



## IBM WebSphere Advanced Single Server Edition 4.0

Before being able to enable SSL on WebSphere, you need to have your own certificate. This certificate can be a self-certificate for testing purpose but in any production case, you should have a certificate issued by a Trusted CA. The following steps describe how to get your own certificate.

### Creating a keystore

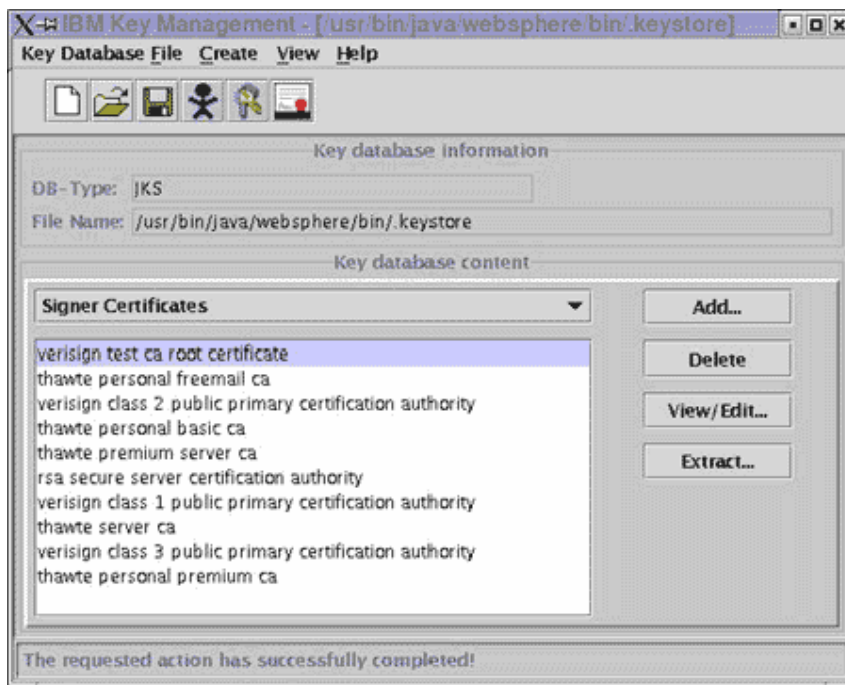
A keystore is where your private key will be saved, in a secure way, and the certificate belongs to it. This keystore can be created either with the SUN keytool or with ikeyman a tool from IBM that is distributed with WebSphere Advanced Single Server Edition 4.0.

Starting ikeyman tool

The command to start it is:

```
./ikeyman.sh
```

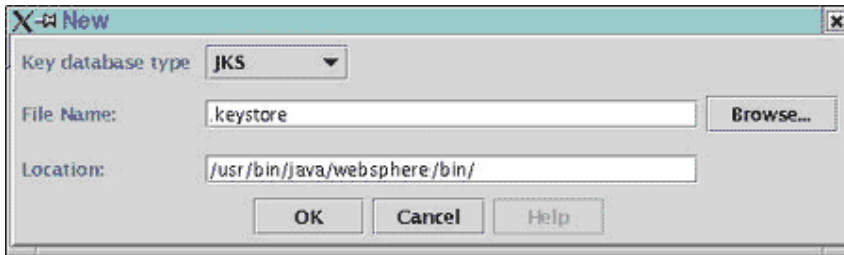
Once it is started, the following screen appears:



### Specifying a keystore

From the main application, you can either use an existing keystore or create a new one. In the example below we want to create a new keystore that will be used only by WebSphere.

In the IBM Key Management console, select the option Key Database File/New. A dialog box will appear:

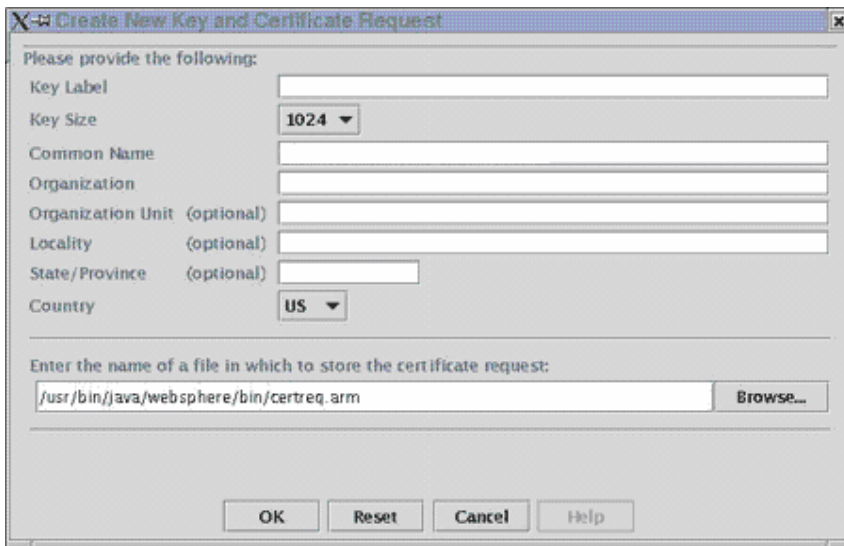


The options are:

| Option            | Value   |
|-------------------|---|
| Key database type | JKS   |
| File Name         | The name of the keystore. In the example: .keystore                       |
| Location          | The location of the keystore. In the example: /usr/bin/java/websphere/bin |

### Creating a certificate request

You first need to create a certificate request before getting your certificate. The certificate request is created in Create/New Certificate Request. A new dialog box will appear where you are asked to enter some information:



The options are:

| Option    | Value   |
|-----------|---|
| Key Label | A name that identify the request in list screen. For instance, sitecert |



|                   |  |
|-------------------|--|
| Key Size          | Use the default value of 1024  |
| Common Name       | This is the Fully Qualified Domain Name, this is what will be in the URL after (but not including) the 'http:/' and before the next '/'.<br>Example www.mydomain.com |
| Organization      | The Organization name. Example Comodo  |
| Organization Unit | The Organizational Unit. Example R&D   |
| Locality          | The locality of your organization. Example Manchester  |
| State/Province    | The province of your organization. Example Salford Quays   |
|                   | The country of your organization. Example GB   |
| Request file name | This is the name of the file where your CSR will be created.<br>In the example: /usr/bin/java/websphere/bin/certreq.arm  |

Now click on OK to generate your request. When the request is created, a key pair is also generated (a private key only stored in the keystore and a public key stored in the certificate you receive). If the request is successfully created, a dialog should inform you about it:



You will need the contents of this file when applying for your certificate