SSL SETTINGS

The Security Validation Director and Linux Actors include self-signed certificates. For many organizations, self-signed certificates are not approved. In some instances, a self-signed certificate could cause issues, such as when your Actor is hosted on AWS.

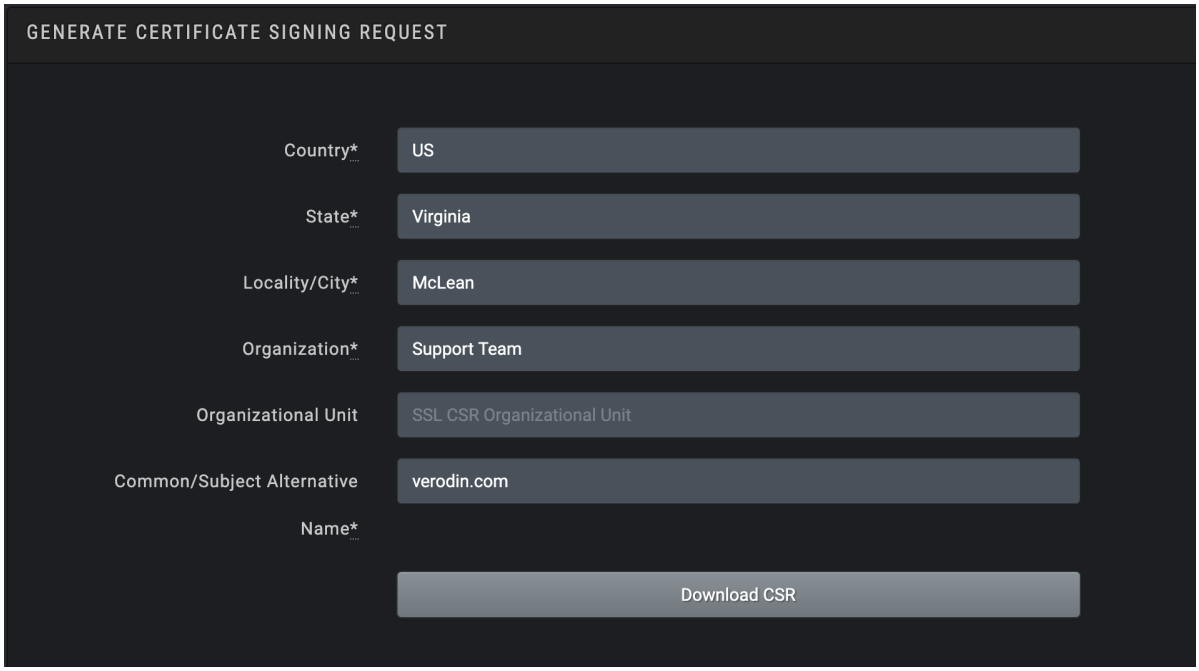
The SSL Settings page is where you can generate certificate signing requests and install signed SSL certificates. Both Signed Certificates and CA Intermediate Certificates may be uploaded for Director use. The root chain can be included with the certificate as long as it's in the correct format. The Validation Platform requires pem-encoded x509 certificates.

Any certificate added to the Director will also automatically be used by the Protected Theater Console. This means you won't have to accept an additional certificate when you launch the PT Console.

To generate the Certificate Signing Request

1. Go to **Settings** > **Director Settings**. The Systems Settings page opens.
2. From the Settings menu, select **SSL**.
3. Fill out the **Generate the Certificate Signing Request** form using your organization's information and then click **Download CSR**. This will add the private key to the Director.

NOTE: If you generate a new CSR, the previous CSR becomes invalid. Any certificates that are already installed will continue to work. However, if you try to install a certificate that was generated from the previous CSR, it will fail.

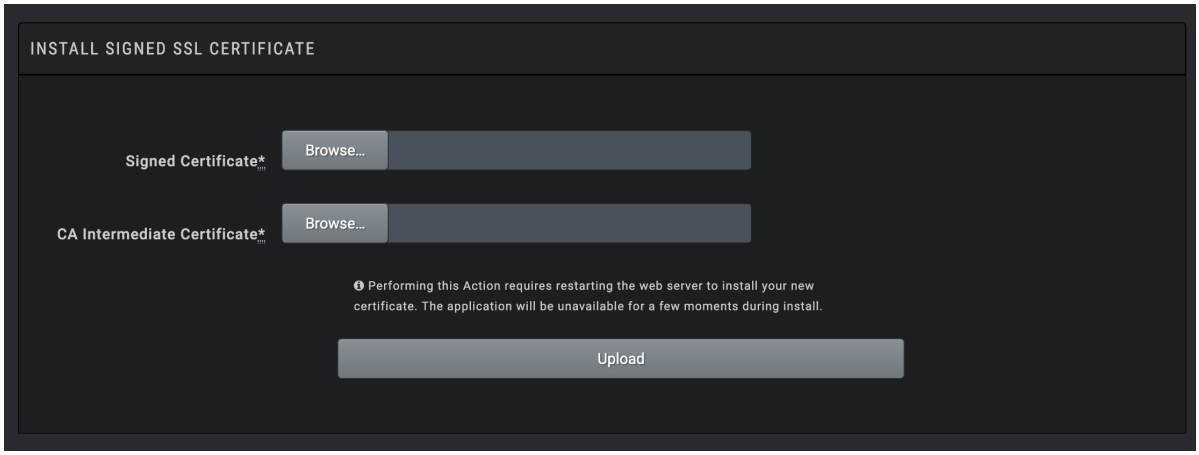


Generate CSR

To install an SSL Certificate

IMPORTANT: Be aware that applying these settings will restart the web service on the Director.

1. Go to **Settings** > **Director Settings**. The Systems Settings page opens.
2. From the Settings menu, select **SSL**.
3. Browse and select your **Signed Certificate**.
4. (Optional) Browse and select your **CA Intermediate Certificate**.
5. Click **Upload**.



Install an SSL Certificate

Configuring HTTP Strict Transport Security (HSTS)

You can enable HTTP Strict Transport Security (HSTS), which is a response header that tells your browser that it can access only sites with the HTTPS protocol, in the SSL settings on the Director. This enablement includes control of individual sub-options, such as max-age, subdomains, and preload.

When a supported browser receives the HSTS header, that browser prevents all communications from being sent over HTTP to the specified domain and sends all communications over HTTPS. Refer to RFC 6797 (HTTP Strict Transport Security (HSTS)) by the IETF, for more information.

This added layer of security helps secure your site and makes it more responsive. It can also improve search engine optimization.

IMPORTANT: While HSTS can improve the level of security of your site, we recommend that you do not include the preload directive by default. Preloading should be opt-in. Be aware that there can be long-term consequences of preloading and inclusion in the preload list cannot be undone easily.

To configure HSTS

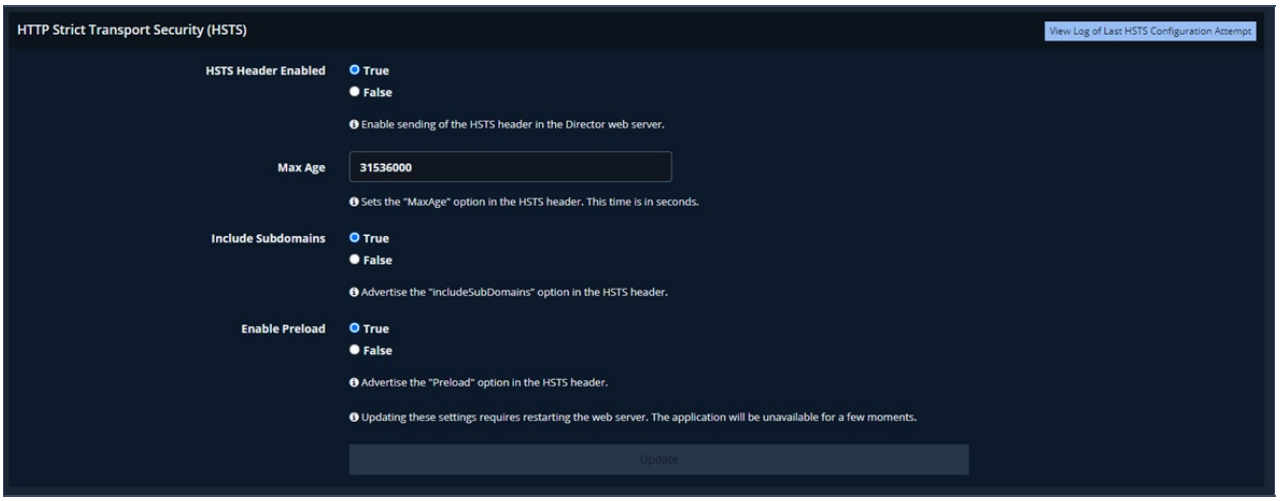
IMPORTANT: Be aware that applying these settings will restart the web service on the Director.

1. Go to **Settings** > **Director Settings**. The Systems Settings page opens.
2. In the HTTP Strict Transport Security (HSTS) window, configure HSTS by selecting the True or False radio buttons for the following options:
    - HSTS Header Enabled
    - Max Age (enter this value in the field provided)
    - Include Subdomains

- Enable Preload

3. Click **Update**.

When you have enabled HSTS, the View Log of Last HSTS Configuration Attempt box displays. Click this box to see the logs associated with the last attempt to configure HSTS.



HTTP Strict Transport Security (HSTS) window