How to request an SSL certificate

Version October 2016

Webpower BV
Koolhovenstraat 1k
3772MT Barneveld

WHAT IS SSL?

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).

SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information. More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

SSL in email makes it so that the assets gets transmitted from our web servers to the clients email client without being intercepted in the mean time. Even more importantly, the web-versions that people view are secured with SSL. This means that both the contents as well as the assets in the mail are all encrypted using SSL, so that 3rd parties cannot intercept the data between the user and our servers.

For an SSL certificate to work you need a couple of components:

- **Private key**

  This should only be on the server and nowhere else, this 'proves' that you are the creator of the certificate.
- **CSR**

  This is a Certificate Signing Request, you use this at a SSL provider to request your certificate.
- **Certificate**

  This is what you install on your server, and it gets send out to the outside world. This is the "lock" you see in your browser on a https page.

- **CA Certificate (also known as Intermediate Certificate)**

  This ties your certificate to a 'trusted' party (Certificate Authority). This is the glue that hold the whole chain together, and links your certificate (that is in term 'linked' to your privatekey) to the party that is trusted. Those trusted parties (CAs) is what your browser will accept as valid certificates. That makes for the whole certificate chain.

HOW DO YOU REQUEST AN SSL CERTIFICATE FOR A LOCAL DOMAIN?

The account manager will need to request the SSL module to be enabled. With this request the account manager will need to provide the following information:

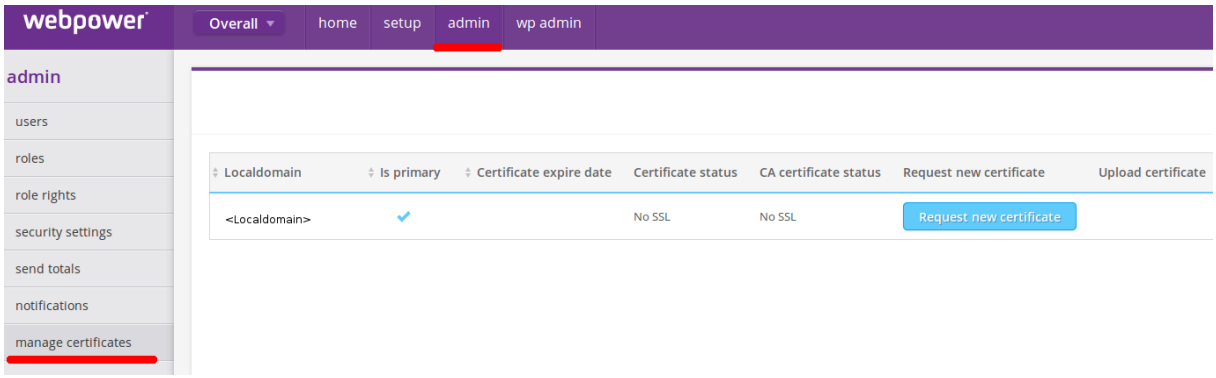
- **Amount of local domains the client wants SSL certificates for (usually 1)**
- **Notification email**

  This is (or are) the email address(es) that will receive an email when the certificate is about to expire and needs renewal. In case of Webpower managing the certificate, a Webpower address should be provided (sales@webpower.nl /es /se and/or mailings@webpower.nl)
- **CSR email address**

  This email address will receive the email with the CSR if the client chooses to let Webpower handle the SSL certificate. This should be set to either mailings@webpower.nl or *sales@webpower.nl /es /se* .. email.

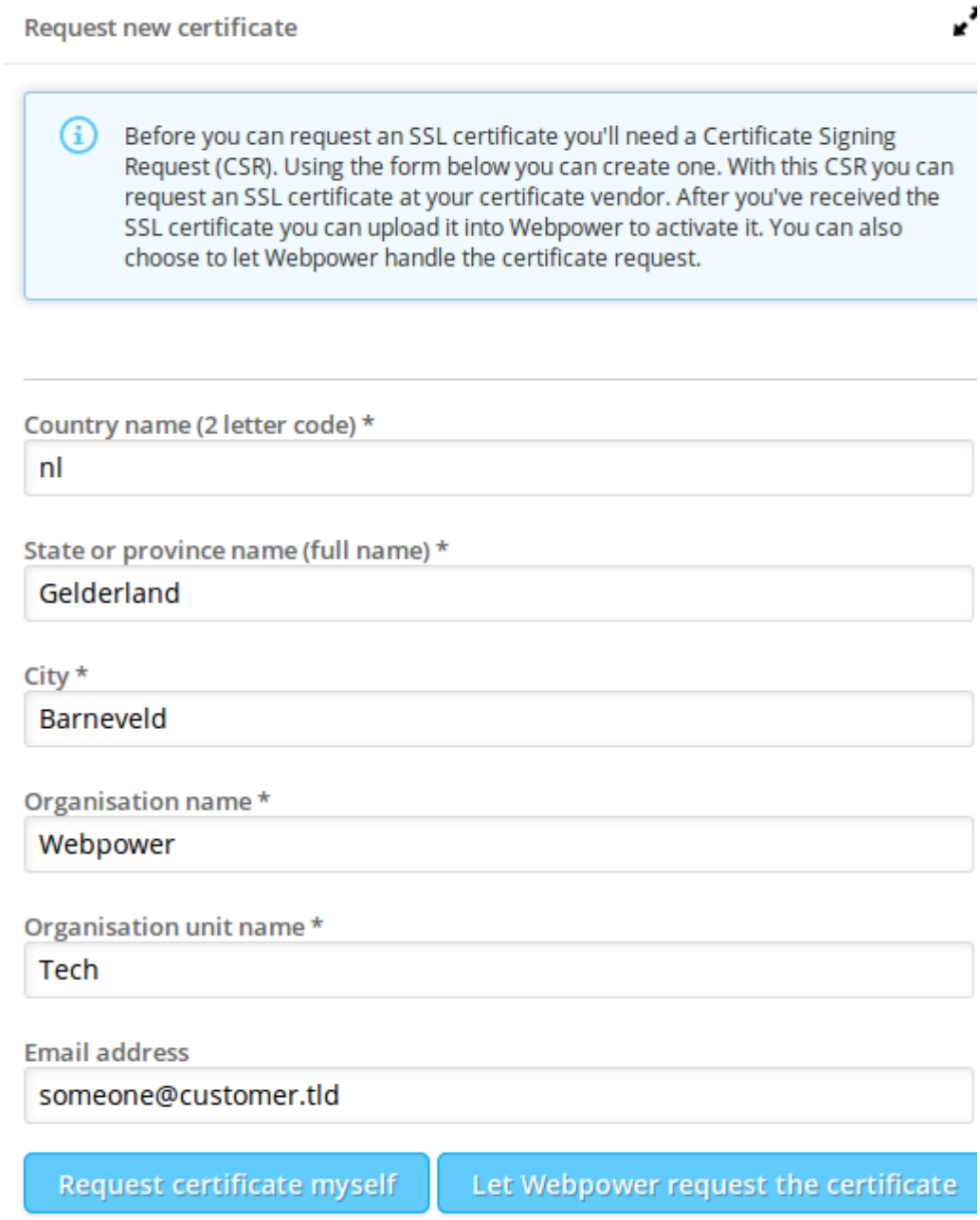
HOW TO PROCEED AFTER THE MODULE IS ENABLED

The following day (after the nightly cleanup) you should see the menu item appear (Admin > manage certificates):



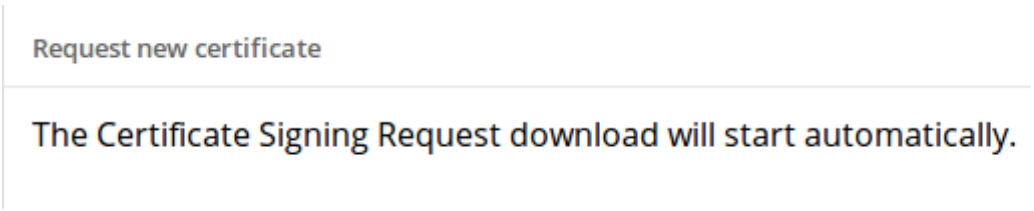
Here you will find all the information about any running certificate, or ongoing requests.

The customer can now click on the "Request new certificate" button and will be presented with the following screen:



Here you will see some sample input, the customer will need to fill this information with their data, and then click one of 2 buttons:

Request certificate myself, will prompt the user with a download for the CSR

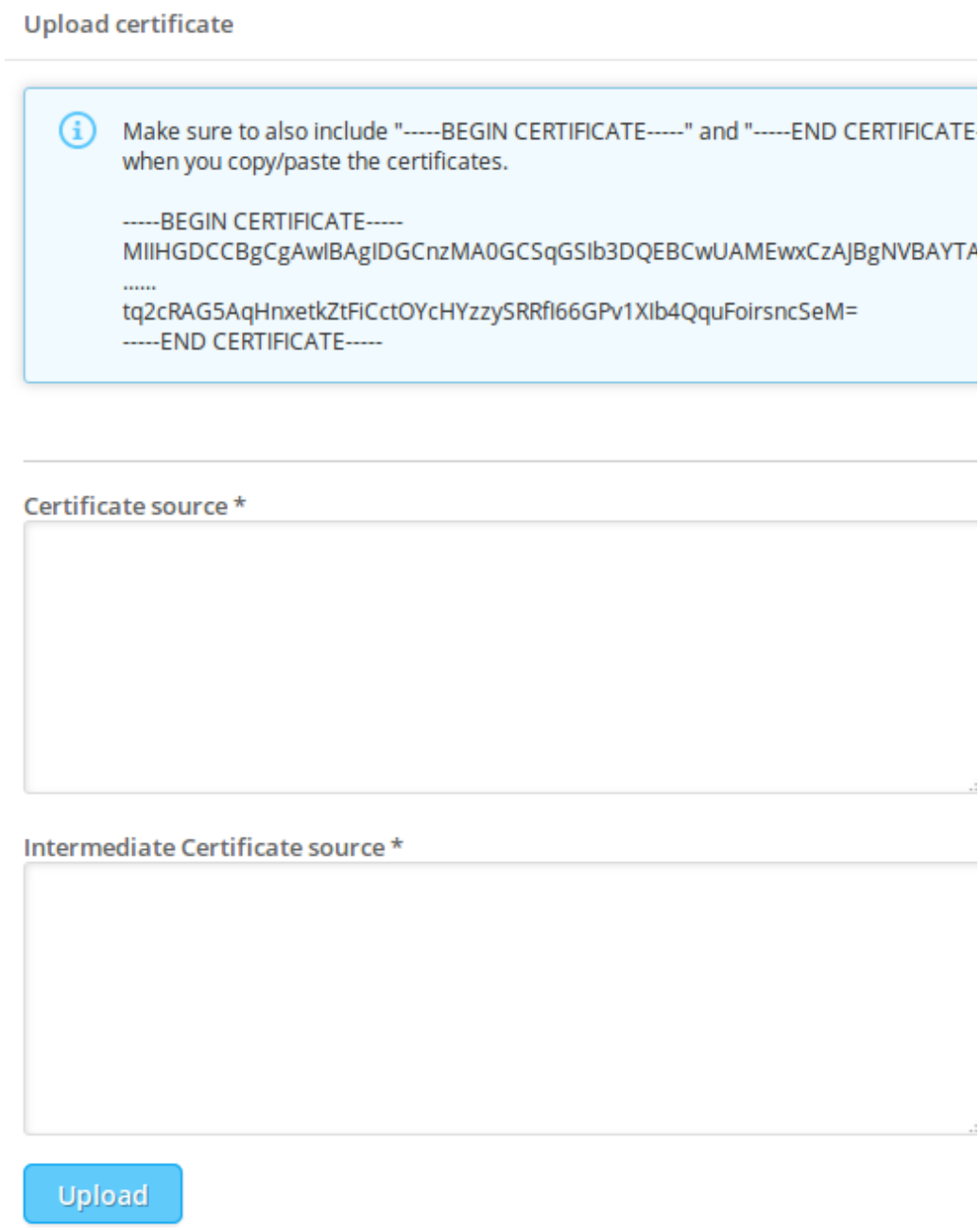


The customer then sends this CSR, that they just downloaded, to their SSL provider, and get certificate and Intermediate CA certificate back (usually within 24 hours).

How the clients gets the 2 certificates varies per ssl provider. Some email it in a format like:

```
-----BEGIN CERTIFICATE-----
MIIHGDCCBgCgAwIBAgIDGGSIb3DQEBCwUAMEwxCzAJBgNVBAYTAkRF
.....
tq2cRAG5AqHnxetkZtFiCctOYcHYzzySRRfI66GPv1XIb4QquFoirsncSeM=
-----END CERTIFICATE-----
```

For both certificates, whiles others may send it as files. If they are send as files, the client will need to open the files with notepad (or equivalent). The with the open menu browse to where they saved the files on their computer. When they open it they will see a similar format as shown above here. They will need to do this for both the Certificate as well as the Intermediate CA certificate and paste the content in Webpower. On the same page as before (Admin > Manage Certificates) and click on the "Upload Certificate" button for the correct localdomain.

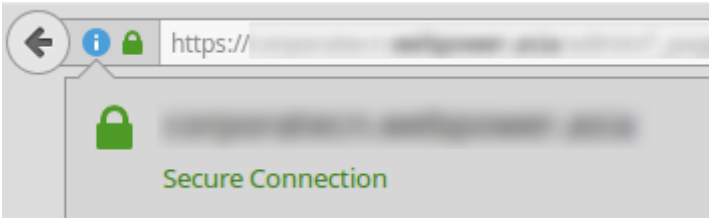


If they click the "Let Webpower request the certificate" an email will be sent with the CSR to the before mentioned and provided CSR email. Then the previous steps should be done by Webpower personnel (request the cert with the CSR, paste the resulting certificate and intermediate CA in Webpower customer environment).

And the final result after everything is uploaded properly:

Localdomain	Is primary	Certificate expire date	Certificate status	CA certificate status	Request new certificate	Upload certificate
dmdacc.webpower.nl	✔	2017-04-29 11:07	Correctly installed	Correctly installed		

Note: Keep in mind that this does not automatically mean that the certificate is already active, the account manager (or the customer) can check this by going to https://<localdomain.tld> (in this example: https://dmdacc.webpower.nl) and click on the (if everything is correct) green lock in the URL bar to see the details.



The back-end updates every 15 minutes of every workday between 9:00 and 16:00 to install new certificates, outside that time frame no SSL certificate is installed.