

How to connect to CME Globex using Secure Logon

CME secure logon provides an ability to logon using SHA256 digital signature technique. This logon feature has been introduced by CME recently and provides highest security.

It's needed to obtain security keys file from CME in order to use it. Once it is available, FIX Antenna can be configured to use secure logon for connecting to CME.

It can be done both ways using API or with configuration file (*engine.properties*).

First approach - using API:

3 members of SessionExtraParameters structure have to be set before passing it to createSession() API call.

1. *cmeSecureKeysFile_* that contains path to CME keys files. E.g.: *CMEKeys.txt*.
2. *customSessionType_* has to be set to *Engine::CME_SECURE_LOGON*. It tells engine to use CME secure logon scheme.
3. *sendLastMsgSeqNumProcessed_* has to be set to *true*.

Second approach - using *engine.properties* file:

3 additional session configuration parameters have to be set.

1. *CMESecureKeysFile* that contains path to CME keys files. E.g.: *CMEKeys.txt*. So for the session with Sender/Target=U74004N/CME it would be *Session.U74004N/CME.CMESecureKeysFile = CMEKeys.txt*
2. *CustomSessionType* has to be set to *CME_SECURE_LOGON*. It tells engine to use CME secure logon scheme. So for the session with Sender/Target=U74004N/CME it would be *Session.U74004N/CME.CustomSessionType = CME_SECURE_LOGON*
3. *sendLastMsgSeqNumProcessed* has to be set to *true*.