iRIS KeyStore and TrustStore Setup

Overview: This guide will cover how to import the application server's SSL certificate into the Java Keystore and TrustStore file. This is required for interfaces such as CITI Feed, LDAPS, SSO, IMAPS, etc…

1) Prerequisites:

a. The SSL cert applied to the site in IIS
b. Need portecle.zip (can be provided by iMedRIS)
c. Need jetty.zip (can be provided by iMedRIS)

2) **<u>Note:</u> it is possible that this setup has already been completed for different interfaces. All of step two is just to check whether or not some of the requirements have been set up already.**

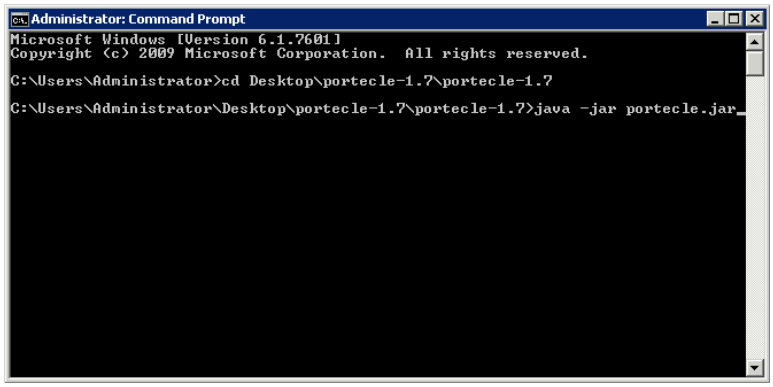
<u>Have they been configured in sa.properties?</u>

a. Open up the sa.properties file
b. Check to see if the following lines are not commented out and have a value:
    i. system.keyStore_1
    ii. system.keyStorePassword_1
    iii. system.trustStore_1
    iv. system.trustStorePassword_1
c. If there is a file path listed for system.keyStore_1 and a password listed for system.keyStorePassword_1 then the JKS file has been created and will need to be verified (follow section 3).
d. If there is a file path listed for system.trustStore_1 and a password listed for system.trustStorePassword_1 then the JKS file has been created and will need to be verified (follow section 3).

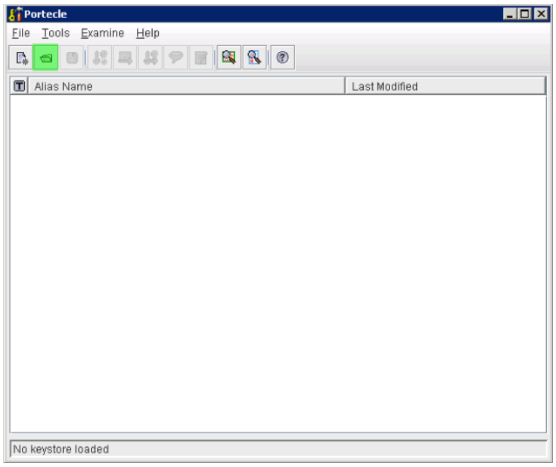
3) Verify KeyStore and TrustStore

Verify (only if the keyStore and/or trustStore exist – Otherwise skip to section 4):

a. Extract the portecle.zip file to the desktop
b. Open up the command prompt and change directory to the extracted portecle folder.
c. Run the following command:
    i. > java –jar portecle.jar

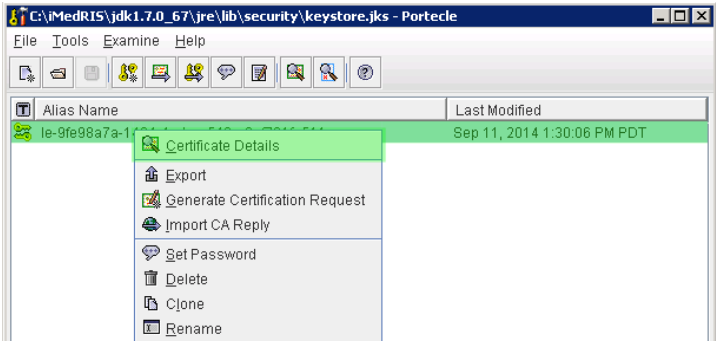


d. The portecle GUI will now open.



Verify Java KeyStore

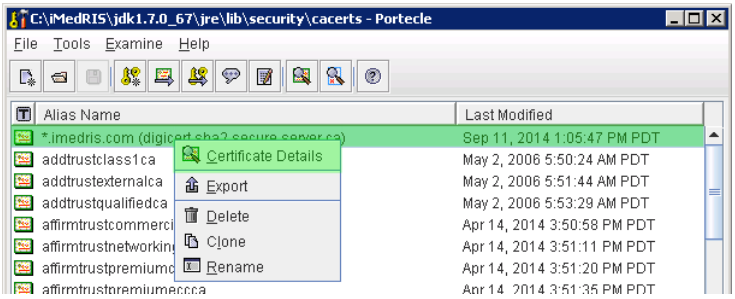
e. Click the open button (highlighted above) and select the file path for the system.KeyStore_1
f. Enter the system.keyStorePassword_1 when prompted for the password
g. Once the key-store has been opened there should be a key-pair.
    i. Right click and select certificate details



ii. Make sure that the certificate is the SSL certificate for the application server.

Verify TrustStore

h. Click the open button and select the file path for the system.trustStore_1
i. Enter the system.trustStorePassword_1 when prompted for the password
j. Once the trust-store has been opened you will find many certificates that have been imported
    i. Sort by date and look at the newest cert
    ii. Right click and select certificate details



iii. Make sure that the certificate is the SSL certificate for the application server.

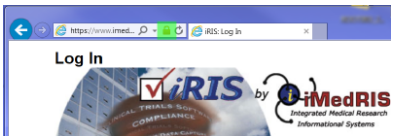
If both of the above have been verified to have the SSL certificate for the URL in it, then interfaces should work over HTTPS when configured and the rest of the guide can be skipped.

4) TrustStore Setup Pre-req:

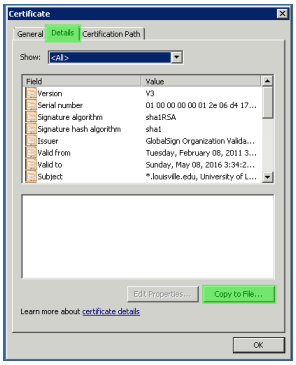
Download the .cer from the SSL protected site:

a. Navigate to the iRIS site that the interface is being set up on

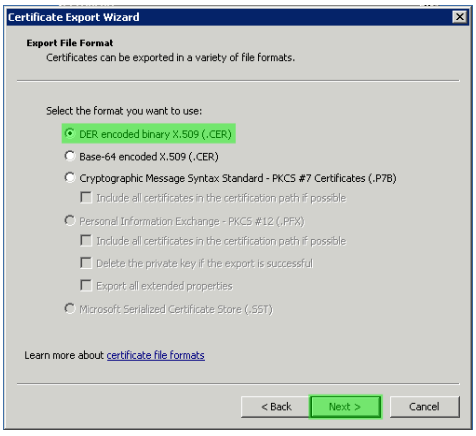
b. Click the lock icon and select view certificate



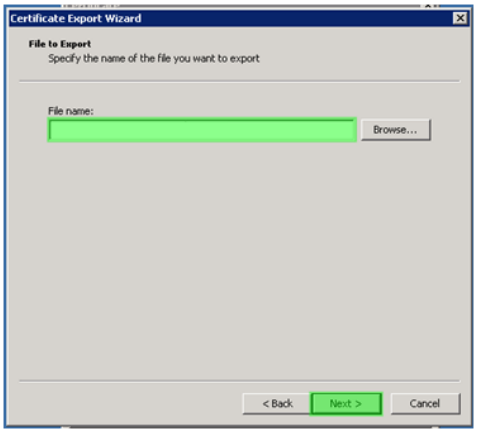
c. Select the Details tab and then click the Copy to File button

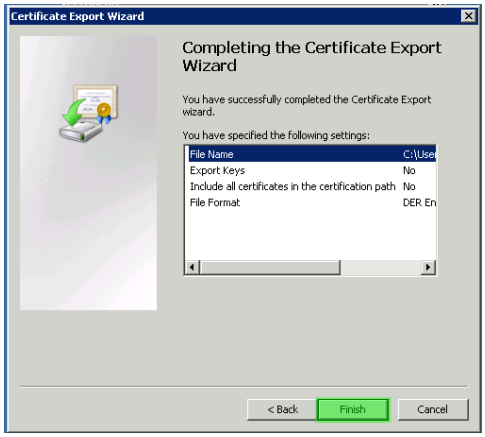


d. In the window that opens, select the DER encoded binary X.509 (.CER) option.



e. Choose where to save to file. Click next and then click finish on the following page.

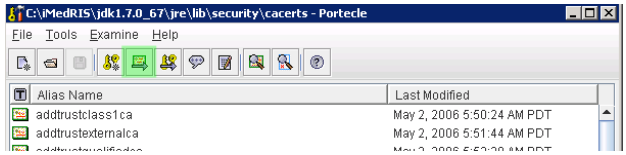

Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
< Back
Next >
Cancel


Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name
Export Keys
Include all certificates in the certification path
File Format
No
No
DER En
< Back
Finish
Cancel

5) Import into TrustStore

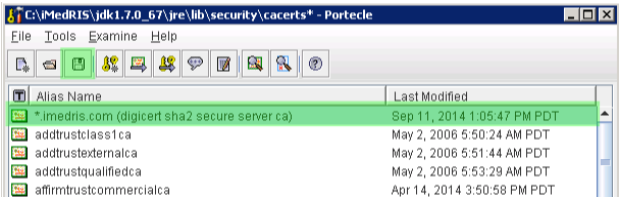
a. Using Portecle, open the TrustStore:
   i. Default Path: %IMEDRIS_HOME%\jdk*\jre\lib\security\cacerts
   ii. Default Password: changeit

b. Click the certificate import button



c. Select the DER converted file (from the previous section) and import.

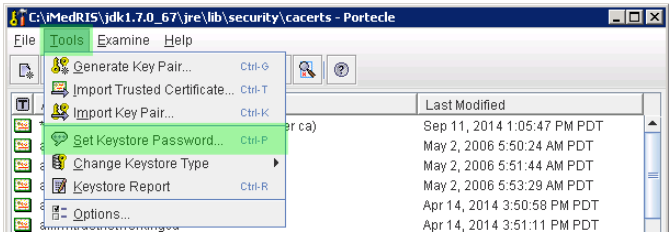
d. Once the file is imported click the Save button



6) Add the TrustStore to the sa.properties file

First change the password:

a. With the TrustStore already open, go to Tools Set Keystore Password



b. Enter the new password and then save the KeyStore.

c. Change to the %IMEDRIS_HOME%\jdk*\jre\lib\security directory.

Add to sa.properties:

d. Add the %IMEDRIS_HOME%\jdk*\jre\lib\security\cacerts path to the system.trustStore_1 property. Make sure that there are two '\' for every 1 '\' in the path

   i. Ex: C:\iMedRIS_jdk1.7.0_67\jre\lib\security\cacerts C:\\iMedRIS\\ jdk1.7.0_67\\jre\\lib\\security\\cacerts

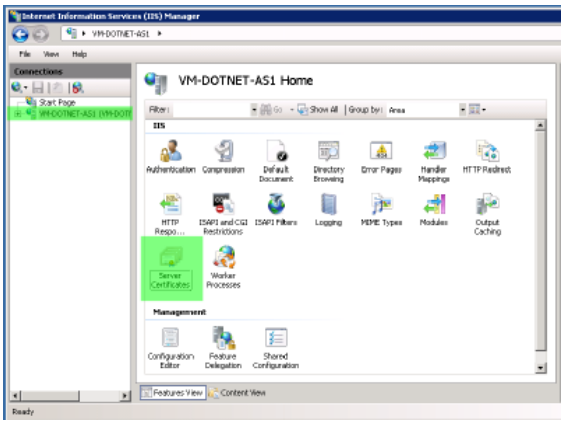
e. Add the password used for the cacert trustStore password to the system.trustStorePassword_1 property.

7) JKS pre-req – Get certificate in .PFX format

This can be skipped if you already have the application server's cert in .PFX format.

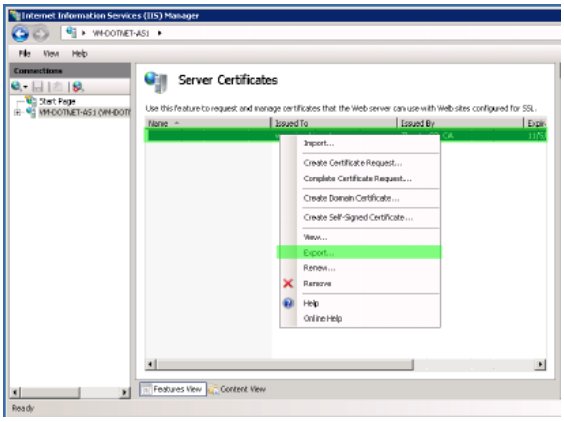
a. Open up IIS on the application server

b. Select the server name in the right pane and then double-click on Server Certificates in the middle pane

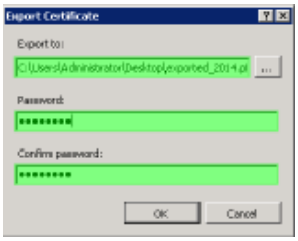


c. Right-click the certificate used for the website and select Export…

i. Note: Some certificates do not allow export – you must obtain the .PFX SSL certificate and a password for it from someone at your institution

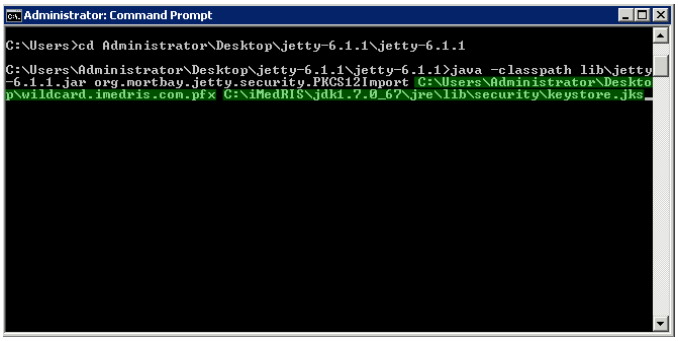


d. Enter the filename and path for the .PFX file to be exported and assign it a password



8) Create the Java Key Store using Jetty

a. Extract the Jetty.zip onto the desktop
b. Open up command line and change directory to the extracted folder.
c. Run the following command:
    i. > java -classpath lib\jetty-6.1.1.jar org.mortbay.jetty.security.PKCS12Import <cert_pfx_file_path> %IMEDRIS_HOME%\jdk*\jre\lib\security\keystore.jks
        1. Input keystore passphrase = <password when exporting the cert from IIS or converting key to .pfx format>
        2. Output keystore passphrase = <choose password>



d. Add the %IMEDRIS_HOME% \jdk* \jre\lib \security\<keystore>.jks path to the system.keyStore_1 property. Make sure that there are two '\' for every one '\' in the path
    i. Ex: C:\iMedRIS_jdk1.7.0_67\jre\lib\security\keystore.jks C:\\iMedRIS\\ jdk1.7.0_67\\jre\\lib\\security\keystore.jks
e. Add the password used for the keyStore to the system.keyStorePassword_1 property.

9) Restart iRIS