How to create an SSL Application

The following instructions can be used to create an SSL Application Identifier for KeyesMail. If you would like KeyesMail to use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to make a secure connection with your mail servers, an SSL Application Identifier will be required.

The following installation procedure will require that you have enough authority to be able to start the HTTP Administration Server and to use the DCM (Digital Certificate Manager) to create a Certificate Store and an SSL Application Identifier.

___ 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.

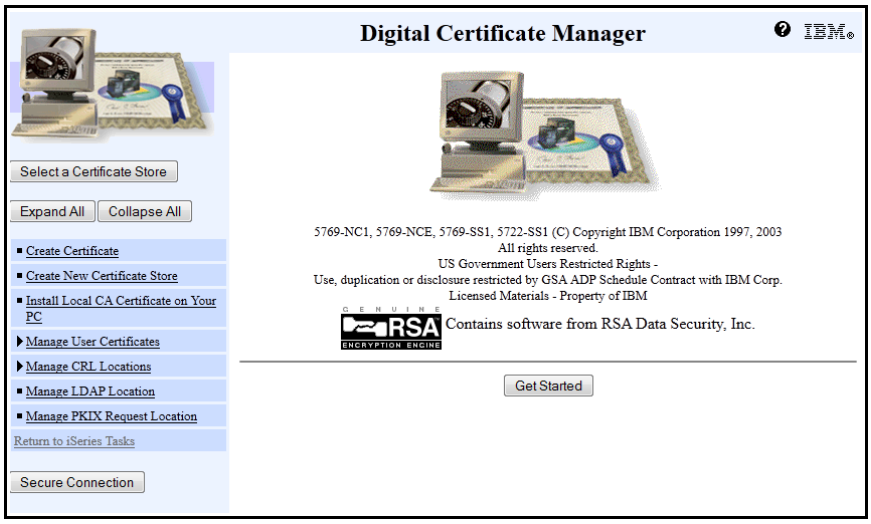
1. Start a web browser.
2. Set your browser to access - **HTTP://your_ibm_i:2001/HTTPAdmin** (case-sensitive)
3. Sign on to the HTTP server as a Security Officer. A number of applications should appear, as shown below:

___ Step 03 Start the Digital Certificate Manager

If you do not see this icon on the AS/400 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 choose "Related Links" to find the Digital Certificate Manager.

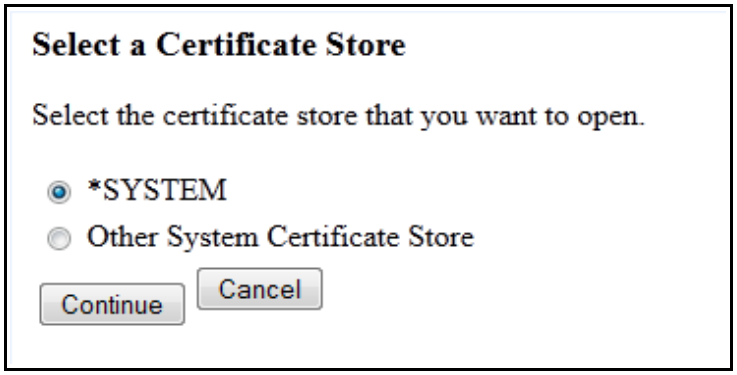
If everything has been installed, you should get to the following screen with a list of tasks that you can perform on the left.



___ Step 04 Select or Create the *SYSTEM Certificate Store

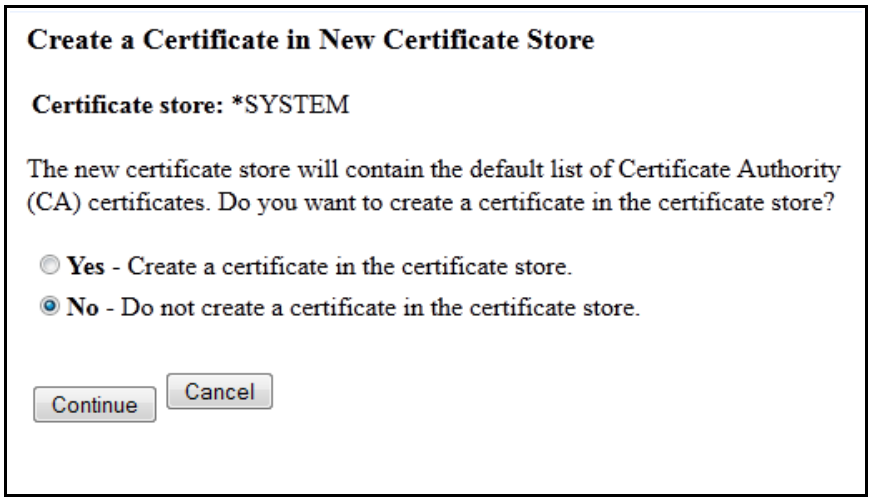
The KeyesMail application will use the *SYSTEM Certificate Store. If it already exists you may select it now. Otherwise, you must create the *SYSTEM store.

1. Press the **Select a Certificate Store** task on the left side of the screen.
2. Select the ***SYSTEM** store. If you do not see it, you must create it.

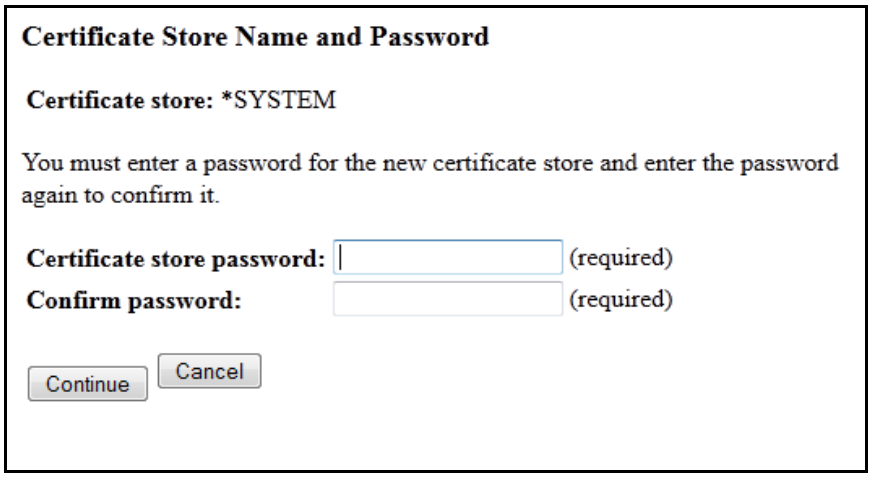


3. If you do not see the ***SYSTEM** store, you must create it. To do this press the **Create New Certificate Store** task on the left side of the screen.

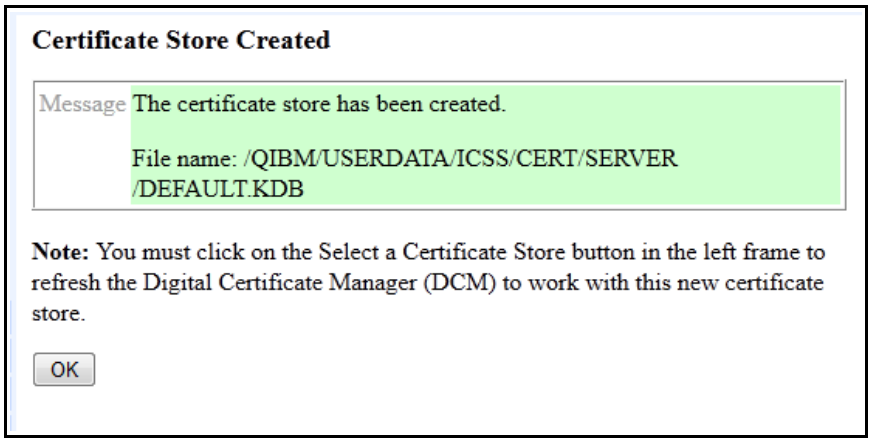
4. Select ***SYSTEM** and press **Continue**.



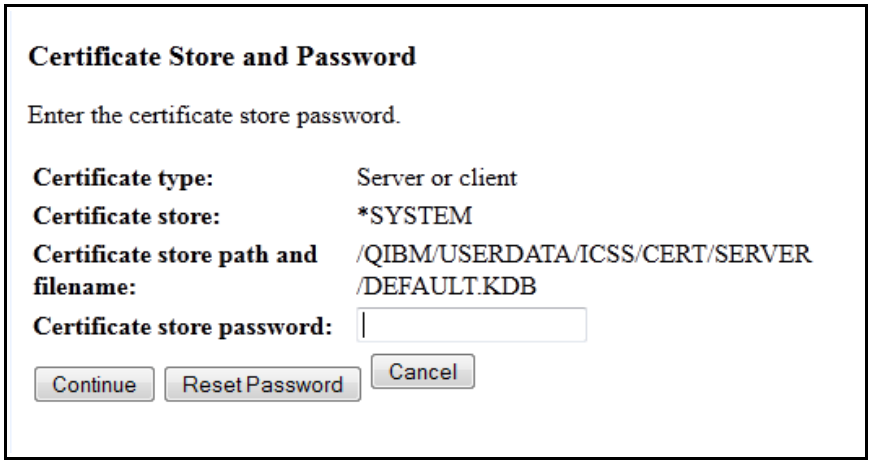
5. Press **Continue**. We do **not** need to create a certificate in the store.



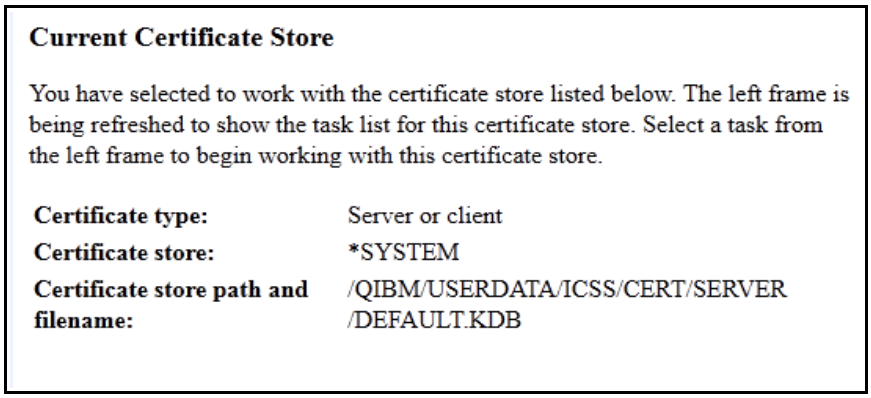
6. Enter a **password** for the store and confirm it, then press **Continue**. Please note that passwords are *case sensitive*.



7. Now you can use **Select a Certificate Store** to select the ***SYSTEM** store.



8. 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

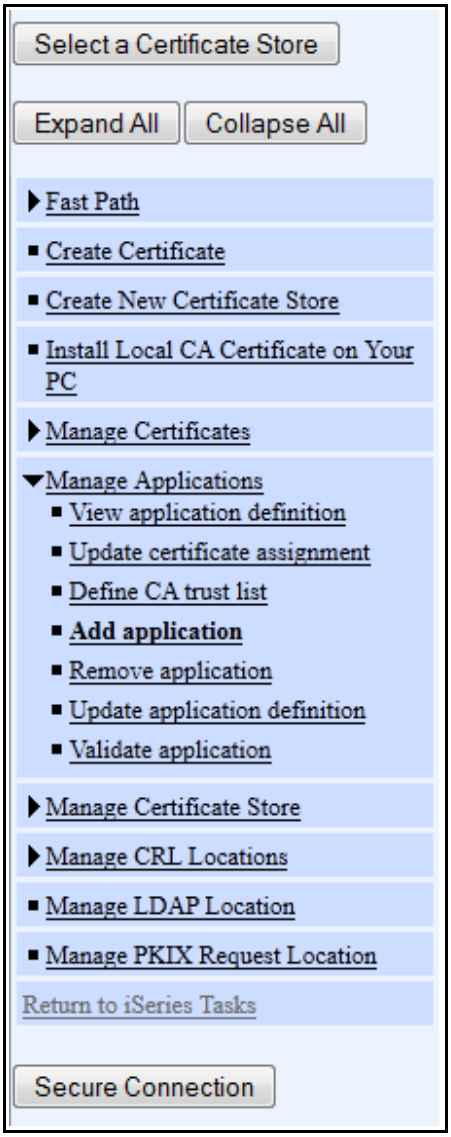
DEFAULT.KDB: Digital certificate database file

DEFAULT.RDB: Certificate request file

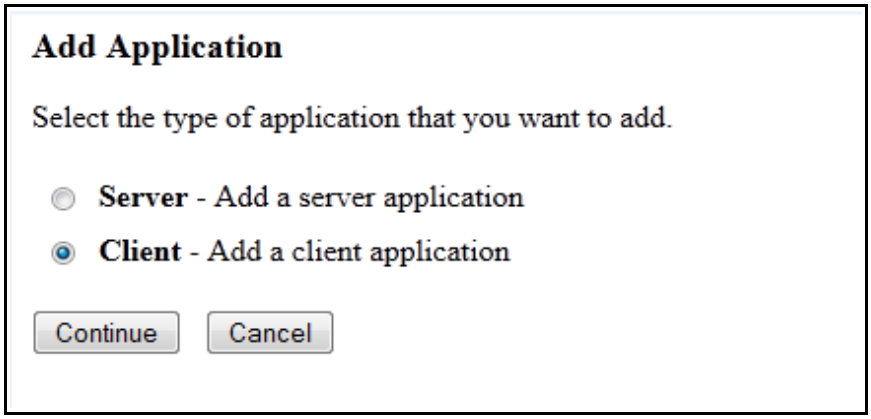
___ Step 05 Create the KeyesMail Client Application

KeyesMail must have an application created for it in order to start an SSL session.

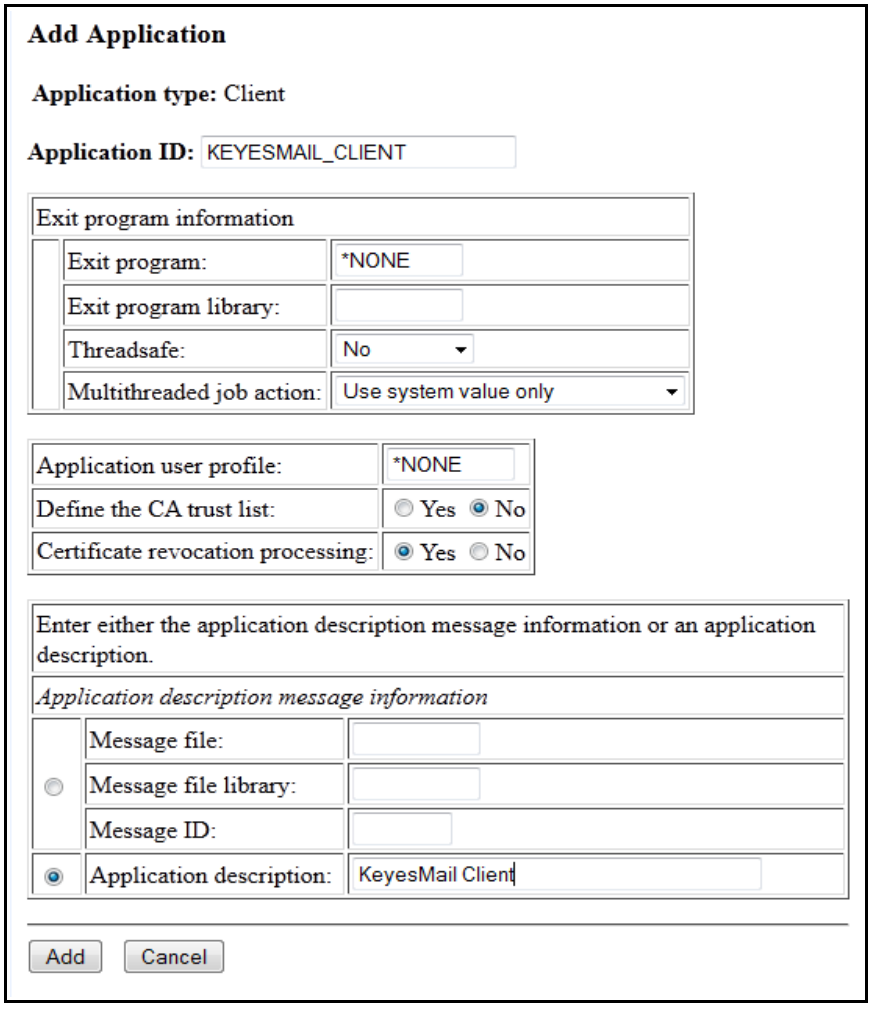
1. Expand the **Manage Applications** task on the left side of the screen.



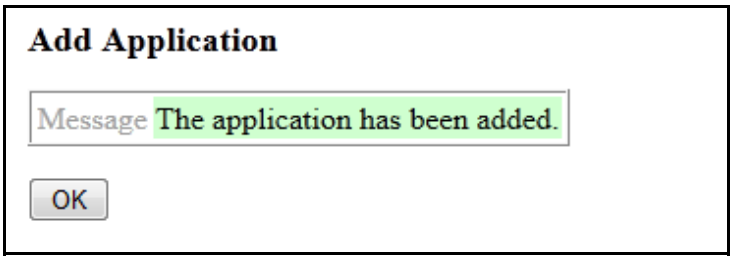
2. Press the **Add application** task.



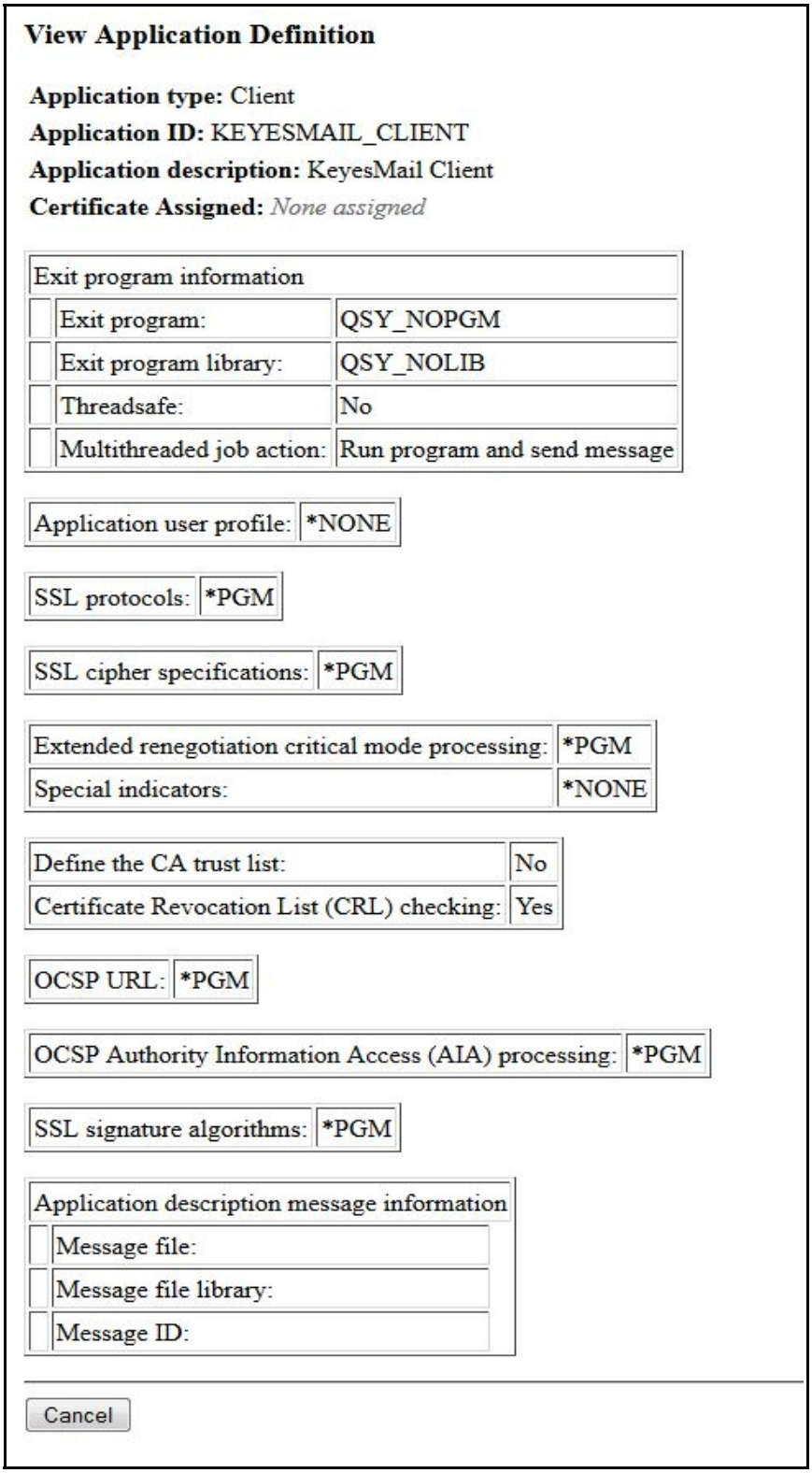
3. Select **Client** and press **Continue** to create a client application. Different versions of the operating system will have this data in different orders on the screen. Leave all other questions to their default values (usually *PGM). The **Application ID** must be entered exactly as shown. (case-sensitive)



4. Fill out the **Application ID** and the **Application description** as shown above and press **Add** to add the **KeyesMail Client** application. Leave all other questions to their default values (usually *PGM).



5. If you go back and select **View Application Definition**, you would see something like the following (this screen is from V7R1).



View Application Definition

Application type: Client
Application ID: KEYESMAIL_CLIENT
Application description: KeyesMail Client
Certificate Assigned: *None assigned*

Exit program information	
Exit program:	QSY_NOPGM
Exit program library:	QSY_NOLIB
Threadsafe:	No
Multithreaded job action:	Run program and send message

Application user profile:	*NONE

SSL protocols:	*PGM

SSL cipher specifications:	*PGM

Extended renegotiation critical mode processing:	*PGM
Special indicators:	*NONE

Define the CA trust list:	No
Certificate Revocation List (CRL) checking:	Yes

OCSP URL:	*PGM

OCSP Authority Information Access (AIA) processing:	*PGM

SSL signature algorithms:	*PGM

Application description message information	
Message file:	
Message file library:	
Message ID:	

Cancel

End of Adding an SSL Application

This concludes the process of adding the KeyesMail Client 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