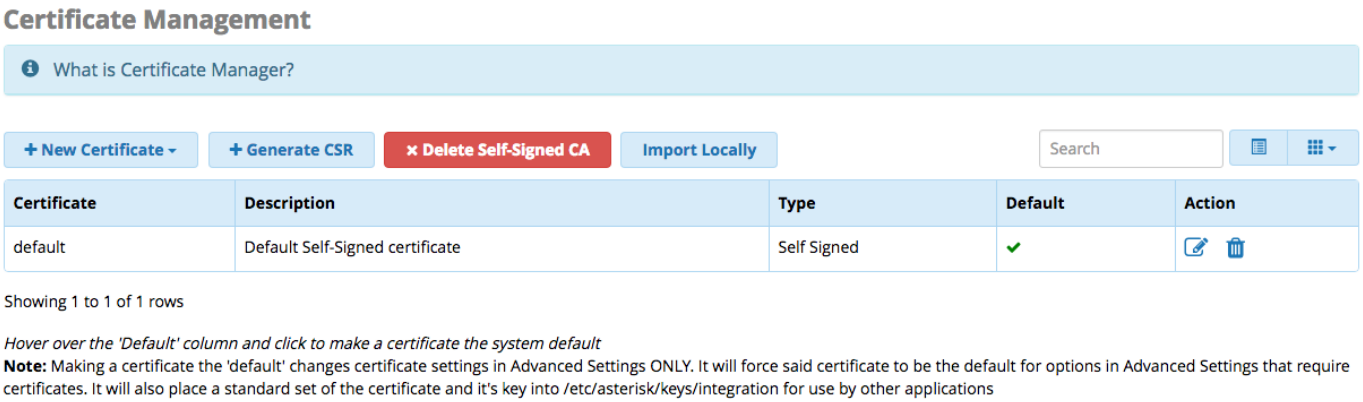
Certificate Management User Guide

Overview

The Certificate Management module is used to manage certificates on your FreePBX server.

Logging In

- From the top menu click **Admin**
- In the drop down click **Certificate Management**



On first login to your PBX a default self-signed certificate will have been created for you.

New Certificate

To add a new certificate click this button and select from one of the three drop downs.

Generate Let's Encrypt Certificate

Let's Encrypt Certificates are completely 100% free TLS certificates that are generated via an automated process designed to eliminate the current complex process of manual creation, validation, signing, installation, and renewal of certificates for secure websites. Your PBX implements this same automated process.

> This process uses the Let's Encrypt HTTP-01 challenge type which uses http only on port 80. To successfully create/renew an LE cert, all of the following must be satisfied:
>
> 1. The local pbx must be able to http get the challenge token from itself using the fqdn provided. If the PBX is behind a NAT router /firewall this may fail depending on your router configuration. It is for this reason that you see references to setting the PBX hostname to the LE fqdn to allow this challenge to succeed.
> 2. Sangoma mirror servers must be able to http get the challenge token by resolving the configured fqdn. It is for this reason that previous firewall recommendations stated that the Sangoma mirror servers must be whitelisted.

3. The Let's Encrypt server(s) must be able to get the challenge token by resolving the configured FQDN. This challenge can come from anywhere, so there is no value in whitelisting for this purpose, port 80 must be open to world for the challenge to succeed.

Current versions of the PBX firewall and Certificate Management module manage the local firewall rules dynamically during cert creation/renewal.

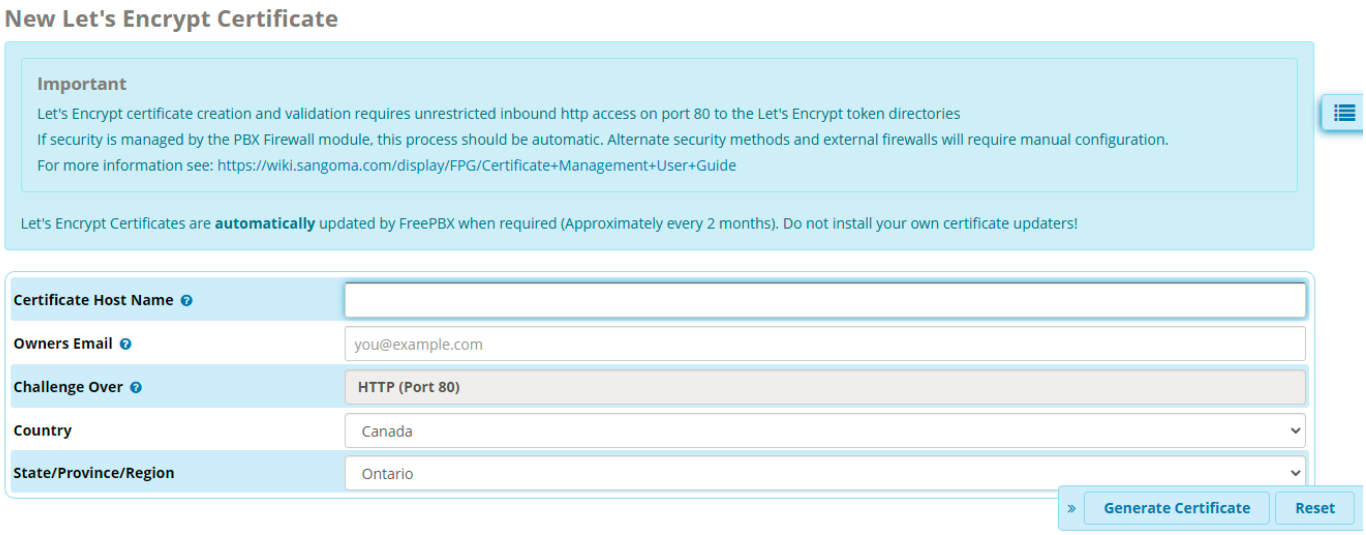
It's not required, but if you have the **Commercial (Full)** Sysadmin module, you can specify that a 'LetsEncrypt Only' service listens on port 80. See the Port Management page for more information.

Let's Encrypt certificate creation and validation requires unrestricted inbound http access on port 80 to the Let's Encrypt token directories. If security is managed by the PBX Firewall module, this process

should be automatic. Alternate security methods and external firewalls will require manual configuration.

You can manually enable the custom firewall rule for allowing global access to Lets encrypt token directories by enabling **LetsEncrypt Rules** und er Firewall Advanced settings tab through the GUI or by

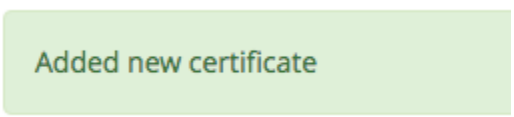
running "fwconsole firewall lerules enable" from the CLI and the same can be disabled by disabling **LetsEncrypt Rules** from GUI or by running "f wconsole firewall lerules disable" from the CLI.



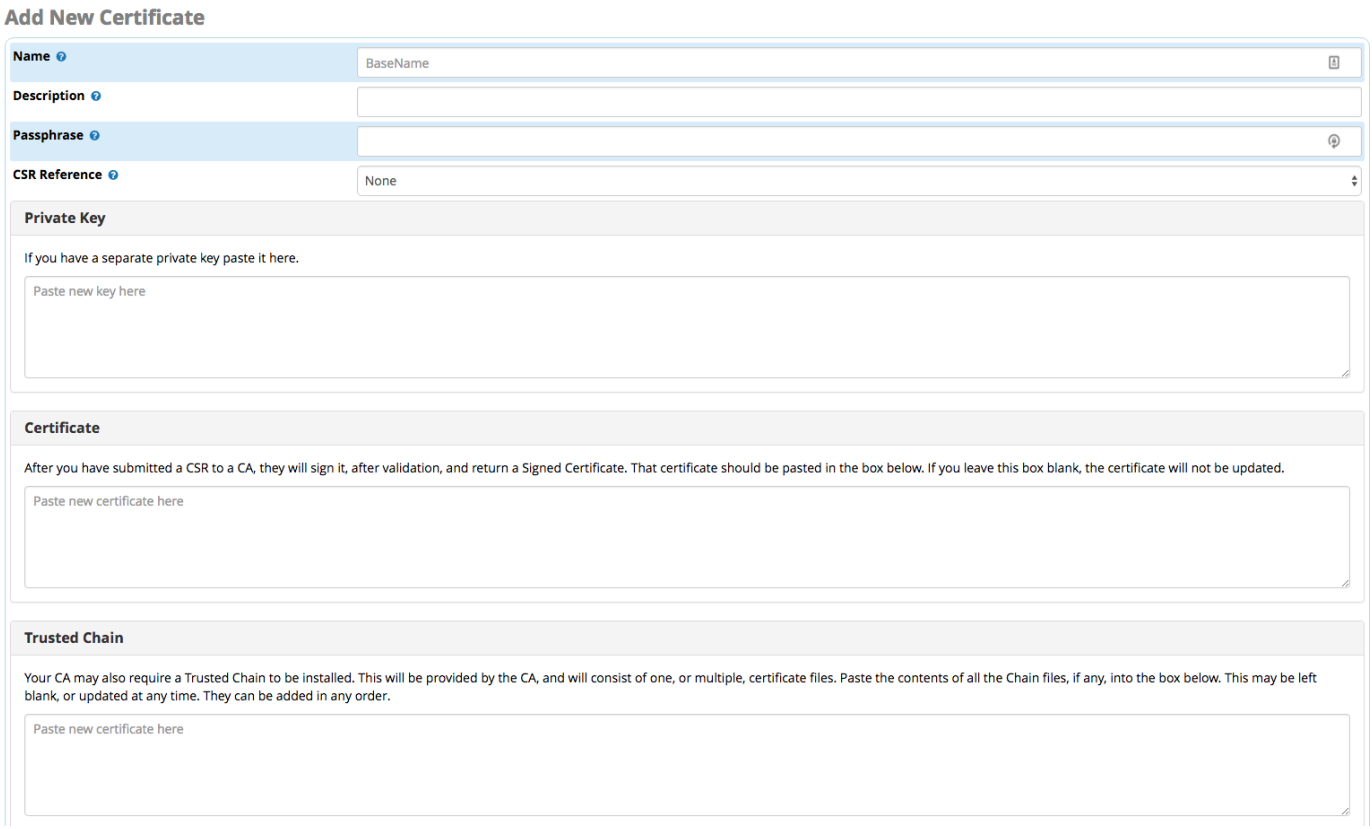
There are several required options to generate a Let's Encrypt Certificate

- **Certificate Host Name:** The hostname you want to use for your certificate. This must be a fully qualified domain name that points back to your PBX.
- **Owners Email:** Your email address. This email is provided to Let's Encrypt to send you important information about your certificate
- **Challenge Over:** The only option here is HTTP (Port 80). The port can NOT be changed.
- **Country:** The country where you are located
- **State/Province/Region:** The state/Province where you are located

Once you are finished click "Generate Certificate". Your certificate will be added and will be automatically update approximately every 2 months



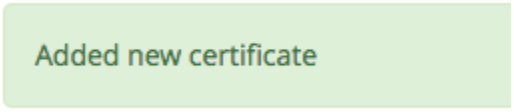
Upload Certificate



- **Name:** Certificate Name. Usually the hast name
- **Description:** Certificate description
- **Passphrase:**The Passphrase of the Private Key. This will be used to decrypt the private key and the certificate. They will be stored unpassworded on the system to prevent service disruptions.
- **CSR Reference:**Certificate Signing Request to reference. If 'None' is selected then you will be able to upload your own private key
- **Private Key:** Paste your private key here
- **Certificate:** Paste your certificate here
- **Trusted Chain:** Paste your trusted chain here

> In order to view the certs to copy, you must open the TLS files using a plain text editor, and not necessarily the default application configured on the workstation.

Once you are finished click "Upload Certificate".

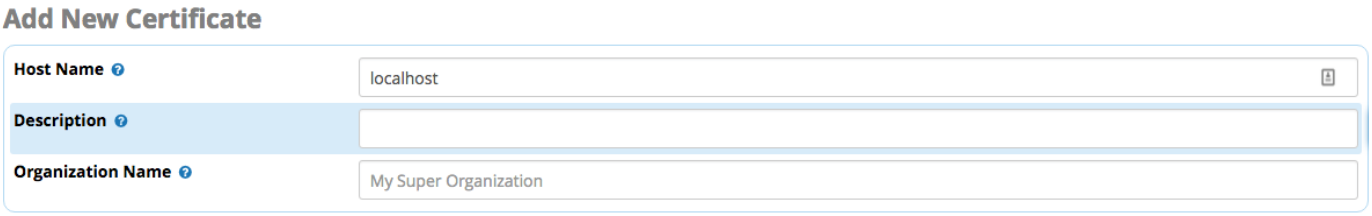


Generate Self-Signed Certificate

Self Signed Certificates are not recommended as many browsers outright reject these certificates, they can, however, be useful for internal testing

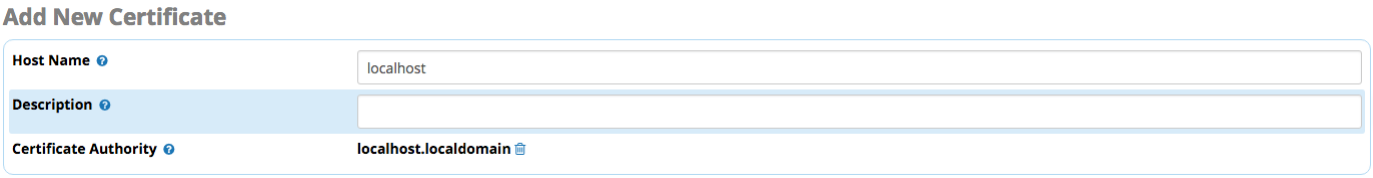
Your PBX also generates a self signed certificate on first boot

If you have previously deleted the self-signed CA when you go to create a new self-signed certificate your screen will look like this:



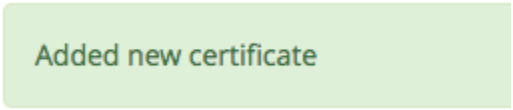
- **Host Name:** The hostname of the system. Should be a fully qualified domain name
- **Description:** Description of this certificate
- **Organization Name:** Organization name, Used in the Certificate Authority generation process

Otherwise the New Certificate screen will look like this:



- **Host Name:**The hostname of the system. Should be a fully qualified domain name
- **Description:** The description of the certificate
- **Certificate Authority:** The Certificate Authority that will generate this certificate. You can delete the CA from this page as well by clicking this icon 

Once you are finished click "Generate Certificate".

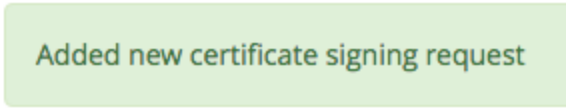


Generate CSR (Certificate Signing Request)

You can generate a CSR from your PBX to be used for the process of obtaining certificates from valid certificate authorities online

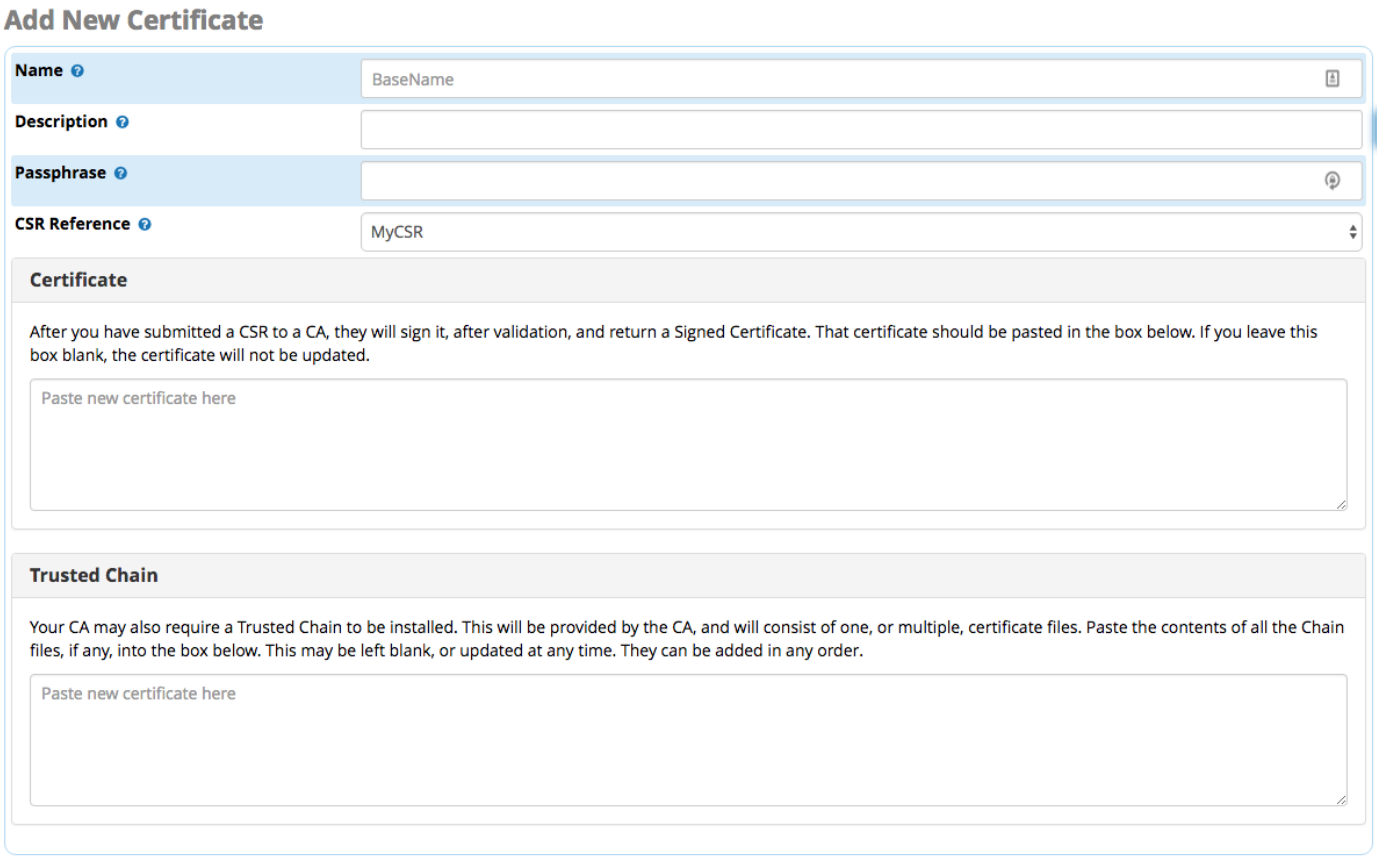
- **Name:** The name of this CSR
- **Common Name (CN):** The common name (also known as hostname)
- **Organization Name (O):** Organization Name such as Sangoma Technologies, Inc.
- **Organization Unit (OU):** Organizational Unit. This can be a doing business as (DBA) name, or the name of a department within the business. This may be left blank.
- **Country (C):** Two letter country code, such as "US", "CA", or "AU".
- **State/Province (ST):** State or province such as "Queensland" or "Wisconsin" or "Ontario." Do not abbreviate. Enter the full name.
- **City of Locality (L):** City name such as "Toronto" or "Brisbane." Do not abbreviate. For example, enter "Saint Louis" not "St. Louis"

Click "Generate CSR".



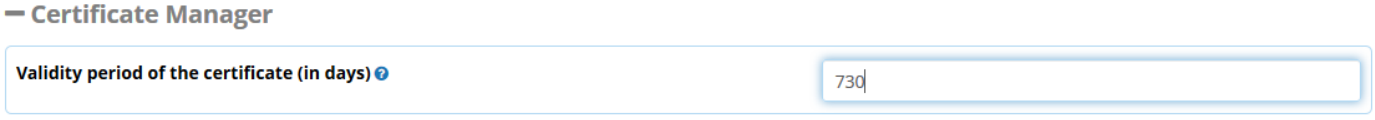
After the request has processed a new button will appear on the main page of Certificate Manager which allows you you download the CSR so you can submit it to a Certificate Authority.

You can then later reference this CSR/Private Key when you upload your certificate:



Change Certificate Validity period

You can change the value of the validity period (*2 years by default*).
Go to Advanced Settings menu and Certificate Manager partand enter a new value (in days). E.g: *2 years = 730 days.*

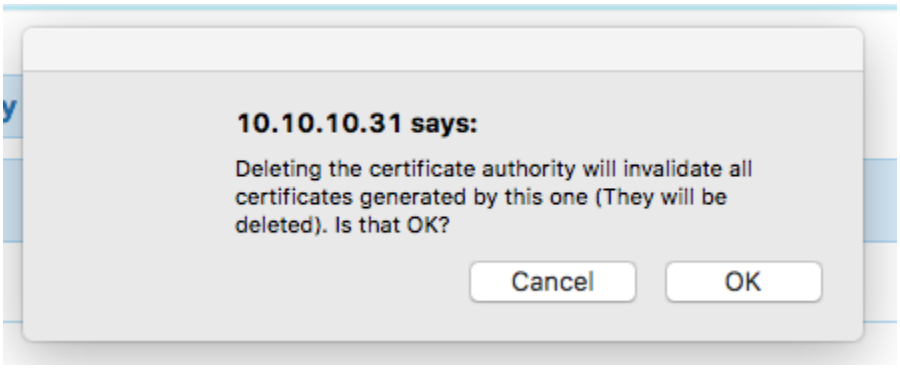


> *Do it before generate any certificates.*

Delete Self-Signed CA

You can delete the self signed certificate authority at any time by clicking the red button labeled "Delete Self-Signed CA".

A prompt will then come up warning you that all certificates that relied on this self signed certificate authority will be invalidated



Once you have deleted the self-signed CA you can then generate another one by clicking "New Certificate" then "Generate Self-Signed Certificate"

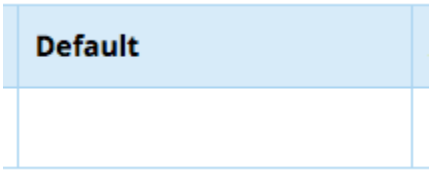
Import Locally

To manually import your certificates you need to drop the *.key and *.crt files into /etc/asterisk/keys. Then click the Import Locally button.

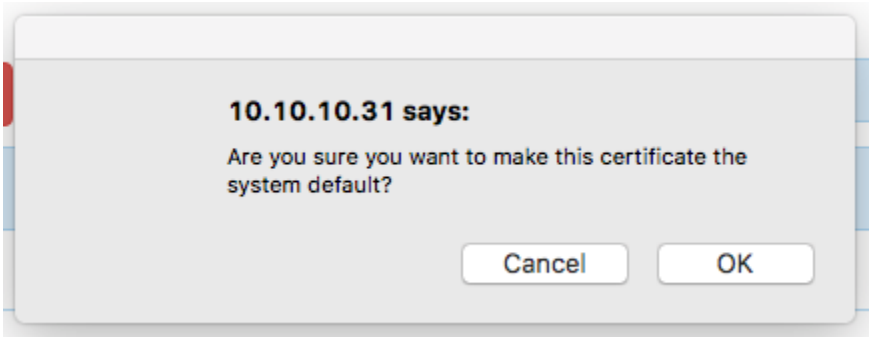
When this has finished your certificates will show up in the list of PBX certificates.

Setting a default certificate

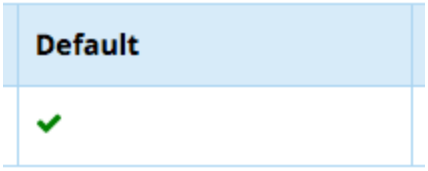
Making a certificate the 'default' changes certificate settings in Advanced Settings ONLY. It will force said certificate to be the default for options in Advanced Settings that require certificates. It will also place a standard set of the certificate and it's key into /etc/asterisk/keys/integration for use by other applications



To select a certificate as the default move you mouse over the blank/empty column in the list of certificates. A grey checkmark will appear. Click that checkmark to make it the default



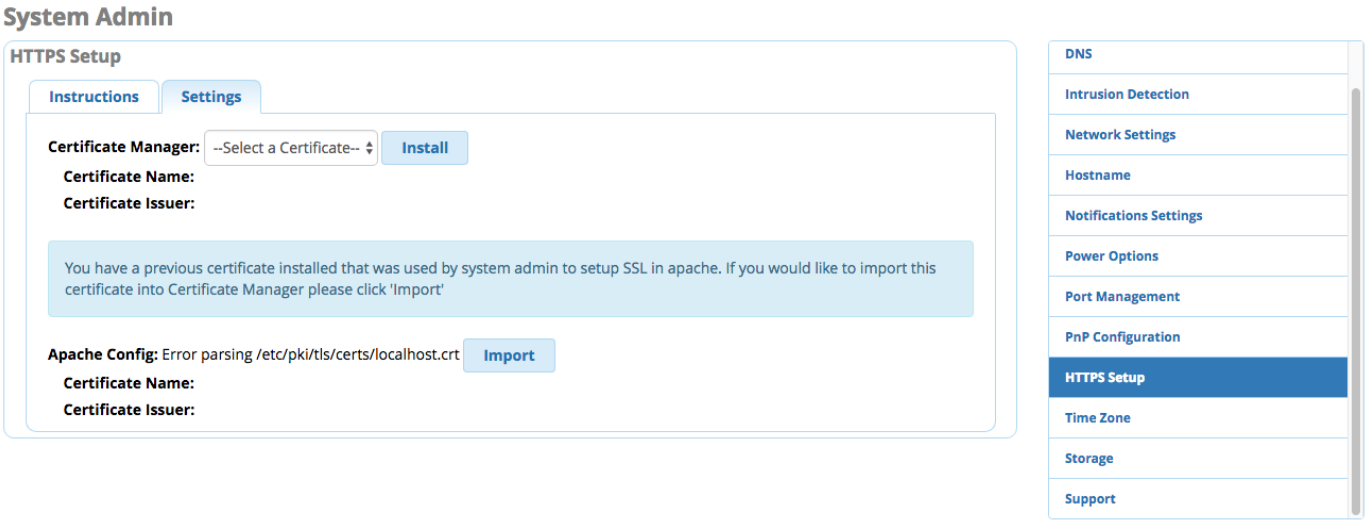
After this process has completed the checkmark will turn from grey to green and stick after you move your mouse away.



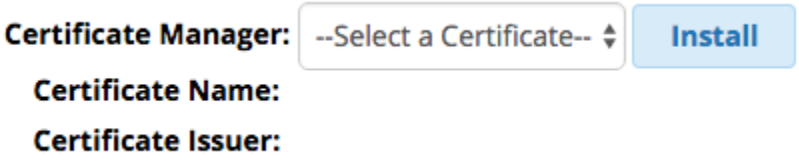
Using a certificate with System Admin

After you have added at least one certificate and activated your system you will be able to select that certificate as the default that system admin should use for the Apache webserver.

Go to System Admin then click "HTTPS Setup". Next hit the "settings" tab.



Select a certificate to use from the list of certificates provided by Certificate Manager:



Then click install. When the process has completed you will see your certificate detailed under "Apache Config"

Certificate Manager: localhost Install

Certificate Name: localhost

Certificate Issuer: localhost

You have a previous certificate installed that was used by syst
Certificate Manager please click 'Import'

Apache Config: Apache Configured Import

Certificate Name: localhost

Certificate Issuer: localhost