Link to article: https://discover.claromentis.com/knowledgebase/articles/39

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 - The client to provide the SSL certificate

Step 1: Provide CSR Information

The Claromentis team will need to generate a CSR on your behalf. Please submit a change request and attach the following information:

- **Country:** This should be the country code, for example, GB or US. For a full list see: http://www.digicert.com/ssl-certificate-country-codes.htm
- **State/County/Region:** For example, East Sussex
- **Locality Name (City):** The city where the main organisation office is based, e.g. Brighton
- **Organisation Name:** The legal name of the organisation, this could be for example be 'Client Name Ltd' (including any suffixes such as LTD, CORP etc.)
- **Organisational Unit Name:** This should be the division or department of the organisation – for example, 'ITDepartment'.
- **Common Name:** The fully qualified domain name, for example, client.theirsite.com

Step 2: Generate CSR

A member of the Claromentis team will be booked in to generate the CSR and will upload this to the change request once complete

Step 3: Purchase SSL Certificate Vendor

You should then choose an SSL Certificate vendor and place an order. The CSR provided by Claromentis should be used during this process.

Step 4: Authorisation and Verification

The owner of the website address will need to authorise the SSL Certificate. The approval is carried out by emailing the owner of the website address and a link being clicked from within the email.

This could take 24-48 hours depending on the vendor chosen and email delivery time. In some cases, the vendor may carry out additional verification and this may take an additional 24-48 hours.

Step 5: Installing Authorised SSL Certificate

The authorised SSL Certificate will be sent via the vendor's website, or via email and this is just a block of text. This should then be passed onto Claromentis to install on the server. Installation should take around 10-15 minutes and may require a brief interruption to the site whilst the certificate is added.

Important

Claromentis we require the SSL certificate in Apache **.CRT** format. We will also require the intermediate/root certificates and the private key.

Note: The private key is only needed if Claromentis didn't generate the above-mentioned CSR for your SSL certificate.

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:

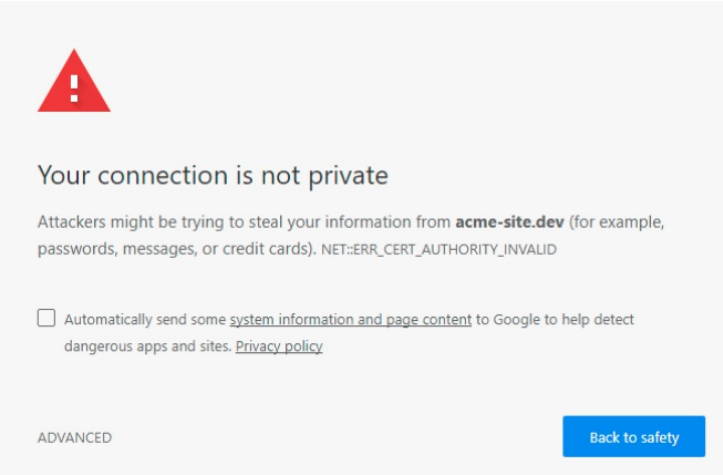
Once the above has been completed, by your team, or Claromentis we will then need to apply this SSL certificate to the site that is hosted on the webserver.

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

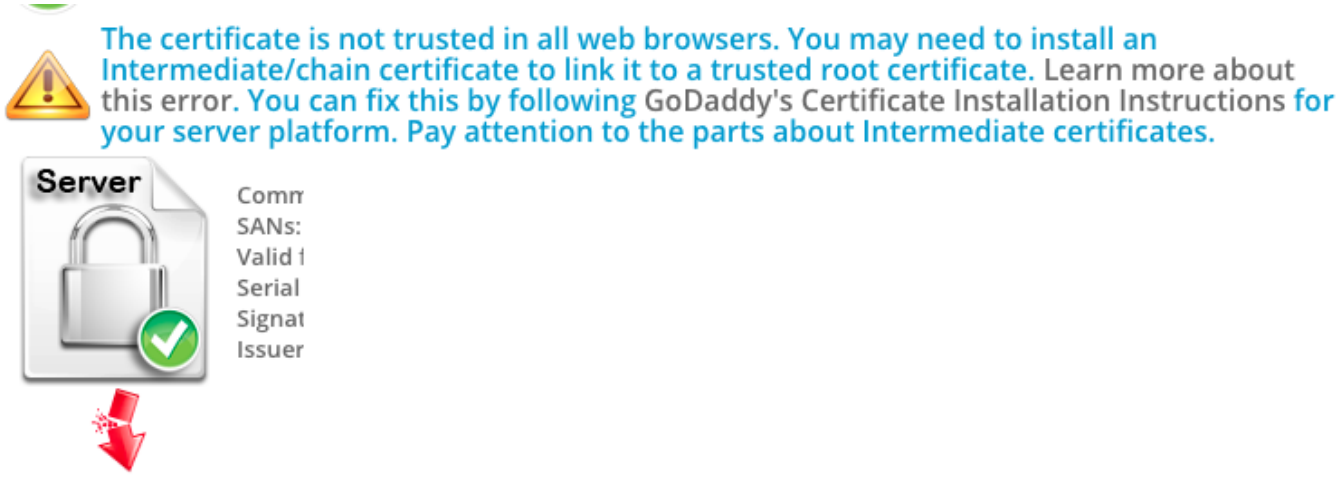
I am getting this error when accessing my site.



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

We **do not** recommend or endorse any specific providers, however, our certificates are provided by DigiCert.

Related Article

SSL CMD To Verify SSL, KEY, CSR

Last modified on 13 December 2023 by Hannah Door

Created on 11 April 2013 by Will Emmerson

Tags: ssl, HTTPS, certificate, tls, CSR, KEY, certificates