Import a (Root) certificate in the java cacerts file

If the http plugin is used to get to a https url, then it could be that the (root) certificate of the sites certificate is not in the java root certificates. This will result in a connection failure, a smart client will be able to add this as an exception, this is stored in the [user.home]/.servoy/servoy.ks file. But for a serverside client like Web or Headless clients you need to import this certificate into the cacerts file your self:

Adding a server's certificate to Java's keystore

1. Get the certificate. The easiest way is to open Firefox, load any URL of the server. Firefox will throw an exception, or this certificate is unknown, what do you want to do. Just view the certificate and export/download to somewhere on your file system.

2. Import the certificate to the Java keystore. Lets say the JRE is in C:\java7. Open a command prompt, go to C:\java7\jre\lib\security. Make a backup of **ca certs**. Then run the following command:

keytool -import -file [the certificated downloaded from step 1, for example, C:\server.crt] -keystore cacerts

You should see something like the following:

C:\java7\jre\lib\security>keytool -import -file server.crt -keystore cacerts
Enter keystore password: changeit
Owner: CN=localhost, OU=ABC, O=XYZ
Issuer: CN=localhost, OU=ABC, O=XYZ
Serial number: 4849790d
Valid from: 6/6/08 1:51 PM until: 12/31/09 12:51 PM
Certificate fingerprints:
MD5: 0D:4A:B3:50\:D4:A9:3D:4F:46:7A:90:B0:C1:27:E2:58
SHA1: 2D:9D:B4:A4:B7:6B:A8:6A:0E:1C:E3:DD:FF:ED:FD:A9:AE:BB:1A:C2
Trust this certificate? [no]: yes
Certificate was added to keystore