|  |  |
| --- | --- |
| AMCAD Logo RGB 72 dpi.png  www.amcad.com | **AMCAD eCommerce**  **Enabling SSL Connections On The Client**  **va_court_2** |

**Table of Contents**

1 Document Revisions 2

2 Procedure 2

# Document Revisions

|  |  |  |
| --- | --- | --- |
| **Date** | **Editor** | **Description of Change** |
| 12/7/2011 | Vivekanand Alampally | Overview & Procdeure of enabling SSL connecting from client machine. |
|  |  |  |
|  |  |  |
|  |  |  |

# Procedure

If there is a problem in connecting to a web service hosted behind SSL protocal then, Web server or the URL you are connecting to, do not have a valid certificate from an authorized CA.

1. First of all you copy the URL that you are connecting to and paste it in your browser. Let us say you are using IE. Just paste the URL in the address bar and press enter.
2. You will now probably see a dialog box warning you about the certificate. Now click on the 'View Certificate' and install the certificate. Ignore any warning messages.
3. Now that the server certificate is installed in your computer, your browser will not warn you when you visit the same site again. If it does then simply ignore it. But your JRE dumb does not know about this certificate's existence until you add it to its keystore. Usually you will use the **keytool** to manage certificates. Keytool is a command-line utility with numerous arguments that allow you to create and manage keystores for housing digital certificates.
4. You can list the current certificates contained within a keystore using the **keytool -list** command

For example:

1. Open cmd as an **administrator.**
2. Then, Go to **C:\Program Files\Java\jdk1.6.0\_27\jre\lib\security**
3. Type,

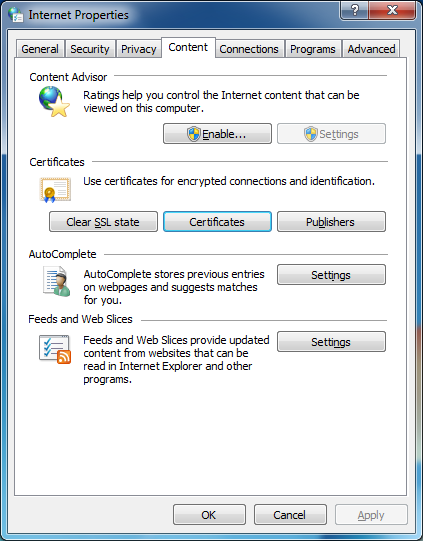
C:\Program Files\Java\jdk1.6.0\_27\jre\lib\security>**keytool -list -keystore cacerts**

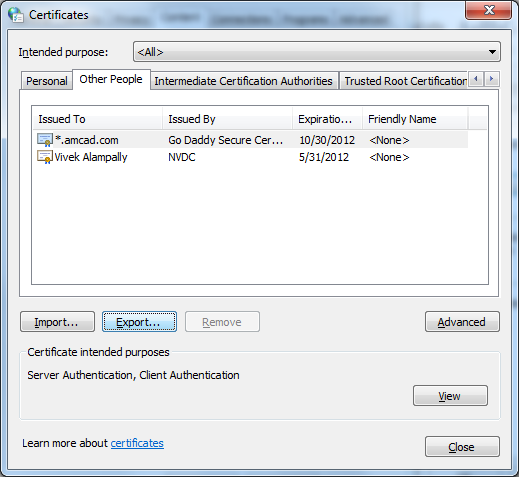
The initial password for the cacerts keystore is **changeit**.

Here you will see all the certificates installed on the machine.

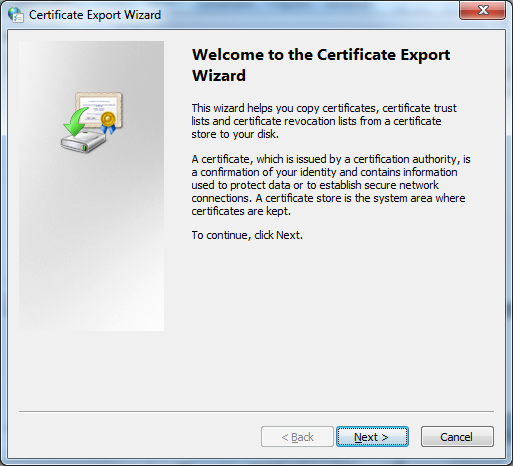
1. Now you have to add the previously installed certificate to this keystore. To add, begin by exporting your CA Root certificate as a DER-encoded binary file and save it as C:\Users\valampally\Desktop\root.cer. (You can view the installed certificates under Tools->'Internet Options' ->Content->Certificates. Once you open the certificates, locate the one you just installed under 'Trusted Root Certification Authorities". Select the right one and click on 'export'. You can now save it (DER encoded binary) under your c: drive.

So, Open Internet Explorer Tools->'Internet Options' ->Content->Certificates.

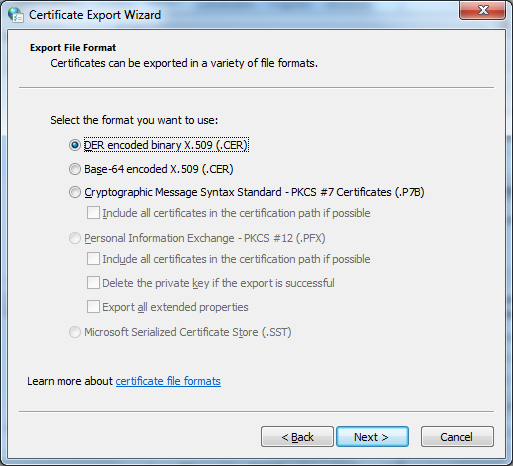




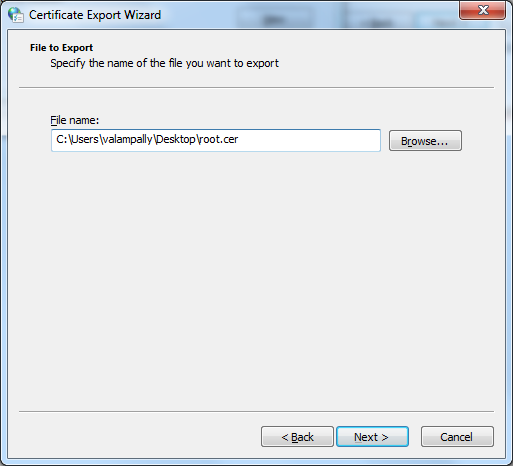
Click on Export,



Click on Next, DER encoded binary X.509 (.CER) selected,



Specify an arbitrary path,



Click on Finish.

1. Type the following command in command prompt.

C:\Program Files\Java\jdk1.6.0\_27\jre\lib\security>**keytool –import –alias myprivateroot -keystore cacerts -file C:\Users\valampally\Desktop\root.cer**

1. Verify whether the certificate is exported into cacerts with the command used before

C:\Program Files\Java\jdk1.6.0\_27\jre\lib\security>**keytool -list -keystore cacerts**

1. Now You Should be able to connect to SSL URL. In URL specify DNS name as an example

Instead of specifying as https://**dt-contract33** /ecomws/EComFacadeService?wsdl

Specify, https://**dt-contract33.amcad.com**/ecomws/EComFacadeService?wsdl