

## SSL Communication Setup – iSeries Source

## Contents

INTRODUCTION	2
What address is iSeries communicating with?	2
CONFIRM ADDRESS ISERIES USES TO COMMUNICATE WITH OUTSIDE INTERNET	2
Explanation:	2
Steps to Complete / Determine:	2
LOCAL DNS IN PLACE?	
How to get IP of iSeries server	
HOW TO PULL UP LOGGING OF ISSUES IN ISERIES:	3
Navigation:	
CONFIGURE SYSTEM VALUES FOR ALLOWED SSL COMMUNICATION PROTOCOLS	4
Log Reflects Following:	
Steps to Correct Issue:	
IMPORT PUBLIC (INTERMEDIATE / ROOT) CERTIFICATES INTO ISERIES CERT STORE	7
Log Reflects Following:	7
STEPS TO CORRECT ISSUE PART I – OBTAIN CORRECT PUBLIC KEYS USING THE BROWSER:	7
STEPS TO CORRECT PART II - COPY OF FILES TO ISERIES IFS CERT FOLDER:	
Using IBM ACS	
Using IBM System I Navigator	
STEPS TO CORRECT PART III - USING IBM DIGITAL CERT MANAGER (DCM) TO IMPORT PUBLIC KEYS TO IBM SYSTEM	1 STORE: 15



## 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 thirdparty 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)

- 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

Command F9=Retrieve F12=Cancel F4=Prompt Verifying connection to host system ROLLACUA at address 10.10.1.1. ===> F4=Prompt F9=Retrieve F12=Cancel Connection verification statistics: 5 of 5 successful (100 %).

## 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

#### **OSSLCSL**

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 li	st

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 Number	Cipher 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:

#### 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

lasks					
🔏 Start InPriv	Open				
📑 Open new 🛞	Run as administrator				
🐚 Reopen las	Unpin from Taskbar				
	Properties				
Internet Exprorer					
📌 Unpin this program from taskbar					

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

Certificate
General Details Certification Path 5.
Certification path
VeriSign     Symantec Class 3 Secure Server CA - Ge     Symantec Class 3 Secure Server CA - Ge     Secure Secure Server CA - Ge     Secure Secure Server CA - Ge     Secure Secur
View Certificate
Certificate status: 7.
This certificate is OK.
OK

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



<b>–</b> Ce	ertificate	×
General Details Certification Pa	th	
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm	V3 0c 79 a9 44 b0 8c 11 95 20 92 sha256RSA	
Signature hash algorithm	sha256 DigiCert High Assurance EV Ro…	
Valid from Valid to	Tuesday, October 22, 2013 7: Sunday, October 22, 2028 7:0 DigiCert SH∆2 Extended Valida	~
	Edit Properties Copy to File	
	O	ĸ

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



56	lect the format you want to use:
	DER encoded binary X.509 (.CER)
[	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	O Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Microsoft Serialized Certificate Store (LSST)

- 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

😌 🍠 (	Certificate Export Wizard
Fil	e to Export Specify the name of the file you want to export
	File name: Browse



é		Save As				×
€ ∋ - ↑ 🎚	→ This PC → Local Disk (C:) →	Temp	~ Č	Search Temp		<i>م</i>
Organize 🔻 Ne	w folder				•	0
Documents Downloads	▲ Name	<u>۸</u>	Date modified	Туре	Size	
<ul> <li>This PC</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Local Disk (C;)</li> </ul>	~					
File name:	SymantecClass3CA-G4					~
Save as type:	Base64 Encoded X.509 (*.cer)					~
Aide Folders				Save	Cancel	

- 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



IBM i Access Client Solutions					
IBM i Access Client Solutions					
File Edit Actions Tools Help					
Welcome	Integrated File System provides an interface for browsing the integrated file system objects in the integrated file system in the following ways:				
System: HTEDEV3 v General Data Transfer	<ul> <li>Create new folders (directories, libraries, and folders)</li> <li>Delete objects</li> <li>Rename objects</li> <li>Copy objects between your client system and your IBM i</li> <li>Copy objects within the integrated file system on an IBM i or to the integra</li> <li>Send objects to another IBM i (or to several)</li> <li>View properties of objects</li> </ul>				
<ul> <li>5250 Emulator</li> <li>Integrated File System</li> <li>Navigator for i</li> <li>Printer Output</li> </ul>					
Database	Note: Copying or sending objects from one IBM i to another uses the QFileSvr.400 fil				
<ul> <li>Schemas</li> <li>Run SQL Scripts</li> </ul>	This task requires a system configuration. To add or change a system configuration, sele from the <b>Management</b> tasks.				
Use the <b>back button</b> to navigate	e back to the root folder ome/QCWW2 on HTEDEV3 – $\Box$ ×				
Directory					
/home/QCWW2 <	, <b>t</b> <i>C</i>				
Name	Size (KB) Last Modified				
0	/ on HTEDEV3 – 🗆 🗙				
File Edit View Actions					
HTEDEV3	✓ Filter ×				
/ <	, <b>t</b> <i>c</i>				
Name	<ul> <li>Size (KB)</li> <li>Last Modified</li> </ul>				
081111	1 August 10, 2011 2:46:45 PM EDT				
AA000008.TXT	1 June 19, 2012 4:09:24 PM EDT				

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

3.



8	/ on HTE	DEV3		- 0	×
File Edit View Actions					
HTEDEV3		✓ Filt	er		×
Directory					~
/				L	3
<			>		
Name	*	Size (KB)	Last Modified		
&FLRFIL2		7368	January 6, 2017 3:2	24:57 PM EST	^
081111		1	August 10, 2011 2:4	46:45 PM EDT	
2 1094C_Request_00000_	Mi New Folder	22	August 29, 2016 4:	16:55 PM EDT	
1094C_Request_BB0BD_	_M Upload	114	August 30, 2016 10	:13:45 AM EDT	
AA000008.TXT	Dente	1	June 19, 2012 4:09	:24 PM EDT	
AA1099.CSV	Paste	13	November 20, 2012	4:06:04 PM ES	Т
AAAexport.csv		222	January 6, 2011 6:2	27:47 AM EST	

- 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.



0	Upload	×
Destination: / Select a file: s\RLLA\Paymer	ntusDigcertBase.cer	Browse
Replace exi	sting file Cancel	

- 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.

CERT	г					
<u>File</u> <u>E</u> dit	: <u>V</u> iew <u>A</u> ctions					
RollaCUA					Filter	×
Director	rγ					
I CERT				m		
	Name	^	Size (KB)	Last Modified		
	DigiCertCA.cer DigiCertROOT.cer			1 January 4, 2018 2:1 1 January 4, 2018 2:1	12:47 PM CST 12:10 PM CST	

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



0	System	i Nav	igator				x
File Edit View Help							
19   X 🖻 🛍   X 😭   🏈 🔢 🛇						0 minutes	old
Environment: My Connections	Htedev3: Root Path: /						
Management Central (Htedev3.htenet.com)	Name		Size	Туре	Changed	Accessed	^
Imagement Central (Htedev3.htenet.com)         Imagement Central (Htedev3.htenet.com)         Imagement Central (Htedev3.htenet.com)         Imagement Central (Htedev3.htenet.com)         Imagement Central (File System)         Imagement Central (Htedev3.htelev3.htelev3.htelev3.htelev3)         Imagement Central (Htedev3.htelev3)         Imagement Central (Htedev3.htelev3)         Imagement Central (File System)         Imagement Central (File System)         Imagement Central (File System)         Imagement Central (File System)         Imagement Central (Htedev3.htelev3)         Imagement Central (Htedev3)         Imagement Central (File System)         Imagement Central (File System)	Name         Image: Strength of the strengend of the strengt of the strength of the s		Size 7.03MB 2.00MB 1KB 23KB 112KB 23KB 218KB 218KB 300KB 14KB 11KB 300KB 10KB 10KB 10KB 10KB 10KB 10KB 10KB	Type File OLD File File XML Document XML Document Text Document Microsoft Excel Com Microsoft Excel Com Microsoft Excel Com Text Document File Folder File Folder File Folder File Folder File Folder	Changed 1/6/17 3:24:57 PM 3/1/09 9:51:41 PM 8/10/11 2:46:45 PM 8/29/16 4:16:55 PM 8/30/16 10:13:45 AM 6/19/12 4:09:24 PM 11/20/12 4:09:24 PM 11/20/12 4:09:24 PM 11/20/12 4:09:24 PM 11/20/11 6:18:18 AM 8/6/10 8:09:13 AM 10/28/13 7:23:25 PM 2/24/16 11:18:36 AM 4/14/16 11:14:16 AM 9/2/15 12:22:56 PM 9/2/15 12:23:09 PM	Accessed 1/6/17 3:24:50 PM 3/1/09 9:26:51 PM 8/11/11 10:06:38 AM 8/29/16 4:16:15 PM 8/30/16 9:41:45 AM 7/16/13 4:21:41 PM 8/17/15 9:32:43 AM 1/6/11 6:28:11 AM 11/28/12 9:22:16 AM 8/6/15 2:53:47 PM 2/26/14 12:16:03 PM 2/9/18 2:48:36 AM 2/9/18 2:48:36 AM 2/9/18 2:48:36 AM	
🕀 🔁 QS Create Sho	rtcut		ccs				
	this View		CCS				
⊡ 12 Q0 ⊕ 12 QN New Folde	r		cer				
File Sh Check Out			CH				
Htedev3 hten Check In			-				

- 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:

4.

- 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

Contractional Certificate Manager 🛛 🗶	C C I his page can't be displayed	
File Edit View Favorites To	ools Help	
	A Digital Certificate Manager	0 IBM.
Constant of the second		
Select a Certificate Store		
Expand All Collapse All		
<ul> <li>Create Certificate</li> </ul>	5769-NC1, 5769-NCE, 5769-SS1, 5722-SS1, 5761-SS1, 5770-SS1 (C) Copyright IBM Corporation 1997, 2009	
<ul> <li>Create New Certificate Store</li> </ul>	All rights reserved. US Government Users Restricted Rights -	
<ul> <li>Install Local CA Certificate on Your PC</li> </ul>	Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp. Licensed Materials - Property of IBM	
Manage User Certificates	Contains software from RSA Data Security. Inc.	
Manage CRL Locations		
<ul> <li>Manage LDAP Location</li> </ul>		
<ul> <li>Manage PKIX Request Location</li> </ul>	Get Staffed	
Return to IBM i Tasks		
Secure Connection		
	~	
<b>`</b>		

- 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



	_ 🗆 X
C ( ) ( http://172.164.24:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0	Ø ★ 🔒 5 ≝ - Q
🙆 Digital Certificate Manager 🛛 🗙 🎯 This page can't be displayed	
File Edit View Favorites Tools Help	
Digital Certificate Manager	Ø IBM.
Select a Certificate Store	
Select the certificate store that you want to open.	
Select a Certificate Store	
Expand All Collapse All Other System Certificate Store	
<u>Create Certificate</u> Continue     Cancel	
<u>Create New Certificate Store</u>	
Install Local CA Certificate on Your PC	
Manage User Certificates	
Manage CRL Locations	
<u>Manage LDAP Location</u>	
<u>Manage PKIX Request Location</u>	
Return to IBM i Tasks	
Secure Connection	
× ·	

- 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

(<) Ø http://172.16.4.24:2001.	/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0 🖉 🖉 🕻
<i>e</i> Digital Certificate Manager 🛛 🗙 🎸	Fhis page can't be displayed
File Edit View Favorites Tools	Help
	Digital Certificate Manager         Image: Certificate Store and Password
a 10m	Enter the certificate store password.
Select a Certificate Store	Certificate type: Server or chent
Expand All Collapse All	Certificate store path and filename: /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB Certificate store password:
<u>Create Certificate</u> Create New Certificate Store	Continue Reset Password Cancel
Install Local CA Certificate on Your PC	
Manage User Certificates	
Manage CRL Locations	
<ul> <li>Manage LDAP Location</li> </ul>	
<ul> <li>Manage PKIX Request Location</li> </ul>	
<u>Return to IBM i Tasks</u>	
Secure Connection	

- 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**

	Certificate Authority (CA)	Status
۲	DigiCert CA	Enabled
0	DigiCert Root	Enabled
0	Thawte Intermediate G2 2017	Enabled
0	Thawte Root Cert 2017	Enabled
0	GeoTrust Global CA	Enabled
0	GeoTrust True Credentials CA 2	Enabled
Ο	Equifax Secure Certificate Authority	Enabled
0	Equifax Secure eBusiness CA-1	Enabled
0	Equifax Secure eBusiness CA-2	Enabled
0	Equifax Secure Global eBusiness CA-1	Enabled
Ο	Microsoft Root Authority	Enabled
0	Thawte Personal Premium CA	Enabled
0	Thawte Personal Freemail CA	Enabled
0	Thawte Personal Basic CA	Enabled
0	Thawte Premium Server CA	Enabled
0	Thawte Server CA	Enabled
0	Verisign Class 1 Public Primary Certification Authority	Enabled
$\cap$	Verision Class 2 Public Primary Certification Authority	Enabled

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