

## Troubleshooting ALERT IIS Web Service Connectivity

This is a quick guide to troubleshooting; please reference the [Real Time Data Exchange Guide](#) for complete details on setting up SOAP web service interface with ALERT IIS

### CERT INSTALL VALIDATION

- 1) Have you received/imported the certificates (client cert and CA from ALERT IIS)?
  - a. Using Windows: Control Panel, Internet Options, Content, Certificates – Import, to get to Cert Import Wizard. Follow instructions.
  - b. Using IIS7: See attached documentation.
- 2) Do the certificates show in Management Console (Click Start, Run, and enter MMC)?
  - a. The ca.crt should be in the trusted root store (my user account)
  - b. The client cert in the personal store (my user account)
- 3) Test certificate import. Can you browse to WSDL: <https://soa.alertiis.org/webservicesetm/VaccinationBService?wsdl> from the machine where the certificates are installed? *This is only a test to prove that the certificates are installed correctly.* You can skip this step during initial set up but may want to use it if you are getting SSL errors when attempting to connect via your interface engine.
  - a. To browse the wsdl, IE needs the .p12 file. The client .crt or .cer file can be converted to .p12 (or, .pfx) format by exporting the certificate. Be sure to export to the personal folder (in My User Account)
  - b. Check to see the certificates show in IE (tools/options/content/certificates/personal)
  - c. If able to browse the WSDL, you have confirmed that certificates are valid and stored correctly
  - d. Cannot use IE6 to browse the WSDL; must upgrade to 8 or use FireFox.
- 4) Try connecting to Google from server machine where certificates are installed.

### CONNECTING TO WEB SERVICE

- 5) Attempt to connect via interface engine. Make sure that interface engine application (Mirth, Corepoint, Cloverleaf, Rhapsody, etc.) is referencing the certificates when it calls the web service. The interface engine should have all the necessary rights/access to the certificate folders and to get out past the network fire wall.
- 6) In addition to referencing the certificates, the Interface Engine must build a SOAP package that includes the required security parameters (username/psw, correct timestamp format, etc.)
- 7) Capture error message, turn up logging to capture details if necessary. Send error message and external IP address(es) to ALERT Data Exchange Team. Send via email to [alertiis@state.or.us](mailto:alertiis@state.or.us) with Web Service Troubleshooting in subject line.

[About ALERT IIS Data Exchange](#)

Updated: 5/28/15

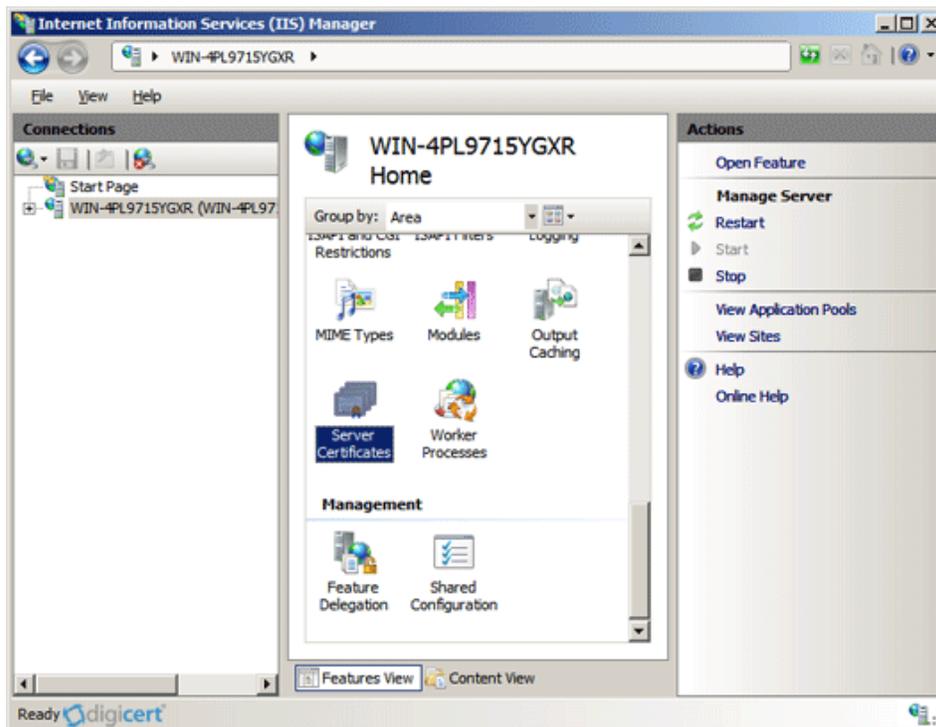
## Using IIS7 for Certificate Installation

### Install Root Certificate:

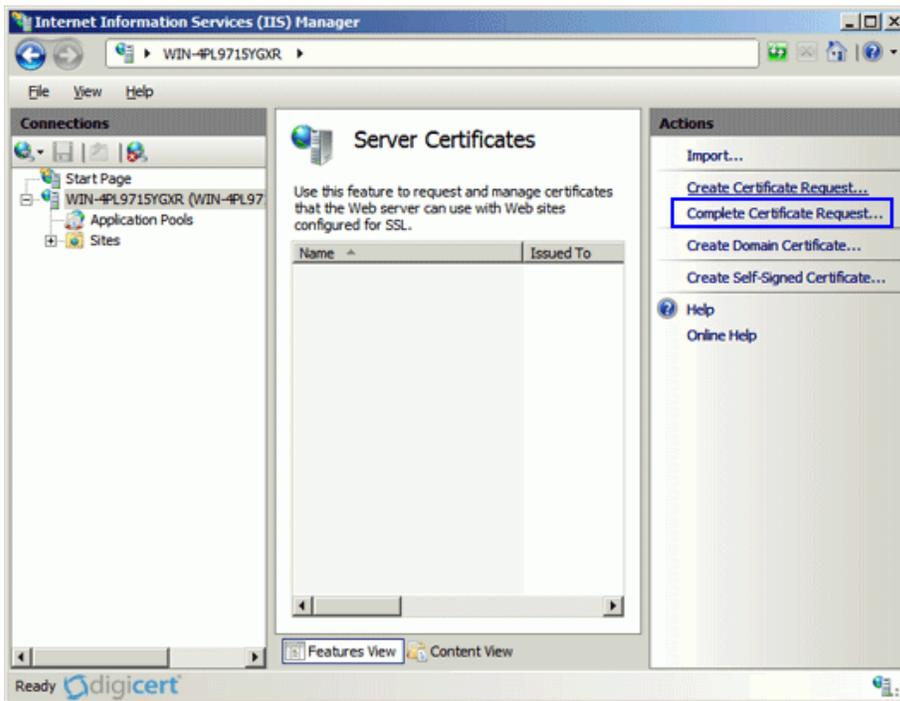
1. Open the ZIP file containing your certificate. Save the files to the desktop of the server you are securing.
2. Double click on the ca.crt and select Install Certificate. Place in Trusted Root Certification Authorities.

### Join Signed Certificate with Private/Public Key via IIS 7:

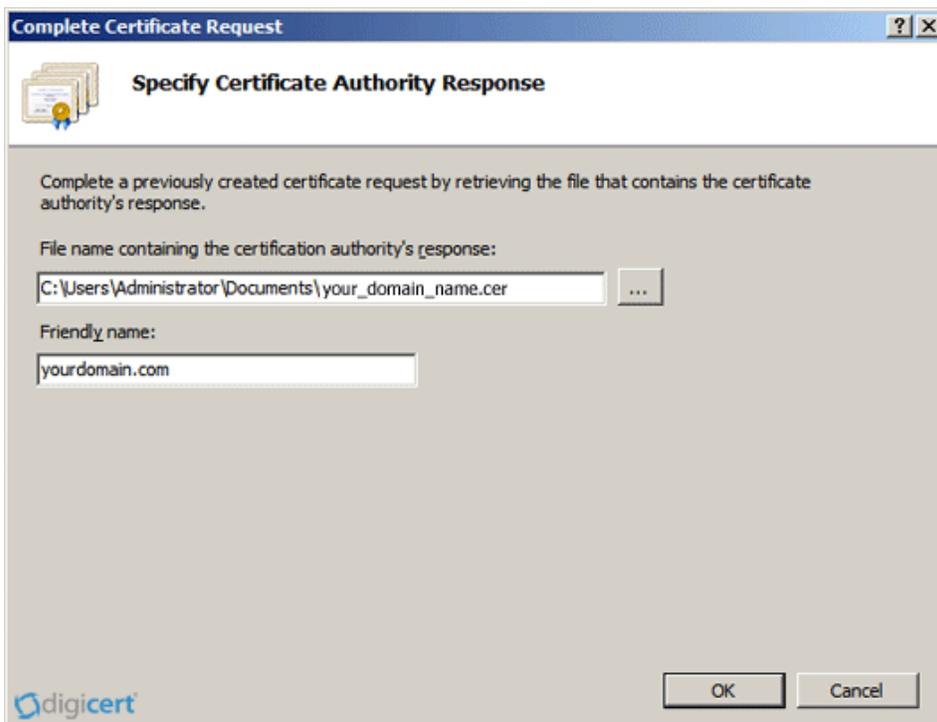
1. Click on Start, then Administrative Tools, then Internet Information Services (IIS) Manager.
2. Click on the server name.
3. From the center menu, double-click the "Server Certificates" button in the "Security" section (near the bottom of the menu).



4. From the "Actions" menu (on the right), click on "Complete Certificate Request." This will open the Complete Certificate Request wizard.



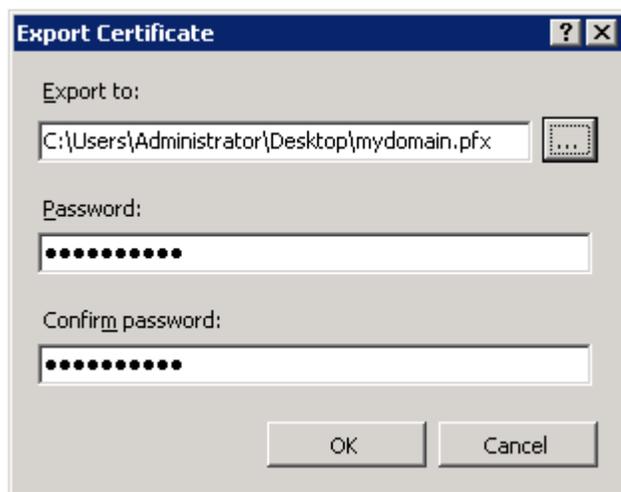
5. Browse to where you extracted the .crt files that were provided to you by HP by changing the file type to \*.\* to select your signed cert (not the ca.crt). You will then be required to enter a friendly name. The friendly name is not part of the certificate itself, but is used by the server administrator to easily distinguish the certificate.



6. Clicking "OK" will install the certificate to the server. You should now see your joined certificate in the Server Certificates window.

Create .pfx file to access the wsdl in a browser

1. Open Microsoft IIS 7.0 Manager
2. In the left-hand pane select the Server Name
3. In the middle window click the Server Certificates icon
4. Select your joined certificate, right click and select export
5. Give the certificate a path/file name and password



6. Click ok. Your certificate and private key should have been exported to a .pfx file
7. Open browser and select Tools, Internet Options then the Content tab.
8. Click on the Certificates button, then the Import button, browse to where you saved the .pfx file, then select Next.
9. Take all the defaults and you should get a successful import message.
10. Enter the url for the service and you should see the service definition.