

# Requesting and Installing a Certificate

Requesting an installing a certificate includes the following steps

1. [Creating a Certificate Signing Request \(CSR\)](#) on the Bridge you want to use the certificate for.
2. [Ordering an official certificate](#) from a certificate authority like e.g. VeriSign.
3. [Installing the certificate](#) on the Bridge.

## Creating a Certificate Signing Request (CSR)

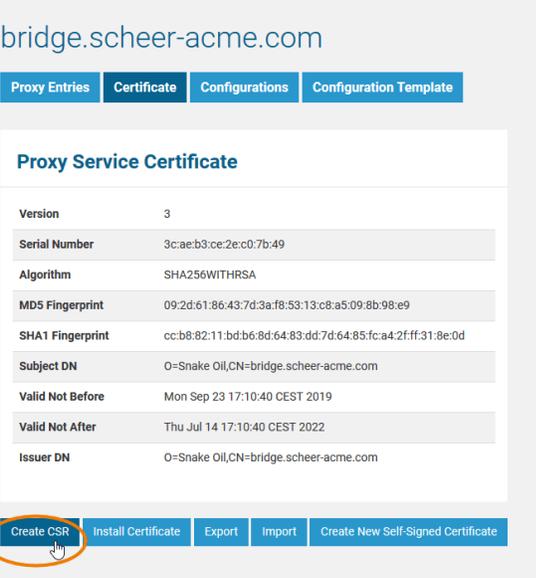
For the enrollment of an official certificate, you need to provide a certificate signing request (CSR). On the **Certificate** tab, all related actions can be executed, if the user has administration rights.

### On this Page:

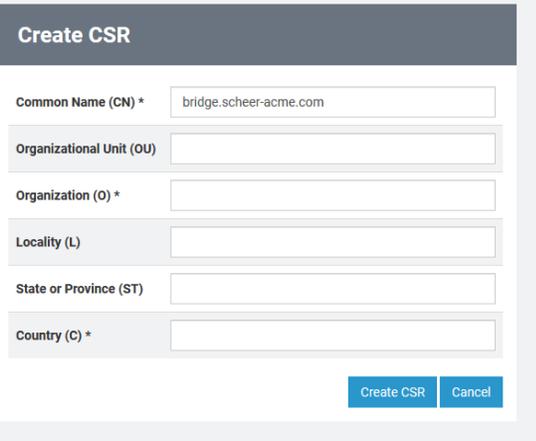
- [Creating a Certificate Signing Request \(CSR\)](#)
- [Ordering an Official Certificate](#)
- [Installing a Certificate](#)
  - [Manual Certificate Installation](#)

### Related Pages:

- [Requesting and Installing a Certificate](#)
- [Importing and Exporting Proxy Server Certificates](#)
- [Renewing the Self-signed Proxy Certificate](#)



In order to create a certificate signing request, click **Create CSR**.



The form to enter all required fields is displayed.

Fields with an asterisk (\*) are mandatory.

| Field                     | Description   |
|---------------------------|---|
| <b>Common Name (CN) *</b> | The common name for the server that will use the SSL certificate must be the fully qualified domain name the domain name and the host name (if applicable). For example, in <b>bridge.scheer-acme.com</b> , <b>scheer-acme.com</b> is the domain name and <b>bridge</b> is the host name. If your fully qualified domain name does not include a host name, simply enter the domain name. A host name will not be included in your certificate. Check the common name during the enrollment process to ensure it is correct and is not the one of another Bridge domain member. After your SSL certificate has been issued, changing the common name requires re-enrollment at the full price of the certificate. |

|                                 |   |
|---------------------------------|---|
| <b>Organizational Unit (OU)</b> | Your department or unit within your company or organization.                    |
| <b>Organization (O) *</b>       | Your company or organization.   |
| <b>Locality (L)</b>             | City, in which your company or organization is physically located.              |
| <b>State or Province (ST)</b>   | State or province, in which your company or organization is physically located. |
| <b>Country (C) *</b>            | Country, in which your company or organization is physically located.           |

After having entered all fields, click **Create CSR**. By clicking **Cancel**, you can cancel this action and go back to the the main certificate page.

The encrypted certificate request is displayed on the next page.

Mark the complete certificate request and copy it. It will be pasted into the order form of the certificate authority application, where you will order the official certificate. After clicking **Continue**, the main certificate page will be displayed again.

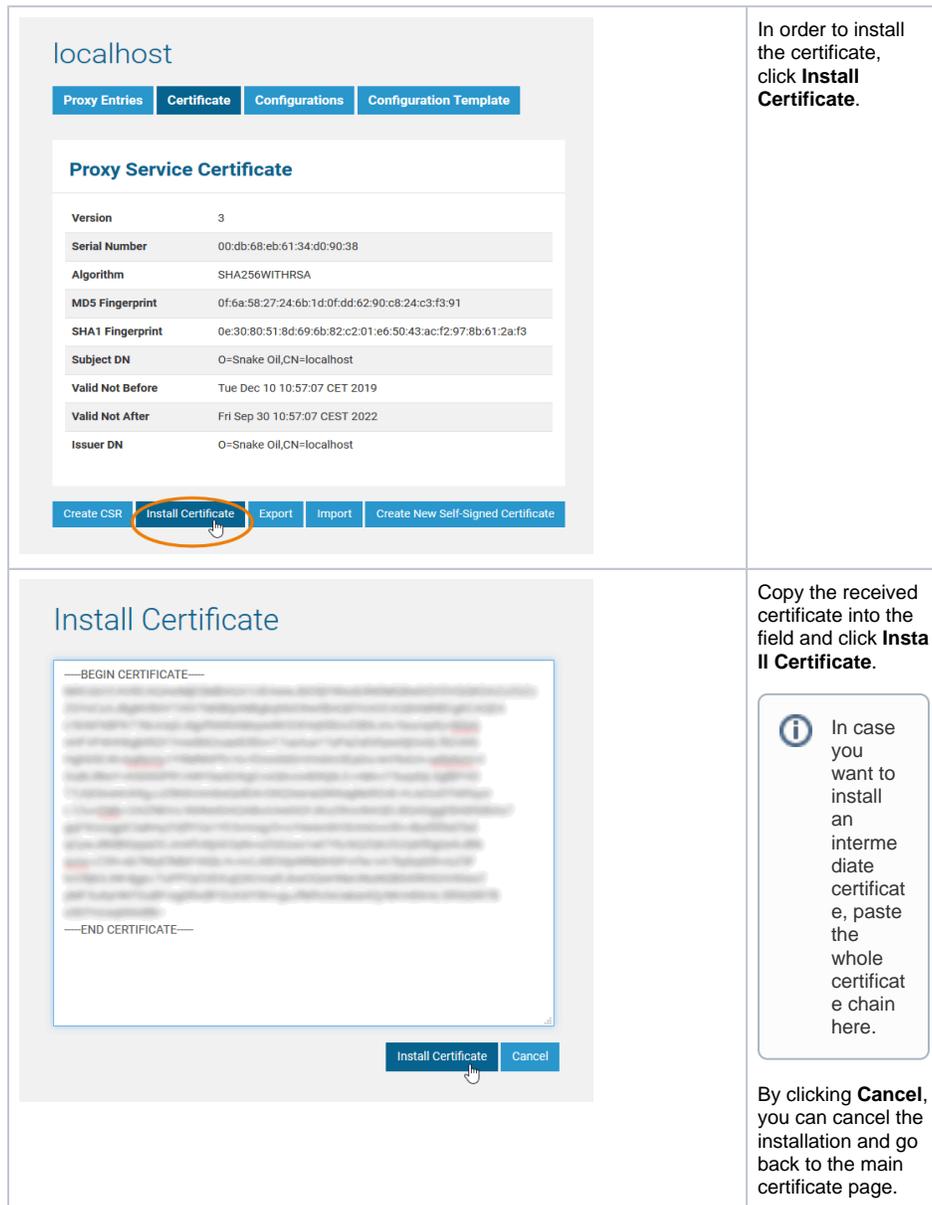
## Ordering an Official Certificate

Order an official certificate from a certificate authority like VeriSign or Thawte. During ordering process you will come to a step where you have to paste the CSR that you have created before in step 1. If asked for a server platform, select **Apache**.

Once you have received the certificate from the certification company, you can continue to install the certificate on the Bridge (see further below).

## Installing a Certificate

Once you received a certificate from a certificate authority, you can install it on the Bridge. On the **Certificate** tab, all related actions can be executed, if the user has administration rights.



The image shows two screenshots from the Bridge interface. The top screenshot displays the 'localhost' page with the 'Certificate' tab selected. It shows details for a 'Proxy Service Certificate' including Version (3), Serial Number (00:db:68:eb:61:34:d0:90:38), Algorithm (SHA256WITHRSA), MD5 Fingerprint, SHA1 Fingerprint, Subject DN (O=Snake Oil,CN=localhost), Valid Not Before (Tue Dec 10 10:57:07 CET 2019), Valid Not After (Fri Sep 30 10:57:07 CEST 2022), and Issuer DN (O=Snake Oil,CN=localhost). The 'Install Certificate' button is circled in orange. The bottom screenshot shows the 'Install Certificate' dialog box with a text area for pasting the certificate and 'Install Certificate' and 'Cancel' buttons.

In order to install the certificate, click **Install Certificate**.

Copy the received certificate into the field and click **Install Certificate**.

**i** In case you want to install an intermediate certificate, paste the whole certificate chain here.

By clicking **Cancel**, you can cancel the installation and go back to the main certificate page.

If the installation of the certificate has been successful, the main certificate page is displayed again. It now shows the information of the official certificate.

If the certificate does not fit to the server it was enrolled for, an error message like 'Wrong or invalid certificate!' will be displayed.

## Manual Certificate Installation

You can also install proxy certificates manually to the Bridge. Proxy certificate locations are stored in file `<your Bridge data directory>/proxies/templates/virtual_host_ssl.conf`. To manually add a proxy certificate, do the following:

1. Copy file **virtual\_host\_ssl.conf** from **<your Bridge data directory>/proxies/system\_templates** to **<your Bridge data directory>/proxies/templates**.
2. Edit the file and add paths to your certificate files:

```
# virtual host ssl settings start
#
SSLEngine On
SSLCertificateFile "${SSL_CERTIFICATE}"
SSLCertificateKeyFile "${SSL_CERTIFICATE_KEY}"
#
# virtual host ssl settings end
```

Replace the placeholders `${SSL_CERTIFICATE}` and `${SSL_CERTIFICATE_KEY}` by valid paths to certificate / key files. The certificate file may also contain a chain of certificates.

3. Restart the Bridge proxy via the Bridge administration console.