SSL Security Levels and CuteFTP

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- Secure FTP Server™
- EFT Server™
- CuteFTP Pro®

DISCUSSION

EFT Server and Secure FTP Server can provide three basic levels of security when used with CuteFTP Pro as the client:

1. **Secure (server certificate only)**
   - The server creates a public certificate/key/passphrase for SSL
   - The client has SSL only enabled
   - The client connects, is asked to trust certificate from server, and accepts the certificate, which is stored in the client's cache. After certificate acceptance, the user is not asked to trust the certificate again; it is assumed.
2. **More Secure (server certificate AND client certificate)**
   - The server creates a public certificate/key/passphrase for SSL.
   - The server requires a certificate from client.
   - The client has SSL enabled AND creates a certificate/key/passphrase
   - The client connects. The connection fails the first time, and the server can choose to trust or not to trust the client certificate.
   - The server trusts the client certificate.
   - The client connects and does not fail again because the client certificate is now trusted by the server.
3. **Most Secure (server certificate AND a signed client certificate)**
   - The server creates a public certificate/key/passphrase for SSL.
   - The server requires a certificate from client.
   - The client has SSL enabled AND creates a certificate/key/passphrase.
   - During this process a certificate signing request (csr) is generated.
   - Use the Secure FTP Server or Enhanced File Transfer Server signing utility to sign the certificate or...
   - Send the CSR to a trusted 3rd party such as Verisign to be signed. Verisign then sends back a signed certificate which replaces the CuteFTP Professional certificate.
   - The client connects. The connection fails the first time, and the server can choose to trust or not to trust the client certificate.
   - The server trusts the client certificate.

- The client connects and does not fail again because the client certificate is now trusted by the server.