User: vel000576str2
Pin: Welcome1
Password: Welcome1

vel000576trd2
Welcome1
Welcome1

Production Institutional SSL Connectivity

FIX Market Data (Stream)

Field	Data
Host (Americas)	63.111.184.125
Host (Europe)	91.229.92.125
Host (Asia)	103.22.167.125
Port	443
SenderCompID (Stream)	**vel000576str2**
TargetCompID	CNX

FIX Orders (Trade)

Field	Data
Host (Americas – NY6)	63.111.184.126
Host (Europe – LD4)	91.229.92.126
Host (Asia - KVH)	103.22.167.126
Port	443
SenderCompID (Trade)	**vel000576trd2**
TargetCompID	CNX

Client Certificate (Mandatory)

Self Service Cert installation:

1. Go to the following Website: https://enroll.currenex.com/enroll-prod/enroll.html
2. On the enrollment page:
    - Select 'I have read and accepted my client agreement and the privacy policy.'
    - Enter User/Comp ID, for 'Pin' enter the pin provided by the Broker.
    - Select 'Enroll'.
    - If all is correct, the system will display the message "**Certificate was exported. Please save the file and open it to import the certificate into your keystore".**
    - Client 'save' and 'Open Folder'.

Note: New certificate should reside in path ('This PC' and 'Downloads') unless otherwise directed during download.

To convert the '.p12' file holding the certificate to a ".pem" file:

1. The cert is in .p12 format and can be converted to .pem via openssl or directly installed into browser by double clicking on the cert. The password is the same as 'enrollment key' and can be change upon export after installation.
2. Move this ".p12" file to a machine where 'openssl' is installed and run the following command:
    - openssl pkcs12 -in <SenderCompId>.p12 -out <SenderCompId>.pem -nodes
3. If using Stunnel, store the .pem file where Stunnel can read it; i.e., Stunnel needs to point to the .pem file via the "cert" parameter set in the Stunnel config file; e.g., cert=C:\some\path\.pem
4. A full restart of the stunnel process is required to take up this new certificate.

CA Certificate (Optional)

If you would like to validate the Currenex server certificate with the CA, please follow the below instruction.

If your FIX engine is using Java and negotiates SSL within the application, follow one of steps (upgrading Java is strongly preferred):

1. Upgrade to a version of Java better than or equal to 1.8.0_91 or 1.7.0_u101 (this is only available if you have an extended support contract with Oracle)
2. Add both of the Digicert CA's to your Java installation's cacerts file with the following command. The DigiCertGlobalRootCA.crt can be downloaded here (https://dl.cacerts.digicert.com/DigiCertGlobalRootCA.crt) and the DigiCertGlobalCAG2.crt file can be downloaded here (https://dl.cacerts.digicert.com/DigiCertGlobalRootG2.crt):
    - keytool -import -file DigiCertGlobalCAG2.crt -keystore %JAVA_HOME%\lib\security\cacerts -storepass changeit
    - keytool -import -file DigiCertGlobalRootCA.crt -keystore %JAVA_HOME%\lib\security\cacerts -storepass changeit
3. Copy the attached jssecacerts file into your system's java directory (%JAVA_HOME%\lib\security\jssecacerts)
4. Point your application (FIX engine) to a custom trustStore (attached is one that covers both Symantec and Digicert named cx_trust_store.jks) add the following arguments to your commandline:
    - -Djavax.net.ssl.trustStore=cx_trusted_ca.jks -Djavax.net.ssl.trustStorePassword=currenex

5. Use the jssecacerts file for a single application and not alter your java installation. Same as number 4, drop the file anywhere on your filesystem and add these arguments.

    - -Djavax.net.ssl.trustStore=jssecacerts -Djavax.net.ssl.trustStorePassword=changeit

If your FIX engine is using stunnel to negotiate SSL, follow one of these steps:

You can choose any of the 3 options below

1. Set "verify=0" in your stunnel config
2. Set "verify=2" in your stunnel config and append the new root certificates to the end of file pointed to by the CAfile parameter:

    - https://dl.cacerts.digicert.com/DigiCertGlobalRootG2.crt
    - https://dl.cacerts.digicert.com/DigiCertGlobalRootCA.crt

3. If you have "verify=3" you'll need to download our new certificate after we update it and append it to the end of the file pointed to by CAfile. (we strongly discourage this particular setting).