BusinessLink
Software Support

V2R5
Upgrade Instructions
Existing SSL Installations

SSL Certificate Conversion
Pre-Upgrade

Table of Contents

Overview **1**
Requirements For Certificate Conversion **1**
OS/400 System Requirements 1
Strategi Installation Requirements 1
1 - Digital Certificate Manager (DCM) Setup **2**
1.1 – Start Digital Certificate Manager 2
V6R1 2
V5Rx 2
1.2 – Create Certificate Store 3
2 – Download/Install Strategi PTF for Convert Certificate Command (CVTCTFSGI) **4**
3 – Certificate Conversion **5**
3.1 – Run the CVTCTFSGI Command 5
3.2 – Confirm Certificate Conversion 6
4 – Certificate Import **7**
4.1 – Download/Save Intermediate and Root CA Certificates 7
4.2 – Import the Intermediate and/or Root CA Certificates into DCM 10
4.3 – Import the Server Certificate into DCM 11
4.4 – Certificate Import Troubleshooting 13
5 – Strategi Upgrade **13**
6 – Assign SSL Certificates to Strategi Applications in DCM **14**
6.1 – Troubleshooting Strategi Application Registration 15
7 – Start Strategi and Test SSL **15**

Overview

As of Strategi V2R5, SSL Certificate Management has been moved out of Strategi and into IBM's Digital Certificate Manager (DCM).

For existing SSL installations, this means that you will now manage your certificates with DCM, rather than from the Strategi Resources website. This will require some steps to be performed prior to or after your upgrade to the V2R5 release.

Upgrades from Strategi V1 or V2R1 to V2R5M1+ require that your existing SSL certificate be converted to a PKCS12 format for import into DCM. Once the certificate is converted and imported, it can be used in your Strategi V2R5M1+ installation.

These steps will outline the system requirements, setup and upgrade instructions for the V2R5 release and converting and importing your existing Strategi SSL certificate into DCM.

Requirements For Certificate Conversion

These instructions need only be followed if you intend to convert your existing Strategi SSL certificate into a DCM compatible PKCS12# formatted file.

If you are fine with replacing or purchasing a new SSL certificate or your upgrade happens to coincide with your normal SSL certificate renewal period, then you do not need to convert your existing SSL certificate.

OS/400 System Requirements

- OS/400 V5R3+
- OS/400 Java version 1.5+

Strategi Installation Requirements

- V1R9 or V2R1 to convert certificate prior to V2R5 upgrade
- V1R9M6 PTF SGI196P015 or V2R1M6 PTF SGI216P030

  Note: These PTFs contain the command and programs that perform the certificate conversion and can be applied to any V1R9 or any V2R1 release.

1 - Digital Certificate Manager (DCM) Setup

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.

1.1 – Start 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* 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*
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.

1.2 – 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 Strategi SSL certificate/s.

2 – Download/Install Strategi PTF for Convert Certificate Command (CVTCTFSGI)

In order to convert your existing Strategi SSL certificate, you must have the CTVCTFSGI command. This command is available in the form of a Strategi PTF SGI196P015 for the V1R9

releases and SGI216P030 for the V2R1 releases. You do not need to upgrade Strategi to the 1.9.6 or 2.1.6 releases in order to apply these PTFs.

Note:
If on any release prior to V1R9, you would need to upgrade to the Strategi GA release, apply PTFs and then convert your certificate OR upgrade directly to the V2R5 release and convert your certificate/s.

1. Download the SGI196P015 or SGI216P030 PTF
2. Install the PTF per the above instructions

   PTF Installation Instructions can be found at:
   http://support.businesslink.com/docs/bulletins/strategi/tsb_sgi030.htm

3. Restart the subsystem

3 – Certificate Conversion

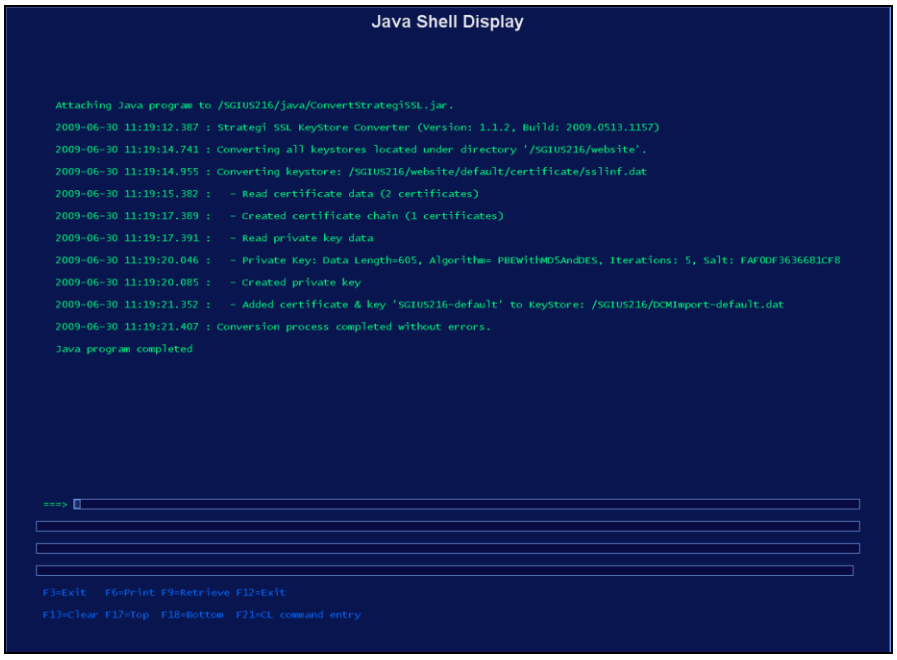
3.1 – Run the CVTCTFSGI Command

This process will convert your existing Strategi SSL certificate/s to one that can be imported into DCM (PKCS#12) format.

1. Prompt the Strategi **CVTCTFSGI VRBOUT(*YES)** command
2. In the Certificate Store Password parameter, enter a password that will be used to secure your certificate and press Enter

   Note: You will be asked for this password when importing this file into DCM

3. A Java Shell Display screen will display while your certificate/s are being converted



3. When conversion is complete, the message “Java program completed” will display. Press F3 to exit.

**Note - If you run into any errors with Java when running the command, please contact BusinessLink Support and we will provide you with information on how to find the appropriate JVMs on your system.

3.2 – Confirm Certificate Conversion

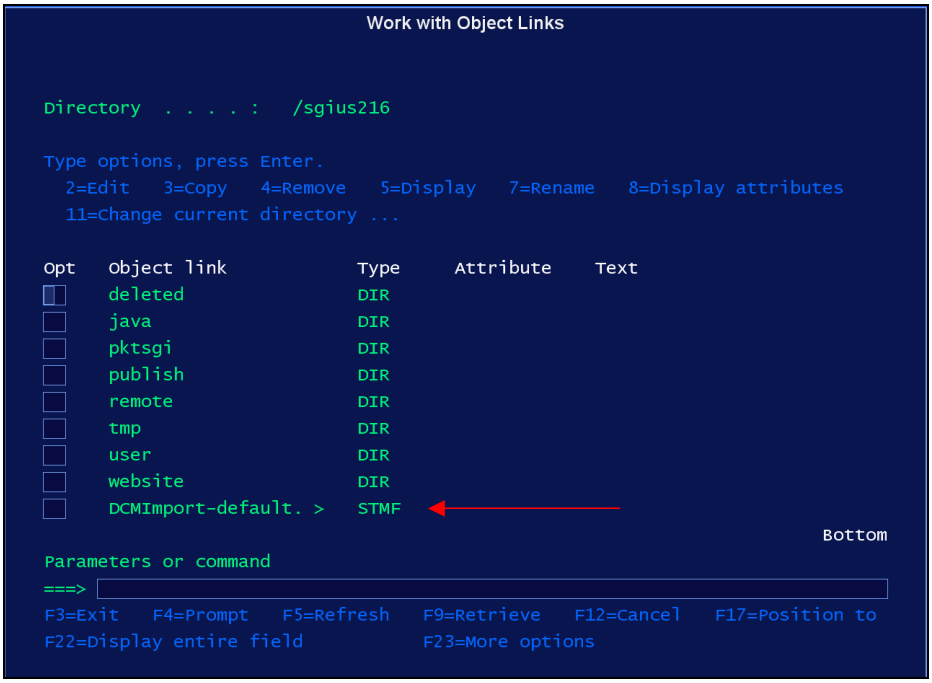
The conversion will create PKCS#12 versions of your certificate/s in the Strategi root directory.

You should confirm that the certificates exist as follows:

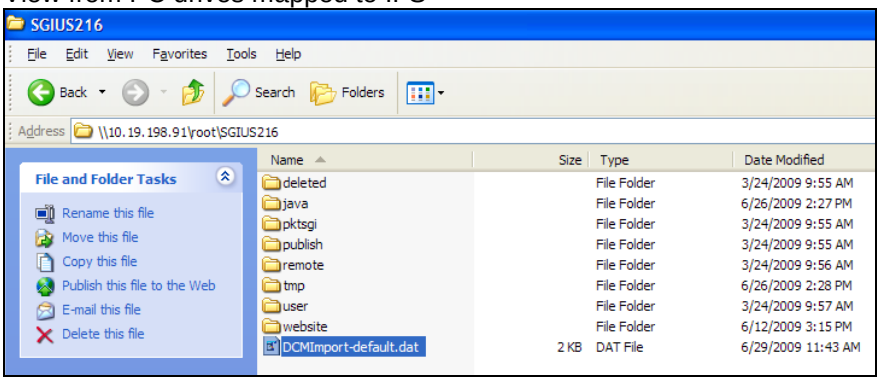
1. Using command line WRKLNK '/strategi', Ops Navigator or a mapped drive to your IFS display the Strategi IFS root
2. In the directory, you will see converted certificate file/s with the following naming convention:

   DCMImport-***website_code***.dat
   (where "*website_code*" is the website name as listed in Work with Websites)

   View from iSeries WRKLNK command



   View from PC drives mapped to IFS



3. If all website certificates have been found, you can move to the next step.

4 – Certificate Import

Once the certificate has been converted, you will now need to import it into DCM.

In order to import your server certificate into DCM, you must first import the root and/or intermediate certificates (if not already present). If you are sure that your root and intermediate certificates are already there, you can proceed to step 4.3.

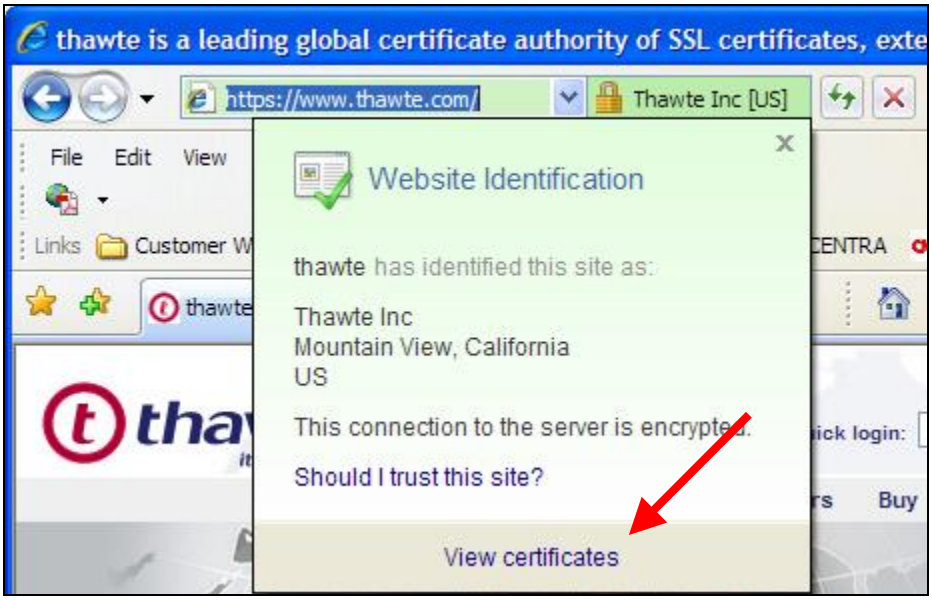
4.1 – Download/Save Intermediate and Root CA Certificates

The quickest way to get your intermediate and root certificates is to bring up your existing Strategi SSL certificate from your website and copy them to your PC or directly to the iSeries IFS for import.

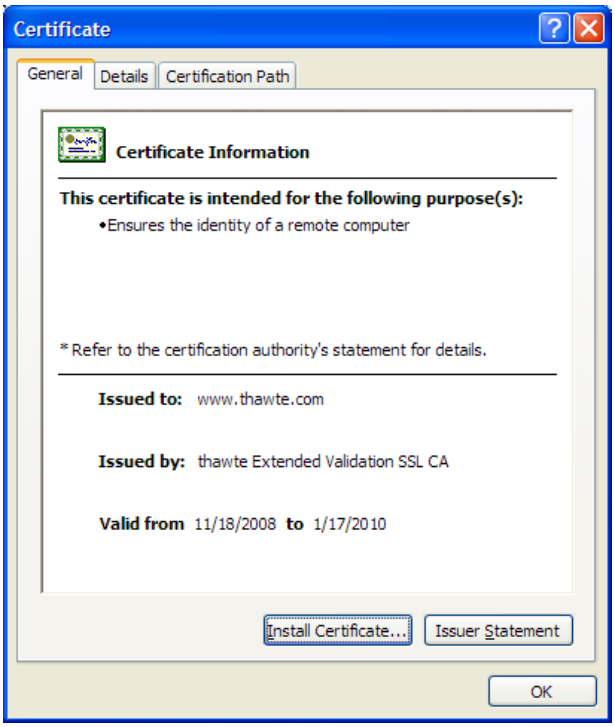
The instructions below will detail how to save the root and intermediate certificates from your existing Strategi installation.

1. Go to your current Strategi website with HTTPS (e.g., https://www.thawte.com)
2. Depending on your browser, you will see a lock icon somewhere near the address bar. (For demonstration purposes, we will use Internet Explorer to show this)

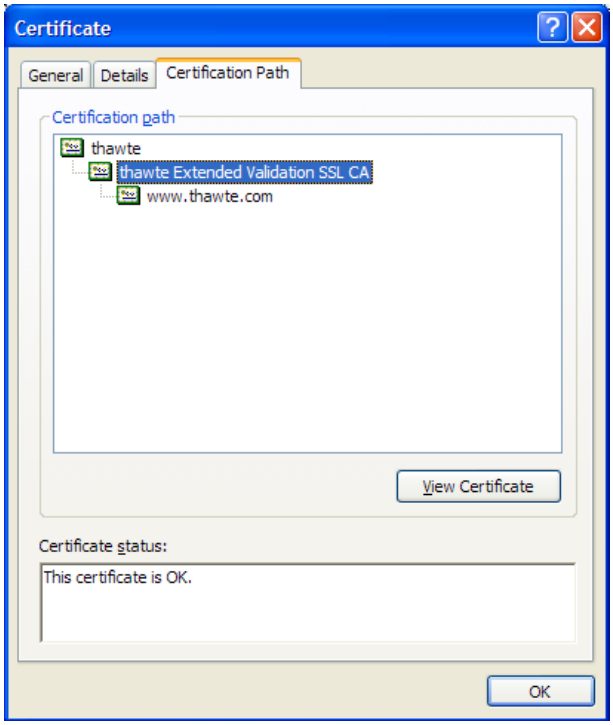
3. Click the lock icon and then click the “View Certificates” link



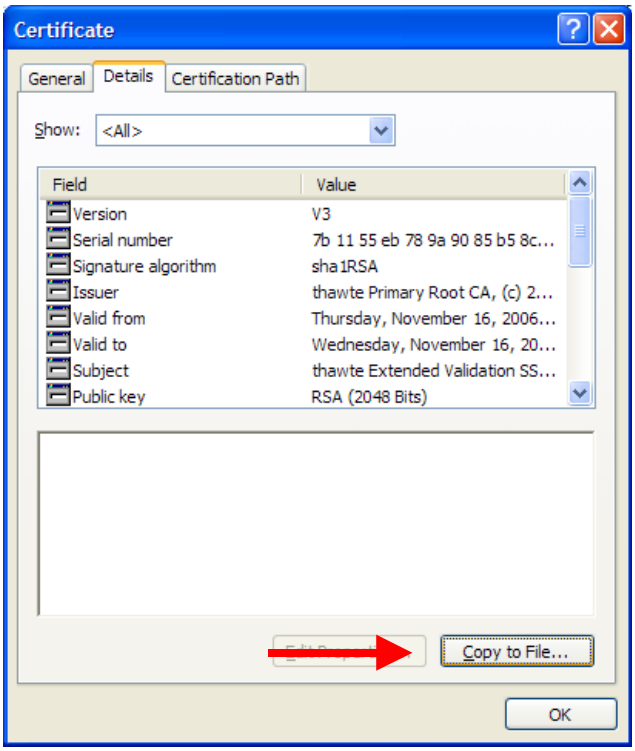
4. The Certificate window will display



5. Go to the **Certification Path** tab. You will see 3 certificates in the certificate chain. The first and second ones are the Root and Intermediate CA's respectively.

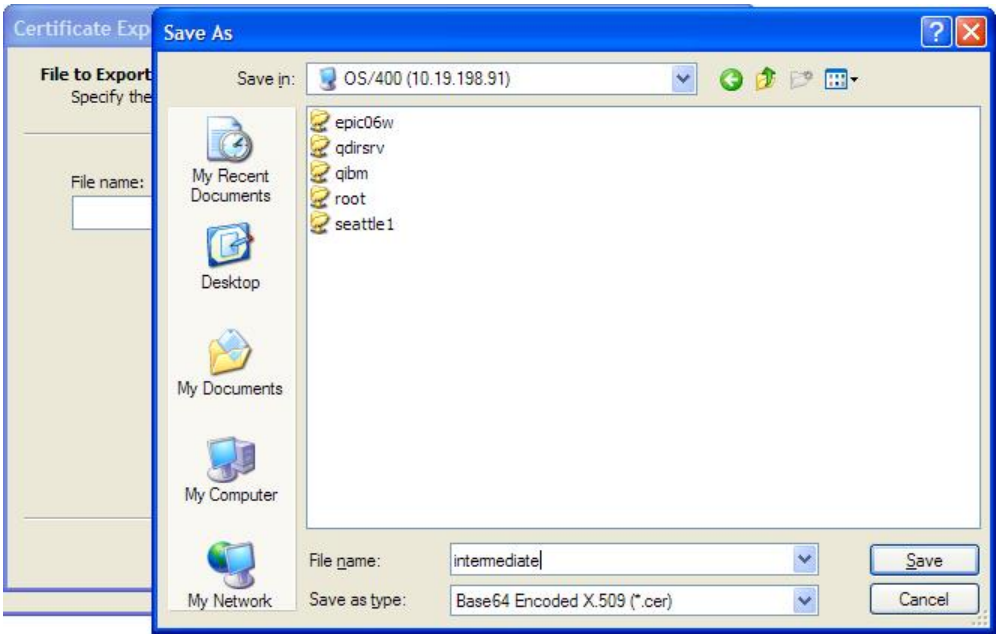


6. To download the intermediate certificate, double-click on the second one. Another certificate window will open.
7. Click on the **Details** tab and click the **"Copy to File…"** button



8. The **Certificate Export Wizard** window will display

9. Click the **Next** button
10. Select **"Base-64 Encoded X.509 (.CER)**" and click **Next**
11. On the **File to Export** screen, click the Browse button. If you have a PC drive mapped to your iSeries IFS, select that drive and a folder within it.
    (If you do not have a mapped drive or are using Ops Navigator, you can just save the file to your PC for copying to your IFS at a later time)
12. Save As file name "intermediate" (the file will be saved as "intermediate.cer")



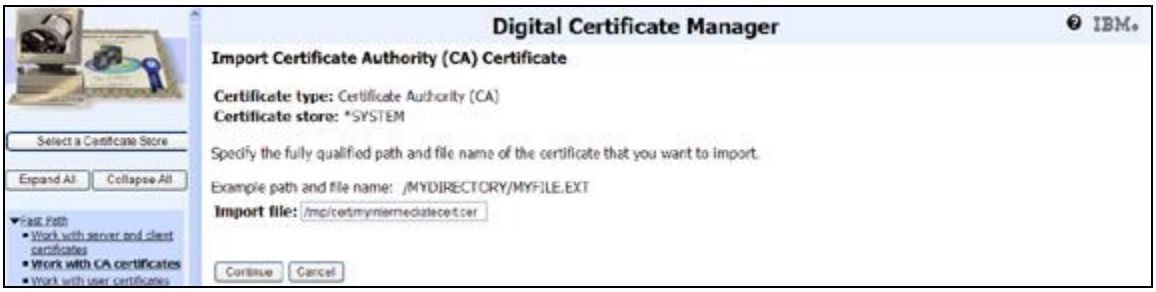
13. Click the **Save** button, click **Next** and then click **Finish**
14. To save the Root certificate, go back to the original certificate window and repeat the same procedure, naming the file as “root” when you save it to the IFS (the file will be saved as “root.cer”).

You are now ready to import the Root and/or Intermediate CA certificates into DCM.

4.2 – Import the Intermediate and/or Root CA Certificates into DCM

1. Go to IBM Digital Certificate Manager (DCM) (http://your_system_name:2001) and login with your iSeries user profile
2. In the navigation frame, click **Select a Certificate Store** and select ***SYSTEM** as the certificate store to open
3. Enter the Certificate Store password and click Continue
4. In the Navigation frame, click **Fast Path** and select **Work with CA certificates**
5. Click the **Import** button

6. On the Import Server Certificate Authority (CA) Certificate screen, enter the path to the intermediate or root certificate that you saved previously in the IFS (e.g., **/tmp/cert/intermediate.cer**) and click Continue



7. Specify a label used to describe the certificate you are importing (e.g., Thawte Intermediate CA)

8. You should receive a screen similar to below when your certificate has been imported successfully

** For problems importing your certificate, see Certificate Import Troubleshooting below. **

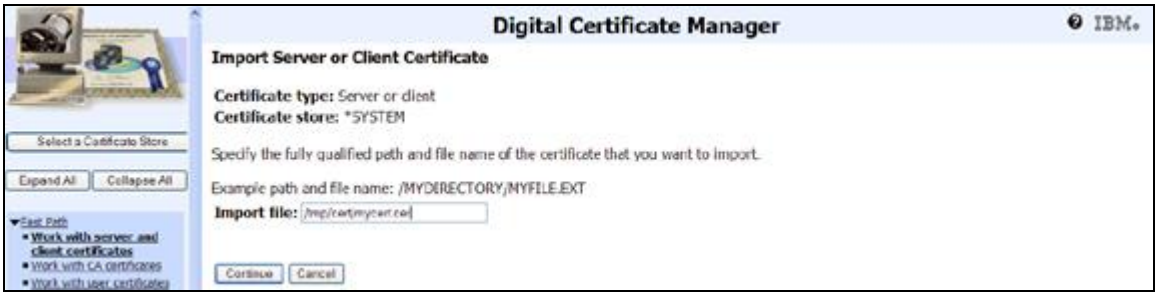
You are now ready to import your server certificate into DCM.

4.3 – Import the Server Certificate into DCM

1. Go to IBM Digital Certificate Manager (DCM) (http://your_system_name:2001) and login with your iSeries user profile
2. In the navigation frame, click **Select a Certificate Store** and select ***SYSTEM** as the certificate store to open
3. Enter the Certificate Store password and click Continue
4. In the Navigation frame, click **Fast Path** and select **Work with server and client certificates**
5. Click the **Import** button

6. On the Import Server or Client Certificate screen, enter the path to the server certificate that was converted using the CVTCTFSGI command and click Continue.

   For most systems this path will be **/strategi/DCMImport-default.dat**



7. You will be prompted for the password. Enter the password you created when running the CVTCTFSGI command and click Continue

   Note: If you do not remember the password, you will need to re-run the CVTCTFSGI command and give it a new password as the password is required to import it into DCM.

8. You should receive a screen similar to below when your certificate has been imported successfully

Your certificate is now available to assign to your Strategi website.

4.4 – Certificate Import Troubleshooting

An error occurred during certificate validation. The issuer of the certificate may not be in the certificate store or the issuer may not be enabled.

This means that a certificate in the chain above the current certificate is not in the CA list. You will need to import the missing certificate prior to importing the current one.

A duplicate key exists in the certificate store. The certificate or the label may already be in the certificate store. The label must be unique.

This means that the certificate you're attempting to import is already present in the CA list and cannot be imported again.

5 – Strategi Upgrade

You are now ready to complete the upgrade to the Strategi V2R5M1 release.

This Strategi release is compatible with all operating systems. If you choose, you can upgrade Strategi prior to upgrading or moving to OS/400 V6R1. If you are moving to a new system, you must be sure to do an entire system save to ensure that Strategi as well as DCM are intact when on the new system.

1. Download the V2R5M1 (RA) release (download instructions should be sent via email from a support team member)

   Upgrade Instructions can be found at:
   http://support.businesslink.com/docs/bulletins/strategi/tsb_sgi006.htm

2. Upgrade Strategi per the above instructions

6 – Assign SSL Certificates to Strategi Applications in DCM

The Strategi upgrade process will register an application ID with DCM for each website that is set to listen on the SSL port.

These instructions will show you how to assign your imported SSL certificate to the Strategi Applications in DCM.

1. Go to IBM Digital Certificate Manager (DCM) (http://your_system_name:2001) and login with your iSeries user profile
2. In the navigation frame, click **Select a Certificate Store** and select ***SYSTEM** as the certificate store to open
3. Enter the Certificate Store password and click Continue
4. In the Navigation frame, click **Fast Path** and select **Work with server and client certificates**
5. Click the "Assign to Applications" button

6. On the Select Applications screen, find the Strategi applications. The Strategi applications names consist of the following naming structure:

   `STRATEGI_strategilibrary_applicationtype_websitecode`

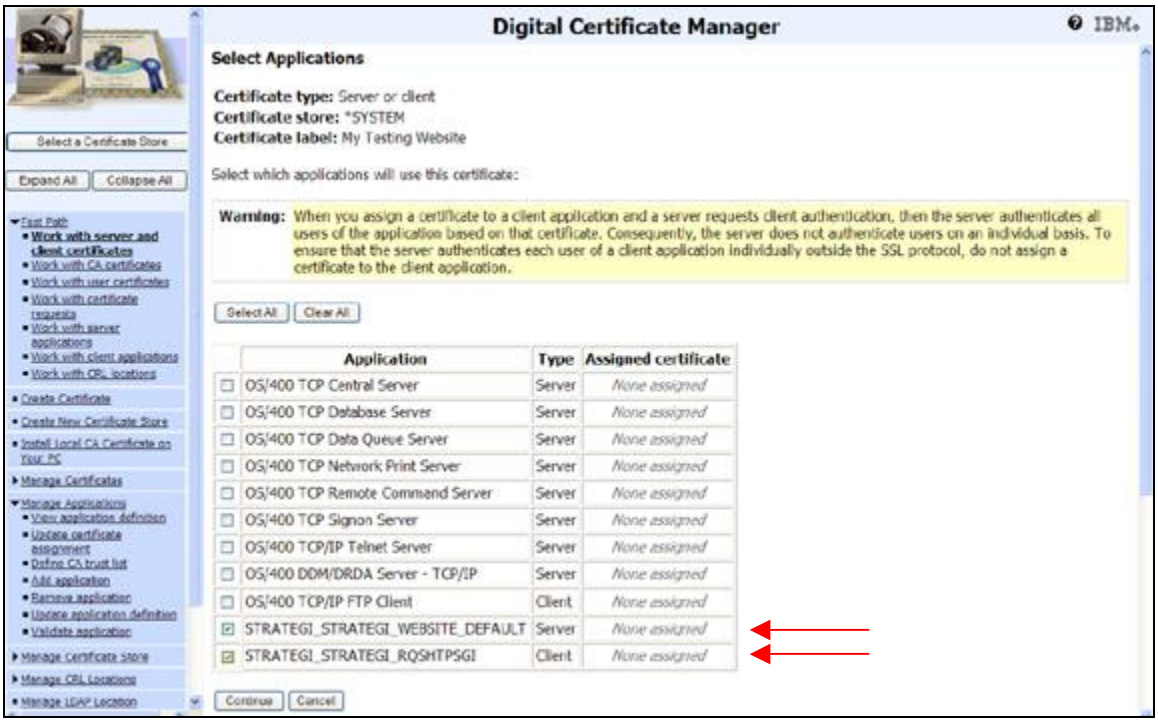
   So if you installed Strategi into library STRATEGI and your website name is DEFAULT, the application name would be STRATEGI_STRATEGI_WEBSITE_DEFAULT

   There will also be a corresponding client application for the Strategi RQSHTPSGI command with a naming structure:

   `STRATEGI_strategilibrary_RQSHTPSGI`

7. Check the box next to both application Ids and click Continue

   Note: IF you do not see the Strategi applications in the list, go to 6.1 below to help troubleshoot the problem.



8. The certificate has now been assigned to your Strategi applications

9. Click the OK button

6.1 – Troubleshooting Strategi Application Registration

If you do not see Strategi Applications listed, there may have been a problem registering them with DCM during the upgrade. Do the following to help determine the cause:

1. Run the Register with DCM (REGSGIDCM)
   At command line: REGSGIDCM

2. Display your job log to see what, if any registration error messages are logged
   At command line: DSPJOBLOG, press F10

3. Send any error messages to BusinessLink support
   If no error messages are logged, go back into DCM and see if the Application Ids are registered now.

7 – Start Strategi and Test SSL

1. Start the Strategi subsystem
   ➔ STRATEGI/ENDSGI RESTART(*YES)

2. The subsystem can take anywhere from 5 minutes to several hours to complete startup, depending on your system. During this time, you will see the AUTOSTART job running in the Strategi subsystem.
3. When subsystem startup is complete confirm that SSL is working by going to your website with https. (e.g., https://your.dns.address/resources/main.htm)
4. A locked key should show in the browser (varies depending on what browser is used) and you should be able to view your certificate details in the browser.
   (If a locked key does not show or it fails https does not return a Strategi web page, please contact BusinessLink Support)