# Importing an SSL Certificate Authority into the JVM

## Technote (troubleshooting)

### Problem

A Java application running on a Domino server connecting over SSL to another server may require having the SSL certificate authority of the other server imported into its JVM.

### Symptom

When a Java application running on a Domino server connects over SSL to another server, but does not have that server's trusted root certificates, an error may occur. One example of such an error is:

HTTP JVM: javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.g: No trusted certificate found

### Cause

The trusted root certificates that signed the remote server's SSL certificate must be also be trusted by the Domino server's JVM if a Java application is making an SSL connection.

### Resolving the problem

To add the trusted root certificates to a Domino server JVM follow these steps:

**A. Obtain the Certificate to be Imported**
Each browser displays certificates in different ways, but they are usually quite similar. On the browser's URL bar, there is usually a zone that you can click on to display SSL certificate information. For example, you may see a padlock in the status bar, and clicking on the padlock opens the certificate information. Once the certificate information is open, click on the "Certification Path" information. There normally will be a way to export each of the signing certificates (trusted roots). Export the certifiers in the "Base-64 encoded X.509 (.CER)" format. The exported file in this format will be an ASCII text file that has "BEGIN CERTIFICATE" and "END CERTIFICATE" lines at the top and bottom. Once you have exported the certificates that signed the remote server's SSL certificate you can then import them into the JVM.

**B. Import the SSL certifier into the JVM.**
If Domino is on a UNIX server, perform these steps on a Windows workstation, and then move the cacerts to the server after the import is completed.

Import the SSL Certificate into the JVM using these steps:

Open a command line and change directory to C:\Lotus\Domino\jvm\bin.

Run the batch file "IKEYMAN.exe" (a Java application will load).

Click "Key Database File" then "Open".

Browse to C:\Lotus\Domino\jvm\lib\security\cacerts. Note, you will have to view "All Files" to locate cacerts.

Supply the default password of "changeit". Note, consult your administrator if you receive an error pertaining to the password.

Select "Signer Certificates" in the drop-down menu.

Click "Add"

Select "Browse" and locate the .CER file you copied.

Click "OK" and enter a descriptive label.

On the Domino console issue the command "restart task http".

## Document information

**More support for:** IBM Domino
Security

**Software version:** 8.0, 8.5, 8.5.3, 9.0

**Operating system(s):** AIX, Linux, Solaris, Windows

**Software edition:** All Editions

**Reference #:** 1588966

**Modified date:** 13 April 2012