# SSL Communication Setup – iSeries Source

## Contents

## Introduction

This write-up is intended to address steps that are typically needed to allow SSL-based communication from the iSeries to third-party payment provider URLs. Typically, this communication is for void requests to certain third-party payment providers, and similar payment-related requests originating on the iSeries. NOTE: Many of the below steps assume a general comfort level with Windows, iSeries navigation, understanding of CR menus and Paymentus setup, etc.

### What address is iSeries communicating with?

Many setups may allow the iSeries to communicate DIRECTLY with Secure URL (HTTPS / SSL address) of third-party payment processor. However, if client prefers not to allow this communication directly, a proxy server may be able to be setup inside the client's network. NOTE: This option may require additional setup and downtime during or after the implementation window.

## Confirm Address iSeries uses to communicate with Outside Internet

### Explanation:

These steps may be needed for communication from iSeries to various providers on the outside Internet. If the provider protected this communication by IP address these steps will confirm the correct address to provide. NOTE: If the iSeries cannot communicate TO the outside internet, other components (such as a Proxy server) may be required along with additional setup. See Additional Steps heading to determine if iSeries is setup for outbound routing.

### Steps to Complete / Determine:

(From iSeries)

1. Run following command and hit enter:
   **`FTP RMTSYS('170.225.15.31')`**
2. From FTP Command Prompt, type "anonymous" as the login ID:
   Type your email address as the password
3. The status command shows your external IP address. Example:
   **211-Connected to 193.158.21.21**
4. Make not of above address, and Type "quit" to exit FTP session.

### Local DNS in Place?

(From iSeries)
NOTE: Other setup aspects such as routes, etc may be outside the scope of this document

1. Run the following command:
   **CFGTCP**
2. Option 12 – Change TCP/IP domain information
3. Page Down to proceed to second screen
4. Review Internet Address values for Domain Name Server and update as needed

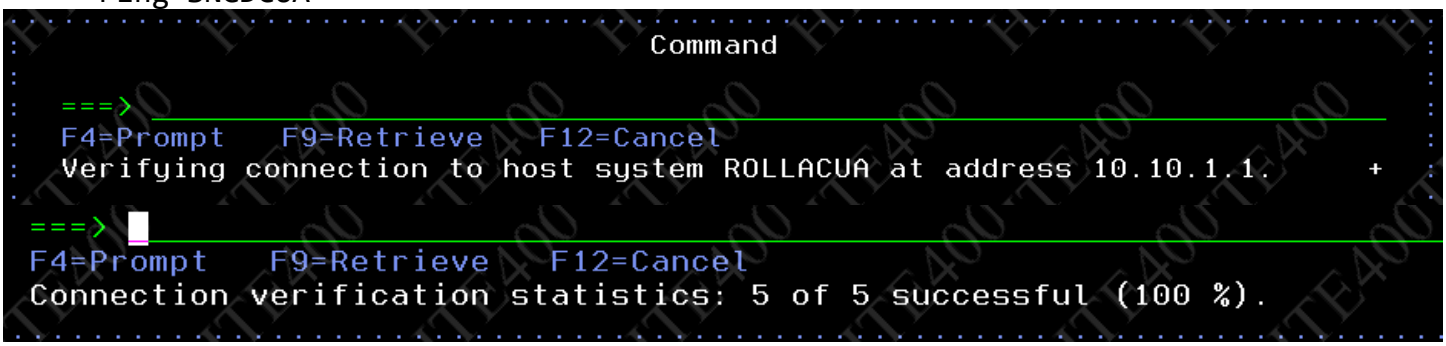
a. NOTE: Recommend making note of old values in case they are updated to an incorrect address and cause issues

5. After exiting out of TCP configuration, can test resolution of external URLs with the following command
   **`PING 'www.yahoo.com'`**
   a. Should output *Verifying connection to host system fd-fp3.wg1.b.yahoo.com at address 98.139.183.24* and present ICMP responses.

### How to get IP of iSeries server

1. Run the following command:
   **CFGTCP**
   option 1 to display TCP/IP Interfaces. Once you display the interfaces, you can hit F11 to display the status and want to choose one that is active as the IP.

   If you know the server name, you can ping it to get the IP address.
   Ping SNGDCUA




## How to pull up logging of issues in iSeries:

***Navigation:***

1. CR Main Menu
2. File maintenance (8)
3. Interface Maintenance (24)
4. TM interface Control (7)
5. Enter to second screen on main settings – confirm debug active set to "Y"
   a. If it is not, will have to enter through remaining screens to apply and then pull TM interface back up again
   b. IMPORTANT – this should be set back to N after troubleshooting complete
6. F11 – Configure Web Services
7. Select the Paymentus Void Request option (2 next to)

8. Enter on first screen
9. Debug Active set to “Y”
10. Enter twice to continue through second screen and apply change
11. F3 to exit
12. F9 if needed to bring up command prompt
    a. Optional – from limited command prompt, can also enter CALL QCMD to get to more extensive prompt (with details on command output)
13. Run below command:

    **WRKLNK OBJ('/sungardps/cr/htedta/debug/')**

    a. NOTE: may have to modify “htedta” portion if test environment or diff library convention
14. 5 – Display next to Debug Object Link
15. Object links represent each individual log – look for the last CRVOIDRQST_debug_<user>_<date>.txt formatted one in the list and take a 5 display on it

## Configure System Values for Allowed SSL Communication Protocols

### Log Reflects Following:

*About to connect() to 10.50.50.31 port 443 (#0)*
*Trying 10.50.50.31... connected*
*SSL_Handshake():* ***Peer not recognized or badly formatted message received.***
*Closing connection #0*
*SSL connect error*

### Steps to Correct Issue:

1. (FROM iSeries)

**WRKSYSVAL QSSL***

    a. NOTE: may not have authority under QHTE profile – have customer assist if this is the case
2. Take a “2” on each of the below options in the sequence indicated and follow the steps

***QSSLCSLCTL***

Change FROM

```
System value . . . . . :   QSSLCSLCTL

Description  . . . . . :   Secure sockets layer cipher control

Type choice, press Enter.

  Cipher control . . . .   *OPSYS          *OPSYS, *USRDFN
```

Change TO:

```
System value . . . . . :   QSSLCSLCTL
```

```
Description  . . . . . :   Secure sockets layer cipher control

Type choice, press Enter.

  Cipher control . . . .   *USRDFN          *OPSYS, *USRDFN
```

---

### *QSSLPCL*

NOTE: This will have to be changed before QSSLCSL IF value is initially OPSYS

Change From (May vary):

```
System value . . . . . :   QSSLPCL
Description  . . . . . :   Secure sockets layer protocols

Type choices, press Enter.

Protocols
*OPSYS
```

Change to:

```
System value . . . . . :   QSSLPCL
Description  . . . . . :   Secure sockets layer protocols


Type choices, press Enter.

Protocols
*TLSV1.2
*TLSV1.1
*TLSV1
*SSLV3
```

---

### *QSSLCSL*

NOTE:  Values may not exist - should use sequence number system to either app the values highlighted in the "Change to" or add them in open lines (make sure the values are below "10").

*Change from*

```
System value . . . . . :   QSSLCSL
```

```
Description  . . . . . :   Secure sockets layer cipher specification list


Type new/changed information, press Enter.
To add a cipher suite, type name and desired sequence number.
To remove a cipher suite, space over cipher suite name.
To change position of a cipher suite, type new sequence number.

Sequence      Cipher
 Number       Suite
     0
    10        *RSA_AES_128_CBC_SHA
    20        *RSA_RC4_128_SHA
    30        *RSA_RC4_128_MD5
    40        *RSA_AES_256_CBC_SHA
    50        *RSA_3DES_EDE_CBC_SHA
    60        *RSA_DES_CBC_SHA
    70        *RSA_EXPORT_RC4_40_MD5
```

*Change to*

```
System value . . . . . :   QSSLCSL
Description  . . . . . :   Secure sockets layer cipher specification list


Type new/changed information, press Enter.
To add a cipher suite, type name and desired sequence number.
To remove a cipher suite, space over cipher suite name.
To change position of a cipher suite, type new sequence number.

Sequence      Cipher
 Number       Suite
     0
    10        *RSA_AES_256_CBC_SHA256
    20        *RSA_AES_128_CBC_SHA256
    30        *RSA_AES_128_CBC_SHA
    40        *RSA_RC4_128_SHA
    50        *RSA_RC4_128_MD5
    60        *RSA_AES_256_CBC_SHA
    70        *RSA_3DES_EDE_CBC_SHA

More...
```

# Import Public (Intermediate / Root) Certificates into iSeries Cert Store

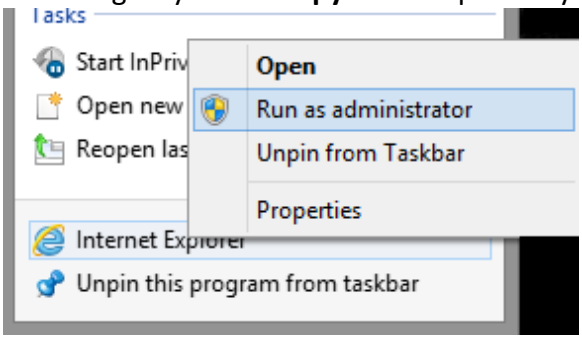
**IMPORTANT: This usually occurs AFTER "Peer Not Recognized" error above**

## Log Reflects Following:

************Beginning of data***************
*- - - - - - - - - - - - - - - - - - - - - - C O N N E C T I O*
*About to connect() to billpay.polkutilities.net port 443 (#0)*
*Trying 172.31.254.62... connected*
*Closing connection #0*
***SSL peer certificate or SSH remote key was not OK***
************End of Data*********************

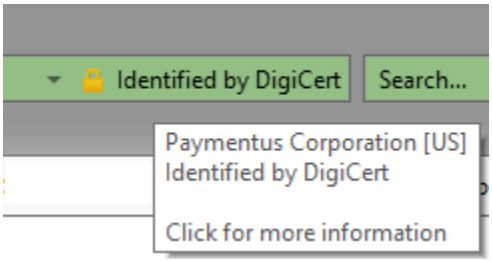
## Steps to Correct Issue Part I – Obtain correct public keys using the browser:

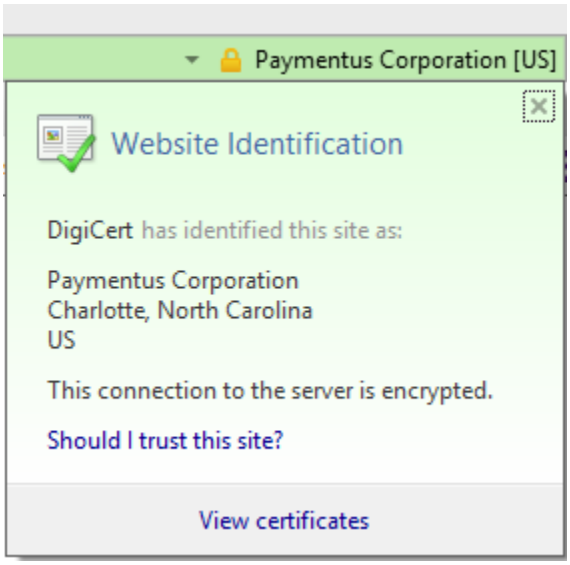
1. You need to be on a server with IBM ACS or System I Navigator
2. Right click on **Internet Explorer** and select **Run as Administrator**
    a. You may have to close existing IE to get it to launch as admin
    b. It won't give you the **Copy to File** option if you are not running as Administrator




3. Pull up the URL used to communicate requests to your third-party payment provider (or the Proxy URL) in a browser.
    a. Example: *https://secure1.paymentus.com/xotp/SNGD*

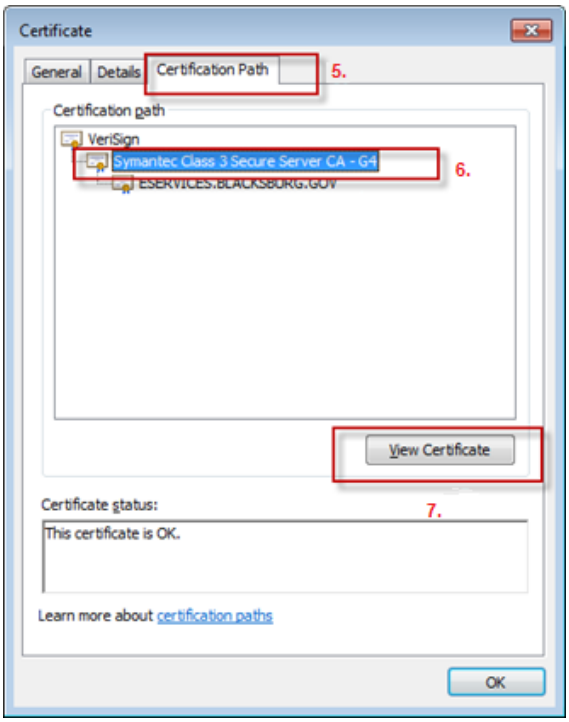
4. Pull up the certificate properties screen in a browser (see example below)
    a. IE should work via **lock icon next to the address bar**
        1. Click on the lock icon
        2. Click **View Certificates**



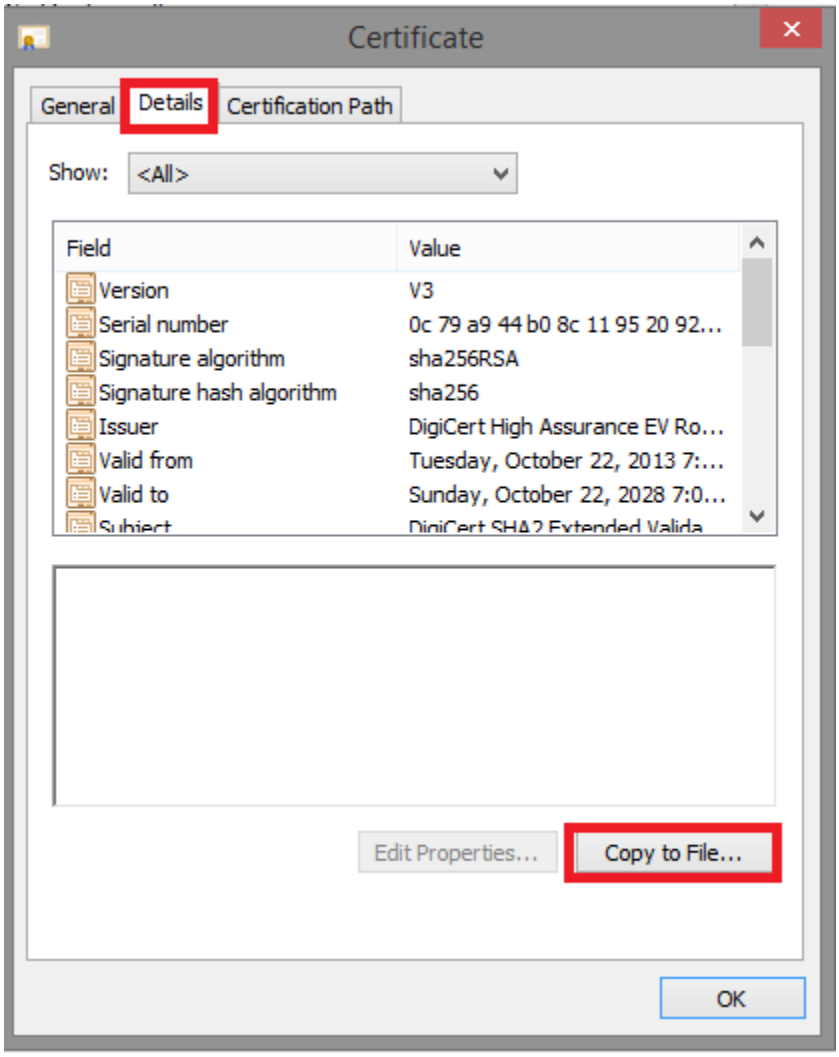



b. Chrome - requires Dev Tools (can bring up via F12) --> click the security tab (not pictured) --> view certificate button (not pictured)

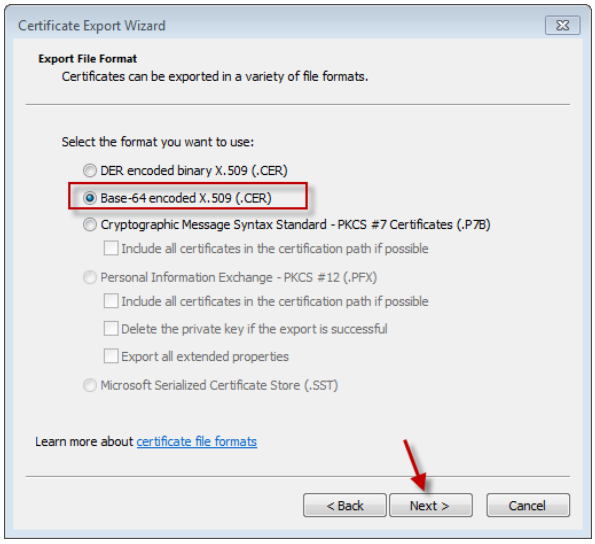
5. **Certification Path** Tab (see below screen shot)
6. Choose cert above one on bottom (see below screen shot)
7. Click the **View Certificate** button



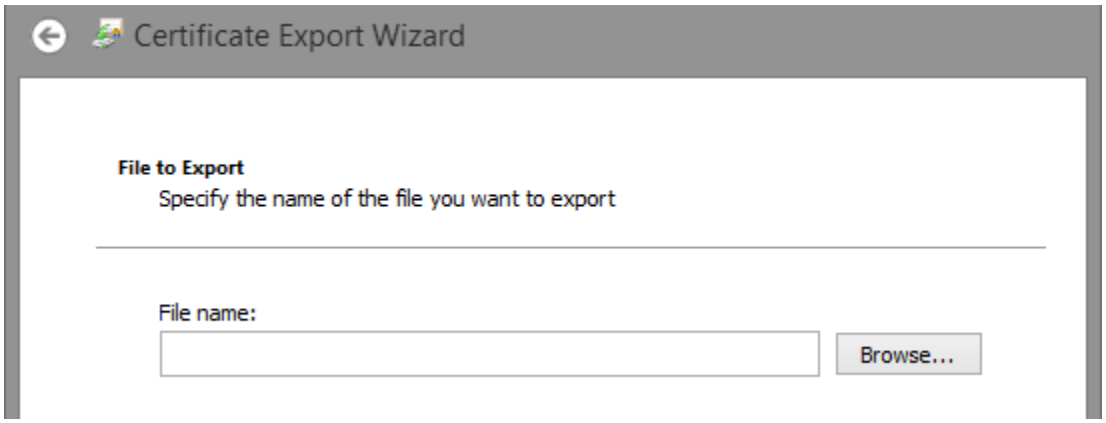

8. In the second certificate window that opens, choose **Details** tab
9. Click the **Copy to File** button

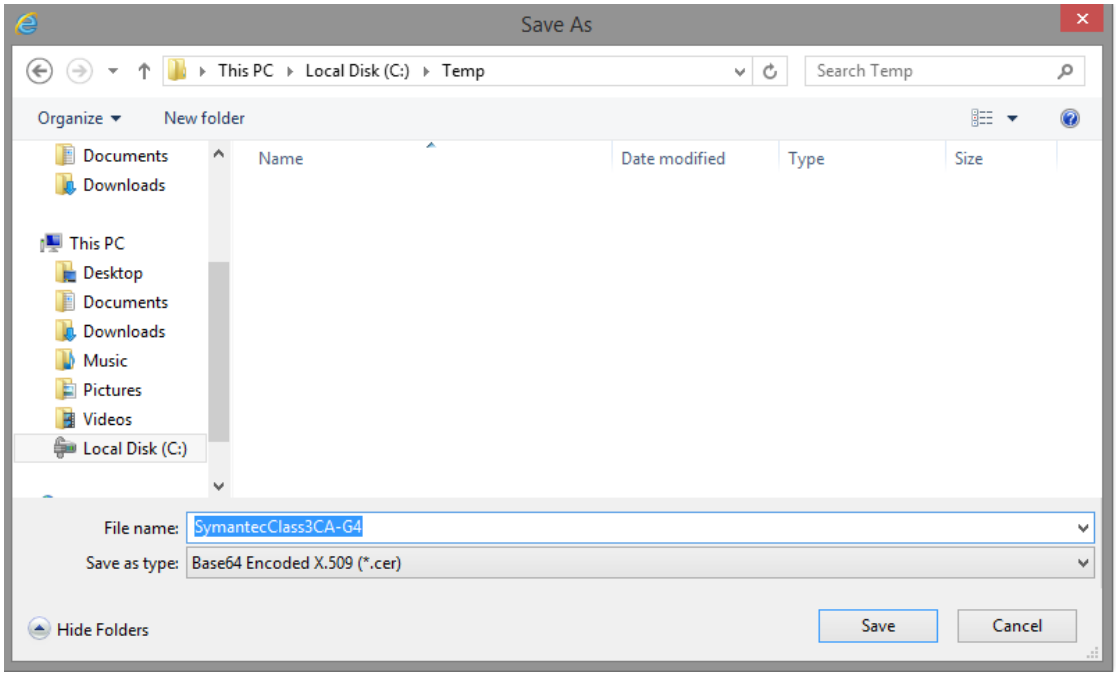



10. **Certificate Export Window** opens - Choose **Next** (not pictured)
11. Choose **Base-64 encoded X.509(.CER)** and click **Next**




12. Follow steps to name and save the file
    a. Click **Browse** to select a folder you can save to.
    b. Enter a **File name** similar to the name of the cert. Example: SymantecClass3CA-G4.cer
    c. Click **Save**





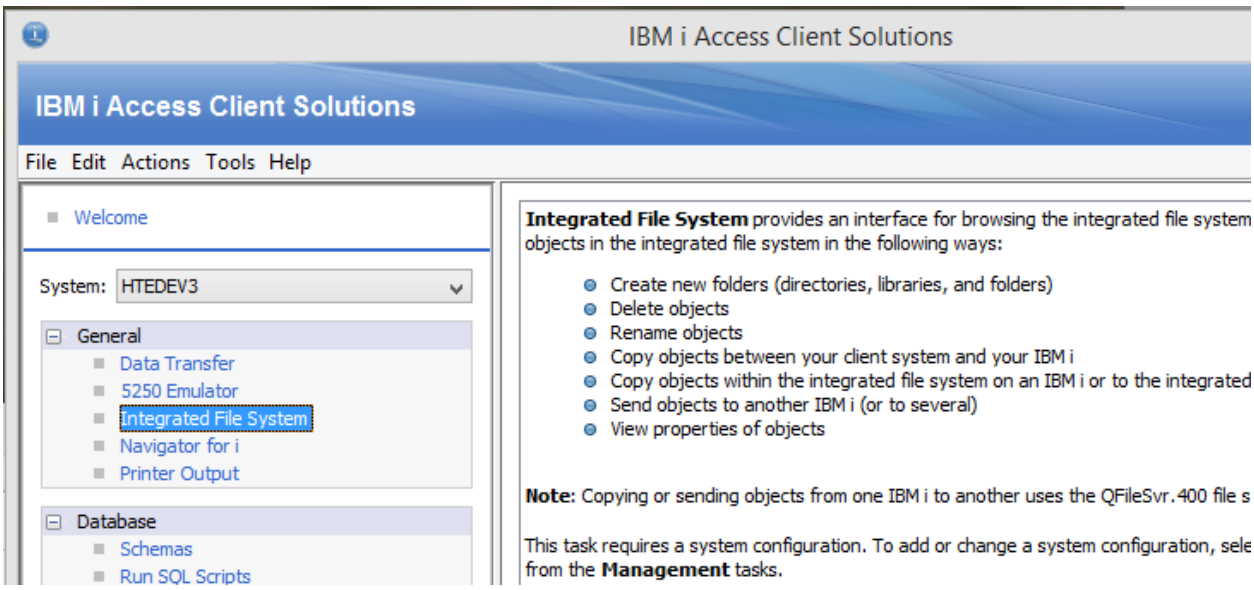

13. Click **Next** to finish cert export.
14. IMPORTANT – Repeat above steps again for any other higher-level (root) certificates in the Certificate Path.
    a. The higher-level certificate will have to be imported FIRST to the iSeries cert store, followed by the lower-level certificates.

### Steps to Correct Part II - Copy of files to iSeries IFS cert folder:

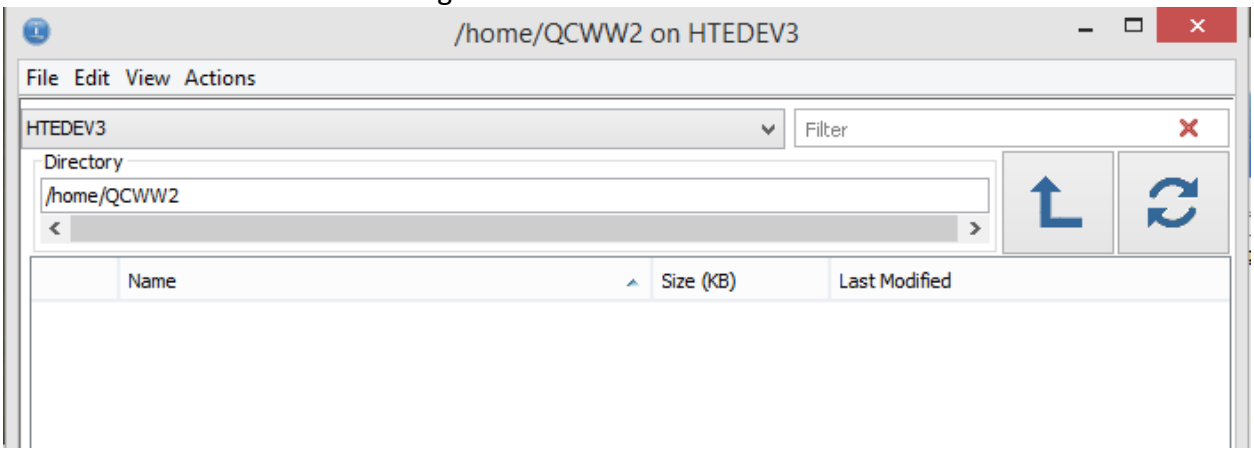
This copies the certificates from your workstation to the iSeries using either IBM ACS or the older System I Navigator

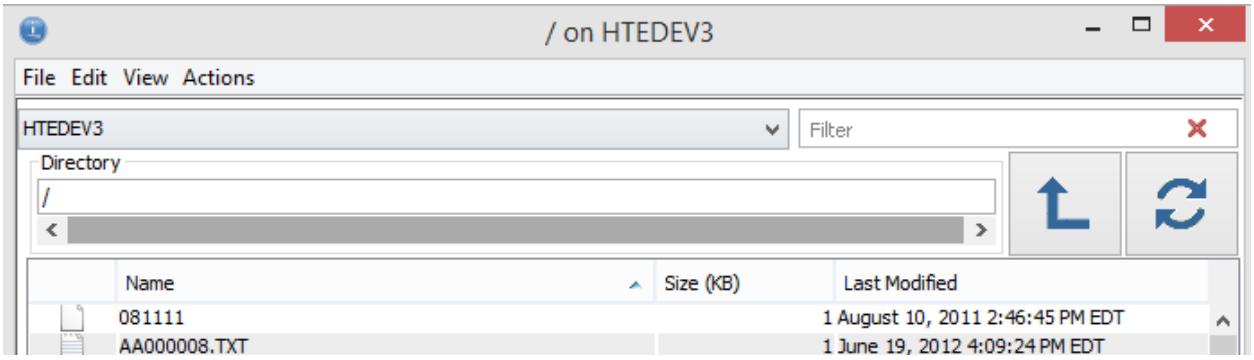
#### *Using IBM ACS*

1. Open IBM I Access Client Solutions and select the NaviLine system you are copying the certs to.
2. Select **General > Integrated File System**
    a. This brings up the File System tool

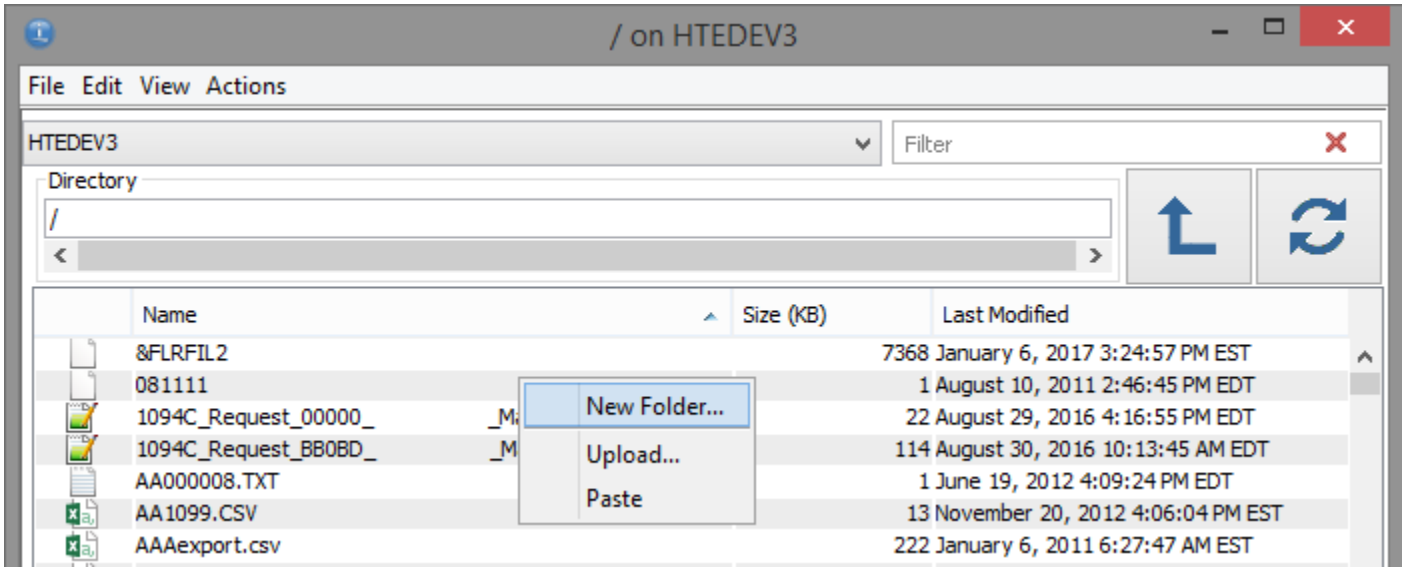



3. Use the **back button**  to navigate back to the root folder

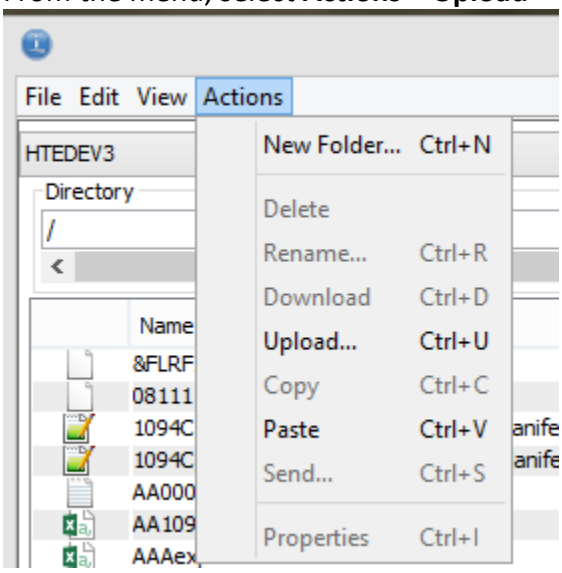


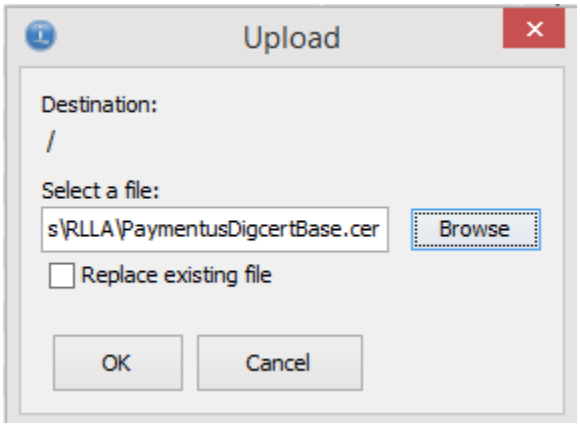

4. Create a **CERT** folder if one doesn't exist.



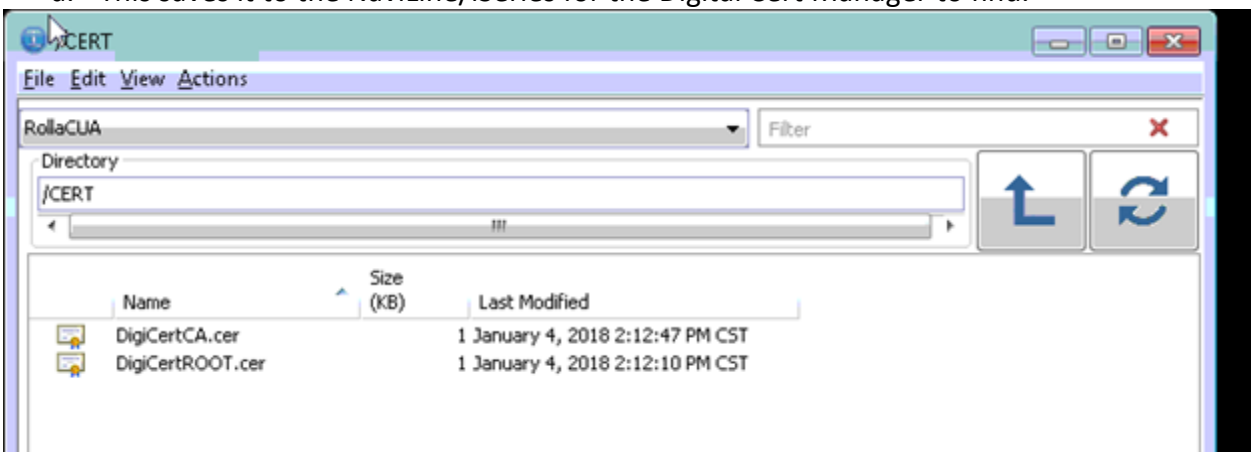

5. Click on the CERT folder to view its contents
6. From the menu, select **Actions > Upload**




7. Click **Browse**
    a. Navigate to the local folder where you saved the certificates to.
    b. Click **OK**.



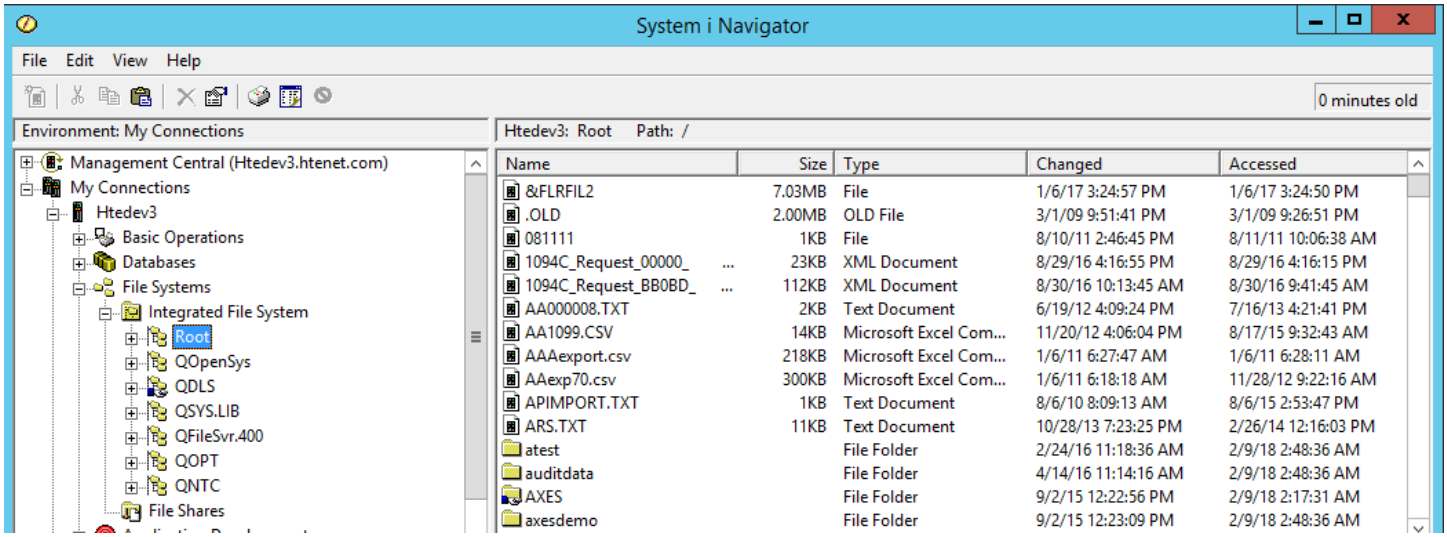

8. You should see the certificate file listed in the folder.
    a. This saves it to the NaviLine/iSeries for the Digital Cert Manager to find.



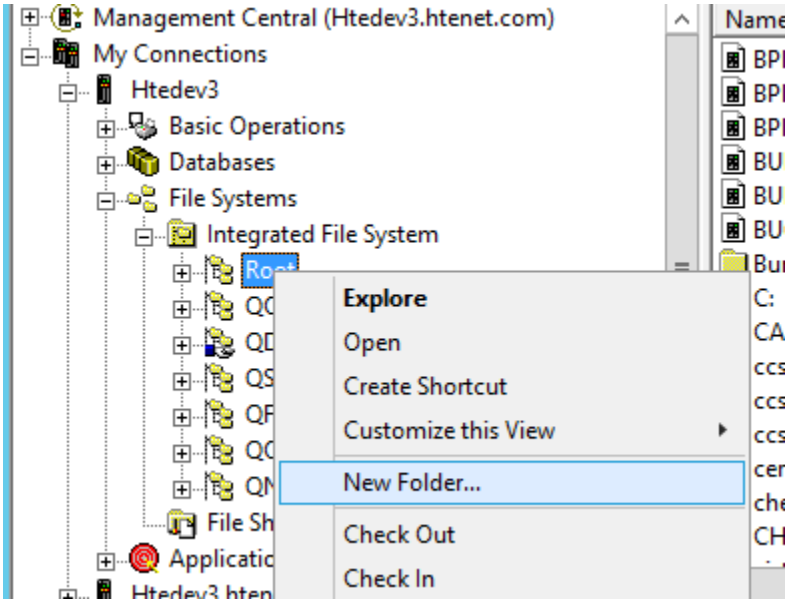

9. Upload each certificate into the CERT folder.

### *Using IBM System I Navigator*

1. Open up IBM System i Navigator
2. Select the iSeries server and login.
3. In the Navigation pane on the left, navigate to **My connections > [iSeries name or IP] > File Systems > Integrated File Systems > Root**




4. Create a CERT folder if one does not exist.



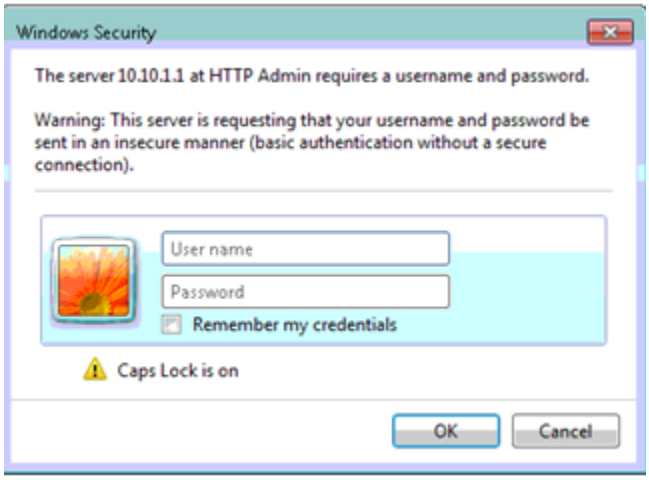

5. Click on the CERTS folder to view its contents
6. Copy the certificate files from your saved location to the CERTS folder
   a. **Drag/Drop:** You can drag and drop from the saved folder to the System I Navigator panel
   b. Copy/Paste:
      1. Select the certificate from the saved folder. Right click and select **Copy**
      2. Right-click on the CERTS folder in System I Navigator and left-click **Paste**

## Steps to Correct Part III - Using IBM Digital Cert Manager (DCM) to Import Public Keys to IBM System Store:

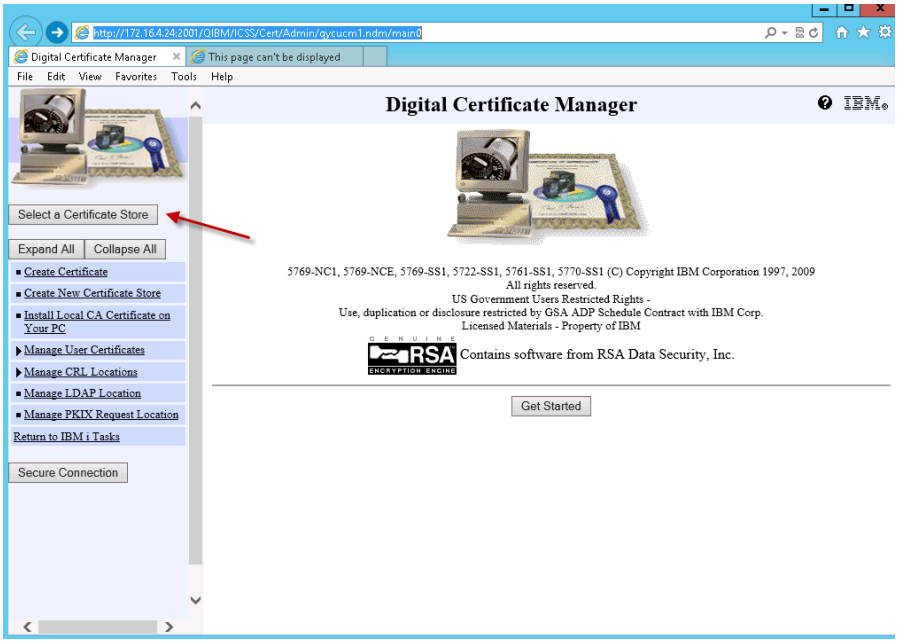
1. From iSeries green screen session:
   **`STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`**

a. Optional - Can also use command `NETSTAT *CNN` --> F14 for ports to confirm port 2001 is running

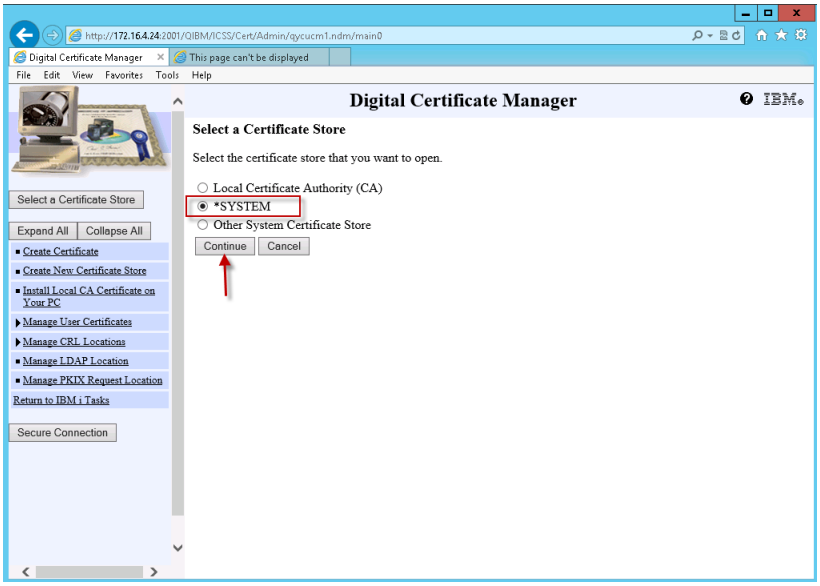
2. Open DCM interface in a browser using the following URL format: (see below)
   http://<iSeriesname-OR-IP>:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0
3. It will prompt for your iSeries username and password



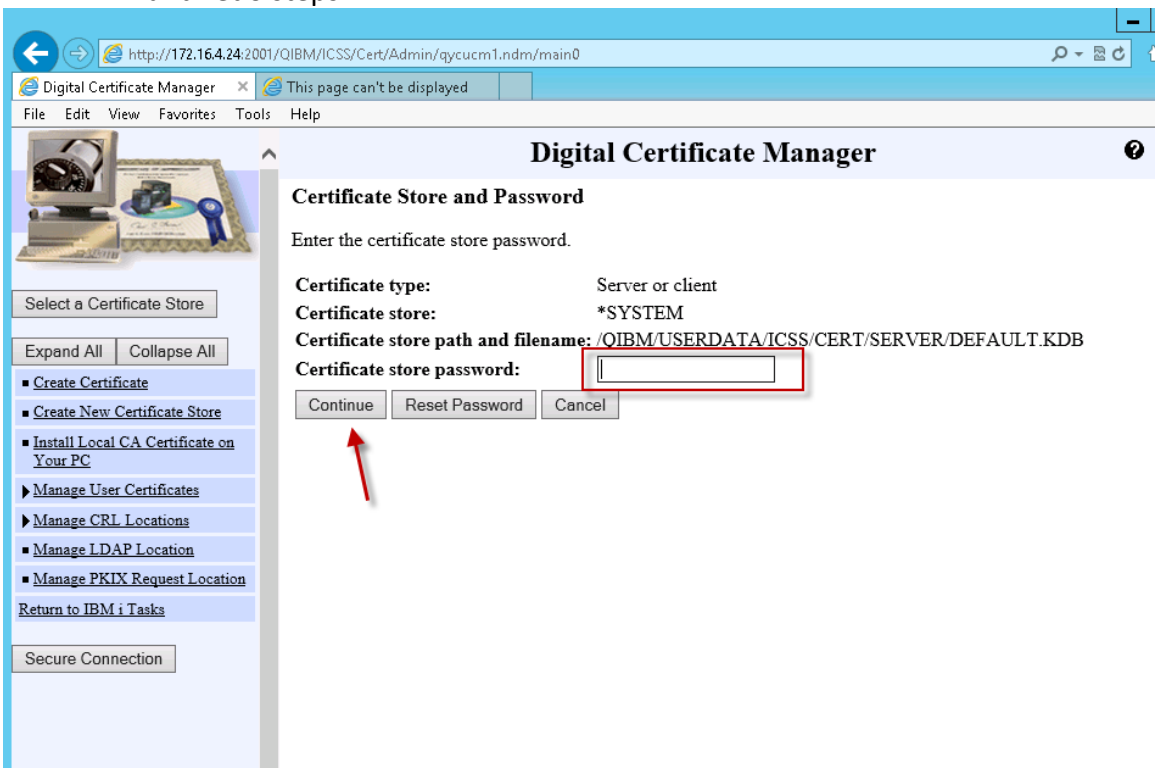

4. From the welcome screen, click **Select a Certificate Store** on the left



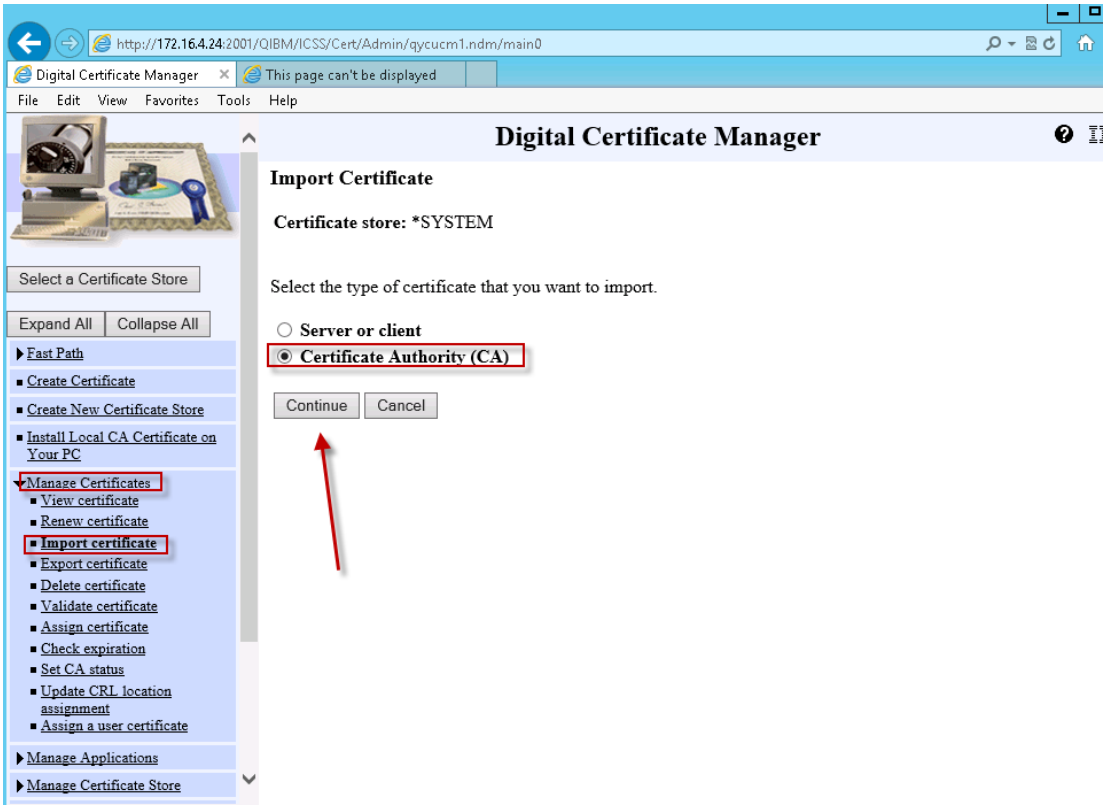

4. Select ***SYSTEM** certificate store and click **Continue** button (see below)
   a. NOTE: if the *SYSTEM cert store does not exist, it can be created with the "Create New Certificate Store" steps (left-hand menu) - although detailed steps are outside scope of this write-up




5. Enter **Certificate store password** when prompted and hit **Continue**
    a. NOTE: May be same as QHTE pass. If not, can choose **Reset Password** button to manually update it and redo steps

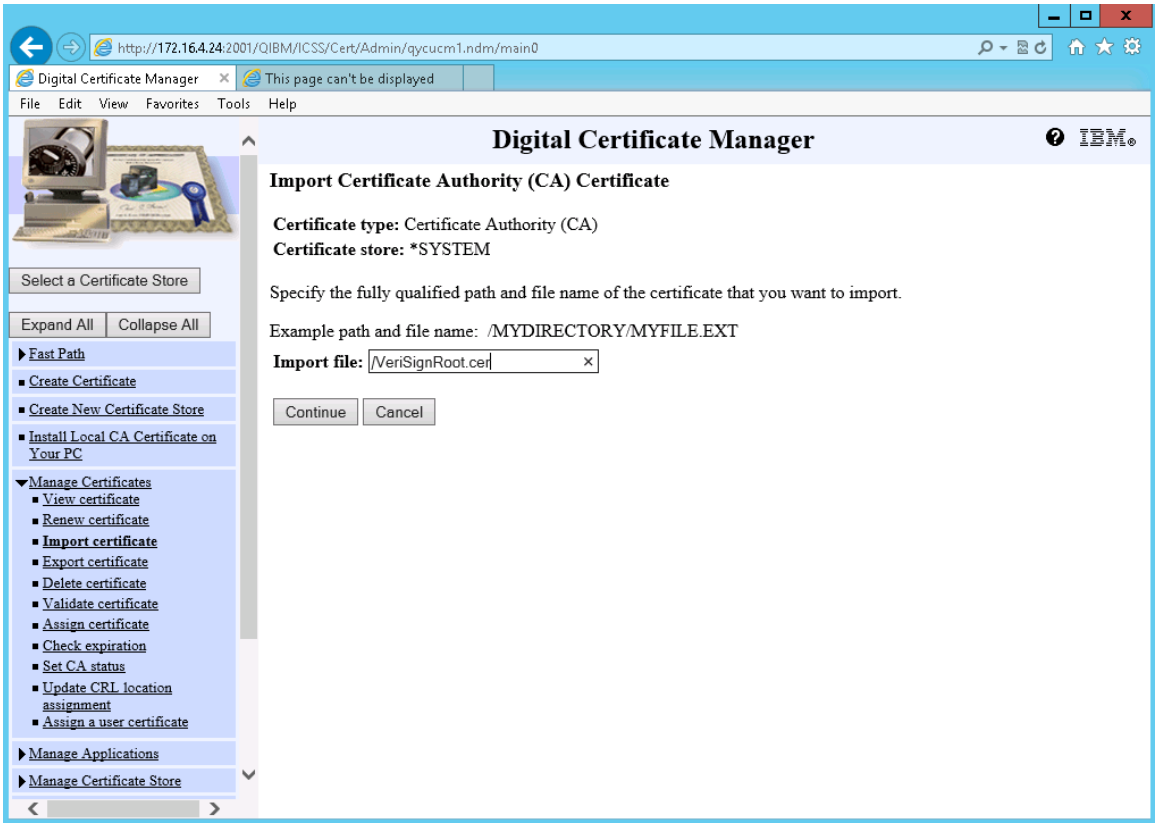



6. Go to the Import Certificates page:
    a. In the left-hand menu, select **Manage Certificates > Import Certificate**
    b. Select **Certificate Authority (CA)**
    c. Click the **Continue** button

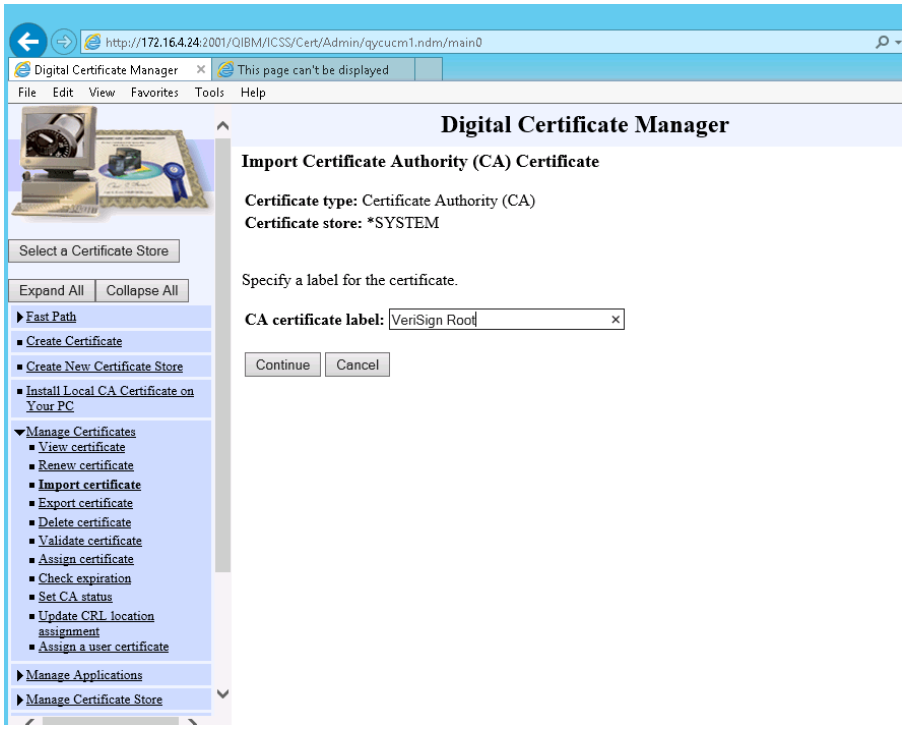



Starting with the highest level certificate, import each certificate file to the CERTS folder

7. Import File text box
    a. Enter **/CERTS/** in the text box, and then the **certificate file name**, INCLUDING the **.CER** at the end.
    b. Ex. /CERT/DigiCertRoot.cer
    c. Click **Continue**




8. Enter the **CA Certificate label** based on the name of cert (ex: VeriSign Root)
9. Click **Continue**
10. Click **OK** if green confirmation box appears
11. Repeat for each lower-level certificate, starting at step 6.




After importing all the certificates, you can view the certificate information to verify.

10. Go to the View Certificates page:
    a. In the left-hand menu, select **Manage Certificates > View Certificate**
    b. Select **a Certificate**
    c. Click **View** to see the certificate information

# Digital Certificate Manager

Select a certificate, then select View to see the certificate information.

| | Certificate Authority (CA) | Status |
|---|---|---|
| ◉ | DigiCert CA | Enabled |
| ○ | DigiCert Root | Enabled |
| ○ | Thawte Intermediate G2 2017 | Enabled |
| ○ | Thawte Root Cert 2017 | Enabled |
| ○ | GeoTrust Global CA | Enabled |
| ○ | GeoTrust True Credentials CA 2 | Enabled |
| ○ | Equifax Secure Certificate Authority | Enabled |
| ○ | Equifax Secure eBusiness CA-1 | Enabled |
| ○ | Equifax Secure eBusiness CA-2 | Enabled |
| ○ | Equifax Secure Global eBusiness CA-1 | Enabled |
| ○ | Microsoft Root Authority | Enabled |
| ○ | Thawte Personal Premium CA | Enabled |
| ○ | Thawte Personal Freemail CA | Enabled |
| ○ | Thawte Personal Basic CA | Enabled |
| ○ | Thawte Premium Server CA | Enabled |
| ○ | Thawte Server CA | Enabled |
| ○ | Verisign Class 1 Public Primary Certification Authority | Enabled |
| ○ | Verisign Class 2 Public Primary Certification Authority | Enabled |