Link to article: https://discover.claromentis.com/knowledgebase/articles/39/how-do-i-enable-https-ssl-tls-access-to-our-site

How do I enable https (SSL/TLS) access to our site?

Overview

Claromentis can support access via HTTPS (SSL/TLS), which provides encryption in transit (it protects the data transferred between the client and the server). The process of purchasing and installing an SSL certificate will differ dependant on whether you are hosted by Claromentis as a SaaS deployment, or whether you host yourselves on-premise.

SaaS/Hosted by Claromentis

Process - Please see the following article

On-Premise Windows hosted by the client

The generation of CSRs and purchasing of SSL certificates are the responsibility of the client. As the server is hosted in your environment you have the ability to generate a CSR (if needed) for your SSL certificate within IIS. Please speak to your internal IT team for further assistance if required.

Please submit a Change Request for assistance from the Claromentis team with installing your purchased SSL certificate within IIS.

Once an SSL certificate has been purchased it will need to be installed as below:

SSL certificates will need to be imported into IIS on the webserver that is hosting the Claromentis intranet. This will be in **.PFX** format.

If you would like Claromentis to install the SSL certificate within IIS we will require:

- The SSL certificate in **.PFX** format

- The password for this certificate

- The location on the server that the SSL certificate has been uploaded to. We would ask that the certificate is directly uploaded to the server, rather than in a Change Request.

Applying the SSL certificate to the Claromentis site:

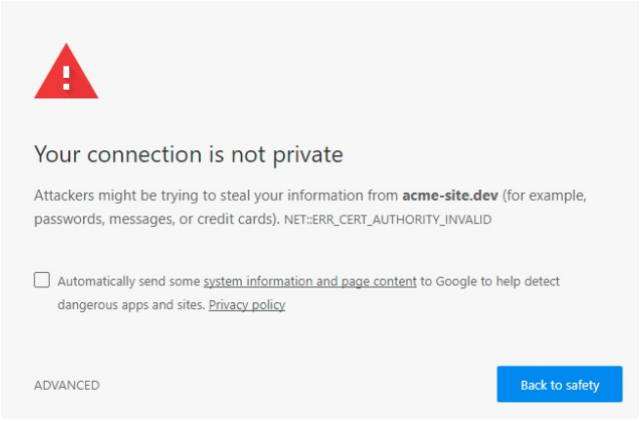
Once the above has been completed, by your team, or Claromentis we will then need to apply this SSL certificate to the site that is hosted on the webserver.

Things to consider:

- **Updating existing links** to your intranet with SSL the Site URL will be starting with `https://` instead of `http://`. You may need to set up redirection.
- Make sure you are keeping up with the **Certificate validity**.
- Make sure that **Intermediate/chain certificates** are installed to ensure the site will be trusted in all web browsers including mobile apps.
- Do not enable '**ssl offloading**' on the ARR proxy in order to get around the missing intermediate certificate.

Troubleshooting

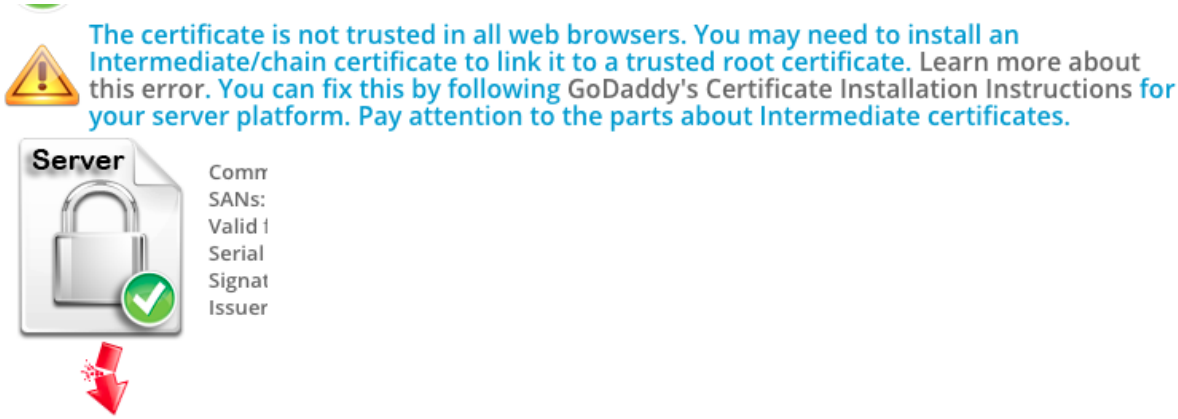
I am getting this error when accessing my site.



This is the sign of improper or invalid SSL certificate or you may be using a self-signed certificate.

Run SSL Checker to find out what's wrong.

I am getting this error when running SSL Checker



You may need to install an intermediate/chain certificate to link it to a trusted root certificate, contact your SSL provider configuration and pay attention to the part about the intermediate certificate.

What server does Claromentis use?

Our cloud servers are using Apache (https) while your on-premise will be Windows IIS

Useful tools

SSL Checker

Related Article

SSL CMD To Verify SSL, KEY, CSR

Last modified on 18 June 2025 by Mike Leggatt

Created on 11 April 2013 by Will Emmerson
Tags: ssl, HTTPS, certificate, tls, CSR, KEY, certificates