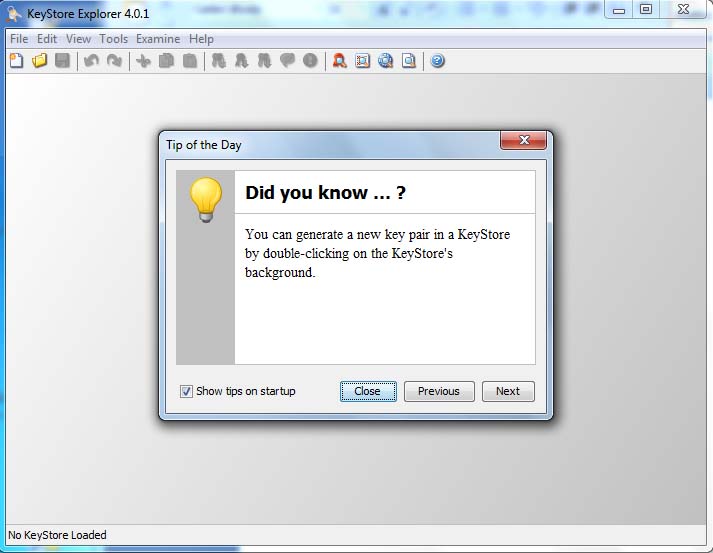
Below is a user friendly way of installing the certificate. For MobilityOne, two certificates are needed to be installed:

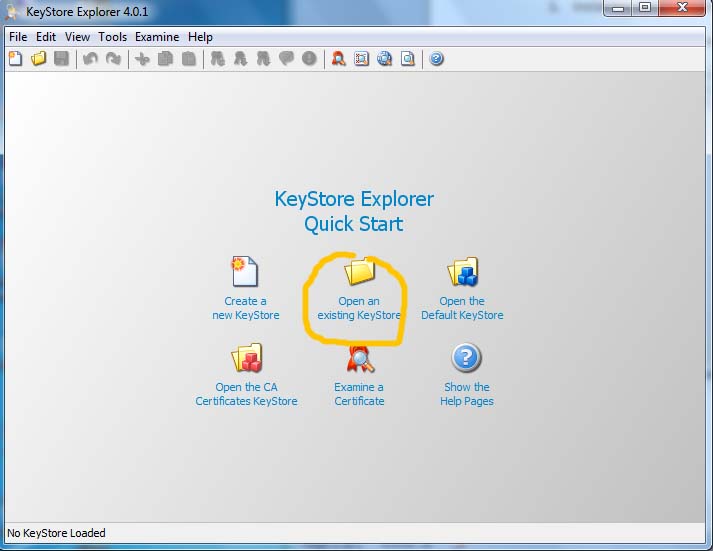
* **203.223.144.228.cer**.
* **M1\_CA.cer**

1. Copy the KFHTrust.jks from kfhib05 to your local pc
2. Install **Keystore Explorer 4.0.1** on your local pc.

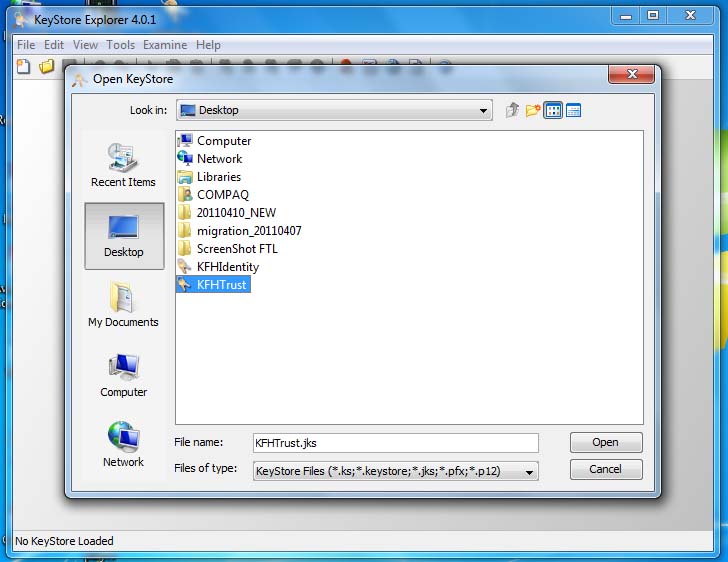
After installed, open the application. The application should look like this.



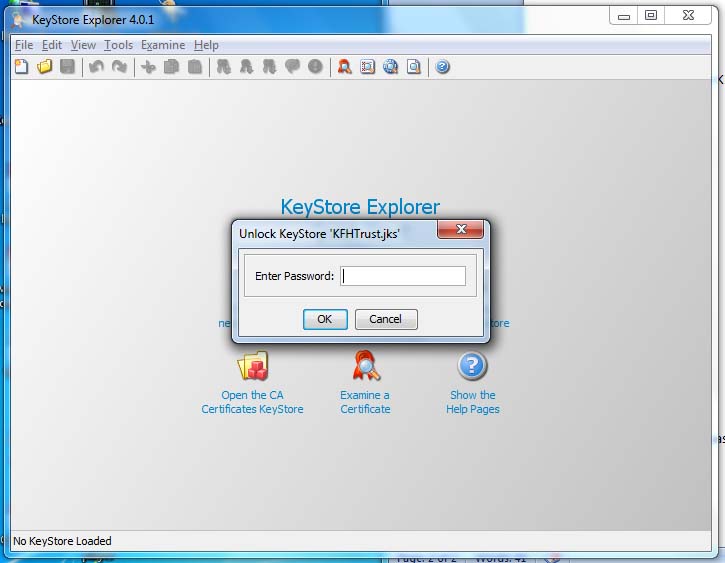
1. Click on ‘Open an existing Keystore’



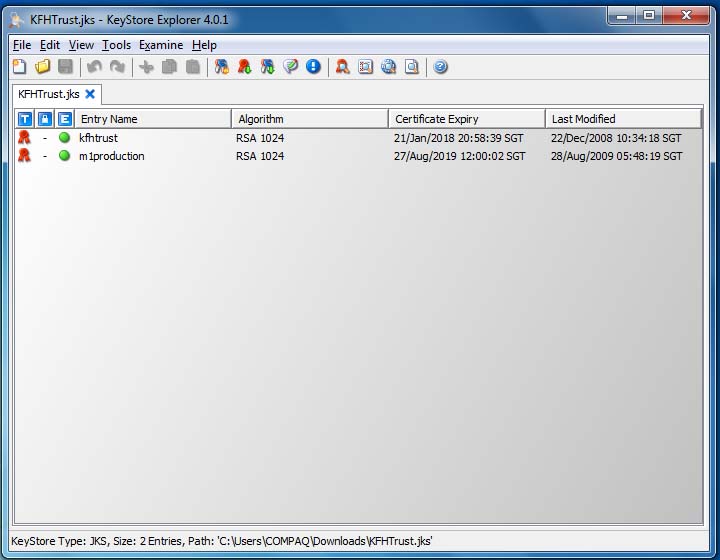
1. Choose KFHTrust.jks



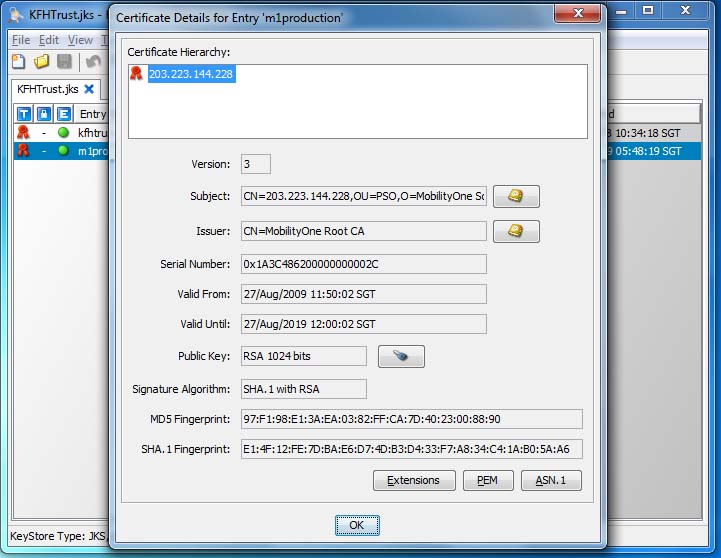
1. Enter ‘password’ as the password



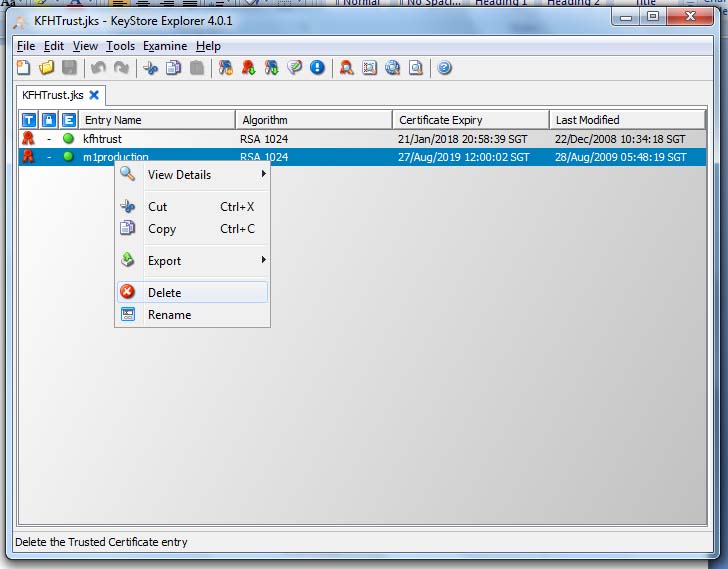
1. The application should show the list of certificates in the keystore. As you can see there are two certificates: **kfhtrust** and **m1production**.



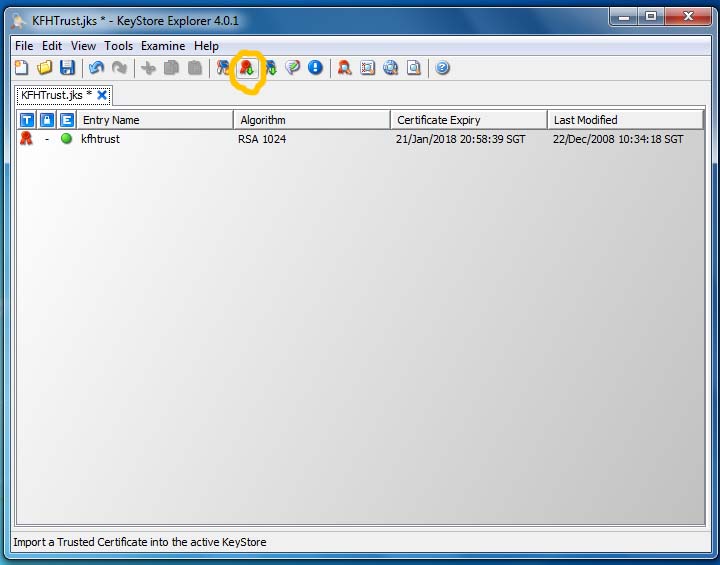
1. Double click on the **m1production** to see the certificate details



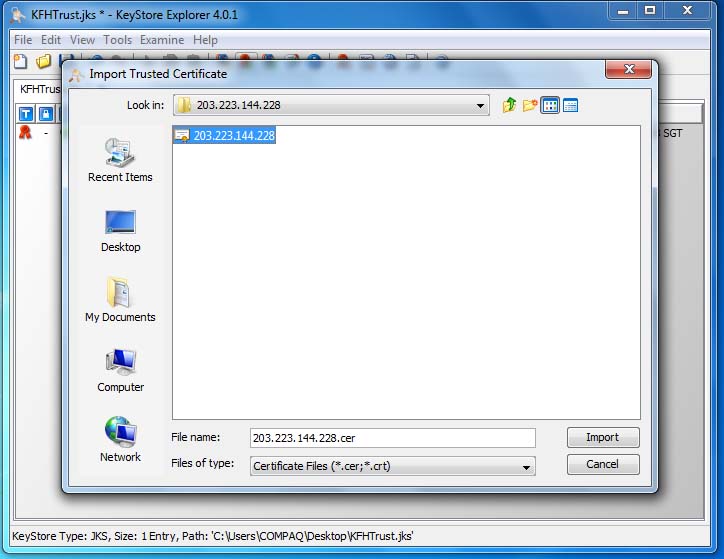
1. Click on OK. Please remember the entry name (**m1production**) as we will use the same entry name to replace the current one with the new certificate. Since we already backup the Keystore, delete the certificate **m1production** from the Keystore. Click on OK to confirm.



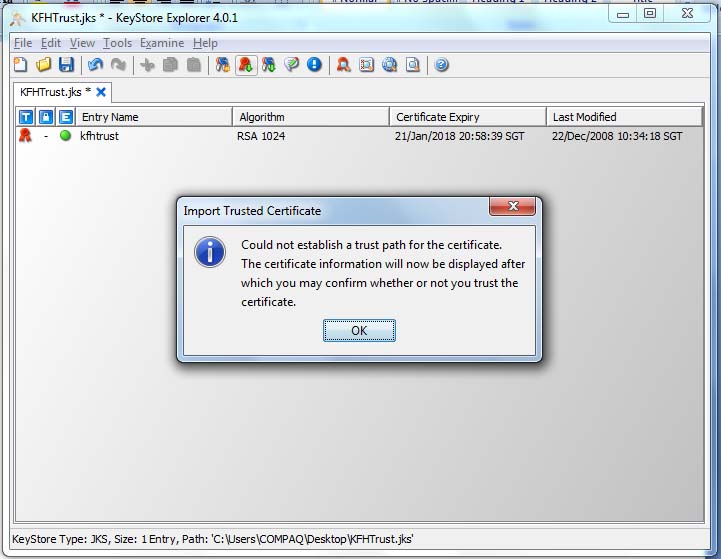
1. Click on the circled icon below to **Import Trusted Certificate** or click Tool tab and choose and click Import Trusted Certificate.



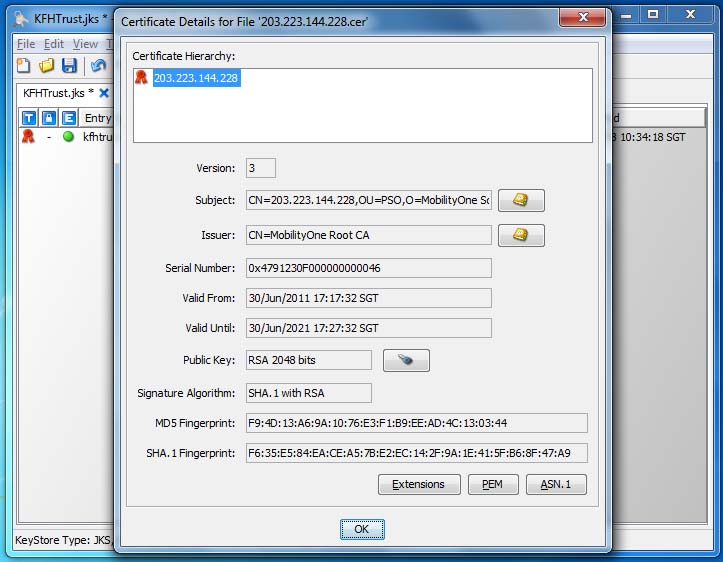
1. Browse for the updated certificate, **203.223.144.228.cer**.



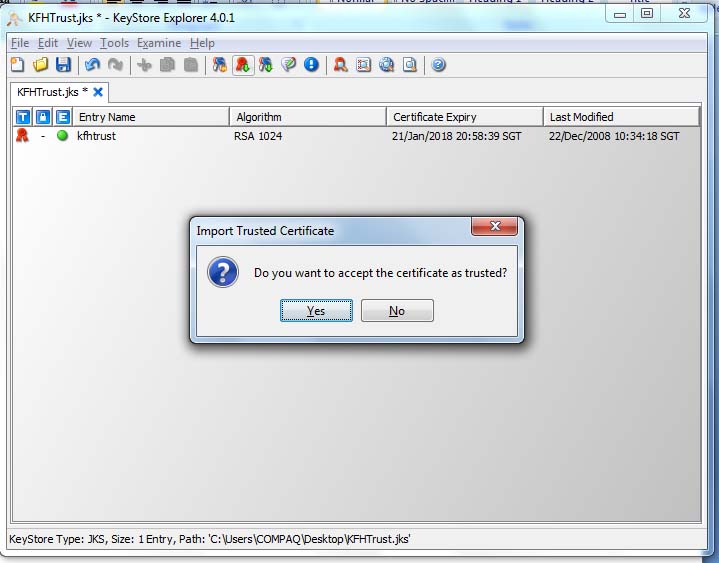
1. A pop up will appear saying that could not establish trust path. Click OK to view the details of the certificate and confirm whether to trust the certificate.



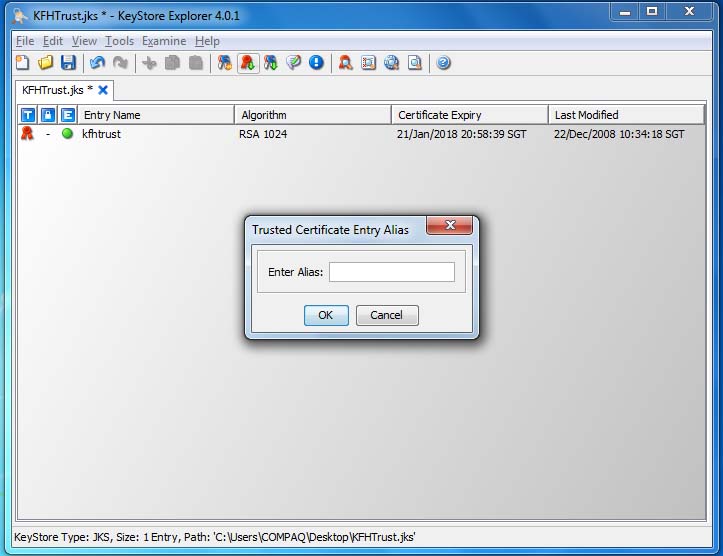
1. Check through the details and click OK to confirm the certificate.



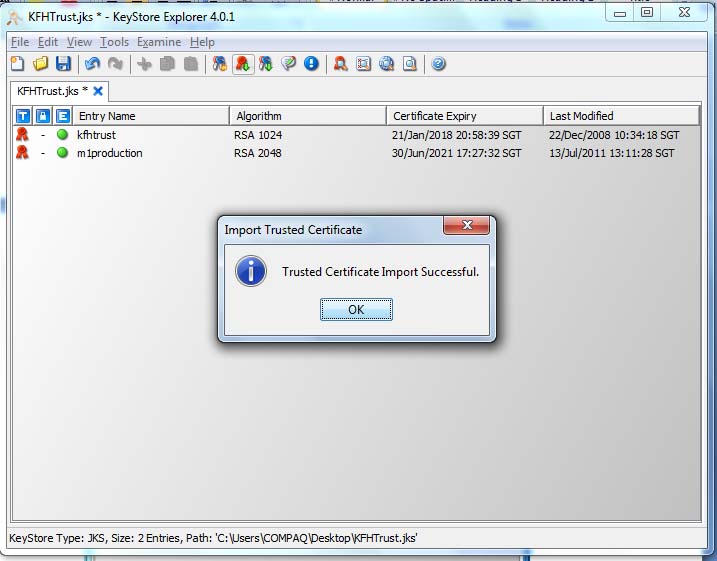
1. Click on Yes to accept the certificate as trusted



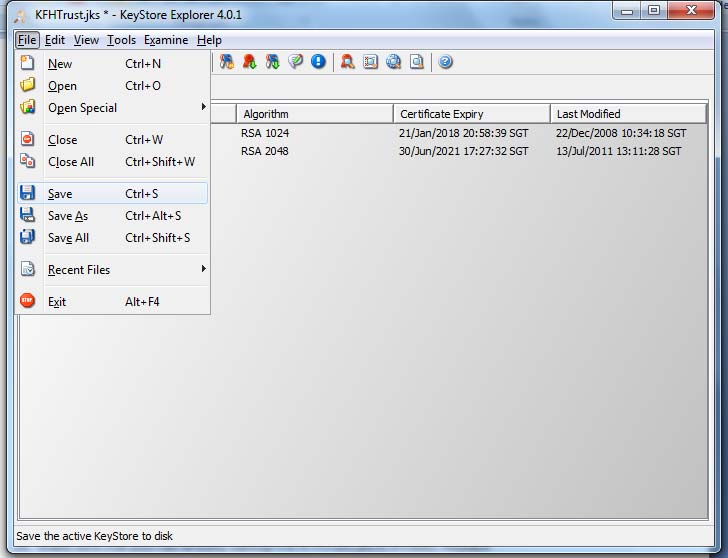
1. Enter alias name similar to the previous certificate(**m1production**)



1. The system will prompt a successful message.



1. Click on File tab and choose Save to save the Keystore.



1. Repeat Step 9 to 16 for adding another certificate, **M1\_CA.cer**
2. Make sure that you had already **backup** the KFHTrust.jks in kfhib05. Replace the old KFHTrust.jks in kfhib05 with the one we had modified.
3. Restart the SSL. Go to http://kfhib05:7001/console

1.        In the Change Center of the Administration Console, click **Lock & Edit**    
2.        In the left pane of the Console, expand **Environment** and select **Servers** .   
3.        Click the name of the server for which you want to restart SSL. First we will do on AdminServer and then ALSBServer. Click on AdminServer.  
4.        Select **Control > Start/Stop**.   
5.        In the **Server Status** table, select the check box next to the name of the server for which to restart SSL channels.   
6.        Select **Restart SSL**.

7. Repeat the whole steps for ALSBServer.

1. Test with a transaction to see whether the certificate installation is successful. If a transaction is still unable to connect to the third party (**m1**) **restarting** weblogic may be necessary.