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 thirdparty 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:

IBM Web Administration for iSeries Configure HTTP servers, application servers and deploy applications iSeries Navigator URL Advisor Learn how to add OS/400 administration tasks into your web applications Digital Certificate Manager Create, distribute, and manage Digital Certificates IBM Directory Server for iSeries Administer the IBM Directory Server IBM IPP Server for iSeries Configure the IBM IPP Server Cryptographic Coprocessor Configure the cryptographic coprocessor iSeries Web-Based Help Server Administer the iSeries Web-based help server

____ 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**.

Select a Certificate Store
Select the certificate store that you want to open.
 *SYSTEM Other System Certificate Store Continue

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

Certificate Store and Pas	sword
Enter the certificate store pass	word.
Certificate type:	Server or client
Certificate store:	*SYSTEM
Certificate store path and filename:	/QIBM/USERDATA/ICSS/CERT/SERVER /DEFAULT.KDB
Certificate store password:	
Continue Reset Password	Cancel

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

Current Certificate Store

You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.

Certificate type:	Server or client
Certificate store:	*SYSTEM
Certificate store path and	/QIBM/USERDATA/ICSS/CERT/SERVER
filename:	/DEFAULT.KDB

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 C

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.

Select a Certificate Store
Expand All Collapse All
Fast Path
<u>Create Certificate</u>
<u>Create New Certificate Store</u>
Install Local CA Certificate on Your PC
Manage Certificates
Manage Applications
Manage Certificate Store
Manage CRL Locations
 Manage LDAP Location
 Manage PKIX Request Location
Return to iSeries Tasks
Secure Connection

2. Select Server or client certificate and press Continue.

Create Certificate	
Select the type of certificate that you want to create	e.
Server or client certificate	
Server or client certificate for another iSerie	es
O User certificate	
Continue	

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

Select a Certificate Authority (CA)
Certificate type: Server or client
Certificate store: *SYSTEM
Select the type of Certificate Authority (CA) that will sign this certificate.
O Local Certificate Authority (CA)
VeriSign or other Internet Certificate Authority (CA)
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.

Create Certificate		
Certificate type: Ser	ver or client	
Certificate store: *S	YSTEM	
Use this form to create	e a certificate in the certificate store	e listed above.
Key size:	1024 - (bits)	
Certificate label:	WAYAHEAD_CERTIFICATE	(required)
Cer Common name:	tificate Information	(required)
Organization unit: Organization name:	Way Ahead	(required)
Locality or city:	Woodway	
State or province:	Washington	(required:minimum of 3 characters)
Country or region:	US (required)	
Continue		

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 MIIBnzCCAOgCAOAwXzELMakGA1UEBhMCVVMxEzARBgNVBAgTC1dhc2hpbmd0b24x
EDAOBgNVBAcTB1dvb2R3YXkxEjAQBgNVBAoTCVdheSBBaGVhZDEVMBMGA1UEAxMM
A2r51Wh11WQu129thLenner Sole Contraction BAGOURATEMADUB1QKBGQDGD95hDLhL
gYEAEAjghYgAEaws7w55xupcuterusyy/
Shvj2QQjsug60+C07amcXsnC8hViilU0wffy7fm/i5w+P+r11K36rLYlt6eScFGi Iot6W0kpZtrv+poEmxTGgdG2Jvz50YUBHOS6fnBdFgA0HRA=
END NEW CERTIFICATE REQUEST
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	
Ocertificate Authority (CA)	
Cancel	

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

Certificate type: Server of c	lient
Certificate store: *SYSTEN	4
Specify the fully qualified pa	th and file name of the certificate that you want to import
Example path and file name:	MYDIRECTORY/MYFILE.EXT
Import file:	

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.

Select a Certificate Store
Expand All Collapse All
Expand: a consport a
▶ <u>Fast Path</u>
<u>Create Certificate</u>
<u>Create New Certificate Store</u>
Install Local CA Certificate on Your
PC
▼Manage Certificates
View certificate
Renew certificate
Import certificate
Export certificate
Delete certificate
 Validate certificate
Assign certificate
Check expiration
 Set CA status
Update CRL location assignment
 Assign a user certificate
A Martingian

- 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.

Application Status
Message The applications you selected will use this certificate
ОК

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