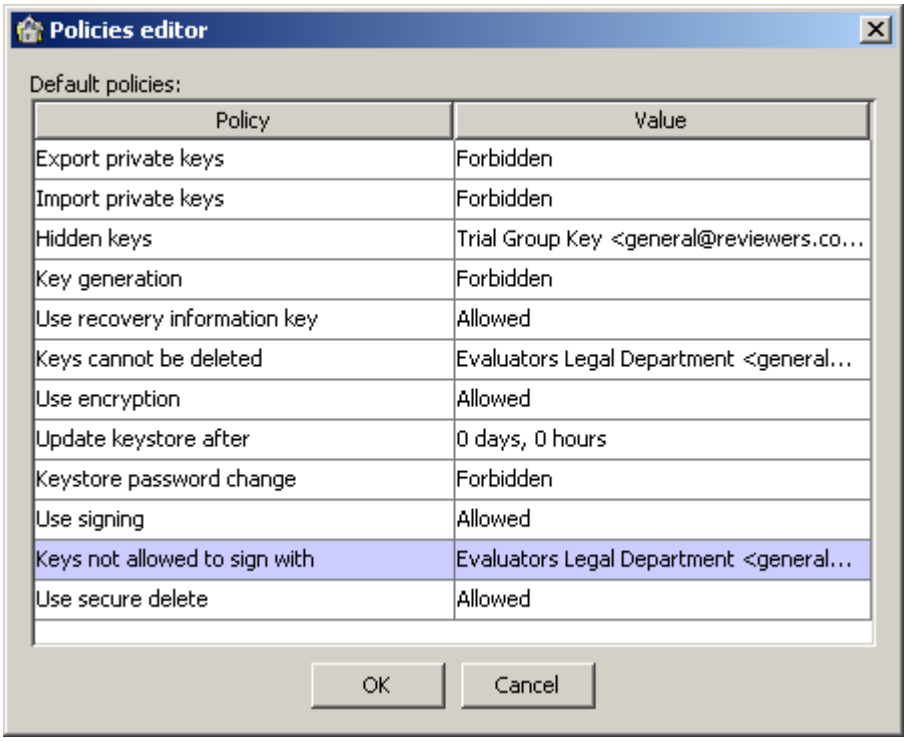
First we are going to make the current keystore one for general staff. So on the save panel we can call the keystore General-staff



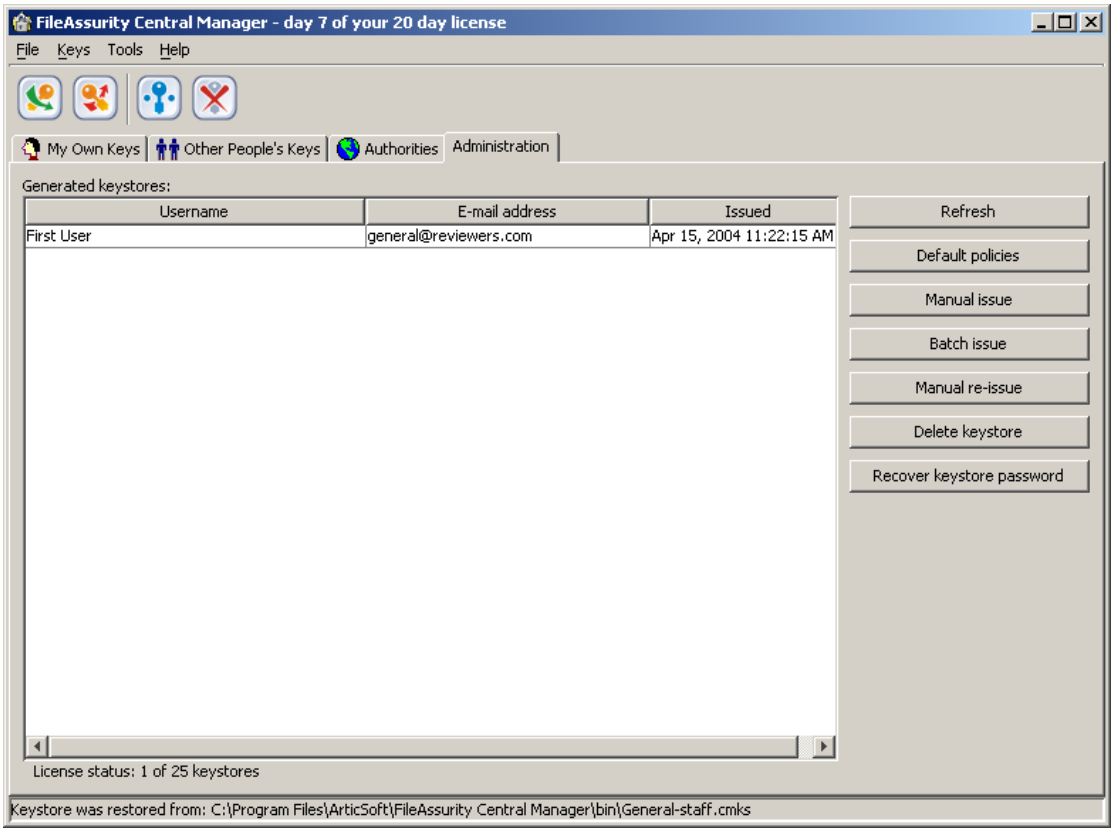
Confirm the backup and save the file. Now let's generate a common key for the legal department. So click on the generate key icon and fill in the panel with the username of Evaluators Legal Department and generate. You will see that the keystore now has two keys in the "my own keys" tab:



You now need to alter the policy rules to prevent the Legal Department users from being able to delete their group key or use it for digital signature. You do that by clicking on the Administration tab and then Default policies. Change the default policies until you have a panel that looks like this:



If you press on OK the default policies will then change to those shown above. Now click on Tools and backup keystore. This time call the keystore backup file Legal-department. Make sure that you have saved the file. Now use Tools and recover keystore to recover the General-staff keystore. You now see on the very bottom line of the panel a message telling you the identity of the keystore you are now using.



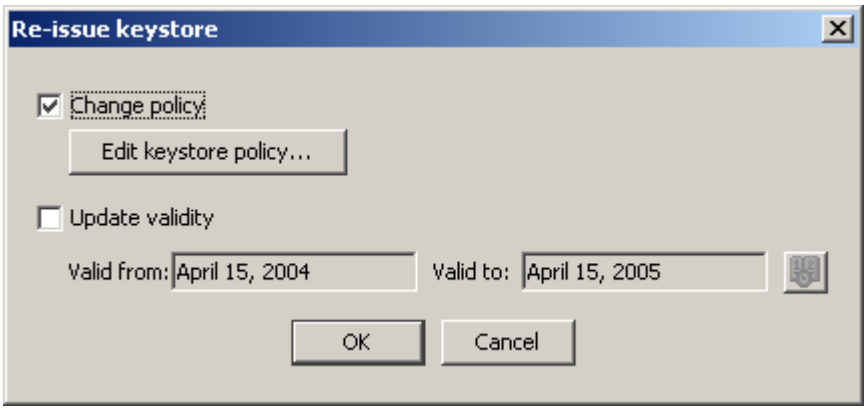
If you now click on Default policies you will see that the General staff default policies are now in force.

You have now seen how you can generate and use multiple master keystores so that you can organize users into groups, can use policy templates to ensure that you can generate user keystores quickly and accurately.

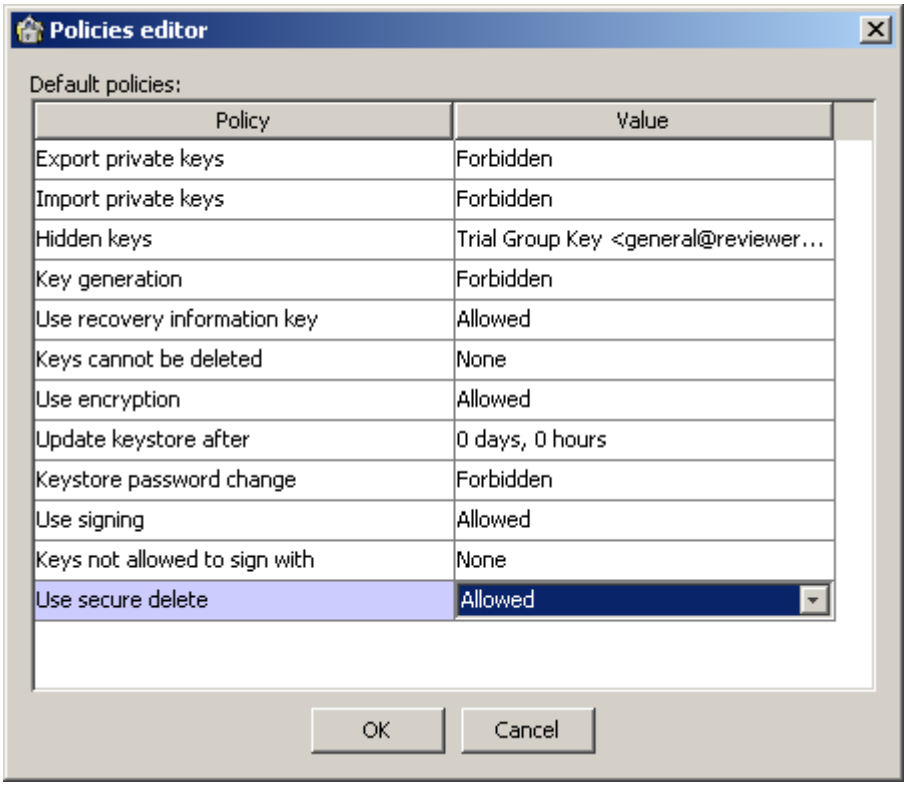
We will now see how to transfer policies and keys using the Manual re-issue feature. This is useful when people change departments or where you need to add an extra group key into their keystore.

First of all, generate keystores for some additional users, say Second User, Third User and Fourth User. For the Fourth User, just before you generate their keystore, manually change the default policy for Hidden Keys to NONE. Then generate their keystore. This means that the Fourth User is able to use the Company key for both signing and encryption. We will come back to check out how that works in the Client review phase.

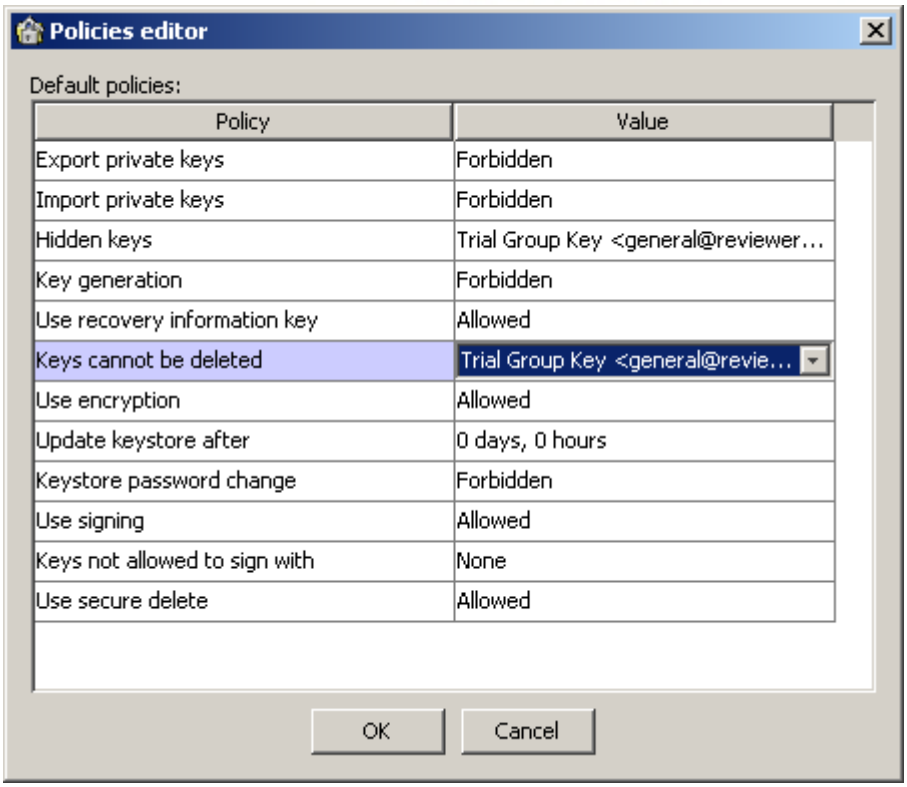
Then restore the Legal Department keystore. Then select Second User and click on Manual re-issue. You can then select change policy and the panel will look as follows:



Click on Edit keystore policy and you will see the following screen:



These are the original policies that were applied to the keystore. However, if you now click on Keys that cannot be deleted you will see that the Legal Department key is available and that policy can now be applied to it.



When you make changes to policy, or simply save the changes having made none, the contents of the active master keystore are added to the user keystore.

You have just seen an exceptionally powerful means of changing the capability of a user through Administration, where you can add to a user's keys, change their authorities and update the authorities that the user will automatically recognize.

Although we did not investigate it during that exercise, you could have changed the validity period of the user's certificate. This would be important because when you issue keys to users you want to be sure that they will not last forever (there might be legal implications). Conventional wisdom says that certificates should last one year, but you cannot easily change user keys, once issued. So to make operational life simpler we have included the facility to be able to renew user keys when that is necessary. (Please note that whether you issue keys in realtime or in batch you can decide on the validity period of the keys, and the user cannot change this.)

You can also change the validity period of the root key for the installation. To do this just click on Tools and the Extend root key validity. This may not strike you as an essential function, but, when you initially generate the system, you will have no idea how many years it may have to be valid for. As a result you may not choose a time period that fits the business requirement. So we have provided a feature that allows the Administrator to extend the life of the whole installation if that becomes necessary. It may not seem important in the next year or two, but further down the track it could become very critical. In the last six months several public authority certificates have gone out of date, causing various problems, which we have prevented. (Please note that if the root key is chained to a public authority it is not

possible to extend the life of the root key beyond that of the chained key that it is linked to. Hopefully the issuer of that key is able to extend their own life!)

So we have now set up a central administration service, set policies that create one company wide key (all Users) and one legal group key (Second User). We are now ready to install one of the clients and check out that policy has been correctly applied, that the client can upload their keystore for central recovery, and that the use of the Group system works.

Managed Client review.

If you have already installed FileAssurity OpenPGP or Command Line Scriptor on your computer you must de-install them before loading the Managed Client.

Managed Client is loaded from

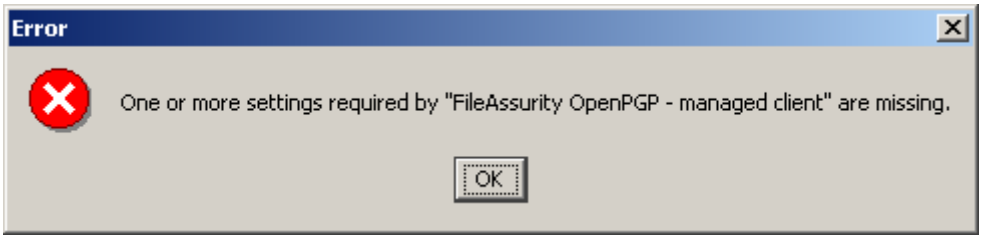
Programs/FileAssurity_OpenPGP_Full_Managed.exe

If you did not remove previous programs the installer will stop and ask you to do so. At installation please choose the default settings for the installation, selecting an icon in the system tray as a means of loading the application.

These instructions assume that you are running Central Manager and Managed Client in the same computer. If you are not, then you will have to move from the client computer to the Central Manager and back again, because we are going to simulate day to day administration of the client base.

Because this is not a real operational environment you will need to change user identities a number of times during the simulation. Normally the user would not need to enter operational parameters, they would have been loaded into the client during the installation.

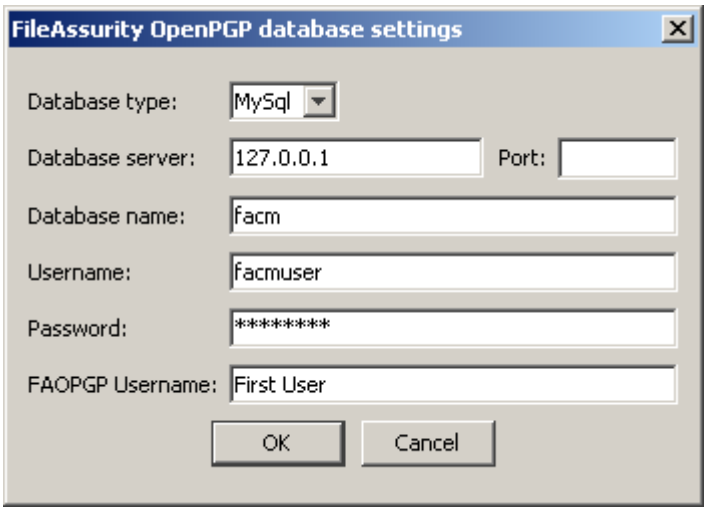
Once the client is loaded you will see a Penguin and key icon appear in the Windows systems tray (bottom right hand side of the screen). It is grayed out. Right click on it and a panel will appear. Select Logon and you will see the following message displayed:



When you press on OK the client will offer you a screen to fill in to provide the connection information needed. This feature is provided to allow users to roam (that is to use the encryption/decryption capabilities that they have on any computer that is able to connect to the master database). It is not essential to protect the connection

between the client program and the master database because all the information being exchanged is encrypted, and therefore cannot be compromised.

The panel you need to complete will look like this:



Please remember to put in the IP address of your database and the correct password (11111111). We are going to connect as First User. (Please note that normally a user would not have to fill any of these fields. Ordinarily when the systems administrator installs the software they will have included a file 'switches.txt' that contains all these parameters which automatically links the user to their keystore.

Assuming that the parameters are all correct you will see a message telling you that the connection has been made and the keystore is being downloaded. As soon as that completes you will be invited to logon. Since the user has not logged on before there is no previous logon time, otherwise the user will be told of the last time that their identity was successfully logged on. (You may need to go back into Central Manager and ask to have the password for First User displayed so that you can now logon. This is available from the Administration panel.)

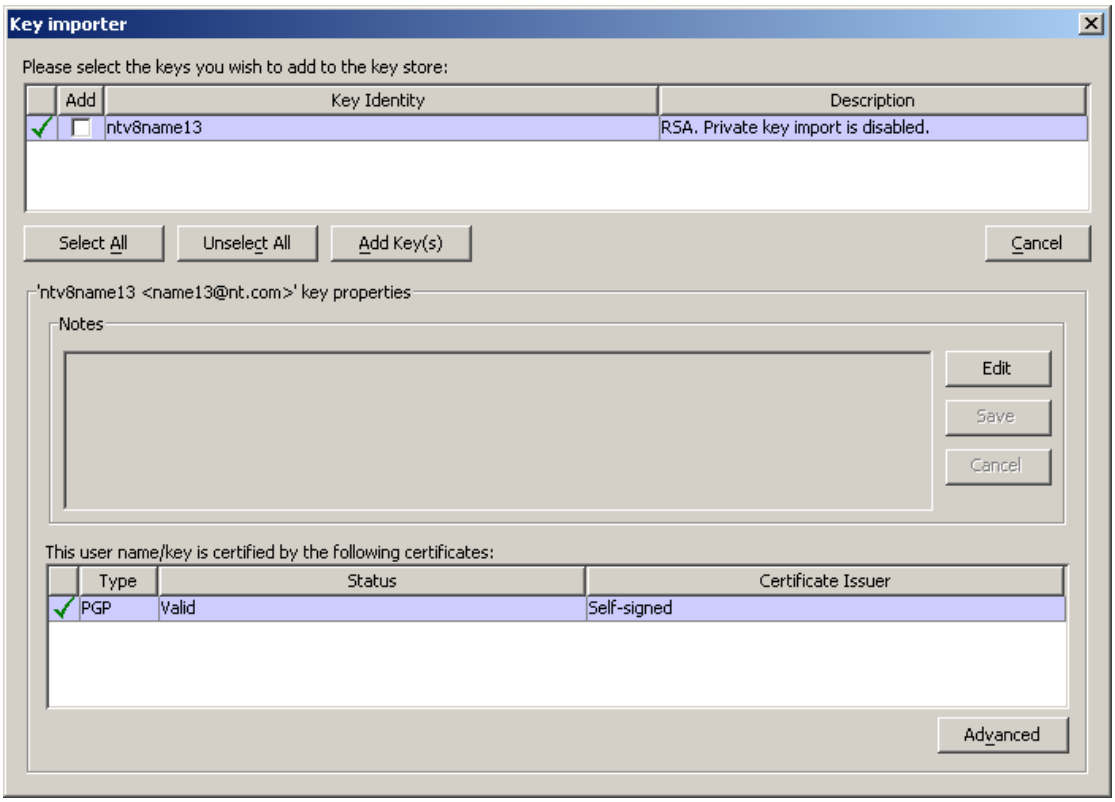
Having entered the password you are then logged on to the Managed Client and you will see the Penguin icon in the system tray light up. If you right click on the icon you are now offered the usual FileAssurity OpenPGP options. Select Key Manager.

If you click on the generate keys (please remember that this was forbidden by policy when you generated the keystore) then you will see the following error message displayed:

You can now see that policy is being enforced.

If you then click on the export key button in Key Manager you will be taken into the Export wizard. However, as you can see from the following screen, the policy forbidding the export of a private key is being enforced because the check box to allow that facility has been grayed out.

Please not that although when you generated a company group key that was part of this keystore you cannot find it on any of the screens. As a result, First User cannot encrypt anything for company-wide acceptance. If you now enter the Key import facility and go to E:\Keys and import the key ntv8name13.asc. The importer will ask you for a password in order to open the file because you are trying to import a key pair and not just a public key/certificate. If you enter the password 'frednt' the importer will open the import panel, but if you look at the key description field you will see that the import is being refused.

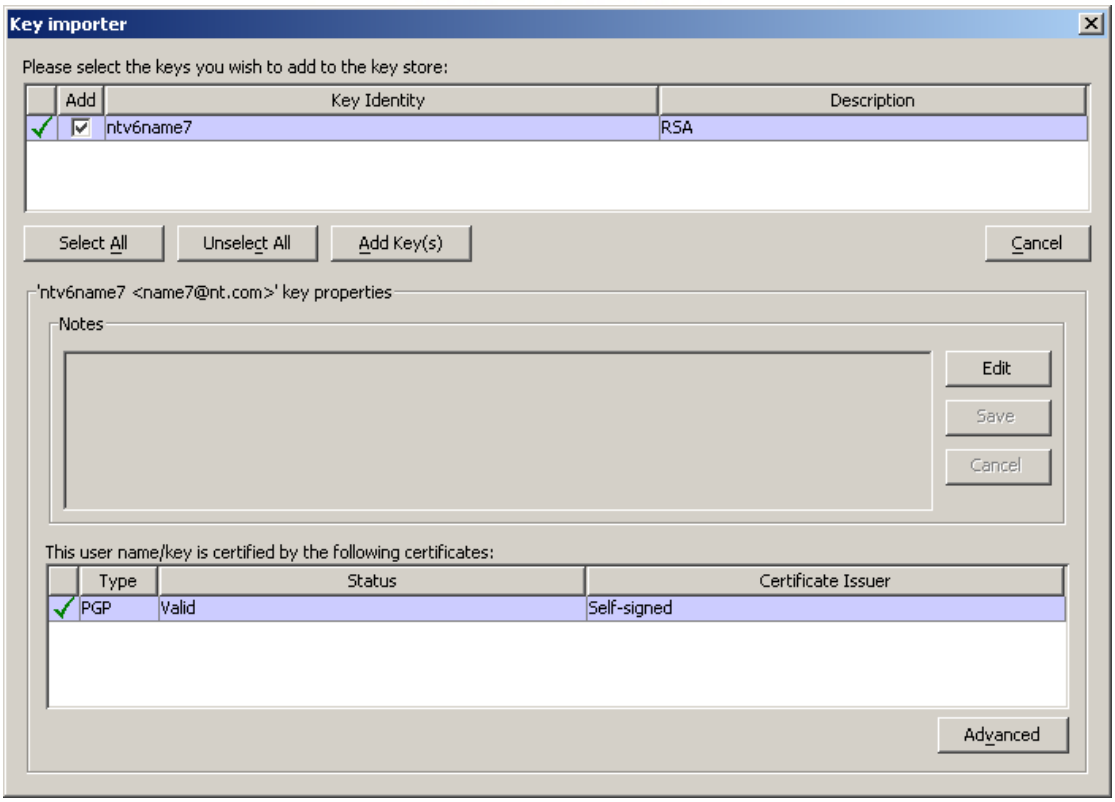


If you attempt to select add you will find that it does not work.

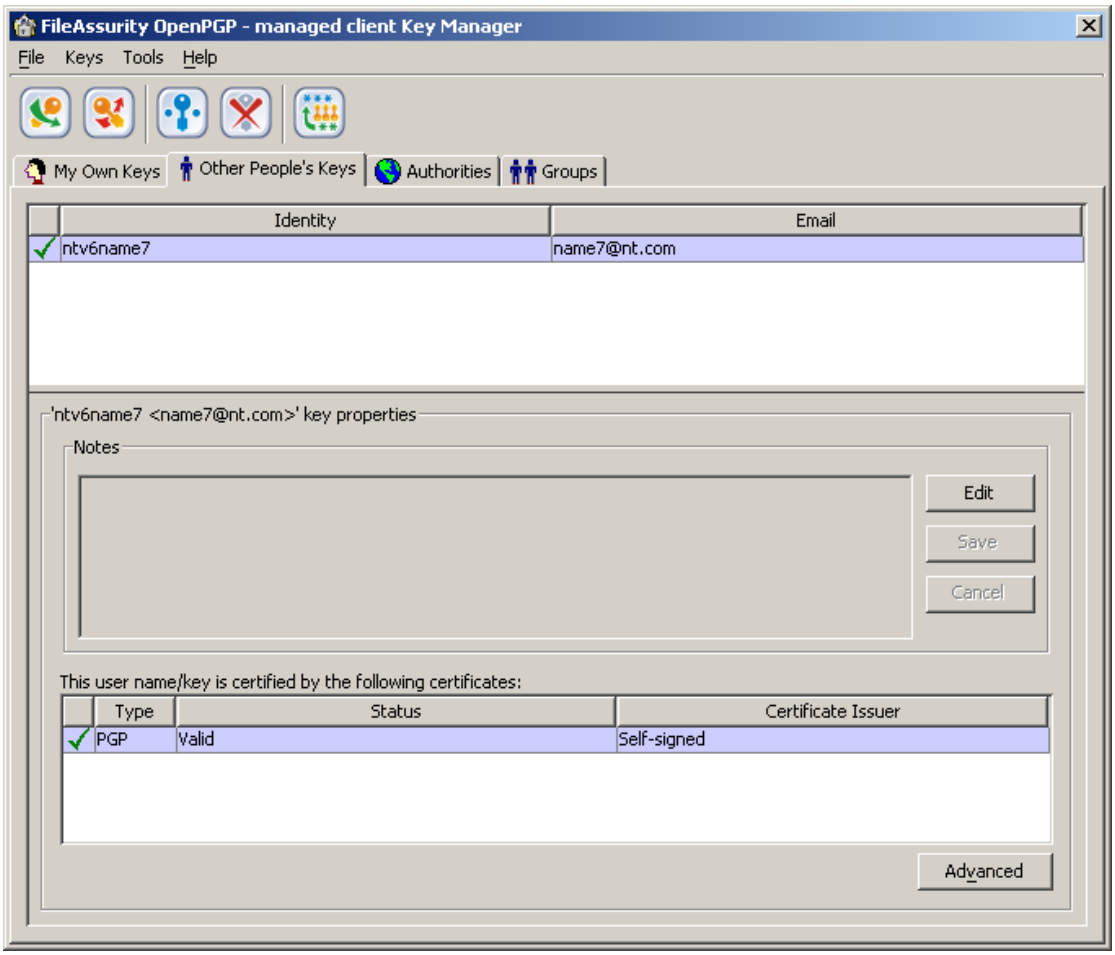
We have now proved that the policy rules set by the administrator are enforced in the client, and the client cannot override those policies.

Now on the computer running the Central Manager and database server click on the Start key > Programs > ArticSoft > FileAssurity Central Manager > Start Tomcat. You need to do this to start the keystore updater service. (In an operational environment this would be included in the Startup sequence to make sure that it was always available for users.) We suggest that you minimize the DOS window that it is running in.

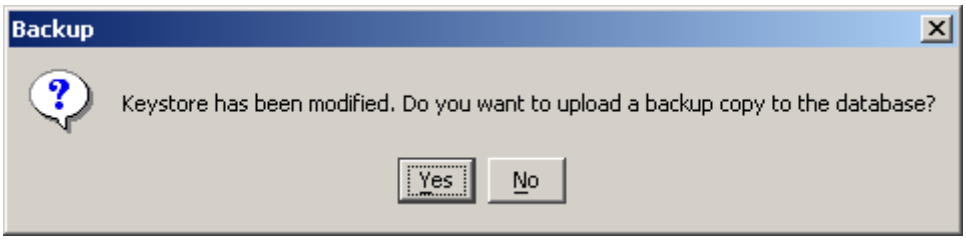
Now, using Key Manager in the client, import the key Keys\ntv6name7.asc. This is just a public key/certificate and you will be able to import it without any difficulty.



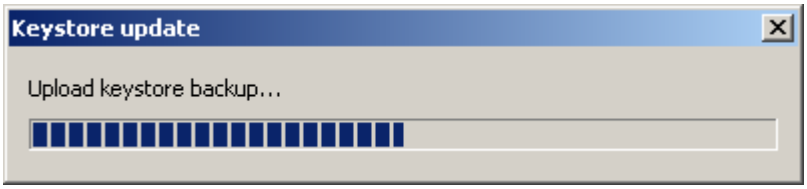
If you look in the 'Other people's keys' tab you will see the key has been successfully imported.



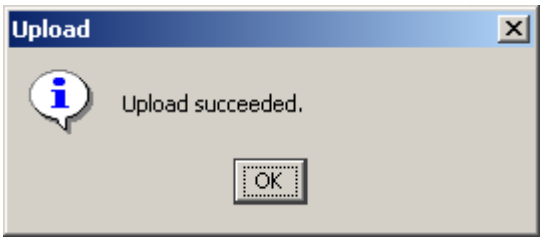
If you now right click on the Penguin icon and select Logoff you will see the following message:



The user is being invited to backup their keystore because it has changed since the start of the session. This could be very important for roaming users who may have added keys whilst away from the home network, and do not wish to lose them. If you answer Yes then you will see the following panel:



And when the backup has been successful you will see the following message:

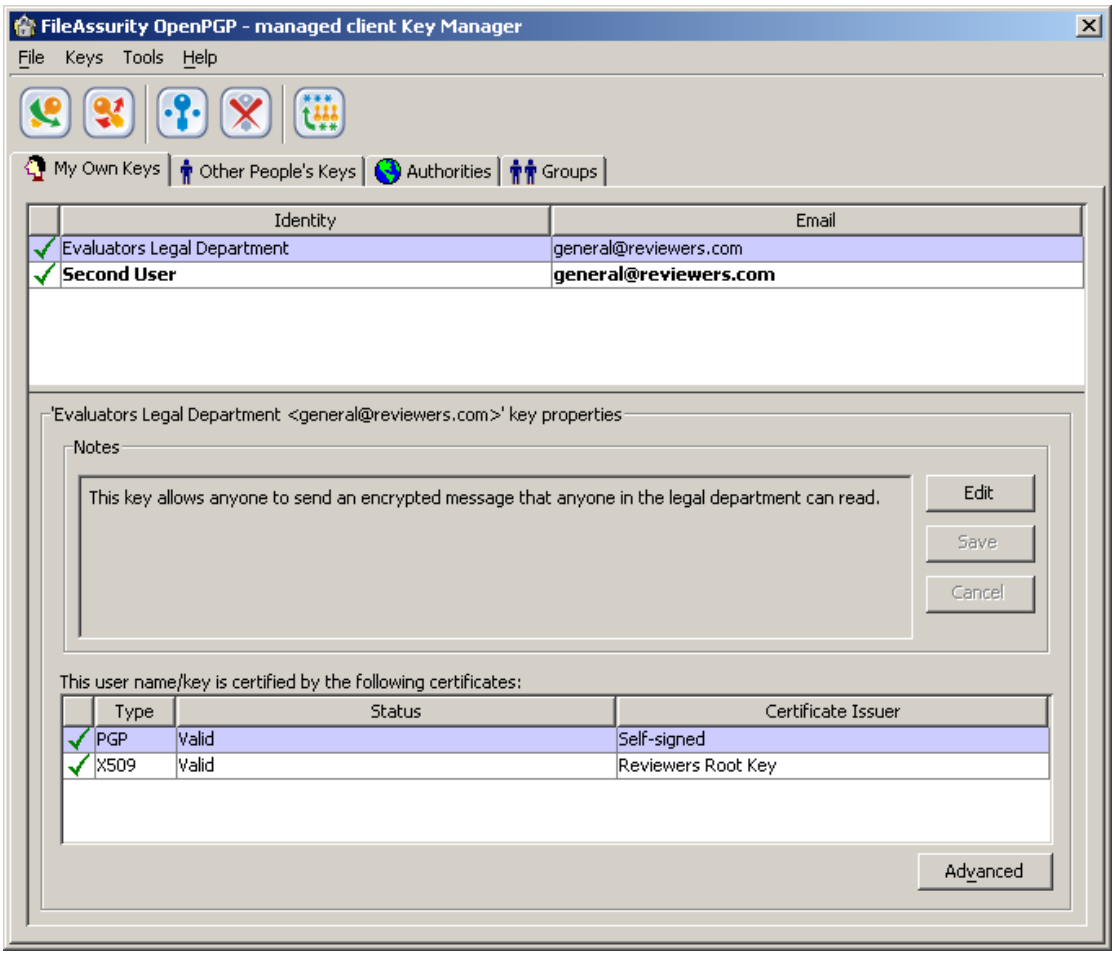


You have now seen that a user can have changes to their keystore backed up on the Central system, and that the backup is successful. Go into Documents and Settings > "your username" > .articsoft > faopenmc and delete the file faopen2.kspgp (this is your keystore file). Then right click on the Penguin and Logon and you will see the following message:

This is telling the user that the system has automatically provided them with a backed up version of the keystore. So you have now seen user keystore backup and recovery running in practice. If you maximize the Tomcat DOS window you will see an entry Upload request for User 1 which is the update running through the Tomcat system. Please be sure to confirm the backup of the keystore to close the program completely.

Next we are going to switch users to Second User so that we can check that the policy and keystore are what we were expecting for the Legal Department user. To do this we need to delete some user pointer files, so go into Documents and Settings > "your username" > .articsoft > faopenmc > program and delete all the files in that folder. When you now logon to the Managed Client (right click on the Penguin) you will be asked to complete the user panel again. (When you come to logon you may need to recover the password for Second User by the Central Administrator.)

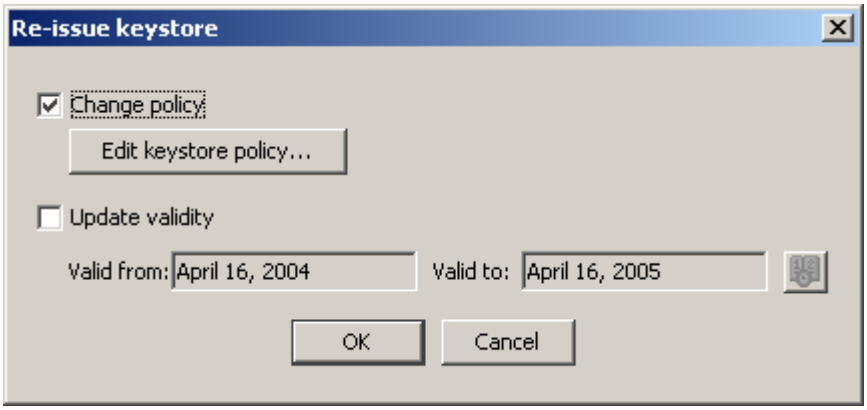
Again you will see the Penguin light up, and if you right click and select Key Manager you should see the following:



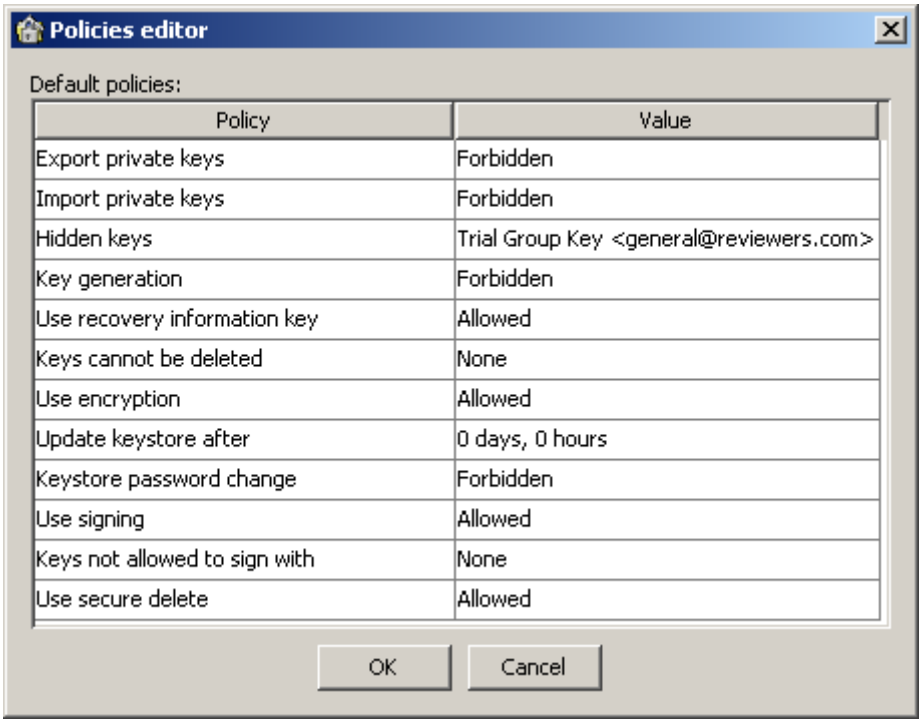
You have now proved that you have the keystore of the Second User, and that they are actually able to see the group key for the Legal Department. You can check that this user is still forbidden from generating keys or importing private keys.

If you now Logoff from the client (right click on the Penguin and Logoff) and go into Central Manager, we are going to change the policy on the Second User keystore.

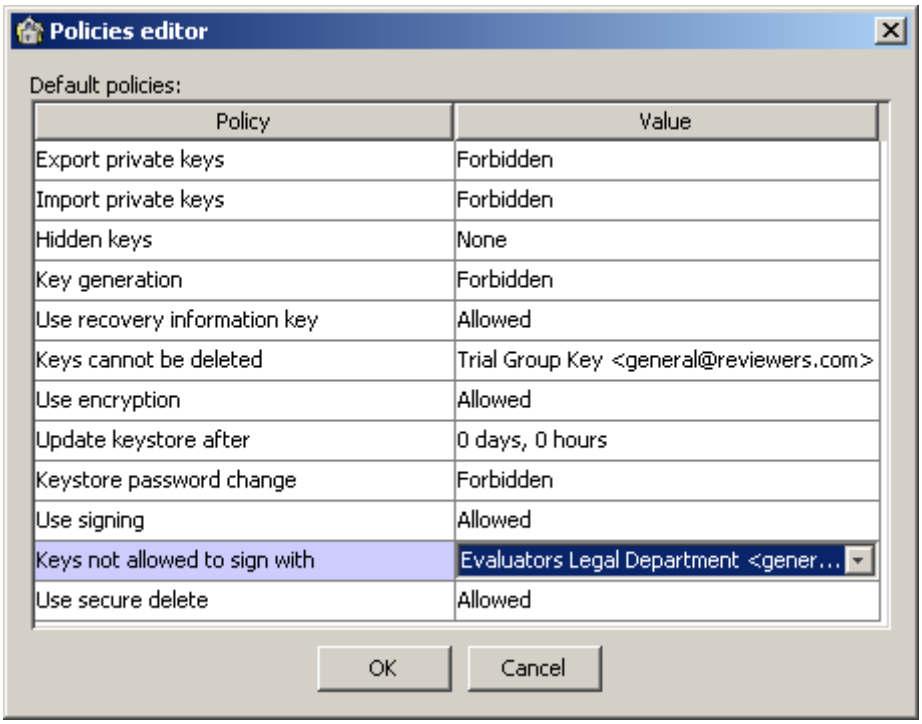
In Central Manager be sure to Restore the Legal Department master keystore if it is not the one in current use (check by looking at the bottom of the panel). Then select Second User in the Administration panel and select Manual re-issue. On the panel select Change policy and then click on Edit keystore policy:



You should now see the following panel:

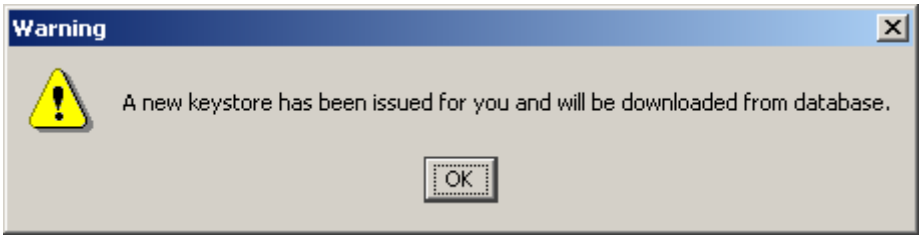


Set the Hidden keys to none, Keys that cannot be deleted to Trial Group Key and Keys not allowed to sign with to Evaluators Legal Department. You should have a panel that now looks like this:



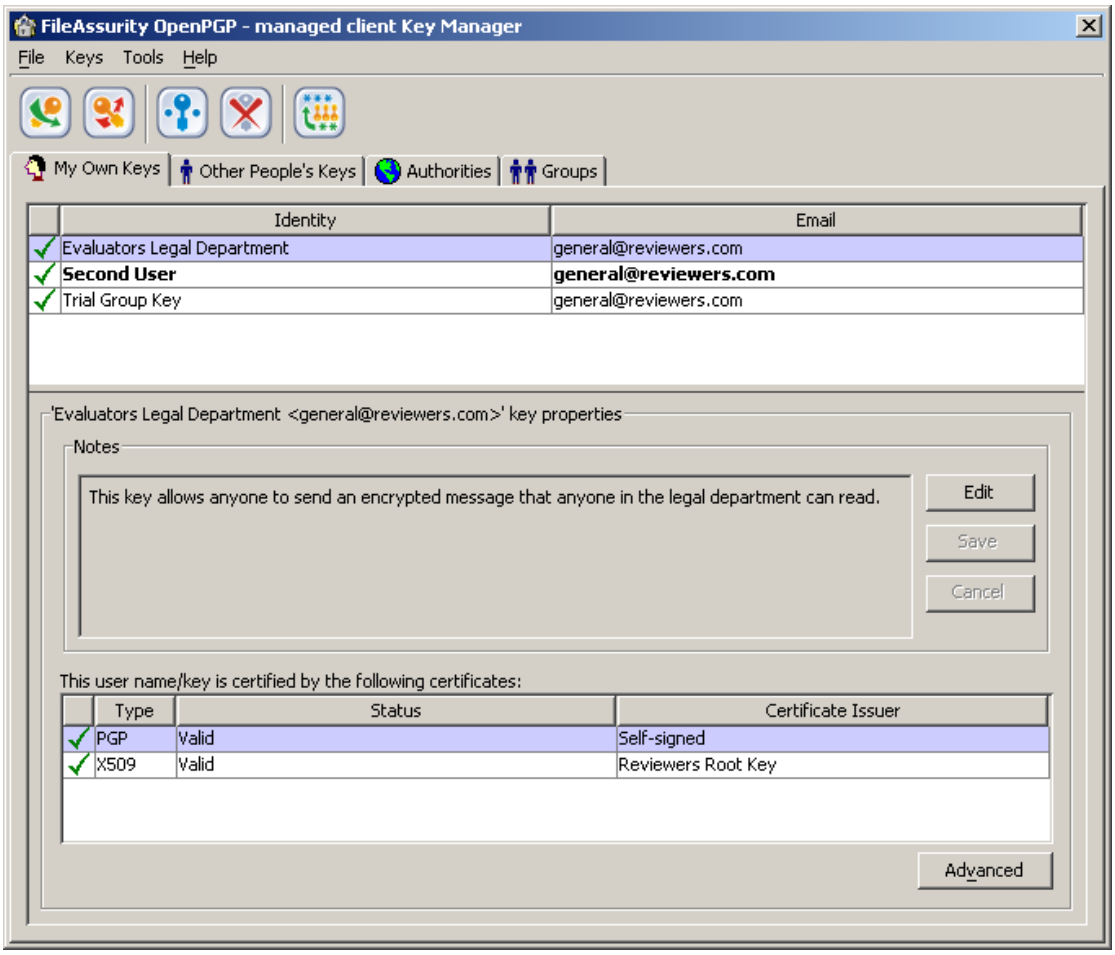
Press OK and then authorize the update to the keystore. You will see the keystore being re-issued to the master database.

If you now go back and Logon again as Second User you will see the following:



This is advising the user that a keystore update has taken place (this is a useful cross check on the integrity of the system).

If you then click on Key Manager you will see the following:



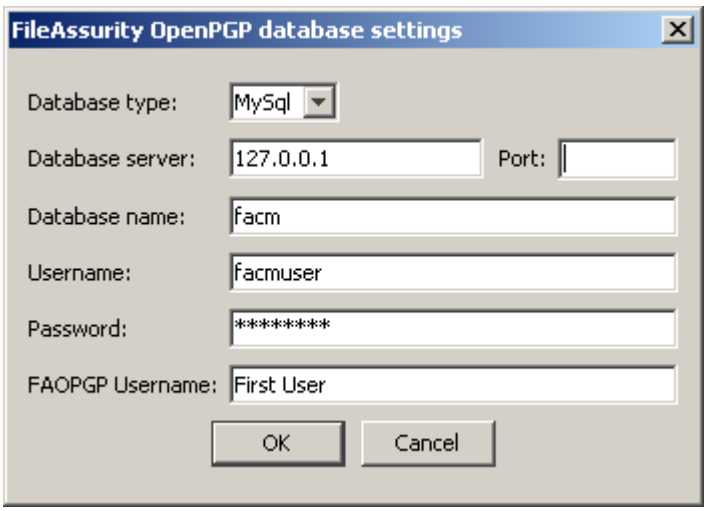
Now no keys are hidden from the user, although they were before. If the Administrator had introduced new keys into the master keystore they would also have been added to the user's keystore.

Go into Windows Explorer and select a file that you wish to encrypt for everyone in the company. Any file will do. Right click on the file and select FileAssurity OpenPGP > Protect. (You may need to close the Key Manager panel if it is still active.) In the Encrypt for box select Trial Group Key and press OK. In Sign as you

will notice that the Legal Department key is not available (as we just set in Policy) but the other keys are available. Select the Trial Group Key and then press the protect button. Please remember where this file is located!

Now we are going to switch back to First User. (To do this we need to Logoff, and then delete all the file in Documents and Settings > "your username" > .articsoft > faopenmc > program.)

Having done that right click on the Penguin and select logon and fill in the panel:



Then enter the password (again you might need to look it up in Central Manager). Once you are logged on go back to the file that you had protected and right click on it and select FileAssurity OpenPGP > Unprotect. You will now see a message displayed asking you if you want to overwrite the original file. Answer 'Yes' so that the decryption process continues. This proves that you have been able to decrypt the file using the Information Recovery key. You will then be left with the following panel on screen:

Obviously your filename will be different, but you can see the keys that were used to sign and encrypt for, and if you go into Key Manager you will not be able to find the private key that was used for decryption. You have now proved that it is possible to decrypt files using hidden keys, and that the whole basis upon which the Group Key system has been organized is correct. You have just seen a unique concept being displayed, that of being able to have secure communication with a group in an enterprise, and not be limited to specific individuals. You will not see this capability being supported in other public key encryption products, even though it is essential to making a Public Key Infrastructure commercially viable because it reflects how businesses really work.

Now that you are experienced in using the Central Manager to impose policy, and in using Managed Client to carry out typical encryption/decryption and digital signature actions you can investigate the many other features that FileAssurity OpenPGP Managed Client delivers. If you are familiar with FileAssurity OpenPGP you don't need to do this because all the capabilities (subject to policy) available in the OpenPGP product are available in the managed client.

The next check is to invoke user revocation. In many proposed architectures this is a highly complex and controversial facility, requiring users to check on the supposed validity of a certificate at the point of receipt of digitally signed information. This relies upon accessing some publicly available server that is not controlled by the enterprise, but by some 'Trusted Third Party' that might not be clearly accountable to

anyone for the actions it either takes or fails to take. The ArticSoft system is both simpler and more pragmatic.

Logoff from First User in the client. The go into Central Manager and using the Administration panel delete the keystore for First User. (Do remember to keep a copy of the right password for First User so that you can enter it when you then try to logon.) Now go back to the Managed Client by right clicking on the Penguin and try logging on. You will find that the program will not run because no keystore is available, even though there is a local keystore file for that user.

At a stroke it is impossible for anyone to use keys without authority. The revoked user cannot digitally sign anything, nor can they decrypt any information. Policy settings ensure that they cannot export personal or group keys to other systems in order to try and circumvent Administration. In short, you have seen a really effective method for implementing user revocation that prevents any misuse of cryptographic keys, and makes certain for the enterprise that when a user has been removed from the system, as of that time they are unable to use any of the services. This is because if a local keystore is present you require the user to check for a keystore before the available keystore can be used. This ensures that when you revoke a keystore and the user is offline they still cannot use the keystore when they next login.

Although other suppliers may claim to have sophisticated revocation services they are all entirely passive. The ArticSoft revocation service is immediate and effective.

Finally, we should address the question of information recovery.

In order to demonstrate this capability you need to go back to Central Manager, Logoff and then log on again.

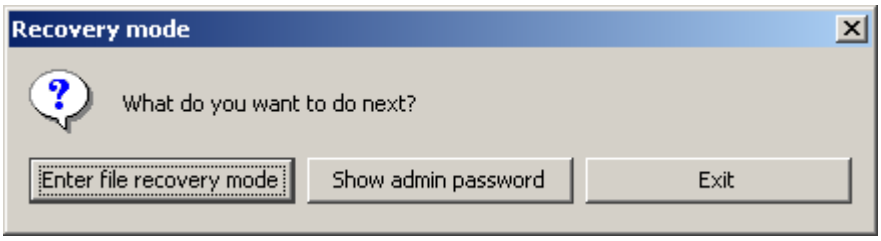
When you are logging back on to Central Manager you will see the following panel:

This time you want to click on the Information recovery tab.

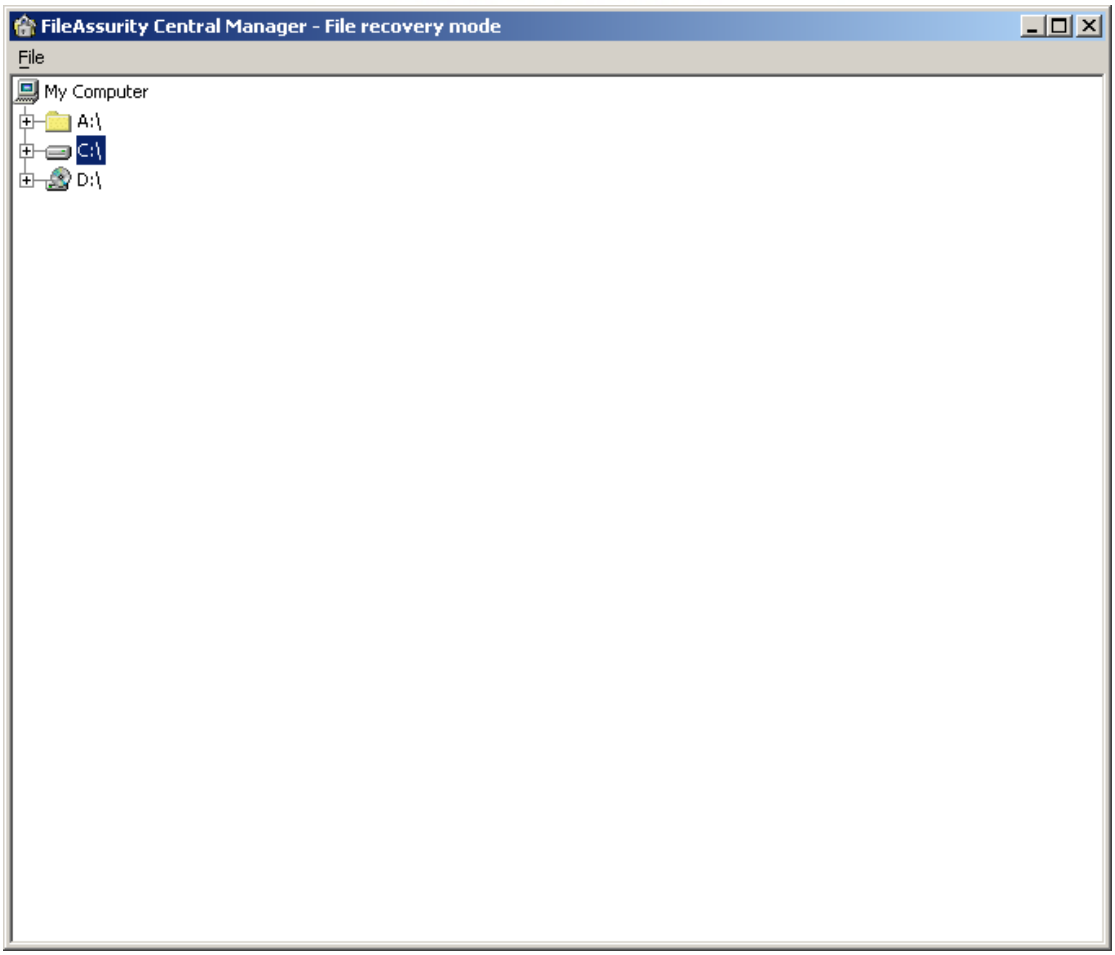
You will see that this shifts to the following panel:

This requires the two separate Administrators to enter their passwords in order to start Central Manager in its Information Recovery mode. If you remember the passwords set up when the system was initialized, they were both 1111111111.

If you enter those then you see the following panel:

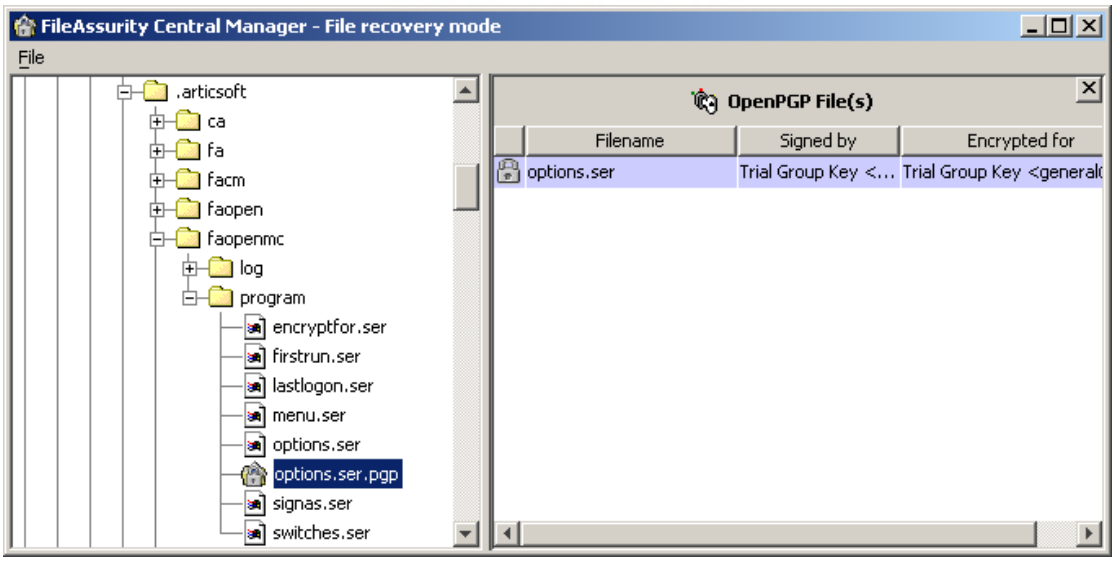


This capability allows the two other Administrators to recover the normal Administrator password or recover file or encrypted e-mail text information. If you then click on Show admin password you will be shown the password of the Central Administrator. If you click on Enter file recovery mode you will now see the following panel:

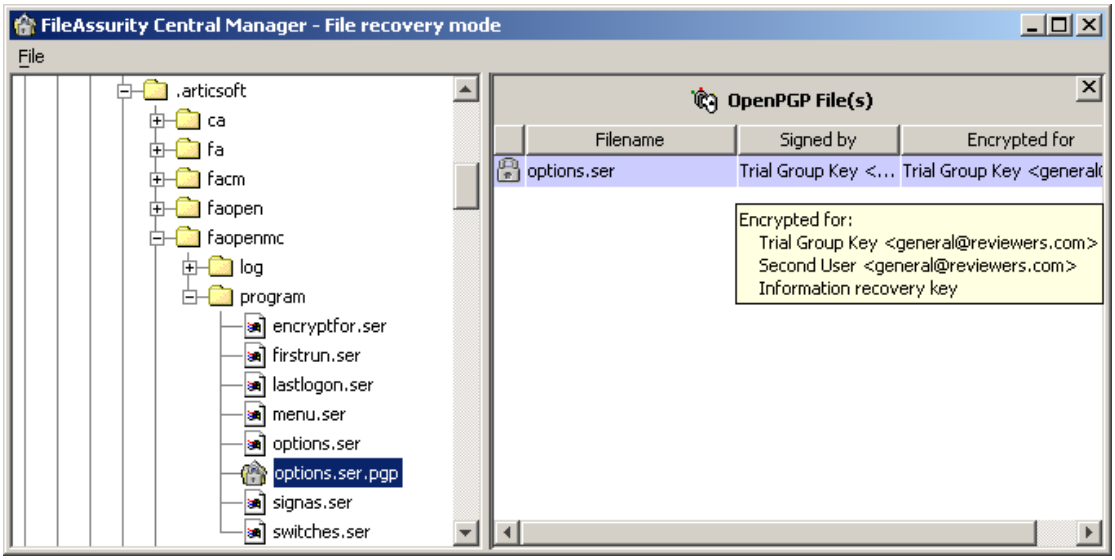


Using this panel, which acts very much like Windows Explorer, you can navigate to the file that you had encrypted with the Second User. (At the time you proved you could decrypt it seamlessly when you logged on as First User even though they did not (apparently) have a valid key.)

Having found the file through the file recovery window, you can double click on it so that you can see the signing and encryption information associated with it. In the case of our trial system the panel you will see looks like the following:

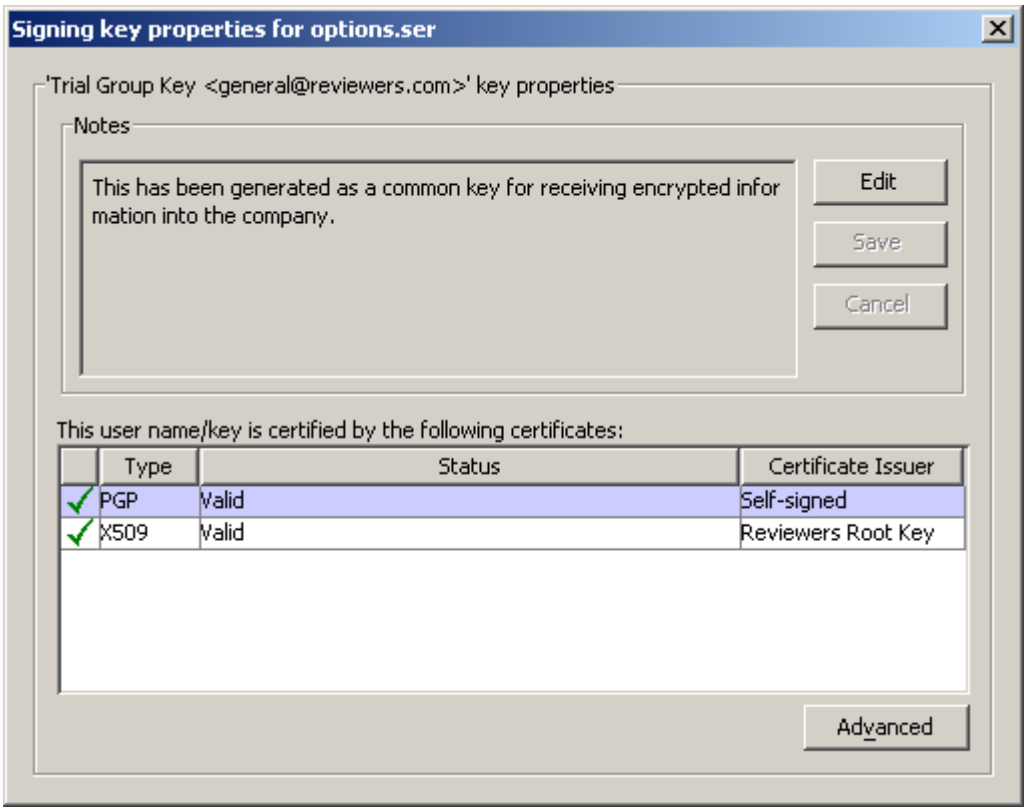


If you hold the cursor over the Encrypted for field you will see the following:



You can see at the bottom of the list that an Information recovery key has been added to the list of keys that the file was encrypted for. If you now right click on the file in the right hand panel you will see options to decrypt the file or to examine the signature on the file.

If you go ahead and decrypt the file it will ask you if you want to replace the original. If you ask about the digital signature you will see the following:



This confirms that the key is recognized, and, using the Advanced button and highlighting the X.509 certificate, you can confirm that the signature key tracks back to the root key for the installation. Double click on the file and it will then decrypt.

You have now seen information recovery working, under a dual control system so that information recovery is only performed.

There are many other capabilities that you could explore in what is a feature rich and complex product, but you have now seen the most important features of the system:

- simple to use Administration setup;
- quick implementation without complexity;
- simple implementation of Managed Client services;
- effective policy administration and implementation;
- unique critical features for effective implementation through the enterprise, including internal group capabilities and the ability of outsiders to deal with a business function as against a single internal individual;
- simple and pragmatic user revocation with immediate effect and absolute control;
- full roaming user support;
- user keystore backup and recovery;
- changes to policy and to keystores are implemented in realtime;
- user revocation is immediate and effective;
- information recovery is controlled, and really takes place;
- scalability using industrial grade products to give the performance needed for large scale implementations;

- internal communications using TCP/IP to facilitate communications efficiency;
- keystore handling using encrypted information, protecting the security and privacy of the users at all times.

You have also seen the system generating its own key pairs, importing PGP keys from versions 5 and 6, as well as being able to automatically recognize keys that have been generated by the system.

In fact, you have just seen a really effective system for the management of cryptographic keys and identities that is completely aligned to enterprise requirements and internal management and control.

Many thanks for carrying out the evaluation and review process.