Link to article: https://discover.claromentis.com/knowledgebase/articles/1018/dns-changes-ssl-certificates-within-saasv2

# DNS Changes / SSL Certificates within SaaSV2

## Introduction and what's changing

The way we generate and provision SSL certificates has changed with our new SaaSV2 deployment. Previously, we asked each customer with a custom domain name to generate an SSL certificate and send it over to us annually. This process was difficult for non-technical users, resulting in an additional cost for the customer (as they had to purchase an SSL certificate at their own expense). We often found that the renewals were missed and resulted in downtime for end users.

To improve this process efficiency, reduce cost for our customers and ultimately prevent downtime during certificate renewals, we're now offering FREE SSL certificates for **any** custom domain, as well as the free *.myintranet.com SSL certificate that we offered previously. This offers the same level of security and encryption, but we take on the ongoing maintenance and automation of the SSL certificates on your behalf, by utilising Google Managed Certificates. You can read more about these here.

## The Process

**1.** A customer-managed DNS entry will need to have an A record pointed at a dedicated, external IP address that Claromentis will provide upon request.

**TTL** (IMPORTANT). When pointing the A record, we would require the TTL to be set to 300 seconds, to make sure changes propagate quickly. Setting a longer TTL when pointing your DNS entry can cause further delays with the DNS change.

**2.** Claromentis will then make the necessary changes internally to provision a Google Managed Certificate. This can take up to 2 hours to be issued and applied to your instance. Once this has been provisioned, the custom domain name will be accessible for use.

To start the above process, please submit a Change Request.

### Important considerations:

- You must own the custom DNS; Claromentis doesn't manage the ownership of these DNS entries. Only *.myintranet.com is owned and managed by Claromentis.

- There will be a time period where your intranet is inaccessible while the SSL certificate is being propagated by Google.

### What happens if we have Single Sign-On?

If Single Sign-On has been integrated with and a URL is changed, this will require re-configuration of your Identity Provider. As Single Sign-On is URL-based, if this value is changed, the configuration will no longer be valid.

*It is important to note that once your URL has been updated, SSO will not function until the below has been completed.*

**1.** Once the URL change has been made, Claromentis will need to send over new URL values to be updated within your Identity Provider, along with a new metadata link or XML file.

**2.** When this has been completed by your team, we will then require an updated IDP metadata.xml file to upload to our configuration.

Once complete, SSO will function as before, on your new FQDN.

---

For On-Premise installations, please see the following article.

---

Created on 18 June 2025 by Mike Leggatt. Last modified on 26 June 2025
Tags: saasv2, ssl