

## Digital Certificate Manager (DCM) Setup

**Product:** Strategi  
**Modified Date:** 07/06/2009

On the system where V2R5 will be installed, you must first set up DCM or confirm that it is already set up and ready to use.

Follow the steps below to get DCM ready for SSL Certificate Management.

### Starting Digital Certificate Manager

Setup is slightly different depending on your OS/400 version. Follow the appropriate setup instructions for your system.

#### V6R1

Before you can use any Digital Certificate Manager (DCM) features, you need to start it on your system. Complete the following tasks to ensure that you can start DCM successfully:

1. Install Digital Certificate Manager.
2. Install IBM® HTTP Server for i5/OS®.
3. Use System i™ Navigator to start the HTTP Server Administrative server:
  - a. In System i Navigator expand your **system** > **Network** > **Servers** > **TCP/IP**.
  - b. Right-click **HTTP Administration**.
  - c. Select **Start**.

OR

Start HTTP Administrative server from command line:  
STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN)

4. Open a web browser and enter [http://your\\_system\\_name:2001](http://your_system_name:2001) to load the IBM Systems Director Navigator for i5/OS web console.
5. From the welcome page click the **i5/OS Tasks Page** link.
6. Select **Digital Certificate Manager** from the list of products on the i5/OS Tasks page to access the DCM user interface.
7. Confirm that no errors are received after clicking on the link. If errors are received, please contact IBM for assistance.

#### V5Rx

Before you can use any DCM functions, you need to start it. Complete these tasks to ensure that you can start DCM successfully:

1. Install 5722 SS1 Option 34. This is Digital Certificate Manager (DCM)
2. Install 5722 DG1. This is the IBM® HTTP Server for i5/OS®
3. Install 5722 SS1 Option 35. This is the CCA Cryptographic Service Provider (**V5R3 and earlier only**)

4. Install 5722 AC3. This is the cryptography product that DCM uses to generate a public-private key pair for certificates, to encrypt exported certificate files, and decrypt imported certificate files.  
**(V5R3 and earlier only)**
5. Use iSeries™ Navigator to start the HTTP Server Administrative server:
  - a. Start **iSeries Navigator** .
  - b. Double-click your system in the main tree view.
  - c. Expand **Network > Servers > TCP/IP**.
  - d. Right-click **HTTP Administration**.
  - e. Click **Start**.

OR

Start HTTP Administrative server from command line:  
STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN)

6. Start your Web browser.
7. Using your browser, go to the System i™ Tasks page on your system at [http://your\\_system\\_name:2001](http://your_system_name:2001)
8. Select **Digital Certificate Manager** from the list of products on the System i Tasks page to access the DCM user interface.
9. Confirm that no errors are received after clicking on the link. If errors are received, please contact IBM for assistance.

If all above tasks have been completed for DCM and you are still unable to access it, please contact IBM support for assistance.

## Create Certificate Store

If this is the first time you've used DCM, you will first need to create a Certificate Store. In most cases, using the \*SYSTEM Certificate Store is sufficient. If you're experienced with using DCM, you can create a new Certificate Store or use an existing one.

These instructions will outline how to set up the \*SYSTEM Certificate Store.

1. In the Navigation pane, click **Create New Certificate Store**. Select **\*SYSTEM** and click Continue

Note: If \*SYSTEM is not listed as an option, that means it has already been created and you do not need to go through these steps to create the \*SYSTEM Certificate Store.



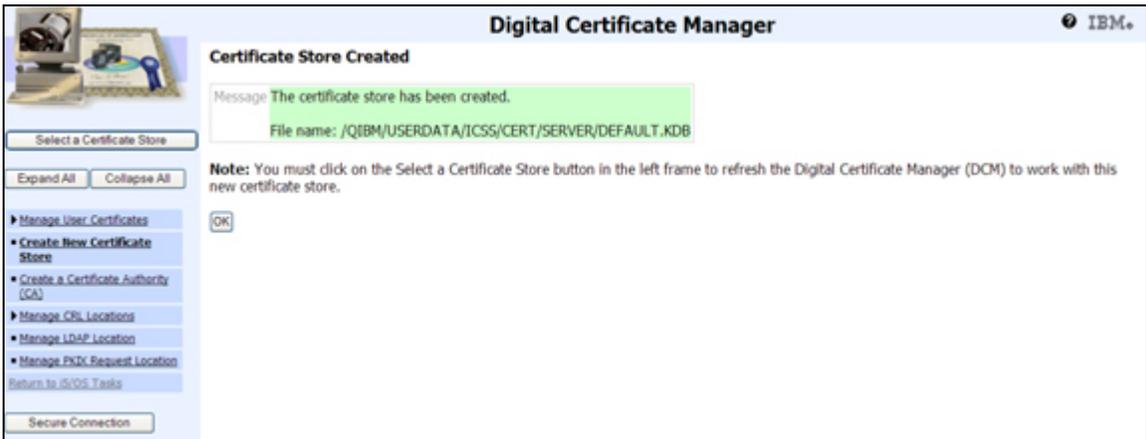
2. Select **"No – Do not create a certificate in the certificate store."** And click Continue. Create a certificate store password and click Continue.



3. Create a certificate store password and click Continue.



4. The \*SYSTEM Certificate Store has been created



You are now ready to use DCM to manage your Stragegi SSL certificate/s.