2X Application Server CSR and Installation Instructions

2X Application Server CSR Creation

By enabling SSL encryption, your 2X Gateway provides encryption to your terminal servers. You can enable clients to connect using SSL by checking the box to "Enable SSL on Port:", usually using 443 as the default SSL setting. You can find this option under the SSL/TLS tab of the 2X Secure Client Gateway Properties window.

To access the Gateway Properties window, click on the Farm in the Navigation panel of the 2X Application Server and Load Balancer Console and then click on Gateways. Next, click the Gateway you want to edit and click "Properties."

To create a CSR for your 2X Application Server, open the Secure Client Gateway Properties window and go to the SSL/TLS tab, and then choose to "Generate new certificate...". A new window will appear, into which you will enter the following information:

1. Country code: If you do not know it, you can find your country code here.
2. Full state or province: The state in which your organization is primarily located.
3. City: Usually the location of your corporate headquarters, as opposed to your current location.
4. Organization: Full legal business name of your organization (or your name, for an individual).
5. Organization unit: Your division within the company, or the division for which the certificate is being requested (e.g., Marketing).
6. E-Mail: Your email address.
7. Common name: Usually the FQDN of the server to which your certificate is being issued (www.domain.com, mail.domain.com, or *.domain.com).
8. Save file to: The location to which your certificate request and private key will be saved.
9. Once you have generated your CSR file, submit to us for our process.

Installing an SSL Certificate on a 2X Application Server

From the SSL/TLS tab of the 2X Secure Client Gateway Properties window, click the "..." link to browse to the Private Key you created during the CSR creation process, and then again to find the Certificate file that was returned to you from i-Trust. If you receive a certificate file that includes an intermediate (one or more intermediates for security purposes), you will want to combine those two files into one .pem file before enabling your certificate.

To create that file, simply open both certificate files in a text editor and copy them into a new file in the following format:

-----BEGIN CERTIFICATE-----
(Contents of your_domain.crt file)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Contents of Intermediate Certificate File
-----END CERTIFICATE-----

You should be able to enable the certificate by browsing to your new certificate.pem file and selecting it like you selected the private key, and then pressing the OK button at the bottom of the window.