Installing CodeLathe's Root CA Certificates as Trusted Certificates

⚠️ SSL Certificates are no longer sold via our sold. This information is here for archival purposes only.

CodeLathe provides SSL certificates for Tonido signed by its own Certificate Authority. This means that when you try to open a Tonido Website which is powered by SSL signed by CodeLathe.com's CA you will get a browser warning saying the SSL certificate is not trusted.

To avoid this browser warning, you can add CodeLathe's root CA in your trusted CA store. Please see instructions below on how to install the root CA for specific browsers.

Internet Explorer (Windows)

1. Download the cacert.crt from here
2. Double-click the file, and a Certificate details dialog will open.
3. Click "Install Certificate" to install the certificate

blocked URL

FireFox (All OSes)

1. Download the cacert.crt from here
2. Click on Menu Tools->Options->Advanced->Certificates
3. Click on "Authorities" tab
4. Click on "Import" and select the cacert.crt file that you previously downloaded

blocked URL

Google Chrome (Windows)

1. Follow instructions for Internet Explorer (Windows)

Safari (Mac OSX)

1. Download the cacert.pem from here
2. Double-click the pem file to open the Keychain Access application dialog which asks you to add the certificate. Select "Login" if you want to add this certificate only for you, "System" if you want to add for all users and then click ok.
3. Click on "Always Trust" on the Keychain Access verification dialog
4. After adding it, locate the codelathe.com certificate again in the key access application and double click on it to open it's settings.
5. Expand "Trust" tab and under the "Secure Sockets Layer(SSL)" select "Always Trust" and close dialog.

blocked URL

blocked URL