Obscuring Passwords

Administering users and groups

By default, Geronimo uses AES to encode login passwords. When the server starts or when a login module starts, any unobscured password is replaced by
`{Simple}<encrypted password>`
This prevents someone from verbatim copying a password out of the `users.properties` file, and keeps your passwords available (the key is in svn even if you lose it locally) but of course anyone can look up the key and decode the password.

If you want your passwords more obscure, you will run the risk of losing your key and making all your passwords completely unusable.

In general to install a different obscuring strategy you need a GBean implementing the **org.apache.geronimo.util.Encryption interface** (in the geronimo-util module). When it starts it will register with the **EncryptionManager** and re-encrypt all the existing encrypted passwords and be used for all future password encryption and decryption.

To install this gbean, include the following code in the **rmi-naming** section of `var/config/config.xml` under `<module name="org.apache.geronimo.framework/rmi-naming/<version>/car">`:

```
<gbean name="org.apache.geronimo.framework/rmi-naming/<version> /car?name=ConfiguredEncryption,j2eeType=GBean
       gbeanInfo="org.apache.geronimo.system.util.ConfiguredEncryption">
    <attribute name="path">var/security/ConfiguredSecretKey.ser</attribute>
    <reference name="ServerInfo"><pattern><name>ServerInfo</name></pattern></reference>
</gbean>
```

where *<version>* is replaced with the version number of your Geronimo server.

This gbean configuration includes the location of the key and a reference to **ServerInfo**. The location will be resolved with respect to the server location using ServerInfo. The server will create a key the first time its started, after that it will keep using the saved key at the location specified.

If you specify another serialized SecretKeySpec in the location, the server will use that key instead. As with the default, this example uses AES algorithm.