West Certificate Update Process

01/10/2024 12:39 pm EST

Read this whole article before performing any of the actions within it.

What is West?

West (formally Intrado) is the company we use for PSAP lookups. They allow us to query a web service for PSAP using a street address or coordinates (lat/long).

Where do we use their service?

We have a web service hosted on our PSAP server loc01.boldgroup.solutions that communicate with the West web services. Our customer's Location Servers make PSAP web requests to loc01.boldgroup.solutions (http://loc01.boldgroup.solutions/PSAP/PsapServiceErl.svc), we make a web request to West and return the results.

Certificates

West issues us certificates to use in order to securely access their web services. When making the web service request, we use the certificate. Without the certificate, West rejects the web request. The certificate has an expiration date where it will no longer be accepted by West. A month or two before the certificates expire, West will send new certificates that we need to test and put into production. They typically send us two certificates, one for their lab service (testing) and one for their production service.

Info from West with new certificates

We typically get two emails and a voicemail from West. One of the emails contains the names of the certificates, their expiration date and the private key password for each certificate. The other email contains a compressed 7z file that has 4 files in it. Two of the files are instructions on how to extract the certificates. The other two are EXE files (they are actually .rename files after you unzip the 7z that you have to rename .exe) that you run that will output the certificates in pfx format.

The voicemail has the password for the 7z file.

What to do with the certificates

Typically you would want to install and test the certificates on a backup PSAP server. At the time of writing this I believe we only have one setup.

Only the production West certificate needs to be installed on our PSAP server. The lab certificate would only be used by a developer when testing (so we don't get charged for each test).

```
rem Install the certificate
certutil -f -v -p "the private key password West sent us for this certificate" -importpfx "the name of the certificate.pfx"

rem Install the certificate in the LOCAL_MACHINE\Personal and give "NETWORK SERVICE" access to use the certificate.
winhttpcertcfg.exe -g -c LOCAL_MACHINE\My -s "the name of the certificate" -a "NETWORK SERVICE"
winhttpcertcfg.exe -g -c LOCAL_MACHINE\My -s "the name of the certificate" -a "IIS AppPool\DefaultAppPool"

rem Install additional certificates that West needs in order to function.
certutil -f -addstore ROOT "ComodoHighAssuranceCA.crt"
certutil -f -addstore ROOT "AddTrust.crt"
certutil -f -addstore ROOT "Startup\Intrado_Chain_Bundle.crt"
```

The ComodoHighAssuranceCA.crt and AddTrust.crt certificates should be in the Startup sub-folder of where our PSAP service is hosted. If this is a new install on a new PSAP machine then get the certificates from Development.

NOTE: If this is an existing install of our PSAP service, then you don't need to install the ComodoHighAssuranceCA.crt or AddTrust.crt certificates because they will already be installed.

Example of a successful install:

C:\>certutil -f -v -p "private key password" -importpfx "BOLD_ERL_2019.pfx"
Certificate "BOLD_ERL_2019" added to store.

CertUtil: -importPFX command completed successfully.

C:\>winhttpcertcfg.exe -g -c LOCAL_MACHINE\My -s "BOLD_ERL_2019" -a "NETWORK SERVICE"
Microsoft (R) WinHTTP Certificate Configuration Tool
Copyright (C) Microsoft Corporation 2001.

Matching certificate:
E=webapplicationsteam.safetyservices@west.com
CN=BOLD_ERL_2019
OU="Tech Ops, Web Applications"
O=West Safety Services
L=Longmont
S=Colorado
C=US

Granting private key access for account:
NT AUTHORITY\NETWORK SERVICE

C:\>certutil -f -addstore ROOT "ComodoHighAssuranceCA.crt"
ROOT "Trusted Root Certification Authorities"
Related Certificates:

Exact match:
Element 8:
Serial Number: 1690c329b6780607511f05b0344846cb
Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE

NotBefore: 04/15/2010 6:00 PM
NotAfter: 05/30/2020 4:48 AM
Subject: CN=COMODO High-Assurance Secure Server CA, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Non-root Certificate
Cert Hash(sha1): b9b4c7a488c0885ec1c83aa87e4ebd2b215f9fa4

Certificate "COMODO High-Assurance Secure Server CA" already in store.
CertUtil: -addstore command completed successfully.

C:\>certutil -f -addstore ROOT "AddTrust.crt"
ROOT "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

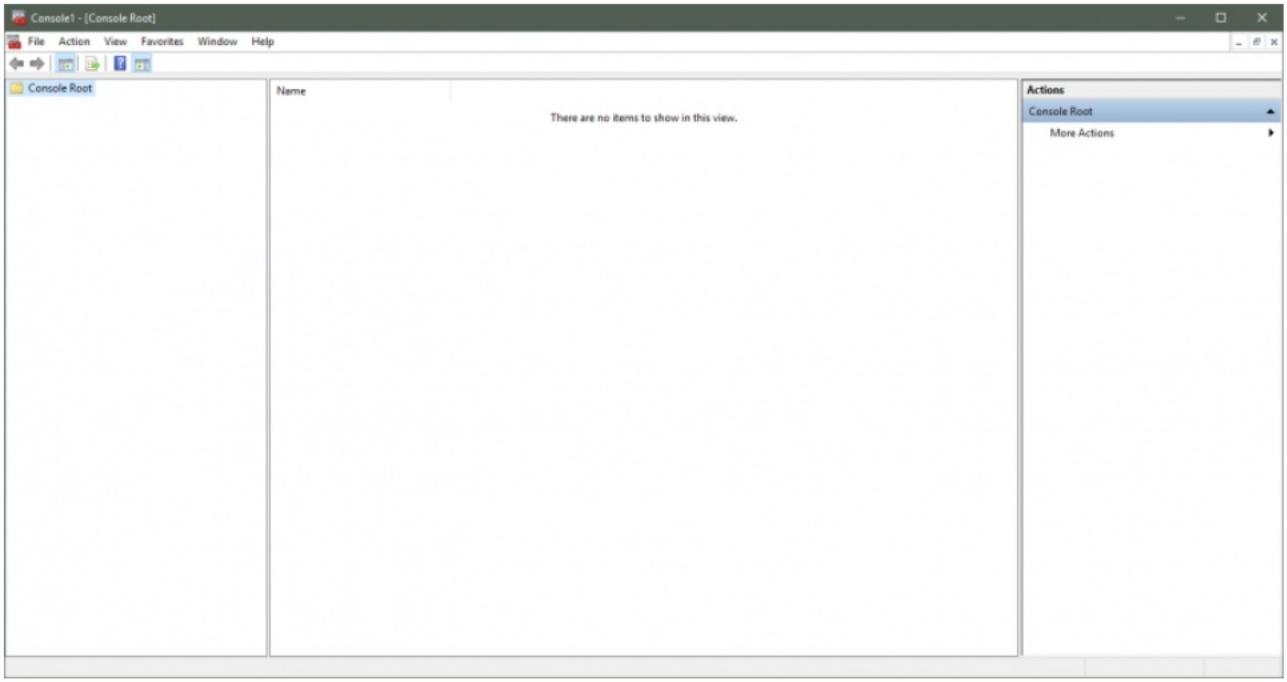
Exact match:
Element 28:
Serial Number: 01
Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
NotBefore: 05/30/2000 4:48 AM
NotAfter: 05/30/2020 4:48 AM
Subject: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 02faf3e291435468607857694df5e45b68851868

Certificate "AddTrust External CA Root" already in store.
CertUtil: -addstore command completed successfully.

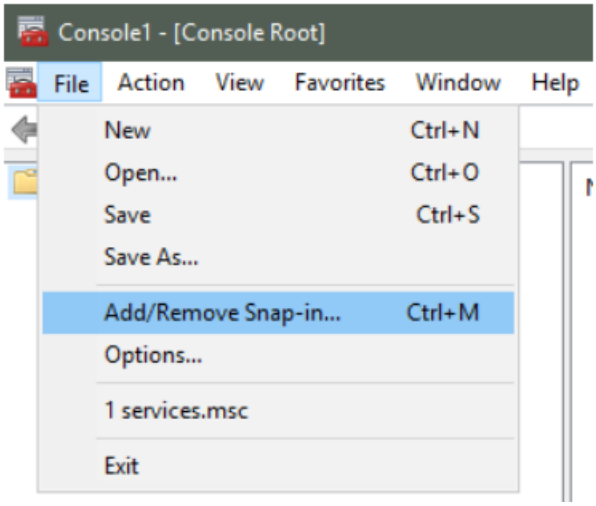
Find the new certificate's thumbprint

After installing the certificates, you need to update our PSAP service's web.config with the new thumbprints from the certificates.

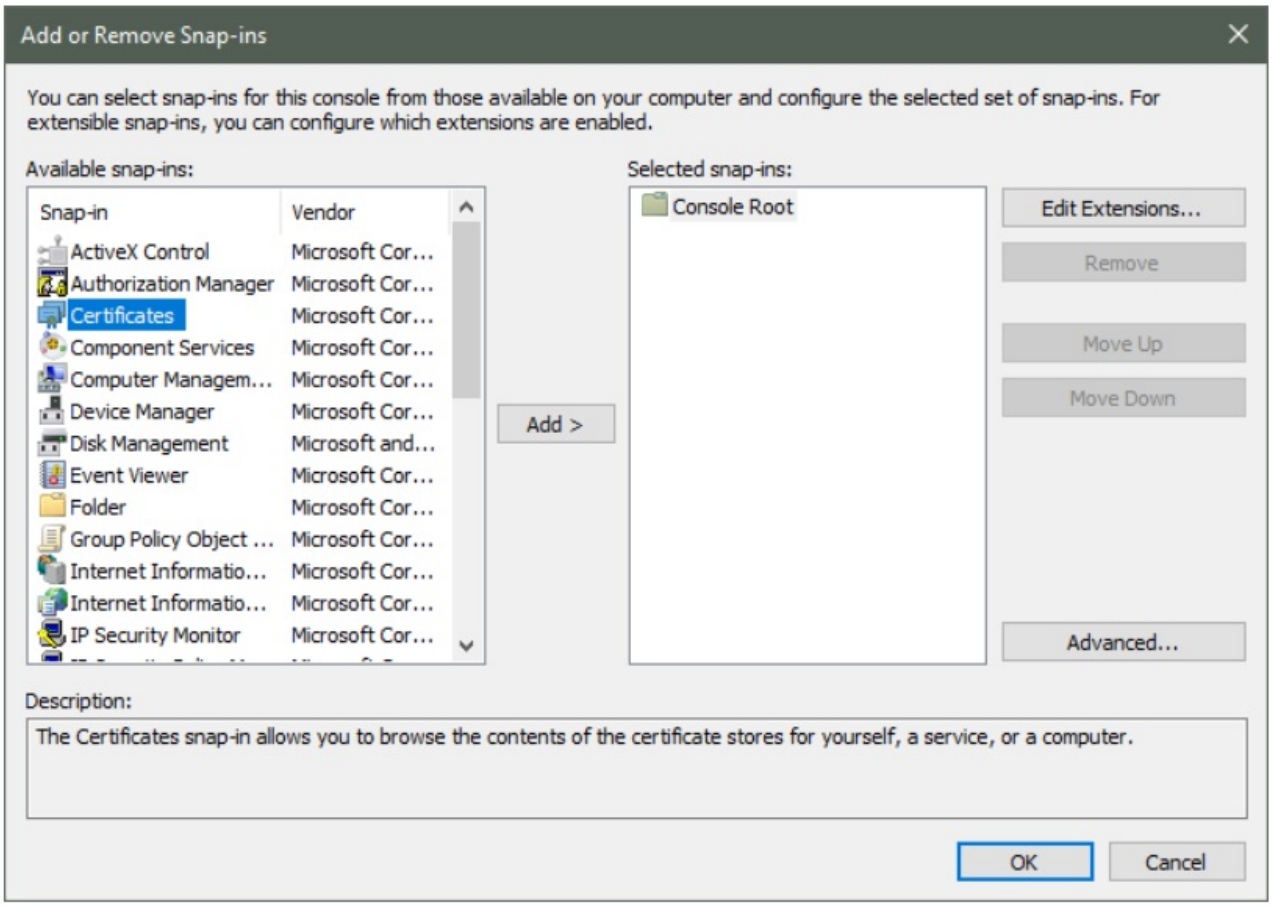
First know what the certificate's thumbprints are. In Windows, run the command mmc.exe. You will see a window like this:



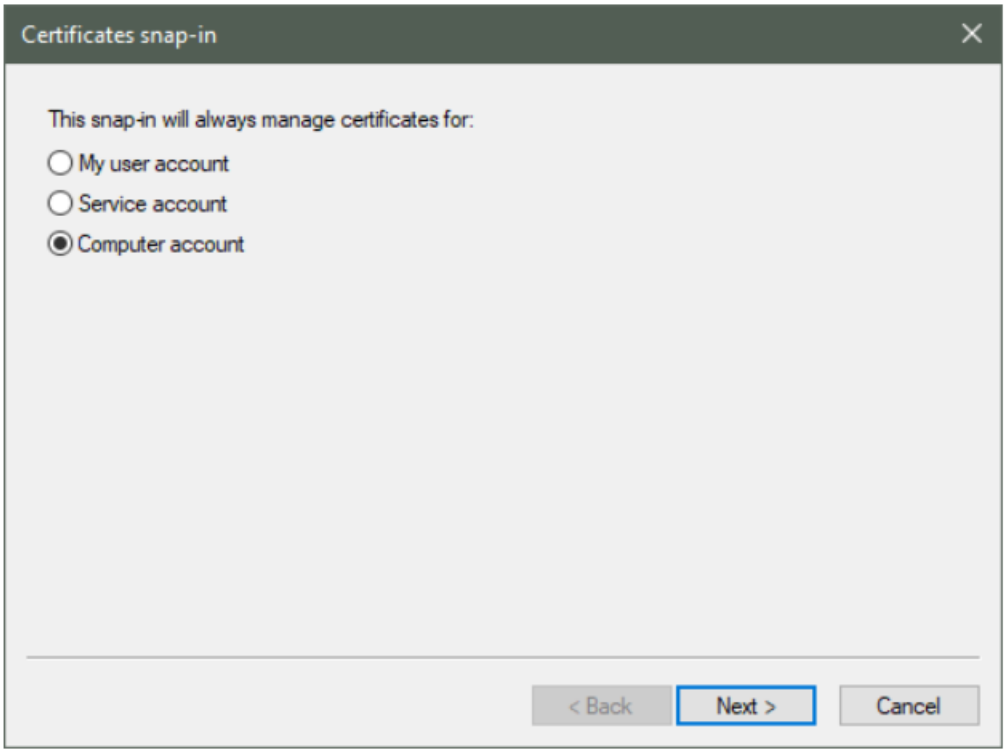
Click File->Add/Remove Snap-in...



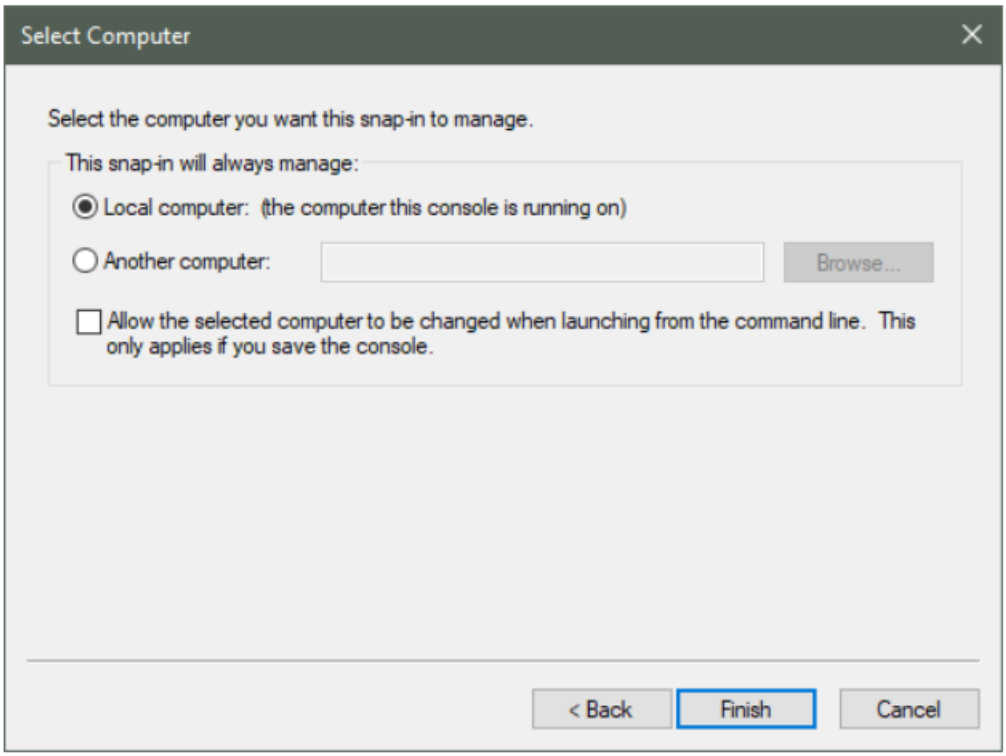
Click on Certificates and click the "Add >" button:



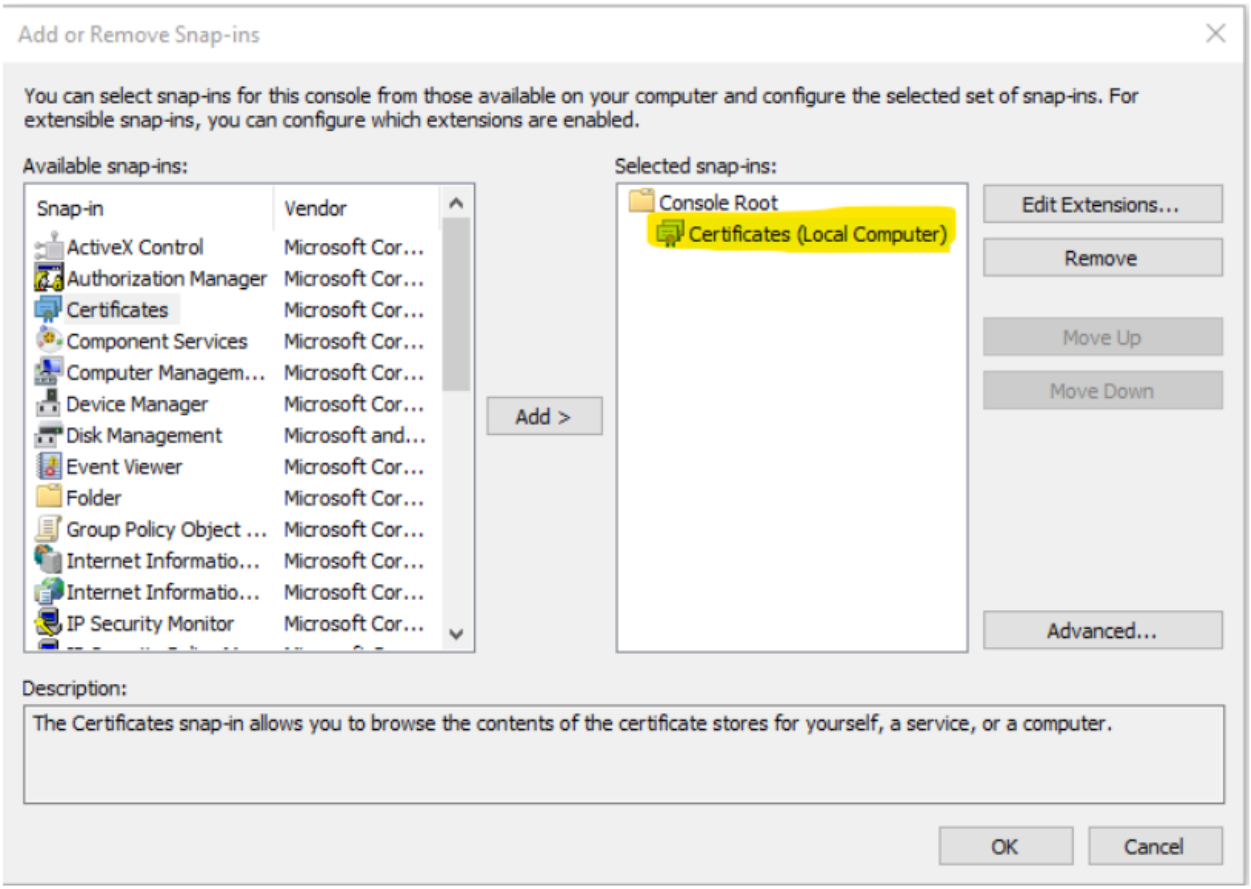
Clicking the "Add >" button will give you the following screen. Click Computer account then click Next.



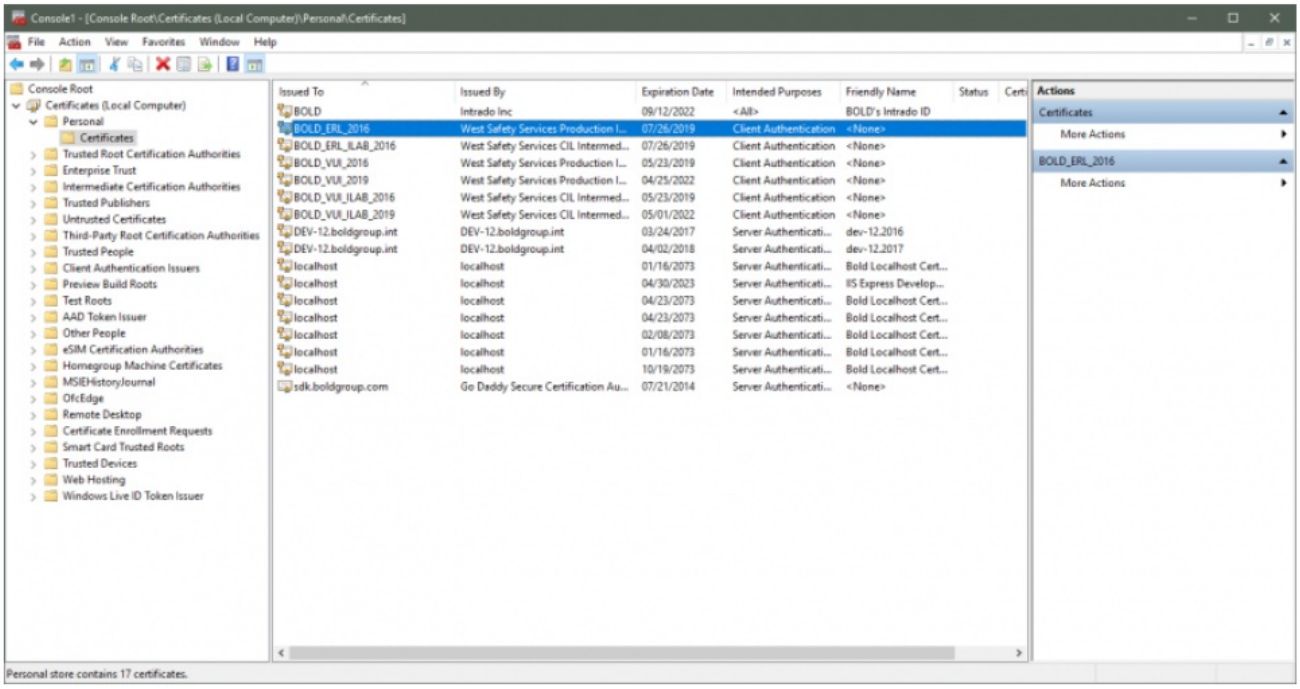
On the following screen select "Local computer: (the computer this console is running on)" and click Finish.



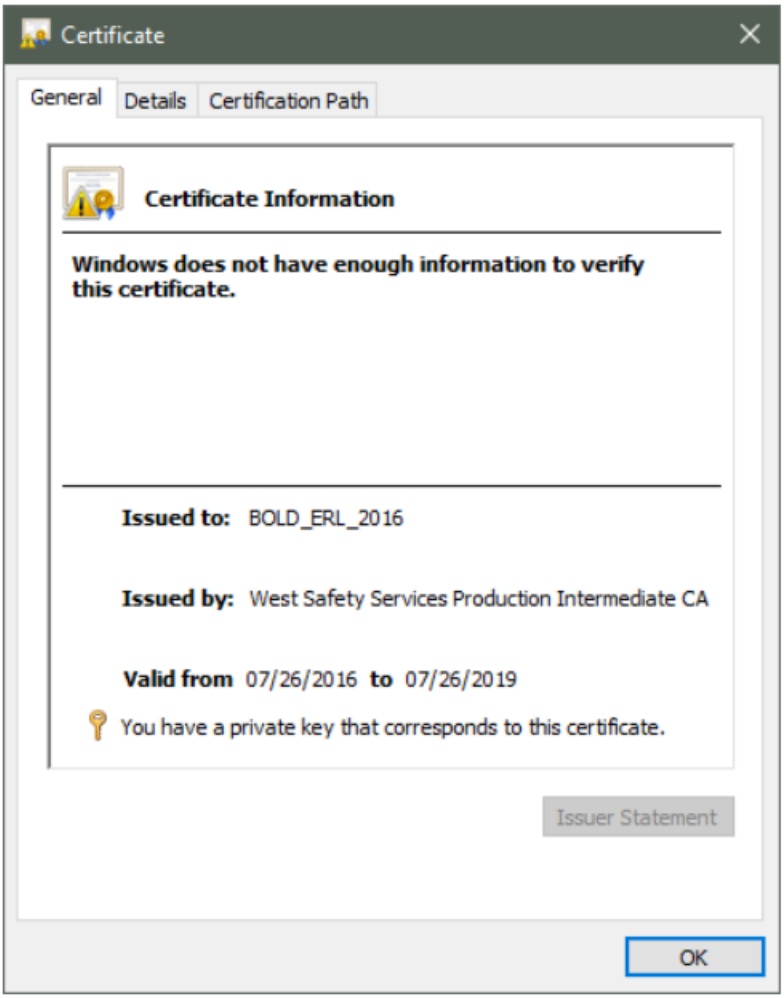
Now you'll be back at the original Add or Remove Snap-ins window but you'll see "Certificates (Local Computer)" in the "Selected snap-ins" list on the right.



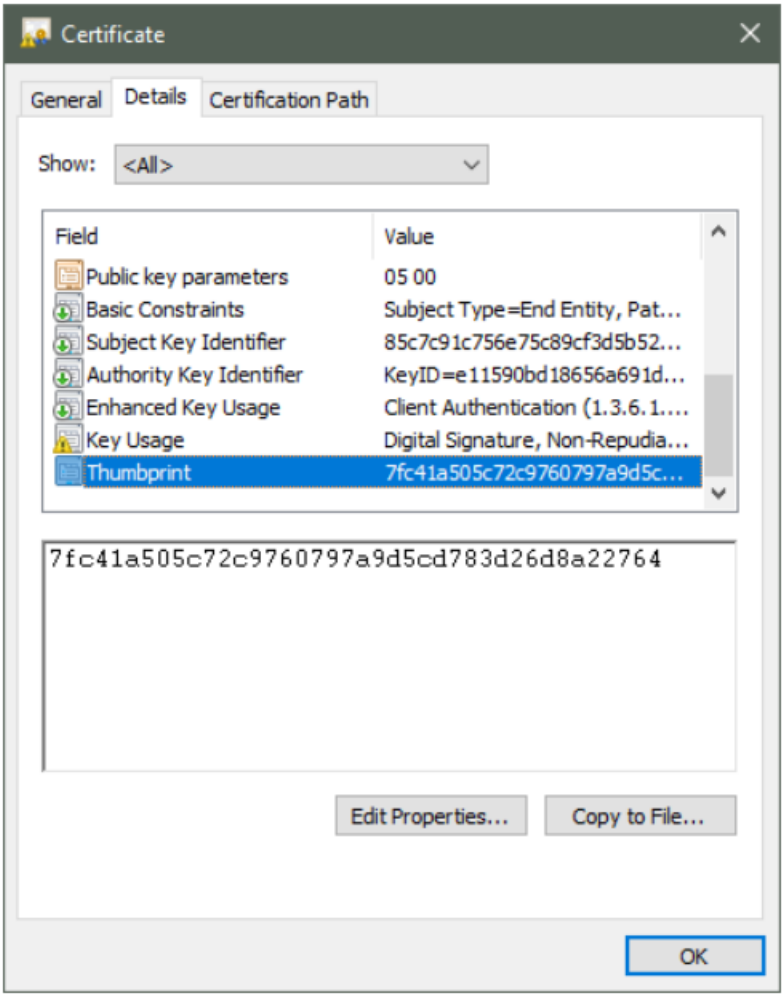
Click OK. In the next screen, drill down into Certificates (Local Computer)->Personal->Certificates.



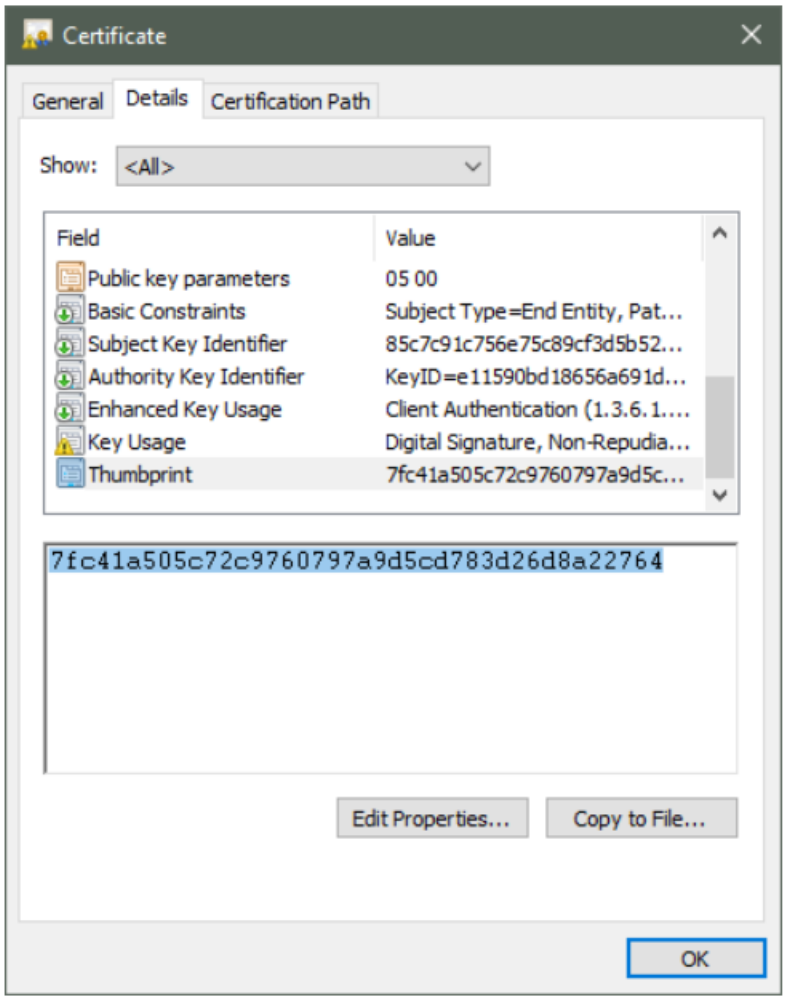
Double-click on the new production certificate.



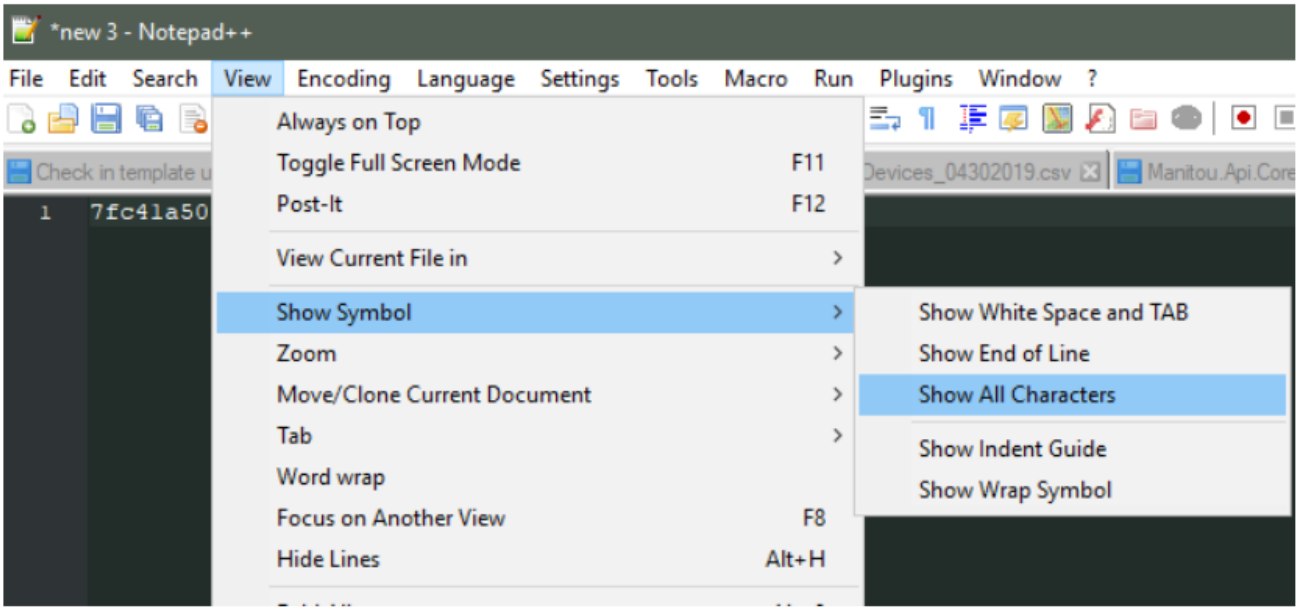
Click on the Details tab, scroll down until you see the Thumbprint field and value and click it.



Highlight the thumbprint and type ctrl+c to copy it into your clipboard.



Open Notepad++ and paste the key into a new tab. Click View->Show Symbol->Show All Characters.



This will show you if there are any unprintable characters in the certificate's thumbprint. If there are any then remove them. Next, put a space between every other character.

If your thumbprint is this:

7fc41a505c72c9760797a9d5cd783d26d8a22764

when you are done it should look like this:

7f c4 1a 50 5c 72 c9 76 07 97 a9 d5 cd 78 3d 26 d8 a2 27 64

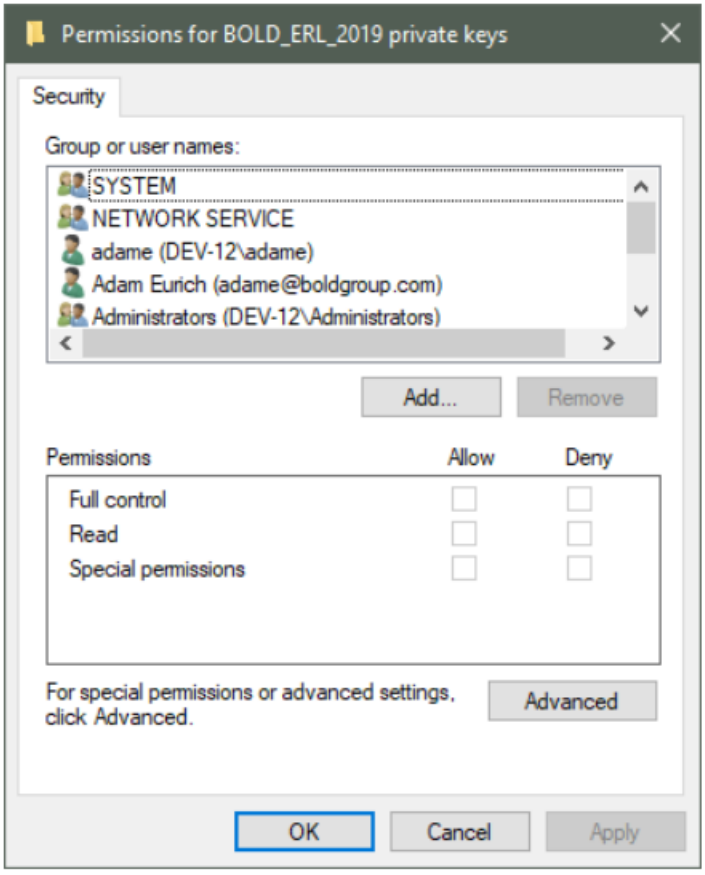
This is the string you will need to copy/paste into our PSAP service's web.config.

Manually adding permissions to the certificate

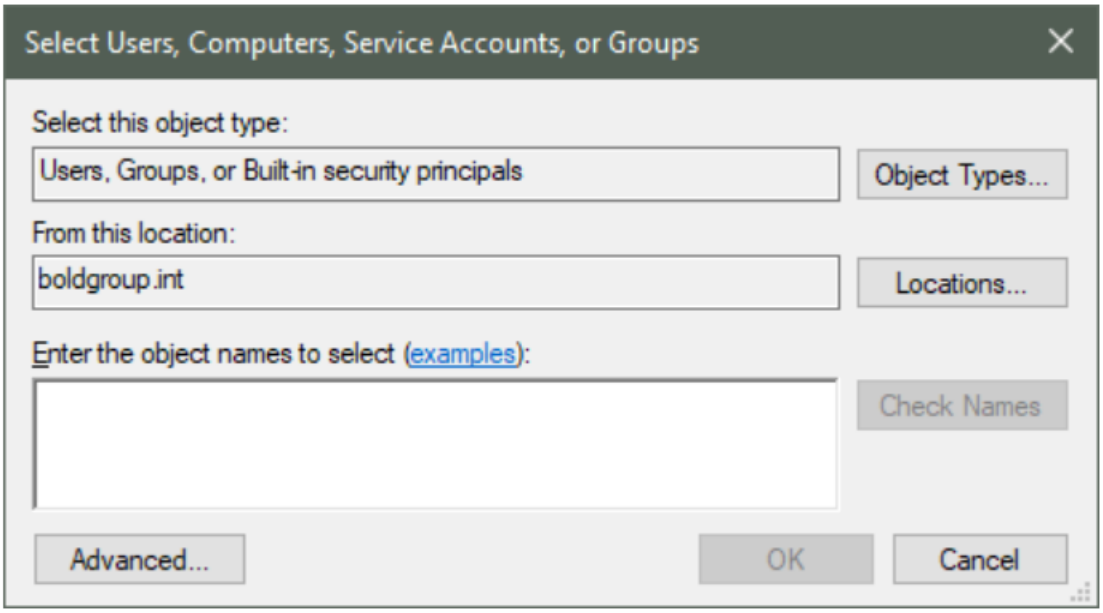
Sometimes adding permissions via the command line up above doesn't work and you have to manually add permissions.

Go into task manager and find the user for the process w3wp.exe.

In MMC, right click on the certificate->All tasks->Manage private keys.



If the user for the w3wp.exe process isn't in the list, click Add...



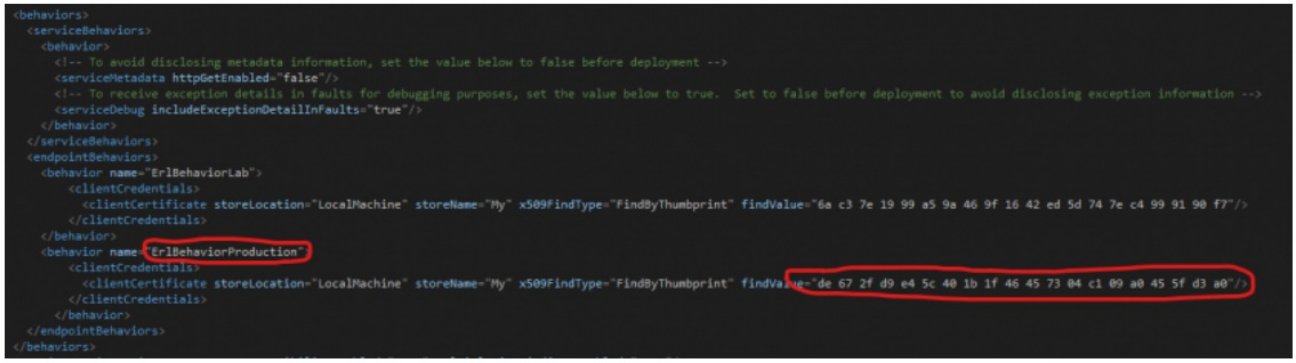
Enter the user's name and click OK. NOTE: if it's DefaultAppPool you need to enter the user as "IIS AppPool\DefaultAppPool".

Uncheck Full control so the user only has Read access.

Click OK.

Editing the web.config

In the PSAP service's web.config there is an endpoint behavior named ErlBehaviorProduction. In that element's clientCertificate element, there is a findValue attribute, remove that value and paste the new certificate's thumbprint info.



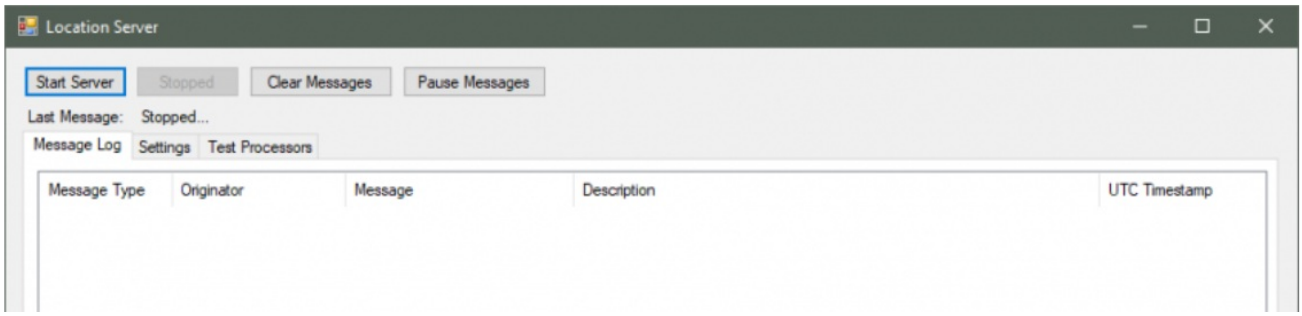
Save the web.config file. You may have to restart IIS to pick up the change.

Testing

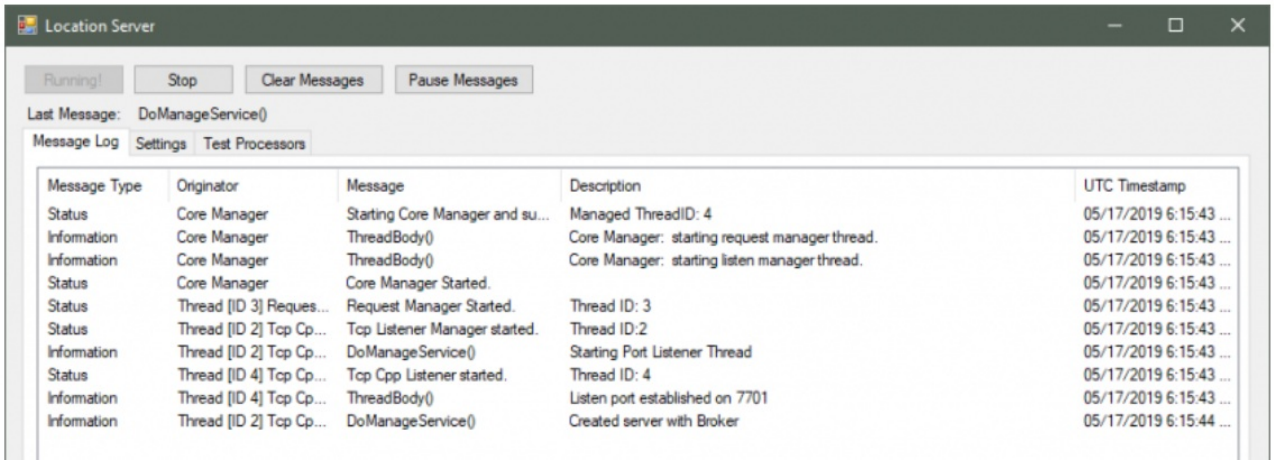
NOTE: It is suggested that you set up a Location Server and test our PSAP service BEFORE you install the new certificate. That way you can verify that you have your Location Server setup correctly in order to test after installing

the new certificate.

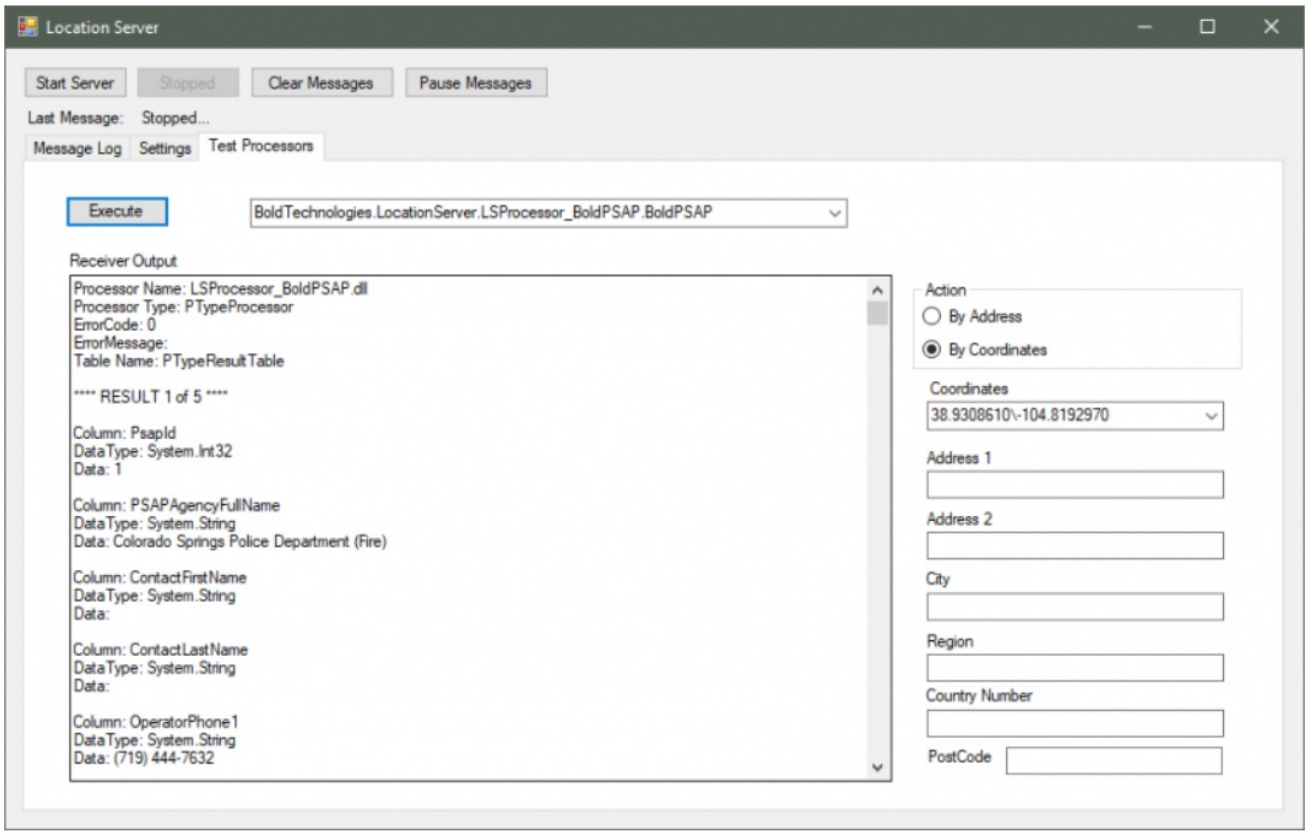
Start the Location Server application GUI.



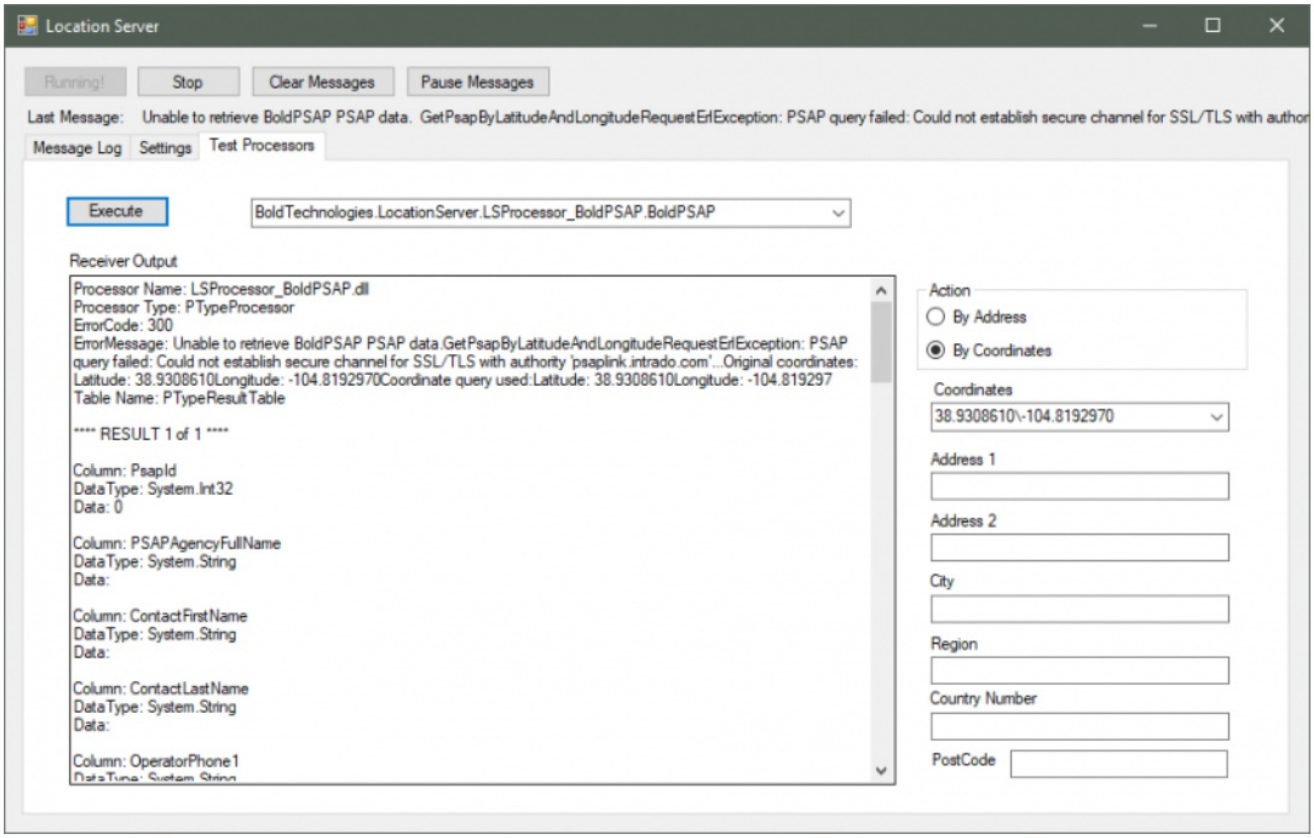
Click Start Server. The Start Server button should change to Running!



Click on the Test Processors tab. On the dropdown, select BoldTechnologies.LocationServer.LSProcessor_BoldPSAP.BoldPSAP. Click By Coordinates. Select the 38.9308610\-104.8192970 coordinates. Click Execute. It should return you results like this:



If you get a result with an error code or error message then something isn't right.



If you get an error message before you have updated the certificate then you need to troubleshoot. If you get an error message after you have updated the certificate and you've done everything properly then you will need to call West to have them troubleshoot. Mark Osler - Sr. Program Manager - 720-494-6222.