

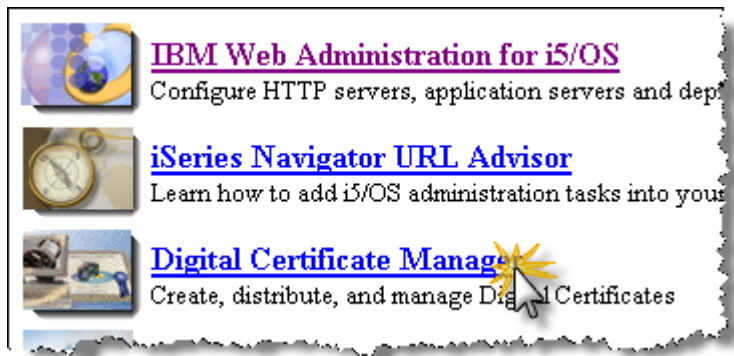
# Create Local Certificate Authority and Self Signed Certificate

(for V5R4 and previous)

This document will detail how to create a Local Certificate Authority(CA) so a self signed certificate can be created. This is an alternative to purchasing a certificate from a respected Certificate Authority like Verisign or Thawte. The advantage to purchasing a certificate from a respected CA is that it then usually means people trying to connect to your web service will NOT need to manually install the CA because it came pre-installed on the machine from the operating system vendor (i.e. IBM, Microsoft, Sun, etc).

## Start the Admin Server

After starting the admin server instance (STRTCPSVR SERVER(\*HTTP) HTTPSVR(\*ADMIN) ) go ahead and sign into the admin instance at <http://myas400ip:2001>. Select the "Digital Certificate Manager" link on the Tasks page. Note that as of V6R1 this process is different and we have not yet developed documentation for that release.

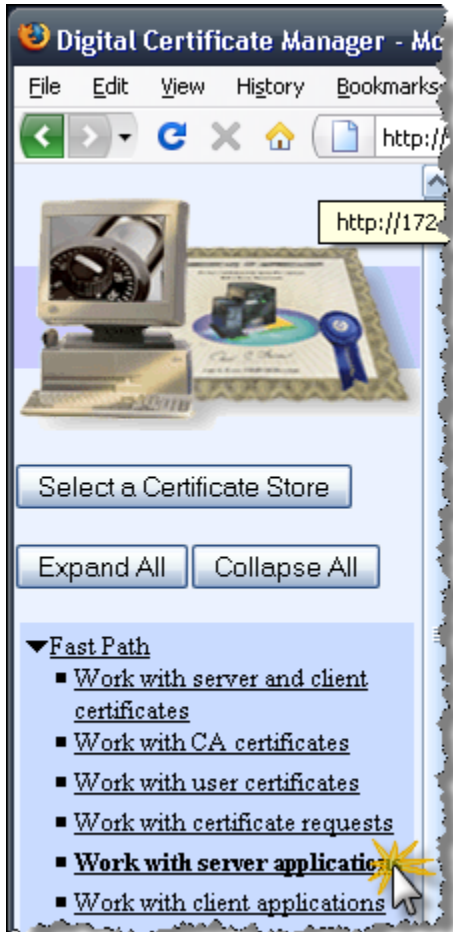


## Create SSL Application

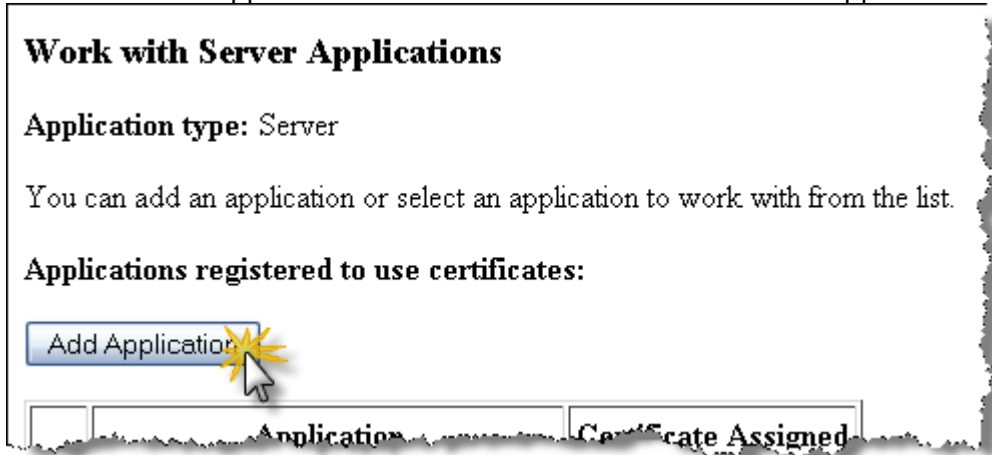
The first general concept is to create an "SSL Application" as a preparation step so that we can use it later in a wizard process when we create the Certificate within the Certificate Authority. To setup an SSL Application you first need to select the \*SYSTEM certificate store by selecting the "Select a Certificate Store" button in the left nav. If the \*SYSTEM store has not been created then it won't be displayed. To setup the \*SYSTEM certificate store please view the following tutorial: <http://rpg-xml.com/SSLSetup.aspx>



To create the SSL Application go ahead and select the "Work with server applications" link within "Fast Path" (note you should have already selected the \*SYSTEM certificate store using the "Select a Certificate Store" button) in the previous step.



Select the "Add Application" button on the "Work with Server Applications" screen.



Fill out the "Add Application" form by specifying the "Application ID" field and the "Application description" field.

### Add Application

Application type: Server

Application ID:

Exit program information	
Exit program:	<input type="text" value="*NONE"/>
Exit program library:	<input type="text"/>
Threadsafe:	<input type="text" value="No"/> <input type="button" value="v"/>
Multithreaded job action:	<input type="text" value="Use system value only"/> <input type="button" value="v"/>

Application user profile:	<input type="text" value="*NONE"/>
Define the CA trust list:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Client authentication supported:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Client authentication required:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Certificate revocation processing:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Enter either the application description message information or an application description.

*Application description message information*

<input type="radio"/>	Message file:	<input type="text"/>
<input type="radio"/>	Message file library:	<input type="text"/>
<input type="radio"/>	Message ID:	<input type="text"/>
<input checked="" type="radio"/>	Application description:	<input type="text" value="SSL app for XML web services"/>

Select the "Create a Certificate Authority (CA)" link. Make sure you have already selected the \*SYSTEM certificate store (i.e. the "Select a Certificate Store" button is used for that).



Fill out the "Create a Certificate Authority (CA)" form. Specify a secure password. Specify the CA name (I usually specify the "official" name of the company). Specify the Organization name (I usually just copy from the CA name). Specify the State and Country. Select the "Continue" button.

## Create a Certificate Authority (CA)

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

**Certificate store:** Local Certificate Authority (CA)

The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.

**Key size:**  (bits)

**Certificate store password:**  (required)

**Confirm password:**  (required)

### Certificate Information

**Certificate Authority (CA) name:**  (required)

**Organization unit:**

**Organization name:**  (required)

**Locality or city:**

**State or province:**  (required, character limit)

**Country or region:**  (required)

**Validity period of Certificate Authority (CA) (2-7300):**  (days)

You will now be presented with the "Install Local CA Certificate" screen. From here you can choose to select the "Install certificate" link if you want to save this for use later on (i.e. provide it to a PC programmer connecting to your web service) or click the Continue button. Note you can get to the certificate later if necessary.

## Install Local CA Certificate

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

**Certificate store:** Local Certificate Authority (CA)

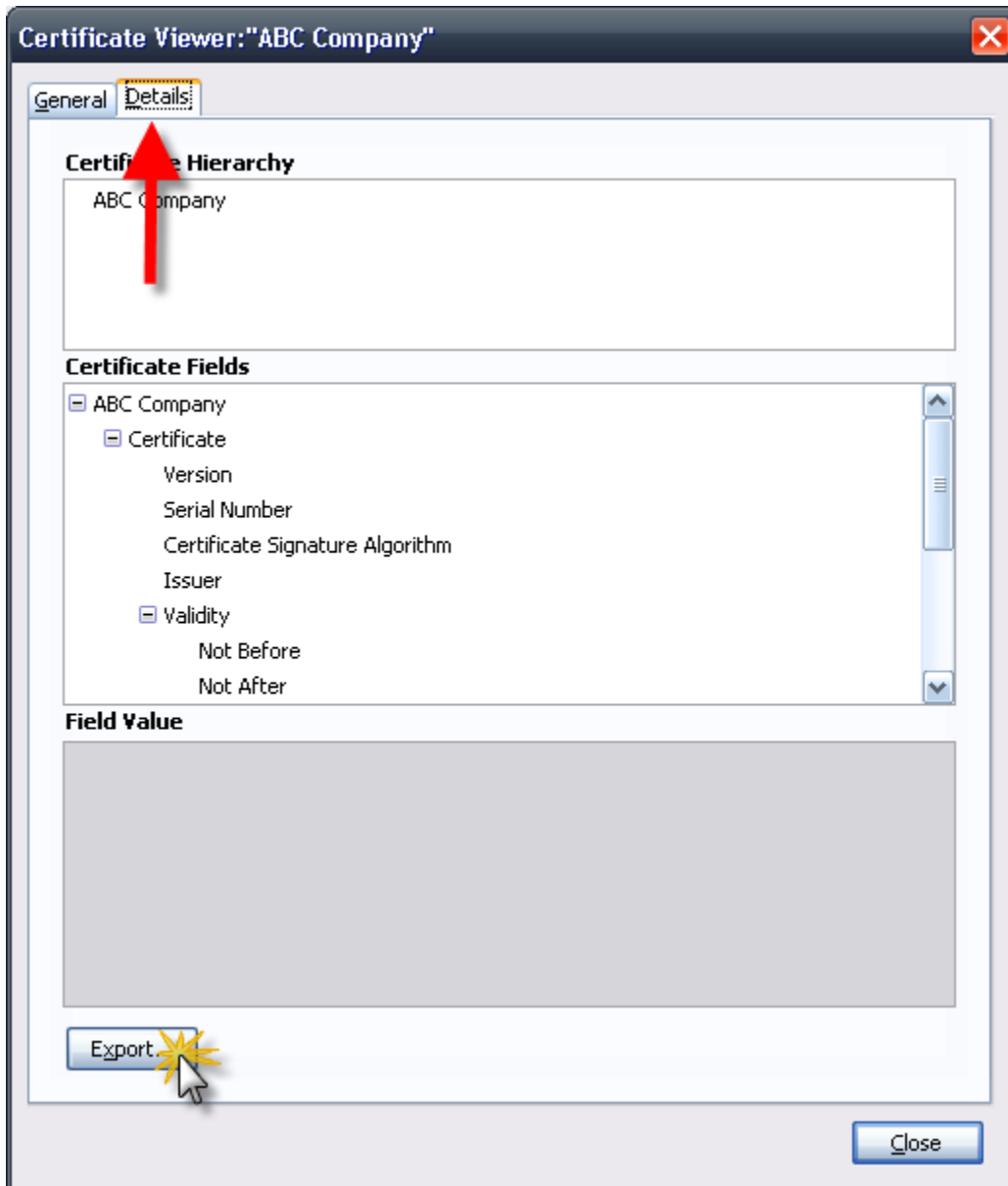
A certificate for your Certificate Authority (CA) was created and stored in the local Certificate Authority (CA) certificate store.

You must install the Certificate Authority (CA) certificate in your browser so the browser can verify certificates that your CA issues. Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.

[Install certificate](#)

After installing the certificate, select Continue so you can provide the policy data that will be used for signing and issuing certificates with this Certificate Authority (CA).

If you select the "Install certificate" link then, depending on what browser you are using (FireFox in the case of this tutorial), you will be presented with a dialog to take you through the process of downloading the certificate to your desktop. The following screen shots show how to export the CA certificate.



Modify the Policy Data values if necessary. Below is a common approach for this page as it keeps the certificates valid for the longest period of time (i.e. 2000 days).

### **Certificate Authority (CA) Policy Data**

Your Certificate Authority (CA) was created with the default policy data shown below. Change the data if you want and then select Continue.

**Allow creation of user certificates:**  Yes  No

**Validity period of certificates that are issued by this Certificate Authority (CA) (1-2000):**  (days)

Days until Certificate Authority (CA) expires: 7300

At this point the Certificate Authority creation process is complete. You can select the "Cancel" button at this point and continue onto the next step detailed next.

### Select Applications to Trust this Certificate Authority (CA)

Message The policy data for the Certificate Authority (CA) was successfully changed.

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

**Certificate store:** Local Certificate Authority (CA)

Select the applications that should include this Certificate Authority (CA) in the application Certificate Authority (CA) trust list:

Select All

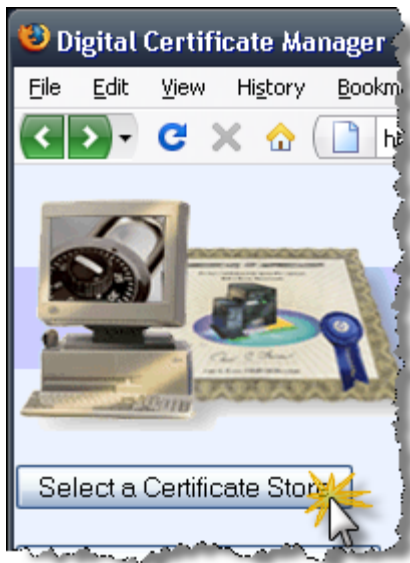
Clear All

	Application	Type	Assigned certificate
<input type="checkbox"/>	i5/OS TCP/IP Telnet Server	Server	<i>None assigned</i>
<input type="checkbox"/>	Cluster Security	Server	<i>None assigned</i>
<input type="checkbox"/>	IBM Directory Server	Server	<i>None assigned</i>
<input type="checkbox"/>	IBM Directory Server publishing	Client	<i>None assigned</i>
<input type="checkbox"/>	IBM Directory Server client	Client	<i>None assigned</i>
<input type="checkbox"/>	i5/OS VPN Key Manager	Server	<i>None assigned</i>
<input type="checkbox"/>	i5/OS TCP/IP FTP Server	Server	<i>None assigned</i>
<input type="checkbox"/>	i5/OS TCP/IP FTP Client	Client	<i>None assigned</i>

Continue

Cancel

The \*SYSTEM Certificate Store **should** be selected at this point, but to ensure it is we will go ahead and select it again. Select the "Select a Certificate Store" button.



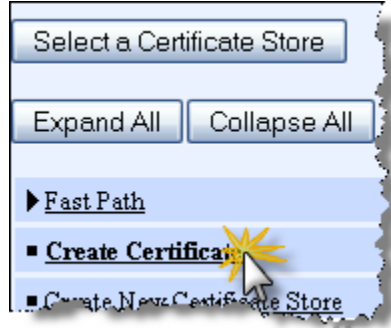
Select the \*SYSTEM certificate store and select the Continue button. Do NOT select Local Certificate Authority (CA) at this point as it looks the same as another screen's radio button that we will select in a bit.



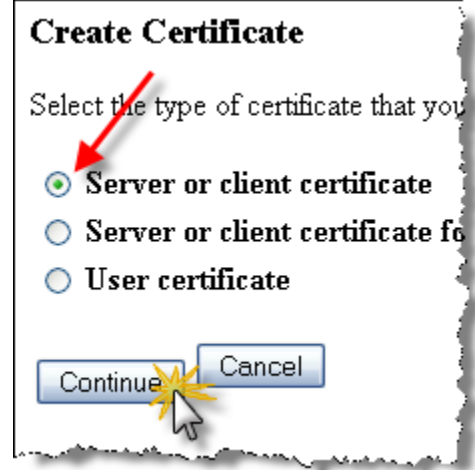
Enter the password and select the Continue button.



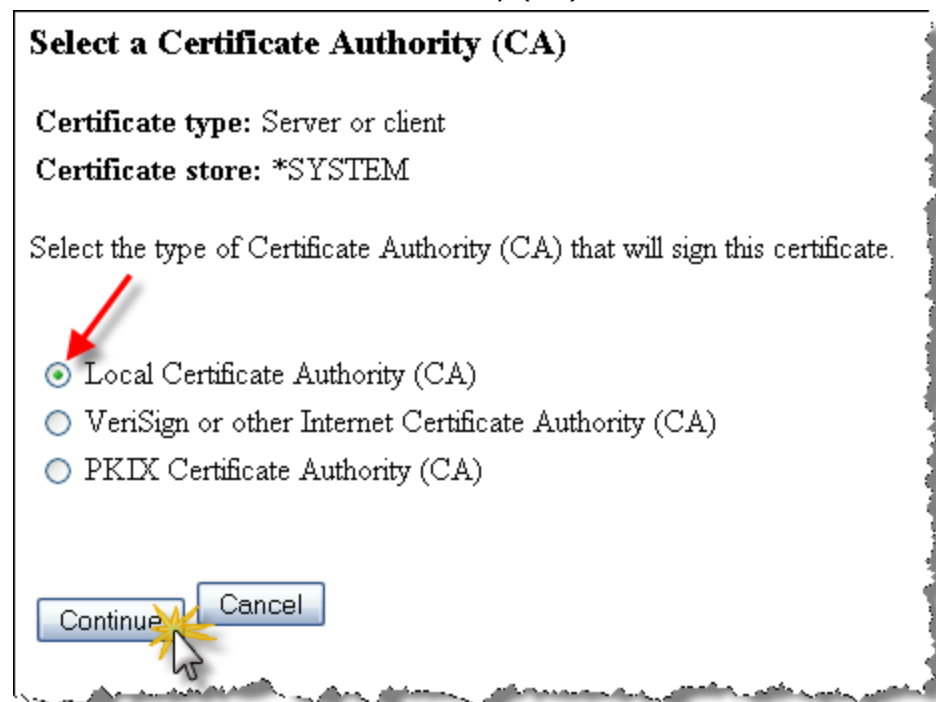
In the left nav select the "Create Certificate" link.



On the "Create Certificate" page select the "Server or client certificate" radio button and click Continue.



Select the "Local Certificate Authority (CA)" radio button and select Continue.



On the "Create Certificate" page fill out all of the fields. The "Certificate label" field can be any value that will allow you to easily reference this later on apart from other certificates that may be created. The "Common name" value is important because you will want it to match the exact URL of the web service being offered on the AS400. If you don't make it the same then there is the potential that not all clients will be able to connect to your web service based on warnings being issues when their program initializes the secure connection (our experience).

As noted, the bottom of the form where the "Subject Alternative Name" appears do not require entry in those fields. We do not use these fields when we create certificates.

## 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:**  (bits)

**Certificate label:**  (required)

### Certificate Information

**Common name:**  (required)

**Organization unit:**

**Organization name:**  (required)

**Locality or city:**

**State or province:**  (required: minimum of 3 characters)

**Country or region:**  (required)

### Subject Alternative Name

**Note:** Certificate extensions are not necessary for Secure Sockets Layer (SSL), but are recommended for Virtual Private Network (VPN).

**IP version 4 address:**  .  .  .

**Fully qualified domain name:**   
(host\_name.domain\_name)

**E-mail address:**   
(user\_name@domain\_name)

On the "Select Applications" page you will now select the SSL application you created earlier – in this case "SSL app for XML web services". Select the "Continue" button.

<input type="checkbox"/>	Enterprise Identity Mapping (EIM)	Client	None assigned
<input type="checkbox"/>	i5/OS TCP/IP FTP Server	Server	None assigned
<input type="checkbox"/>	i5/OS TCP/IP FTP Client	Client	None assigned
<input type="checkbox"/>	Webserver Search Engine	Server	None assigned
<input type="checkbox"/>	HTTP Server Monitor	Server	None assigned
<input checked="" type="checkbox"/>	SSL app for XML web services	Server	None assigned

Finally, select the OK button to complete the creation of the self signed certificate and its assignment to the SSL application.

**Application Status**

Message The applications you selected will use this certificate.

Next the SSL application needs to be associated to an Apache server instance. To accomplish this we need to go back to the iSeries Tasks page at <http://as400ip:2001> and select link "IBM Web Administration for i5/OS".

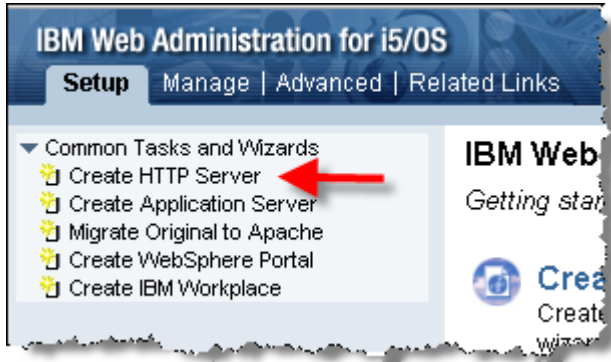
 [IBM Web Administration for i5/OS](#)  
Configure HTTP servers, application servers, and deploy applications

 [iSeries Navigator URL Advisor](#)  
Learn how to add i5/OS administration tasks into your web application

 [Digital Certificate Manager](#)  
Create, distribute, and manage Digital Certificates

You can either add SSL functionality to an existing Apache server instance or create a new one to facilitate the web service SSL requests. To make it more apparent what needs to be implemented for SSL capabilities we will create a very simple Apache server instance.

On the main "IBM Web Administration for i5/OS" screen select the "Setup" tab and the "Create HTTP Server" link.



Give the server a name and description.

### Create HTTP Server

Welcome to the Create New HTTP Server wizard. This wizard helps you set up an HTTP server (powered by Apache).

You must name your new server. This name will be used later to manage the server.

What do you want to name your new server?

Server name:

Server description:

Click **Next** to continue or **Cancel** to leave at anytime.

Take the defaults on the "Server root" value and select the "Next" button.

### Create HTTP Server

The server root is the base directory for your server. Within this directory, the wizard will create subdirectories for your logs and configuration information. Supported file systems for the server root are root and QOpenSys.

Which directory would you like to use as the server root for your new server?

Server root:

**Note:** If the server root directory does not exist, the wizard will create it for you.

Take the defaults on the "Document root" value and select the "Next" button.

### Create HTTP Server

The document root is the base directory from which documents will be served by your server.

Which directory would you like to use as the document root for your new server?

Document root:

**Note:** If the document root directory does not exist, the wizard will create it for you.

Select an IP address and enter a value of 443 into the "Port" field. Select the "Next" button.

### Create HTTP Server

Your server may listen for requests on specific IP addresses or on all IP addresses.

On which IP address and TCP port would you like your new server to listen?

IP address:

Port:

**Note:** Most browsers make requests to port 80 by default.

Take the default for the "access log" setting and select the "Next" button.

### Create HTTP Server

Your server can record activity on your web site using an access log. This information includes information about requests made to the server. This information is used to help you understand how your web site is being used and how many requests have been made.

Do you want your new server to use an access log?:

Yes  
 No

**Note:** An error log is separate from an access log and will be created regardless of your decision to use an access log.

Take the default for the time to keep the log files and select the "Next" button.

### Create HTTP Server

The error and access logs being created for this server will be rotated on a daily basis, to prevent the individual log files from becoming too large. The number of closed out files from becoming too large will be automatically deleted the oldest ones. When enabled, the logs reach a specific age.

Specify the time to keep the log files:

Keep, do not delete  
 Delete based upon age

Delete age:

Review the summary of the instance you are about to create and select the "Finish" button.

### Create HTTP Server

**Server name:** SECURE1  
**Server description:** Secure HTTP CGI instance  
**Server root:** /www/secure1  
**Document root:** /www/secure1/htdocs  
**IP address:** 172.29.141.159  
**Port:** 443  
**Log directory:** /www/secure1/logs  
**Access log file:** access\_log  
**Error log file:** error\_log  
**Log maintenance:** 7 days

Make sure you are in the "Manage" tab and the "Http Servers" tab and that the correct server is selected, then click the "Edit Configuration File" link.

The screenshot shows the IBM Web Administration for i5/OS interface. The top navigation bar includes 'Setup', 'Manage' (selected), 'Advanced', and 'Related Links'. Below this, there are tabs for 'All Servers', 'HTTP Servers' (selected), and 'ASF Tomcat Servers'. The main content area displays 'Server: SECURE1 - Apache' and 'Server area: Global configuration'. A red arrow points to the 'Manage Apache server "SECURE1" - Apache/2.0.58' title. Another red arrow points to the 'Edit Configuration File' link in the left-hand navigation menu. The page content includes a 'Secure HTTP CGI instance' section and a welcome message.

Enter the below text into the text area in the browser on the "Edit Configuration File" page and select the "Apply" button.

```
LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVPGM
Listen 172.29.141.159:443
SetEnv HTTPS_PORT 443
SSLEngine On
SSLAppName SSL_APP1
DocumentRoot /www/secure1/htdocs

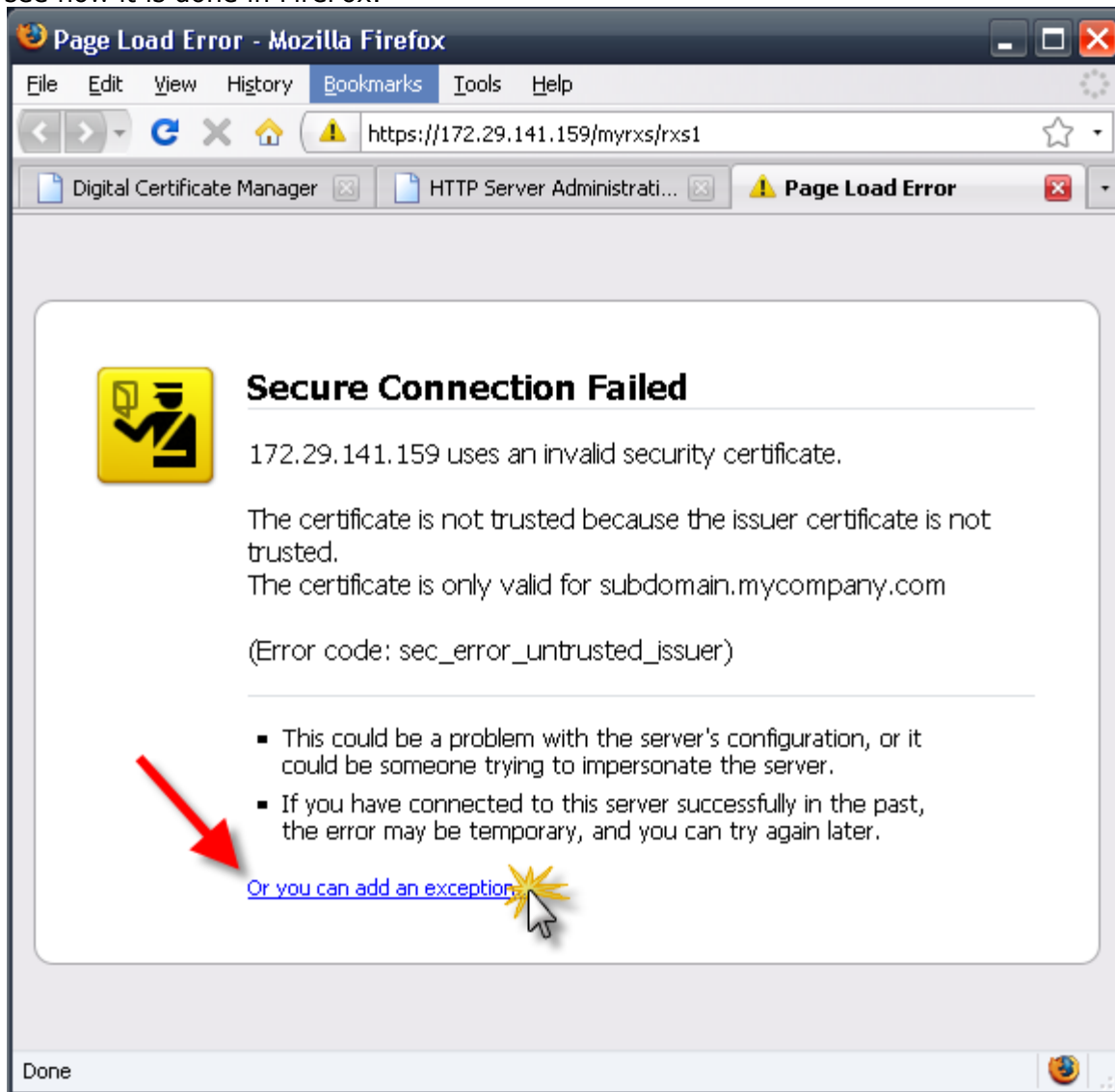
CGIConvMode %EBCDIC/EBCDIC%
ScriptAliasMatch ^/MYRXS/(.*) /qsys.lib/MYRXS.lib/$1.pgm

<Directory /qsys.lib/MYRXS.lib>
  allow from all
  order allow,deny
  options +ExecCGI
</Directory>
```

Stop and start your Apache server instance with the buttons in the upper left of the page. Make sure the HTTP instance is fully stopped before starting it by using the blue refresh button (note, it shouldn't have already been started unless you started it).

This screenshot shows the server status controls in the IBM Web Administration for i5/OS interface. The 'Server: SECURE1 - Apache' dropdown is visible. A red arrow points to the 'Stop' button (a square with a red 'X'). A mouse cursor is hovering over the 'Start' button (a green play icon). The status indicator shows a red stop sign, indicating the server is stopped.

Open up another browser tab and enter this address: <https://as400ip/myrxs/rxs1> where as400ip is the IP of your AS400. Note that by default the browser will go to port 443 when we specify https. Because the Apache instance we created isn't a "trusted" Certificate Authority it will prompt you. Go ahead and accept the certificate. The method of accepting the certificate is different based on the browser. Below you can see how it is done in FireFox.





After accepting the certificate you will be presented with the results of the web service. At this point you are completely done with setting up a Local Certificate Authority, a self signed certificate, and applying all that to an Apache server instance.

