ADVANCED BusinessLink

Technical Support Bulletins

Installing & Renewing SSL for the Strategi Webserver – V2R5 or later

Product:	Strategi
Modified Date:	07/06/2009

In Strategi V2R5+, IBM's Digital Certificate Manager (DCM) is used to manage your Strategi SSL certificates. This document assumes that DCM has already been set up and working on your system.

For information on setting up DCM for your system, see technical support bulletin:
"Digital Certificate Manager (DCM) Setup"

Generate Certificate Signing Request (CSR)

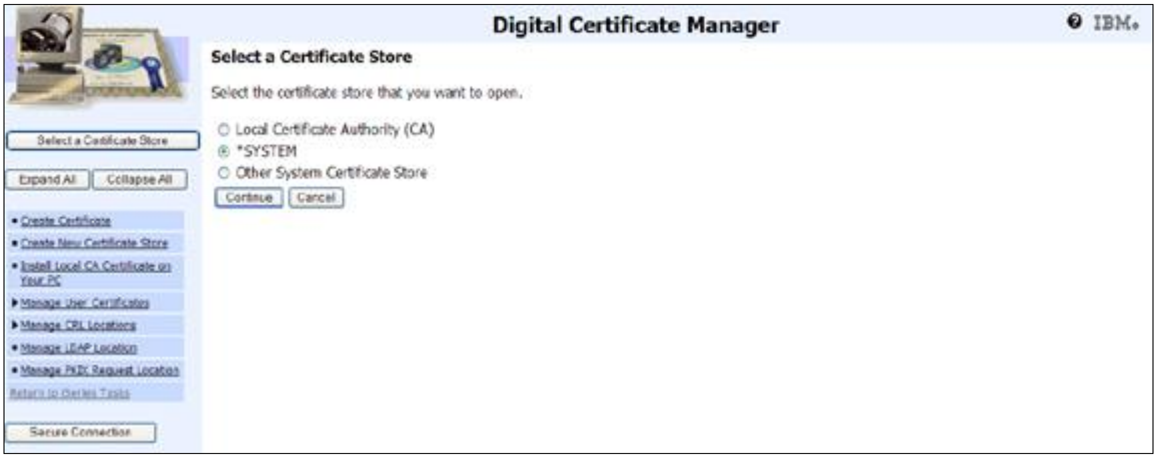
Step 1 – Install SSL Enabling License Key

This step can be skipped if an SSL Enabling License Key has already been installed. If you are renewing, you will generally already have this key installed)

- Contact BusinessLink Technical Support, who will create a new SSL enabling license key for you.
- Install the license key.
- Restart Strategi.

Step 2 – Generate Certificate Request from IBM DCM for Your Strategi Websites

1. On the iSeries where the V2R5M1+ Strategi will reside, go to IBM Digital Certificate Manager (DCM) (http://your_system_name:2001) and login with your iSeries user profile (If on V6R1, click the "**i5/OS Tasks Page**" link and then on the "**Digital Certificate Manager**" link)
2. In the navigation frame, click **Select a Certificate Store** and select ***SYSTEM** as the certificate store to open. Enter the Certificate Store password and click Continue.



Select a Certificate Store

Select the certificate store that you want to open.

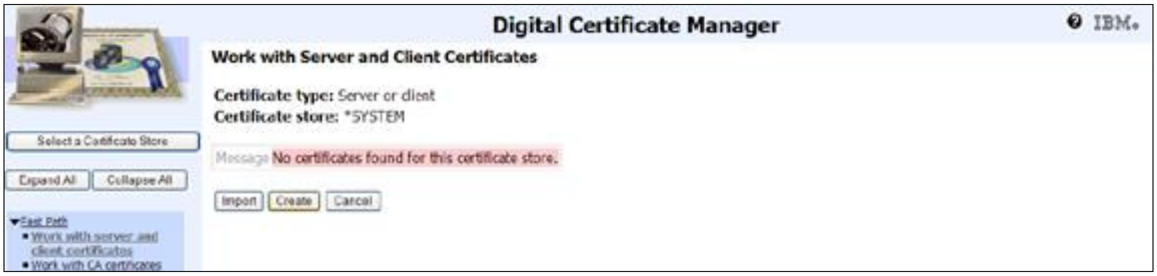
○ Local Certificate Authority (CA)
● *SYSTEM
○ Other System Certificate Store

Note:
If "**Other System Certificate Store**" is the only option that displays, then you must first set up the *SYSTEM Certificate Store.

a. In the Navigation pane, click **Create New Certificate Store**.

b. Select ***SYSTEM** and click Continue.
c. Select “**No – Do not create a certificate in the certificate store.**” And click Continue.
d. Create a certificate store password and click Continue.
e. Now proceed with Step 2, number 2 above.

3. In the Navigation frame, click **Create Certificate**
4. In the Navigation frame, click **Fast Path**
5. Select **Work with server and client certificates**

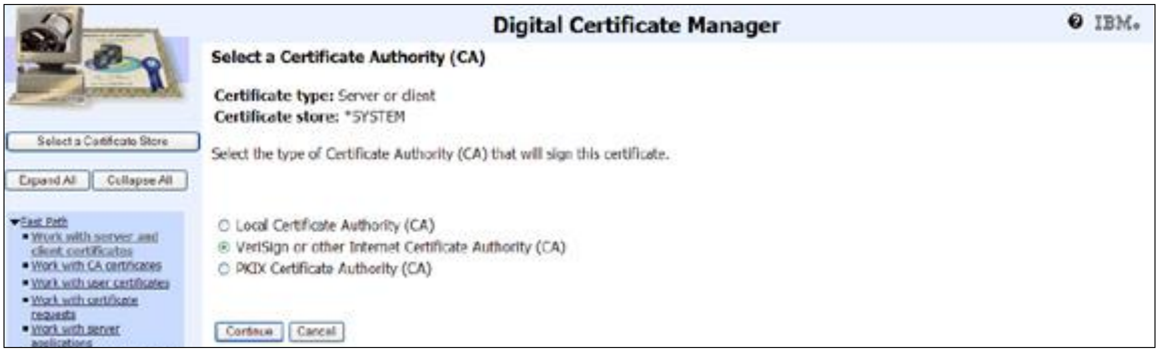

Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Import
Create
Cancel

Work with Server and Client Certificates

Certificate type: Server or client
Certificate store: *SYSTEM

Message No certificates found for this certificate store.

6. Click the **Create** button
7. Select **VeriSign or other Internet Certificate Authority (CA)** and click Continue


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications
Continue
Cancel

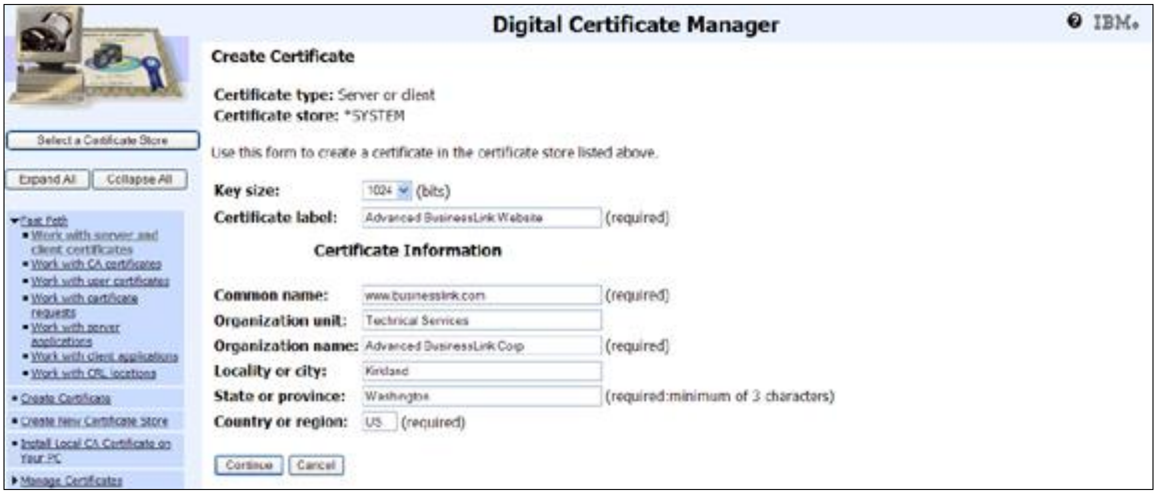
Select a Certificate Authority (CA)

Certificate type: Server or client
Certificate store: *SYSTEM

Select the type of Certificate Authority (CA) that will sign this certificate.

○ Local Certificate Authority (CA)
● VeriSign or other Internet Certificate Authority (CA)
○ PKIX Certificate Authority (CA)

8. The **Create Certificate** screen displays. Complete the form that allows you to provide identifying information for the new certificate and click **Continue**


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications
Work with client applications
Work with CRL locations
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Continue
Cancel

Create Certificate

Certificate type: Server or client
Certificate store: *SYSTEM

Use this form to create a certificate in the certificate store listed above.

Key size: 1024 (bits)
Certificate label: Advanced BusinessLink Website (required)

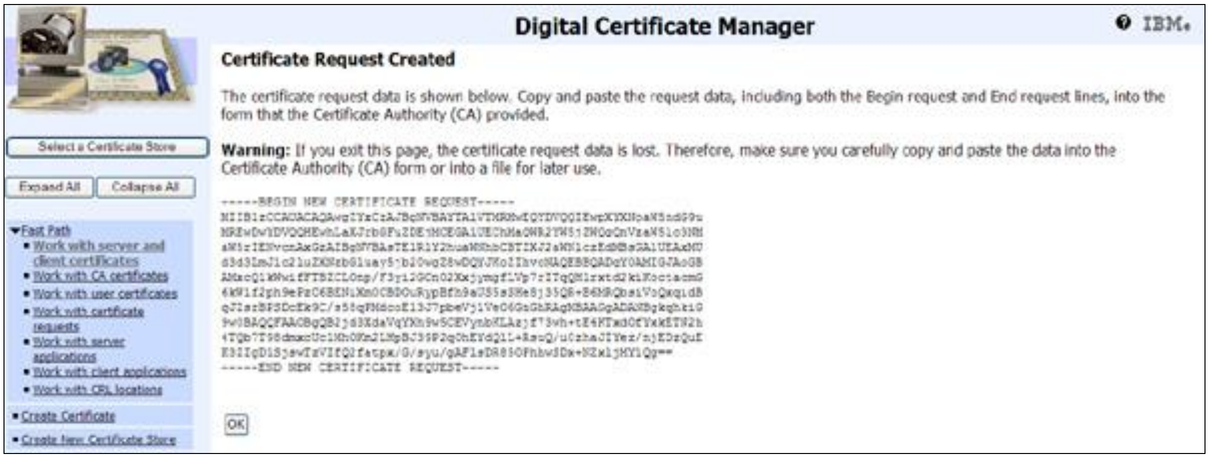
Certificate Information

Common name: www.businesslink.com (required)
Organization unit: Technical Services
Organization name: Advanced BusinessLink Corp (required)
Locality or city: Kirkland
State or province: Washington (required:minimum of 3 characters)
Country or region: US (required)

Key Size: In most cases (1024), though some prefer 2048
Certificate Label: The name that will help you identify which certificate this is within DCM
Common Name: The DNS name of your Strategi site. This must be DNS. If you do not have a DNS name for the IP address that Strategi uses on your iSeries 400, postpone SSL install until a name is acquired.

Organization Unit:	The department this website will represent
Organization Name:	The name of your organization
Locality or City:	City name, or if more appropriate, County name
State or Province:	The full name of your state or province, for example, “Washington”, not “WA”
Country or Region:	Two character country code.

9. Your new certificate request is displayed. Copy and paste the request data, including both the **Begin request** and **End request** lines, into the form the Certificate Authority (CA) has provided. Otherwise copy/paste the request data to notepad and save the data to use when you’re ready to provide it to the CA.


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications
Work with client applications
Work with CRL locations
Create Certificate
Create New Certificate Store
OK

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-----
MIIB1zCCAUACAQAwgIYxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpXYXNoaW5ndG9u
MREwDwYDVQQHEwhLaXJrbGFuZDEjMCEGA1UEChMaQWR2YW5jZWQgQnVzaW5lc3NM
aW5rIENvcnAxGzAIBgNVBAsTE1R1Y2huaWNhbCBTIXJ2aWN1czEdMBsGA1UEAxMU
d3d3LmJ1c2luZXNzbG1uay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AMxcQ1WWwifFTBZCLOng/F3yi2GCn02XxjymgfLVp7rITqQM1rxtd2kiKoctacmG
6kW1f2ph9ePzC6BENiXm0CBDOuRypBfh9aJ55sSHe8j35Q6+B6MRQbsiVsQxqidB
qJIsrBFSDcEk9C/s58qFNdcoE13J7pbeVj1VeO6GsGbRAgMBAAGgADANBgkqhkiG
9w0BAQQFAAOBgQBNjd3XdaVqYXh9w5CEVynbXLAzjf73vh+tE4KTmdOfYkKETN2h
4TQb7T98dmxcUc1Kh0Km2LMpBJ39P2qOhEYdQ1L+RsuQ/uCzhaJIYez/njEDzQuE
E3IIgD1SjswTrVIfQ2fatpx/G/syu/gAF1sDR85OFhbwSDx+NZxljMY1Qg==
-----END NEW CERTIFICATE REQUEST-----
```

Step 2 - Submit Server Certificate Application

You will now submit your CSR to the Certificate Signing Authority of your choice. The most commonly used companies are Thawte and Verisign. For your convenience, links for purchase or renewal for these two companies is listed below, but there are additional companies that can be used.

If this is a first-time SSL Certificate purchase, you can use one of the links below. If you are renewing your certificate, you most likely received an email from your certificate authority with a link, or you can still use one of the links below.

Renewals
Thawte: http://www.thawte.com/renew/
Verisign: http://www.verisign.com/products-services/security-services/ssl/current-ssl-customers/index.html

New Purchases
Thawte: http://www.thawte.com/buy/
Verisign: http://www.verisign.com/products-services/security-services/ssl/buy-ssl-certificates/index.html

- If purchasing a new certificate, read up on the various plans offered. If renewing, you will purchase the same type as last year.
- If using Thawte, you will click "Click to Buy" for a new purchase or "Click to Renew" if renewing. If using Verisign, you will click on "Buy" for a new purchase or "Renew" if renewing.
- When you get to the "Certificate Signing Request (CSR)" page, paste the contents of your clipboard (which should be the CSR from DCM) into the large field designated for your CSR.
- When asked to select your Server Platform or Web Server Software, in Verisign, you will choose "Advanced Businesslink" and in Thawte, you will choose select "Other" and type "Strategi by ADVANCED BusinessLink" in the field to the right.
- The rest of the application is very straightforward. Proceed through until you get through to the screen that tells you your certificate is on the way!

Install the Certificate in DCM

Step 1 – Receive the Certificate from your Certificate Authority (CA)

Your CA will email you a notification that the certificate is ready, and tell you how to pick it up.

1. Copy the certificate contents to notepad and save the file, in the IFS directory of your choice, on the iSeries where you are installing the SSL certificate.
   (IBM requires that the file be available in the IFS for import into DCM)

   For example, copy the contents to notepad and save the file as “server.cer” on your PC. Create a new subdirectory in the root of your IFS called “certificates” and then copy the “server.cer” file to the IFS path ‘/certificates/server.cer’
   (You will need to use iSeries Navigator or a PC drive mapped to your iSeries IFS to copy this file)

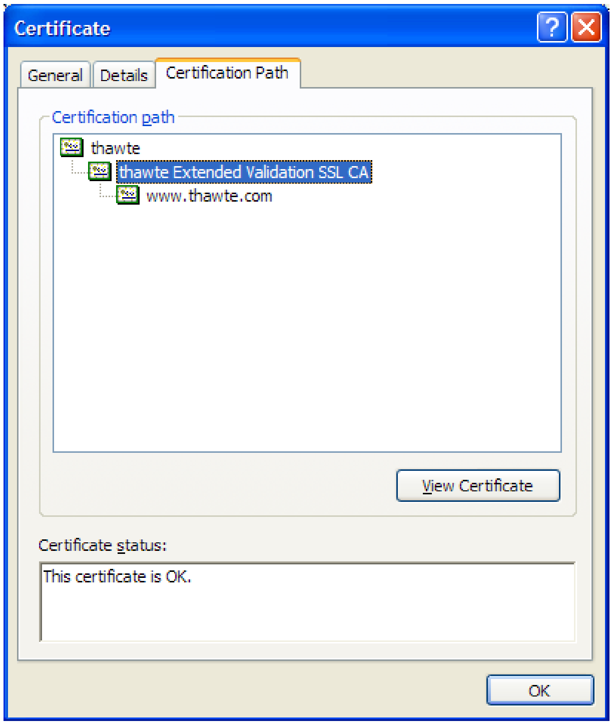
Step 2 – Export/Save the Intermediate and/or Root Certificates

DCM requires that all certificates in the certificate chain be present before it will allow you to import your certificate. This means that you will need to import the root and/or intermediate certificates prior to importing your server certificate.

Most CA’s, especially Verisign, require that the intermediate be installed. Rather than assuming that these certificates are present, it’s easier to just save them and attempt to import them to DCM.

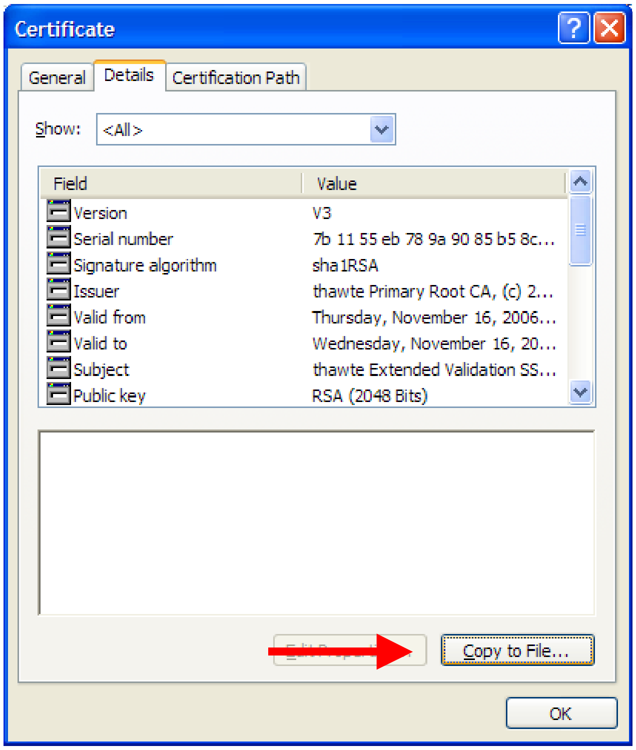
The easiest way to save the root and intermediate certificates for import is as follows:

1. From Step 1 above, you should be able to double-click on your saved certificate file “server.cer”
2. Once open, go to the **Certification Path** tab. You will see the certificate hierarchy. In most cases there will be 3 certificates in the chain



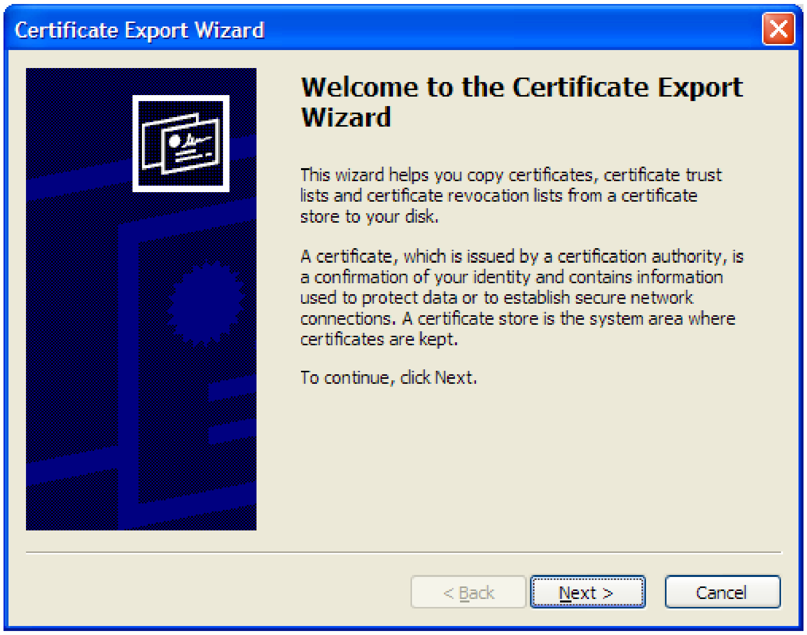
This certificate is OK.

3. To save the intermediate certificate, double-click on the one in the middle. Another certificate window will open
4. Click on the **Details** tab and click the “**Copy to File…**” button.



Field	Value
Version	V3
Serial number	7b 11 55 eb 78 9a 90 85 b5 8c...
Signature algorithm	sha1RSA
Issuer	thawte Primary Root CA, (c) 2...
Valid from	Thursday, November 16, 2006...
Valid to	Wednesday, November 16, 20...
Subject	thawte Extended Validation SS...
Public key	RSA (2048 Bits)

5. The **Certificate Export Wizard** window will open



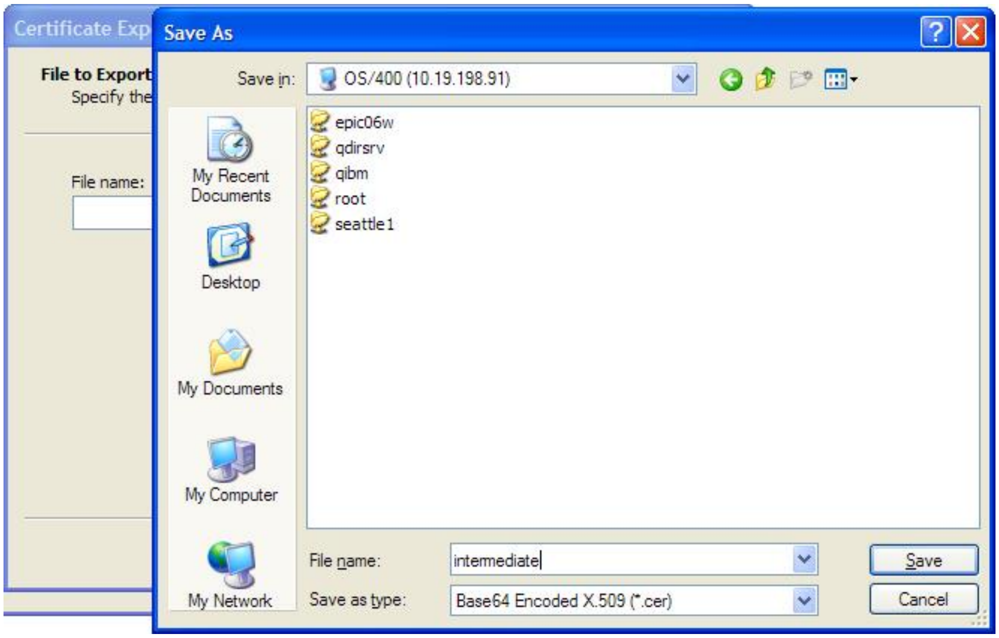
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. Click the **Next** button
7. Select "**Base-64 Encoded X.509 (.CER)**" and click **Next**
8. 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)
9. Save As file name "intermediate" (the file will be saved as "intermediate.cer")



Save in: OS/400 (10.19.198.91)

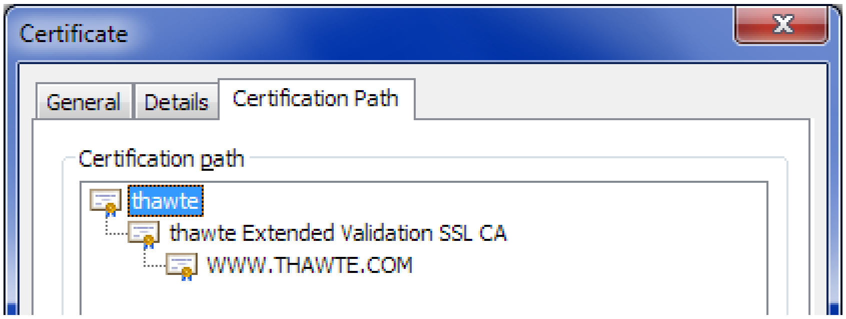
- epic06w
- qdirsrv
- qibm
- root
- seattle1

File name: intermediate

Save as type: Base64 Encoded X.509 (*.cer)

10. Click the **Save** button, click **Next** and then click **Finish**

11. To save the Root certificate, go back to the original certificate window and repeat the same procedure by clicking on the Root certificate (the very first one in the list), naming the file as “root” when you save it to the IFS (the file will be saved as “root.cer”).

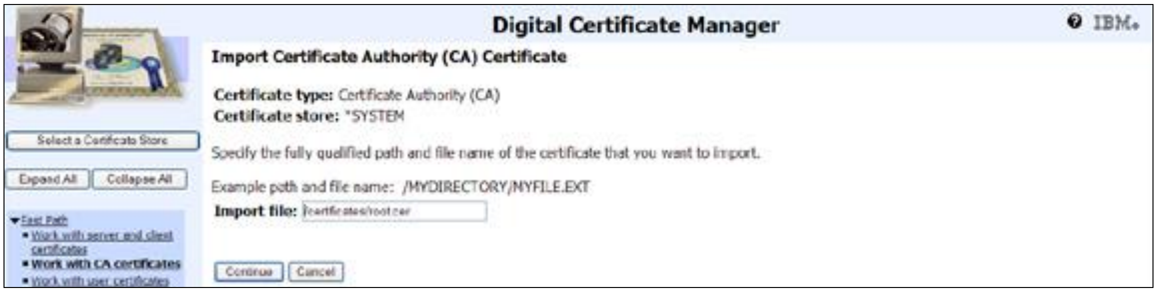


- thawte
  - thawte Extended Validation SSL CA
    - WWW.THAWTE.COM

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

Step 3 – Import the Root and Intermediate 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., **/certificates/root.cer**) and click **Continue**



Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Continue
Cancel

Import Certificate Authority (CA) Certificate

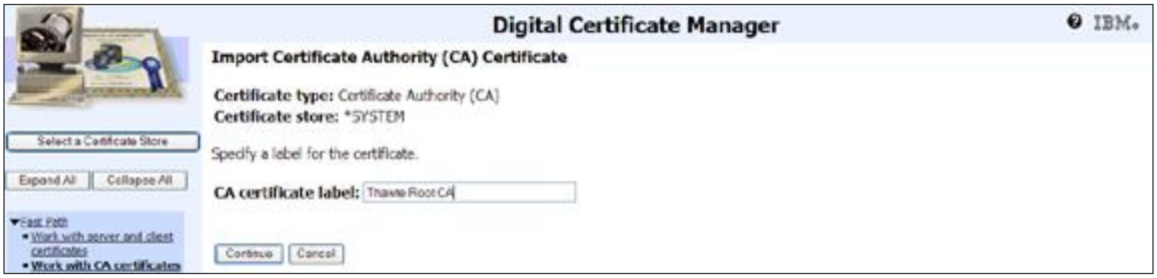
Certificate type: Certificate Authority (CA)
Certificate store: *SYSTEM

Specify the fully qualified path and file name of the certificate that you want to import.

Example path and file name: /MYDIRECTORY/MYFILE.EXT

Import file: /certificates/root.cer

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



Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Continue
Cancel

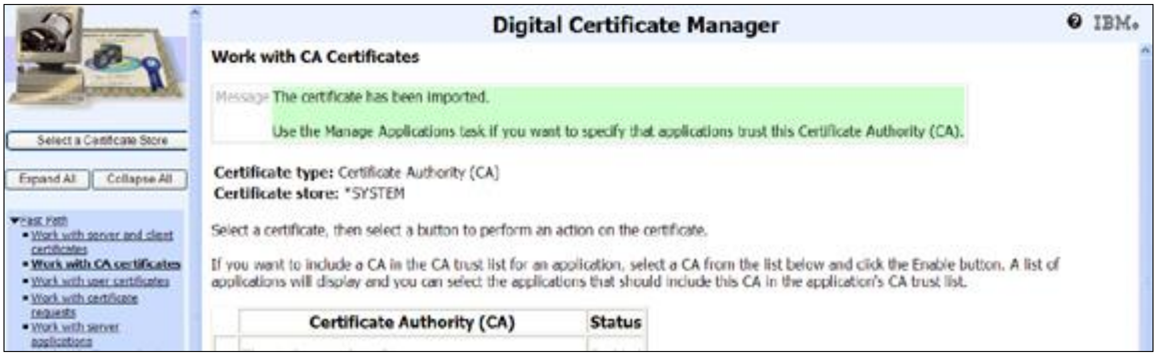
Import Certificate Authority (CA) Certificate

Certificate type: Certificate Authority (CA)
Certificate store: *SYSTEM

Specify a label for the certificate.

CA certificate label: Thawte Root CA

8. You should receive a screen that says “The certificate has been imported” when your certificate has been imported successfully



Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications

Work with CA Certificates

Message The certificate has been imported.

Use the Manage Applications task if you want to specify that applications trust this Certificate Authority (CA).

Certificate type: Certificate Authority (CA)
Certificate store: *SYSTEM

Select a certificate, then select a button to perform an action on the certificate.

If you want to include a CA in the CA trust list for an application, select a CA from the list below and click the Enable button. A list of applications will display and you can select the applications that should include this CA in the application's CA trust list.

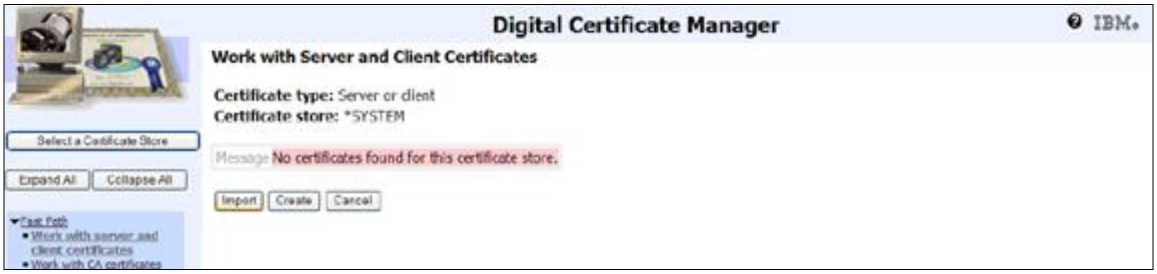
	Certificate Authority (CA)	Status

Note: If the certificate already exists in DCM, you will receive a message that says, “A Duplicate key exists…” and there is no need to import that certificate.

9. Repeat the same procedure for the intermediate certificate

Step 4 – 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**


Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Import
Create
Cancel

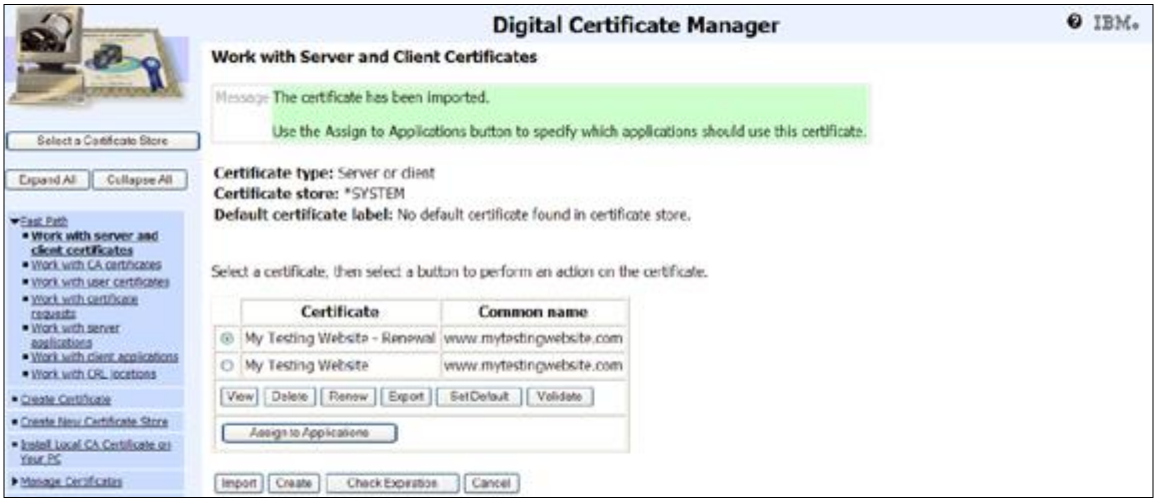
Digital Certificate Manager

Work with Server and Client Certificates

Certificate type: Server or client
Certificate store: *SYSTEM

Message No certificates found for this certificate store.

5. Click the **Import** button
6. On the **Import Server or Client Certificate** screen, enter the path to the server certificate that you saved previously (e.g., **/certificates/server.cer**) and click **Continue**
7. Your certificate will be imported


Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications
Work with client applications
Work with CRL locations
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
View
Delete
Renew
Export
Set Default
Validate
Assign to Applications
Import
Create
Check Expiration
Cancel

Digital Certificate Manager

Work with Server and Client Certificates

Message The certificate has been imported.

Use the Assign to Applications button to specify which applications should use this certificate.

Certificate type: Server or client
Certificate store: *SYSTEM
Default certificate label: No default certificate found in certificate store.

Select a certificate, then select a button to perform an action on the certificate.

	Certificate	Common name
●	My Testing Website - Renewal	www.mytestingwebsite.com
○	My Testing Website	www.mytestingwebsite.com

Your certificate is now available to assign to your Strategi website

Configure Strategi for SSL and Assign SSL Certificate

Step 1 – Add SSL Support to Strategi Website *(This step only required for new SSL installations)*

1. (iSeries 400 Command) GO STRATEGI/SGI
2. Select "Web Sites"
3. Take option "2" to edit your website (in most cases "DEFAULT")
4. If necessary, change "Secure HTTP" from "*NONE" to "*HTTP"

Step 2 – Assign the Certificate to the Strategi Website Application

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**
5. Select **Work with Server and Client Certificates**
6. Select the certificate that you will be assigning to the Strategi applications and click the **Assign to Applications** button
7. Find your Strategi website and RQSHTPSGI applications.

   The application name for Strategi websites consists of the following naming structure:

   STRATEGI_*strategilibrary_applicationtype_websitecode*

For example, if your Strategi library is “STRATEGI” and your Strategi Website Code (as defined in Work with Strategi Websites) is “DEFAULT”, the Application name will be **STRATEGI_STRATEGI_WEBSITE_DEFAULT**

If you use the Strategi RQSHTPSGI command with SSL, you will also need to confirm that it has been registered. Repeat 1-5 above, but then select the Application Type as **Client** and click Continue. The application naming structure for the command is:

STRATEGI_*strategilibrary*_RQSHTPSGI

So in most cases, the application ID will be **STRATEGI_STRATEGI_RQSHTPSGI**

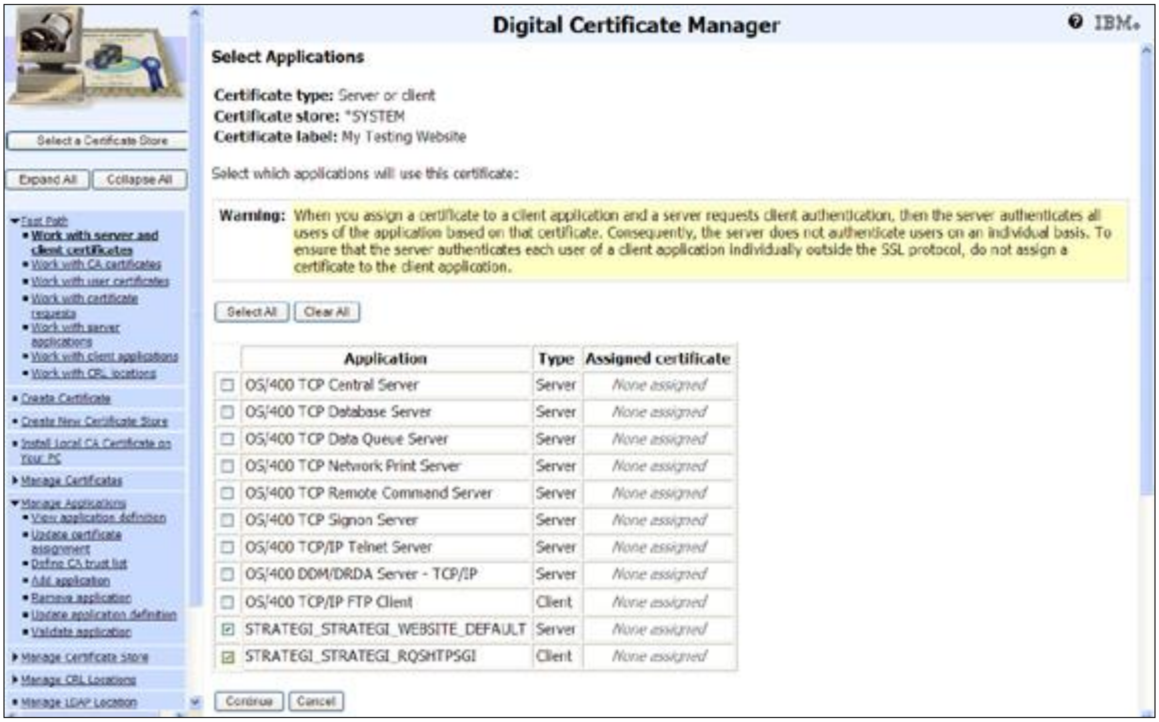
Strategi Application Troubleshooting

If you did not find any registered applications for Strategi, there may have been a problem registering them during upgrade.

Try running the Strategi REGSGIDCM REGGRP(*ALL) command. After the command is run, check your joblog by doing a DSPJOBLOG at command line. Any errors encountered during the registration attempt should be logged. The most common cause of registration failure is missing DCM or Cryptographic Service Provider PTFs.

Contact BusinessLink Support if you are unsure of the cause and we will try to assist you.

8. Check the box next to them and click **Continue**


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with server applications
Work with client applications
Work with CRL locations
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Applications
View application definition
Update certificate assignment
Define CA trust list
Add application
Remove application
Update application definition
Validate application
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Select All
Clear All
Continue
Cancel

Select Applications

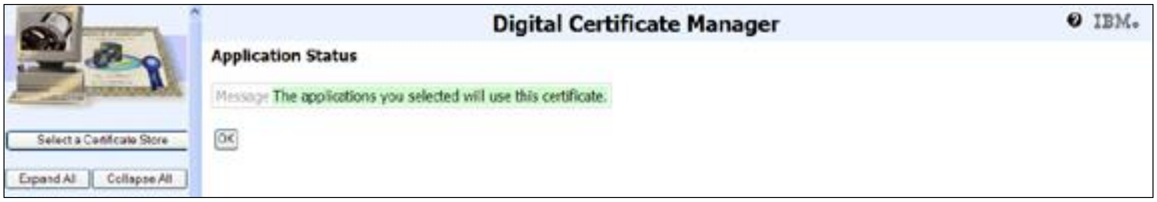
Certificate type: Server or client
Certificate store: *SYSTEM
Certificate label: My Testing Website

Select which applications will use this certificate:

Warning: When you assign a certificate to a client application and a server requests client authentication, then the server authenticates all users of the application based on that certificate. Consequently, the server does not authenticate users on an individual basis. To ensure that the server authenticates each user of a client application individually outside the SSL protocol, do not assign a certificate to the client application.

	Application	Type	Assigned certificate
□	OS/400 TCP Central Server	Server	*None assigned*
□	OS/400 TCP Database Server	Server	*None assigned*
□	OS/400 TCP Data Queue Server	Server	*None assigned*
□	OS/400 TCP Network Print Server	Server	*None assigned*
□	OS/400 TCP Remote Command Server	Server	*None assigned*
□	OS/400 TCP Signon Server	Server	*None assigned*
□	OS/400 TCP/IP Telnet Server	Server	*None assigned*
□	OS/400 DDM/DRDA Server - TCP/IP	Server	*None assigned*
□	OS/400 TCP/IP FTP Client	Client	*None assigned*
☑	STRATEGI_STRATEGI_WEBSITE_DEFAULT	Server	*None assigned*
☑	STRATEGI_STRATEGI_RQSHTPSGI	Client	*None assigned*

9. You should receive a message “The applications you selected will use this certificate.”



Application Status

Message The applications you selected will use this certificate.

10. Certificate assignment is complete. Click OK
11. Restart the Strategi subsystem to pick up the new SSL certificate

Step 3 – Test SSL

1. Go to https://your.dns.address/resources/main.htm
2. A "locked key" should show in your browser window. If one does not, discuss this with BusinessLink technical support