How to add an SSL Certificate

The following instructions can be used to create an SSL Certificate to be used by the kLink Server Application. An HTTPS secure connection for a server requires a Certificate. You can either obtain a Certificate through a public Certificate Authority (CA) or create your own local CA. If you will be using kLink with users outside of your company, we recommend that you use a third-party Certificate Authority. Otherwise browsers may give the users warning that the Certificate Authority was not trusted.

Note: You should follow the instructions for *Creating an SSL Application* for kLink before adding a Certificate.

___ Step 01 Start the HTTP Administration Server

If the HTTP Administration Server is not already active, you will have to start it, as follows:

Enter: STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

___ Step 02 Sign On to the Administration Server

You will use a web browser to access the HTTP Administration Server.

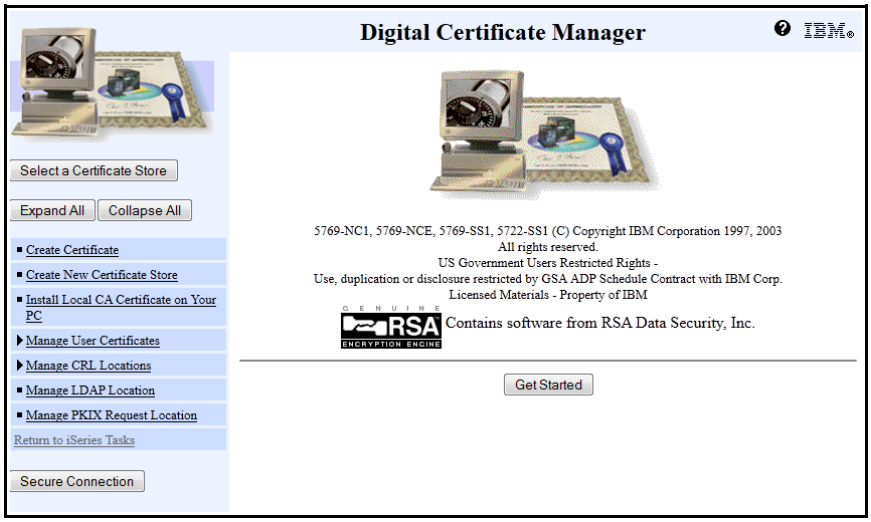
1. Start a web browser.
2. Set your browser to access - **HTTP://your_ibm_i:2001/HTTPAdmin** (case-sensitive)
3. Sign on to the HTTP server as a Security Officer. A number of applications should appear, as shown below:

___ Step 03 Start the Digital Certificate Manager

If you do not see this icon on the IBM i tasks page, you may have to use GO LICPGM option 11 to install the OS/400 option 34 (Digital Certificate Manager) and you must install one of the cryptographic access provider products on your system before using the Digital Certificate Manager (DCM) functions.

Or, you may have to select "Related Links" to find the Digital Certificate Manager.

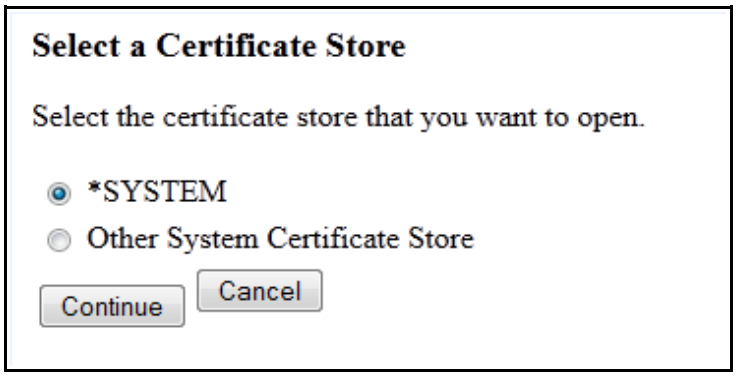
If everything has been installed, you should see the following screen with a list of tasks that you can perform on the left.



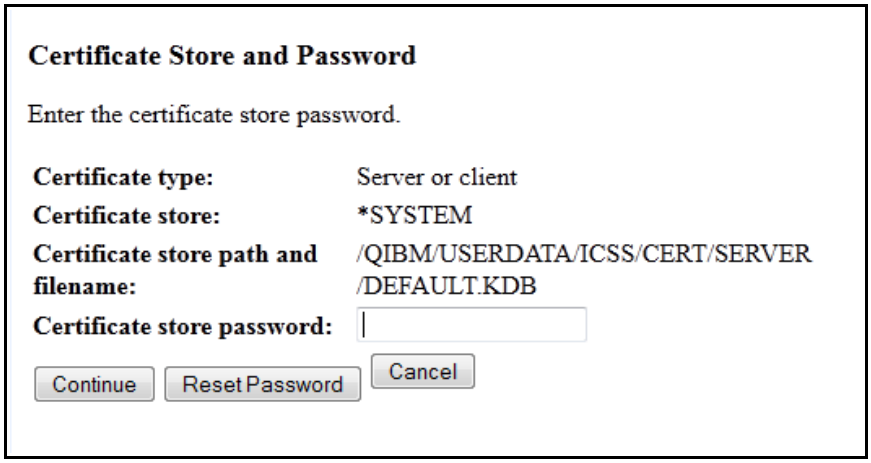
___ Step 04 Select the *SYSTEM Certificate Store

The kLink application will use the *SYSTEM Certificate Store. It should already exist so you can select it.

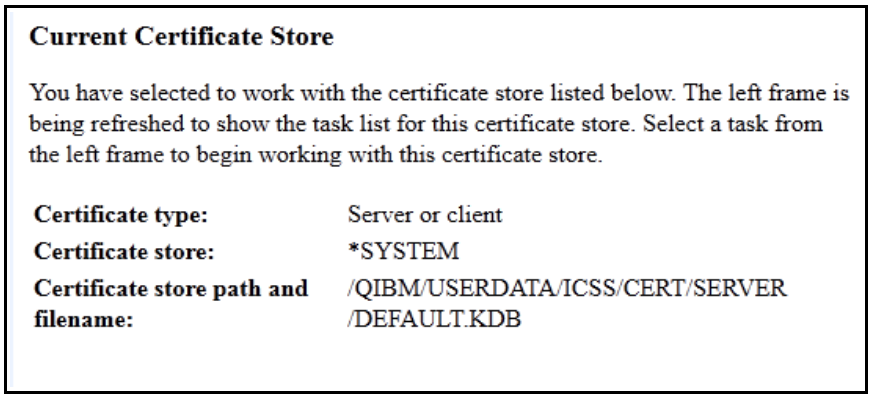
1. Press the **Select a Certificate Store** task on the left side of the screen.
2. Select the ***SYSTEM** store and press **Continue**.



3. The ***SYSTEM** Store will ask for a Password.



4. Type the password for the store and press **Continue**.



When you create a ***SYSTEM** store, the DCM uses a fixed location in the IFS to store the keys. They are located in the following objects:

/QIBM/USERDATA/ICSS/CERT/SERVER: Directory

DEFAULT.KDB: Digital certificate database file

DEFAULT.RDB: Certificate request file

___ Step 05 Create a Certificate

If you do not already have a certificate that can be used by kLink, you will need to create one.

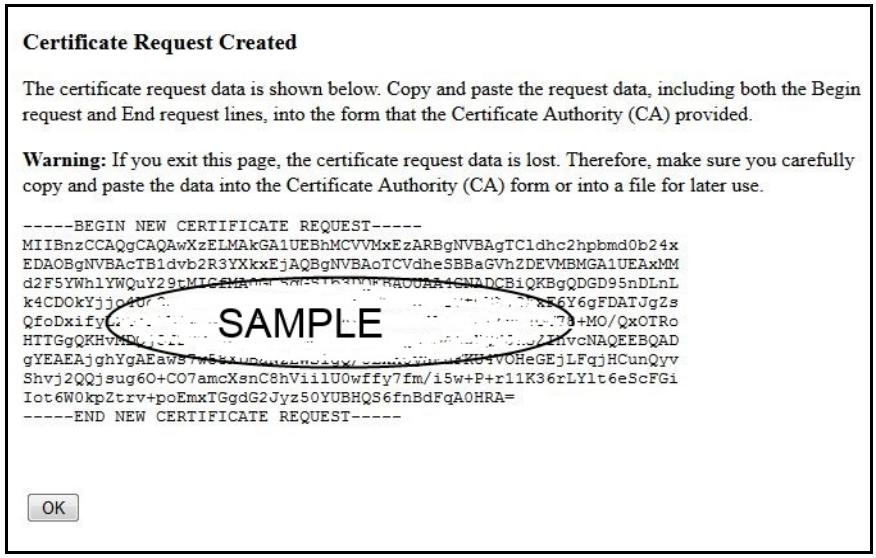
1. Press the **Create Certificate** task on the left side of the screen.

2. Select **Server or client certificate** and press **Continue**.

3. Select **VeriSign or other Internet Certificate Authority (CA)** and press **Continue**.

4. Fill out the **Certificate Information** for the new certificate and press **Continue**. You may use the Help (?) key to find information about each of the fields.

5. A **Confirmation** page will be displayed.



Certificate Request Created

The certificate request data is shown below. Copy and paste the request data, including both the Begin request and End request lines, into the form that the Certificate Authority (CA) provided.

Warning: If you exit this page, the certificate request data is lost. Therefore, make sure you carefully copy and paste the data into the Certificate Authority (CA) form or into a file for later use.

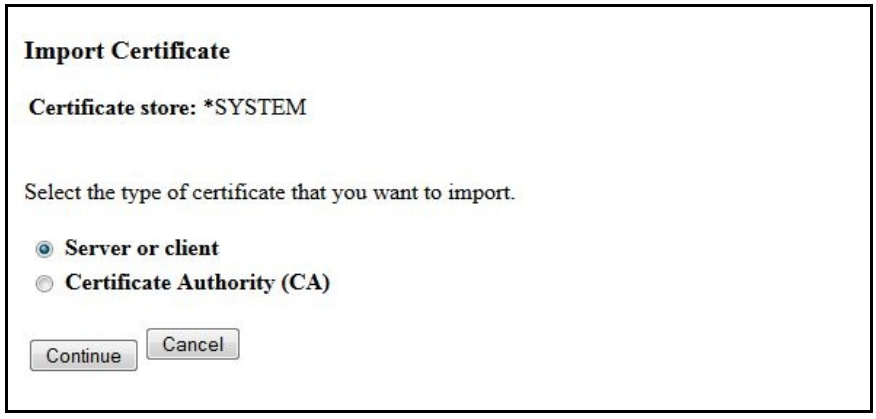
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBnzCCAQgCAQAwXzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24x
EDAOBgNVBAcTB1dvb2R3YXkxEjAQBgNVBAoTCVdheSBBaGVhZDEVMBMGA1UEAxMM
d2F5YWhlYWQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGD95nDLnL
k4CDOkYjjo4U
QfoDxify
HTTGgQKHvMD
gYEAEAjghYgAEaWs7w5
Shvj2QQjsug6O+CO7amcXsnC8hVi1lU0wffy7fm/i5w+P+r11K36rLYlt6eScFGi
Iot6W0kpZtrv+poEmxTGgdG2Jyz50YUBHQS6fnBdFqA0HRA=
-----END NEW CERTIFICATE REQUEST-----
```

SAMPLE

OK

6. Copy and paste this CSR data into a file to save it. This same CSR data will be copied into a file or form for the public CA that you have chosen to issue and sign your certificate.

7. When you receive the signed and completed certificate from the public CA, select the ***SYSTEM** certificate store, again. Then, select **Manage Certificates** in the navigation frame and use the **Import certificate** task to receive the completed certificate into the store. Press **Continue**.



Import Certificate

Certificate store: *SYSTEM

Select the type of certificate that you want to import.

- (•) **Server or client**
- ( ) **Certificate Authority (CA)**

Continue Cancel

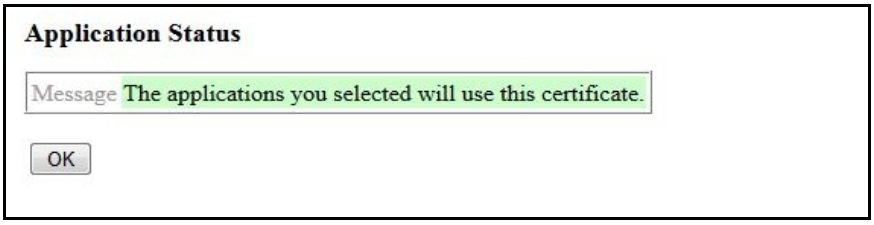
8. Enter the qualified path and filename of the file that contains the certificate to import and press **Continue**.

___ Step 06 Assign the Certificate to the kLink Server

kLink will have an application created for it to be used with an SSL session.

1. Expand the **Manage Certificates** task on the left side of the screen.

2. Press the **Assign certificate** task.
3. Select a certificate and press the **Assign to Applications** button.
4. Select the desired **kLink** Application and press the **Continue** button.



End of Adding an SSL Certificate

This concludes the process of adding and/or selecting a Certificate to be used by the kLink Server Application. If you have not been able to complete these instructions, please contact Computer Keyes for assistance. We would be happy to help you.

Computer Keyes
Technical Support
Toll free: (800) 356-0203 US & Canada Only
Voice: (425) 776-6443
Fax: (425) 776-7210
E-mail: support@ckeyes.com