How To Create Keys On CMI

Introduction

Keys are used within SAML to create a trust relationship between Sentry (acting as an IDP) and a SAML-compliant service provider. It is important that you create your own keys for this integration and keep the private key secure.

Generating Keys

From the CMI Main Menu select the Appliance Option, then select Sentry Menu option.

You will see the keys that are currently being used by Sentry (if any).

Select Option 1 to Generate New Keys

Give the key a name eg SentryProductionKey Select the key type, RSA or DSA

Some integrations require keys of a specific type so refer to the appropriate integration guides

You then need to enter the information required to generate the key. These parameters are

- Country Name e.g. US. This should be the standard 2-letter ISO country code.
- State or Province e.g. Washington.
- Locality: e.g. Seattle.
- Organisation: Your Company or Organisation Name.
- Organisation Unit: Relevant unit, e.g. Information Technology.
- Common Name: The full server hostname, e.g. sentry.domain.com.
- Email Address: contact email address for the certificate.

Once you have entered all the details the new keys and certificate will be created.

You will be asked if you want to start using the new key immediately. If you say NO you can select the key at a later date.

WARNING: Changing the key being used will impact any existing SAML-based integrations. The existing service providers will need to be updated with the new keys.

Selecting a Key

Select the Select New Key option will list all the keys that have been created on the appliance. You can select the key you wish to use.

NOTE You need to restart tomcat for the changes to take affect