FAQ - Ordering and Validation

Can an OV/EV certificate be ordered by a private entrepreneur?

Question

Can an OV/EV certificate be ordered by a private entrepreneur?

Answer

Yes, that is possible.

Enrolling Private Entrepreneur has to forego a face-to-face* verification, which would require providing additional documents, filling out a verification form and mailing it directly to Comodo using postal or courier service.
Please note Russian PE's are eligible for OV certificates only ;

* If PE has passed face-to-face verification during the registration in the local commercial registry, Comodo's face-to-face verification is not required ;

Is "www" automatically included in my SSL order?

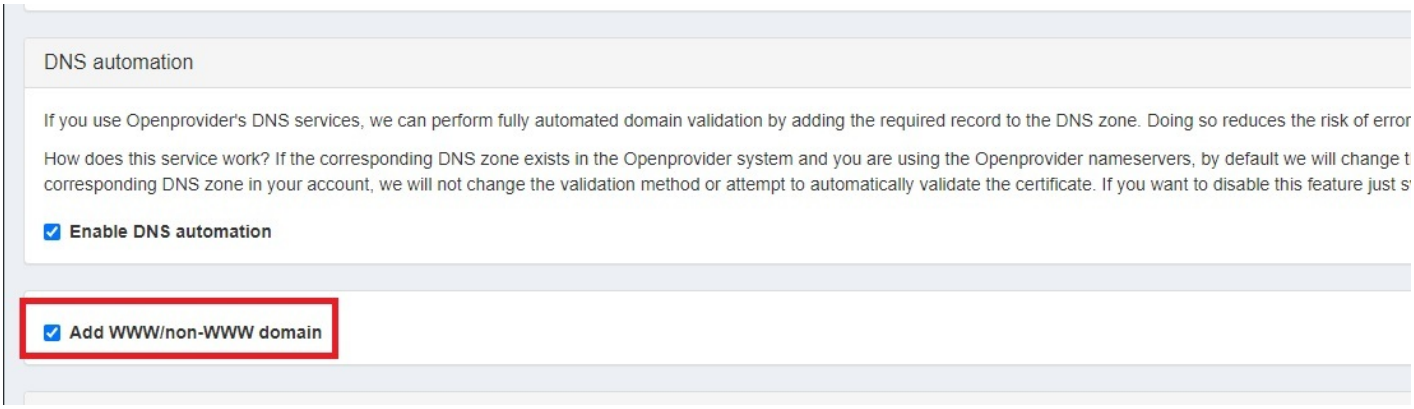
Question

Would the certificate for "www.example.com" protect "example.com" (and vice versa)?
Would "www.subdomain.example.com" protect "subdomain.example.com" as well?

Answer

Single Domain Certificate: When requesting a certificate in the SSL panel, there is a dedicated checkbox that allows selecting if you wish to request the certificate for both variants - with and without WWW. By default, both variants will be requested (checkbox will be selected). If you wish to receive the certificate just for a specified domain name, e.g. example.com (without WWW), please uncheck it.

Note: *when you request both variants, the validation method can only be changed for the main domain. In case of using DNS or EMAIL validation methods only the main domain is validated, the free SAN is not validated although the method will be visible next to it in SSL panel. If you choose HTTP (file-based validation) then both hostnames must be validated - relevant instruction is provided in SSL panel.*



* if you do not see this checkbox yet, please clear your cache / cookies for sslpanel.io from the browser, to make sure the latest release of the ssl panel is shown.

Important for Openprovider API users:
When requesting a certificate using our API, if you wish to request a certificate for a domain with WWW and without WWW, you have to specify host names and domain validation methods for both variants. For example:

```
"domain_validation_methods": [
  {
    "host_name": "domain.com",
    "method": "https"
  },
  {
    "host_name": "www.domain.com",
    "method": "https"
  }
],
"host_names": [
  "www.domain.com"
]
```

Multidomain Certificate: No, you must add both www and non-www domains which you want to secure in the list of domains (SAN domains).

Wildcard Certificate: In case you add a wildcard (*.domain.com) in the multidomain order, the www. is considered a subdomain so this is covered by the wildcard domain. Check this article how to order a wildcard in a multidomain ssl.

Certificate renewals: When processing a renewal request, the Openprovider system will first check which variants where initially issued for the particular domain; with WWW and without WWW variant or with just one. If you received first certificate with both, then the renewed certificate will include WWW and non-WWW domain.

If you received the certificate with just one variant but need both, you can always reissue it in SSL Panel with the above checkbox selected.

Order been flagged for a brand validation, what does that mean?

Question

My order has been flagged for a brand validation, what does that mean, what should I do?

Answer

The Certificate Authority will try to manually validate your company information stated in the order because CA’s system flagged it for such review. Reasons may vary: a match for a certain keyword has been found in the order details, your company business considered to be risky (banking, gambling, legal services). The manual review takes up to 48 hours.

If after this period order is still in the brand validation phase - contact support.

The domain in the CSR is restricted

Question

While requesting a certificate with domain *.no-ip.org in CSR, SSL Panel returns an error: The domain in the CSR is restricted.

Answer

That is because the customer does not own the root domain and therefore is never able to complete the validation steps. The blocked domains are:

'synology.me',

'now-ip.com',

'dyn.com',

'changeip.com',

'afraid.org',

'freedns.io',

'routable.org',
/\.(dyndns|no-ip)\.(com|net|org)$/

What do the warranties for SSL certificates mean? What is covered by them?

Question

What do the warranties for SSL certificates mean? What is covered by them?

Answer

SSL certificates services include a limited Warranty to provide your site extra assurance that your site is safe to conduct online business.

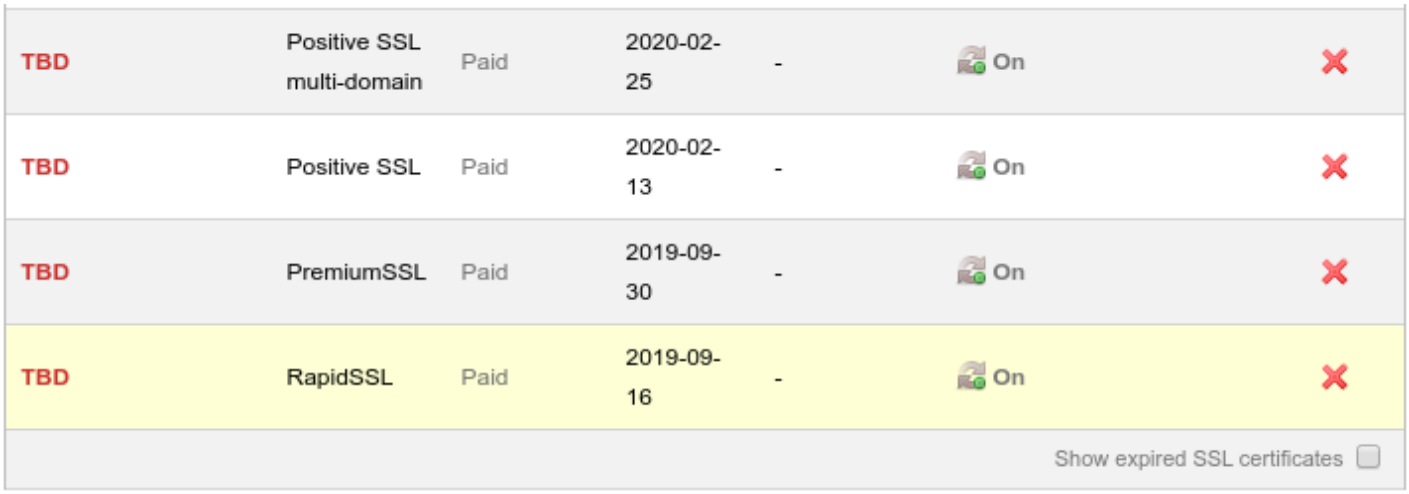
Warranty is payable to your visitors who rely on the SSL and who incur losses resulting directly from an online card transaction as a result of a mis-issued SSL certificate.
Warranties start at $10,000 (most DV certificates) and go up to $50,000, $100,000, $250,000+ for OV and EV.

Certification authority will refund you in the event something goes wrong on their end and the website will be hijacked that is why you should feel confident with an SSL certificate.
If anything goes wrong that causes you to lose the money - you are covered.

What does "TBD" SSL mean?

Question

I've noticed one or more certificates with domain: "TBD" in RCP. What does that mean?



Answer

"TBD" means "To be done". That normally happens when you started ordering SSL and did not complete that and saved the request as a draft. This is an order that is not yet sent to CA. You can open it, fill in the required information and sent to CA, or cancel such order.

If you cancel the TBD order, the reserved balance will be returned directly to your balance.

Why I can't re-request confirmation email or change validation method for my DV certificate?

Question

Why I can't re-request confirmation email or change validation method for my DV certificate?

Answer

The most common reason is that your certificate has already passed the DV check.
No reason to change methods or send additional emails to the domain owner.

Why file is uploaded but file validation is not finished yet?

Question

We have uploaded the .txt file to our server 2 hours ago, but HTTP(s) Validation is not finished yet. What is the reason for the delay?

Answer

Following reasons are possible:

a) The file name or contents are incorrect:

The file name should always be in uppercase letters
The file contents should always be in lowercase letters

b) The file is placed incorrectly. Only the following locations are allowed:

```
http://www.example.com/FileName
https://www.example.com/FileName
http://example.com/FileName
https://example.com/FileName
```

For Multi-domain certificates, only the full name is checked, so the valid locations would be:

```
http://www.example.com/FileName
https://www.example.com/FileName
```

c) The file contents may contain unreadable or additional characters. To check that please use curl utility with the command of a similar pattern:

```
curl -A "COMODO DCV" http://www.example.com/FileName
```

Please check the following:

a) Make sure that the URL containing the file does not redirect to any location aside from the ones that are stated in the section Ib of this FAQ.

b) Please check that the server accepts “COMODO DCV” as a User-Agent.
Some websites block this in their configuration or .htacess file.

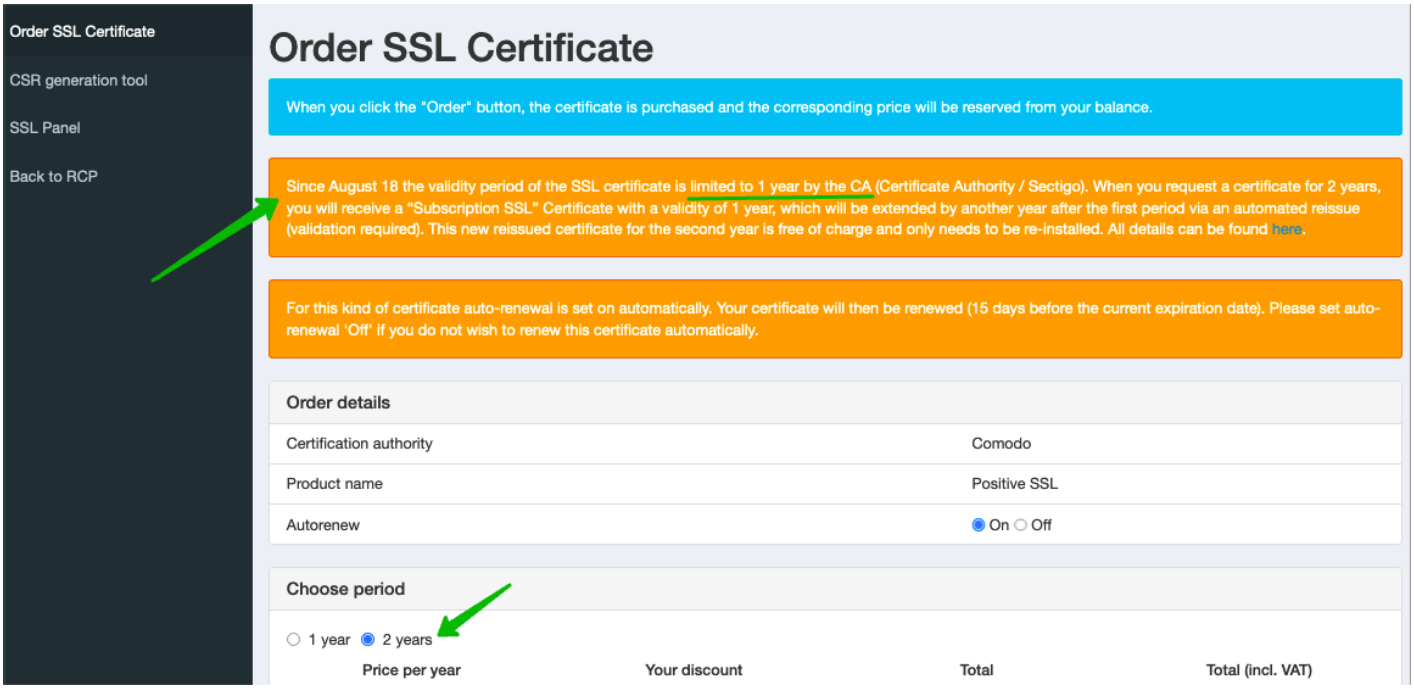
c) The file and server must be accessible from anywhere in the world.

Why is my SSL Certificate only valid for 1 year when I ordered it for 2 years ?

This article provides the explanation about the 1 year validity of the SSL Certificate and current Sectigo Policy for the certificates.

From Aug-Sep 2020, Google and Mozilla (together with Apple, who did it first) will no longer accept freshly issued certificates having a validity term of more than 398 days.

All publicly trusted SSL server certificates with a longer validity period issued before September 1, 2020 will be maintained for the whole duration.



If you have ordered a SSL Certificate after this period for *2 years*, Sectigo will grant initially the certificate for 1 year (365 days) and at the end of 1 year period another year will be added to your certificate via an **automatic initiated reissue for which validation is required!**

You will receive a notification once the reissue for the second period is initiated.

More information about this reissue can be found here:

Article**:** **Why-was-a-reissue-automatically-initiated-for-my-SSL-Certificate-**

General subscription SSL information in this article.

Why is my SSL not issued yet ?

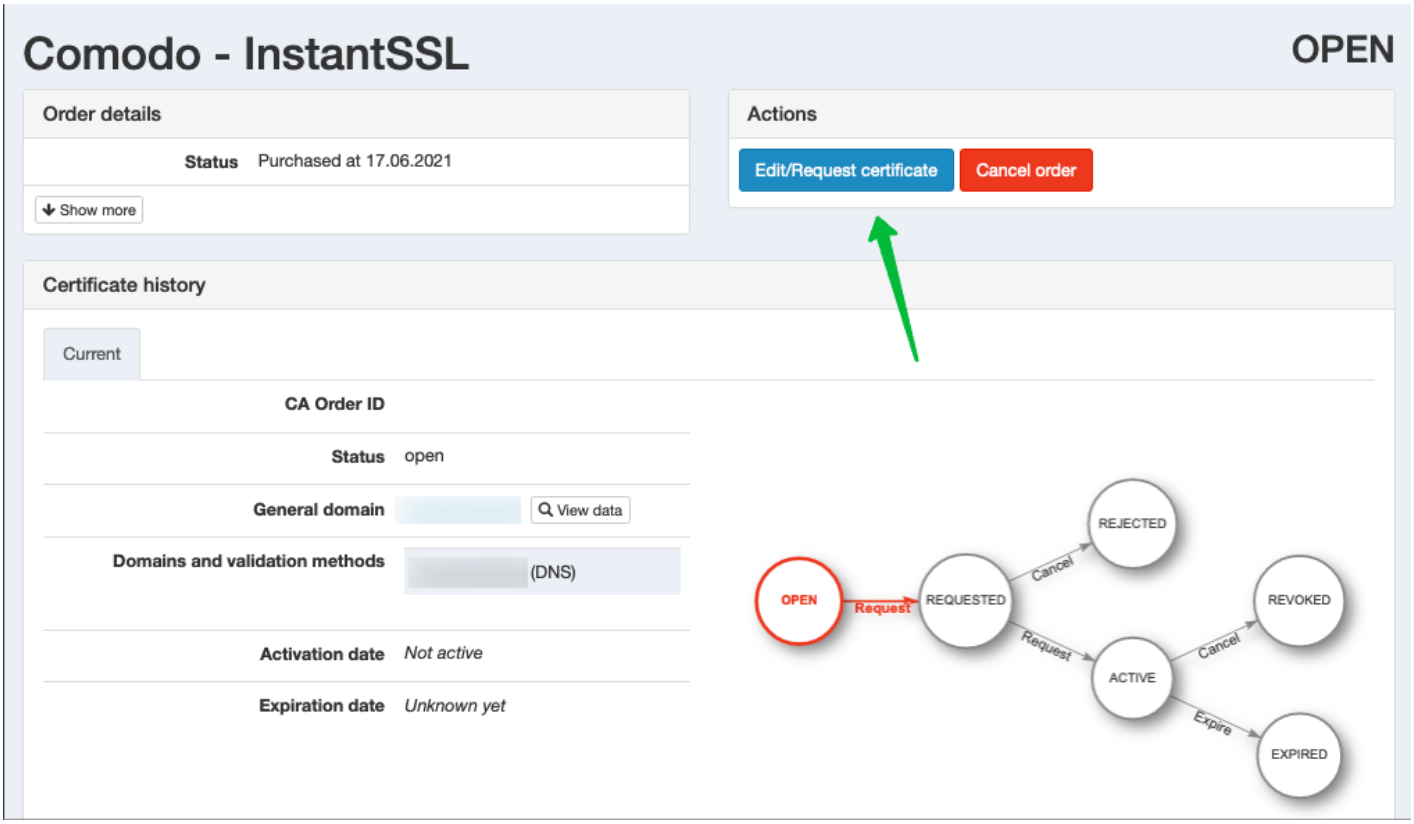
This article explains the factors that may be the reason that the SSL is not issued yet.

The SSL panel will show the status of your SSL request. You can see the steps which will be taken before your ssl can be issued. "Not applicable for this order" means that those steps are skipped for your selected ssl type.

In case you notice that the issuing of your SSL takes longer then you are used to, please review the topics below.

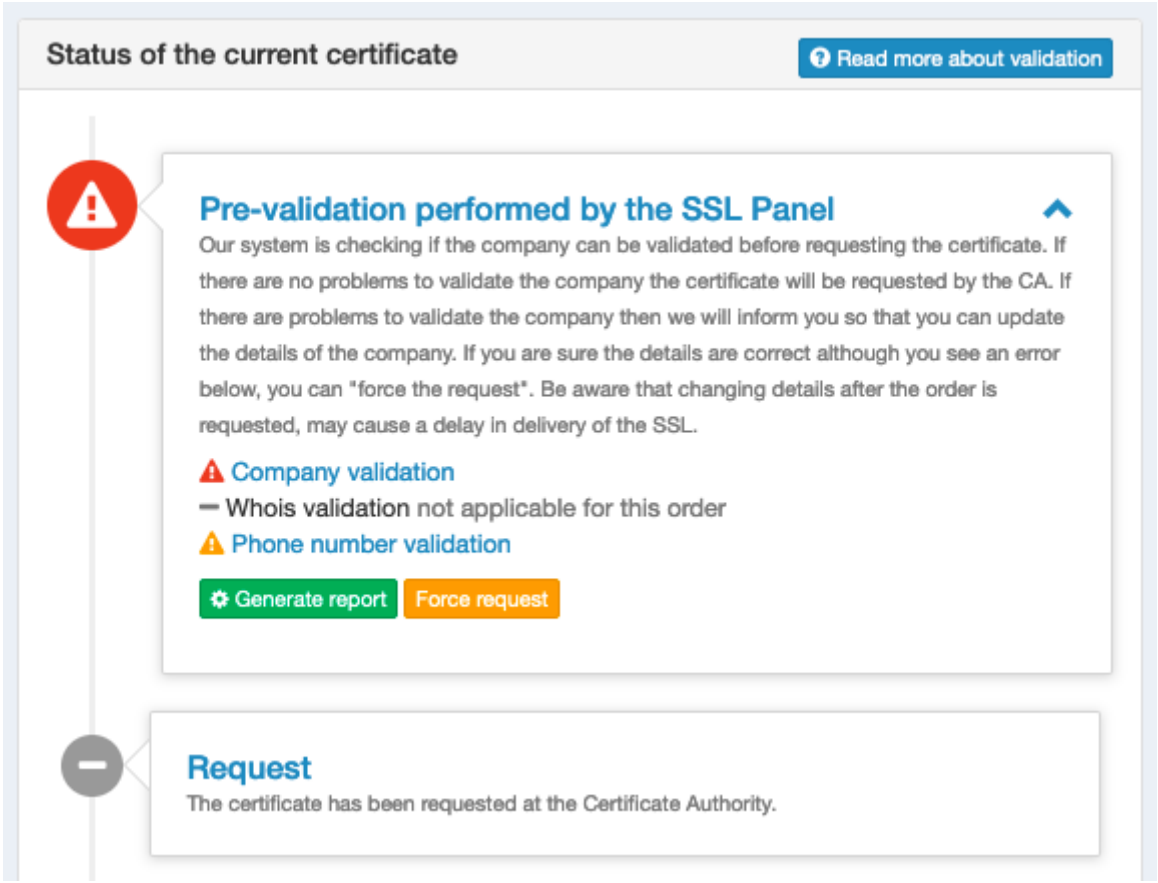
SSL status is "OPEN" - Did not pass the pre-validation

After creating the SSL order, our system can preform a *pre-validation check.* This will be done for certain orders, where the business registration database can be reached by API to validate and match your provided details. In case the order did not pass the pre-validation, it stays in the status "*OPEN*" and is not forwarded yet to Sectigo.



We advise to *Edit* the order details, before submitting your request to Sectigo for validation. Changing details once the order is submitted to Sectigo is less easy.

You can review the pre-validation results in your ssl panel.

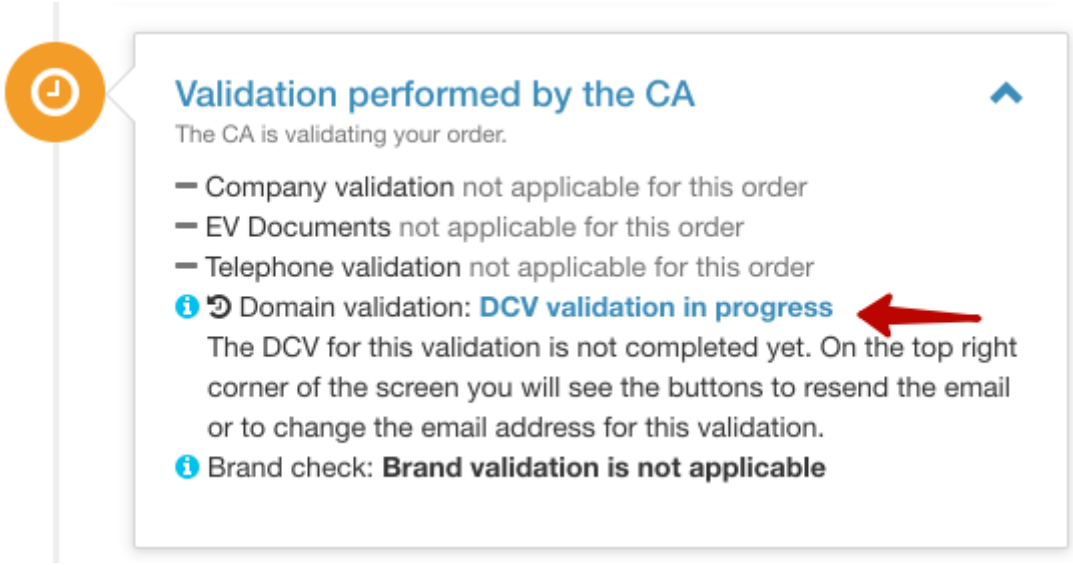


Domain Validation PENDING

Domain Validation is one of the most important part of SSL Certificate Process.

Domain validation is required for all SSL certificates: DV, OV and EV.

Sometimes, you can see that on the SSL Panel, the following message is displayed.

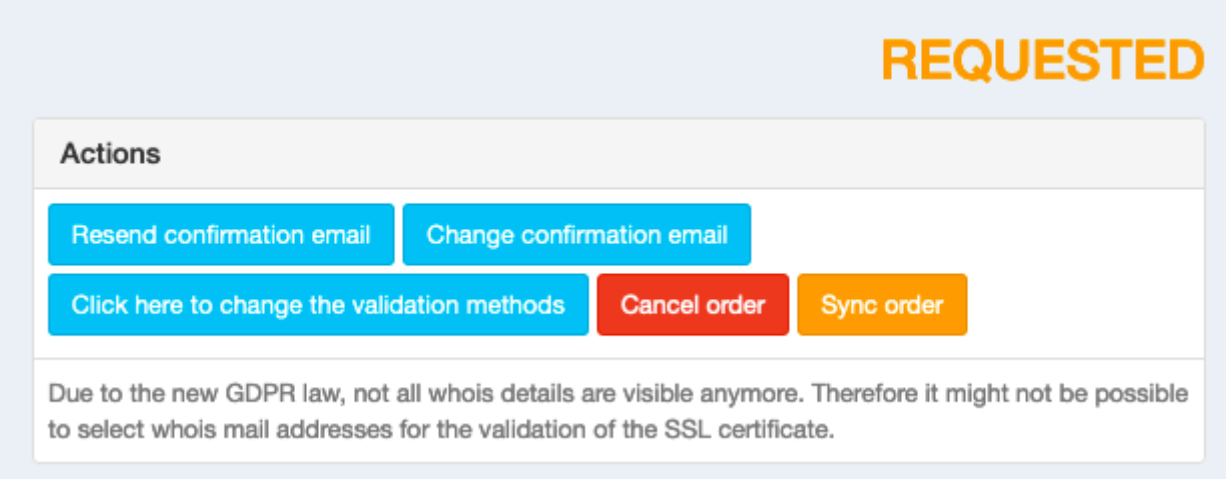


Make sure that you have followed all the steps correctly for domain validation.

1. Is the email already successfully verified?
2. Or was the correct Cname value added in the dns zone?
3. Is the file correctly uploaded without a redirect for file based validation?

In case you want to change the validation method, use the buttons in the Action section to change this. More information about how to confirm your domain ownership can be found here.

Before performing domain validation, do checkout our article for pre-validation checks here.

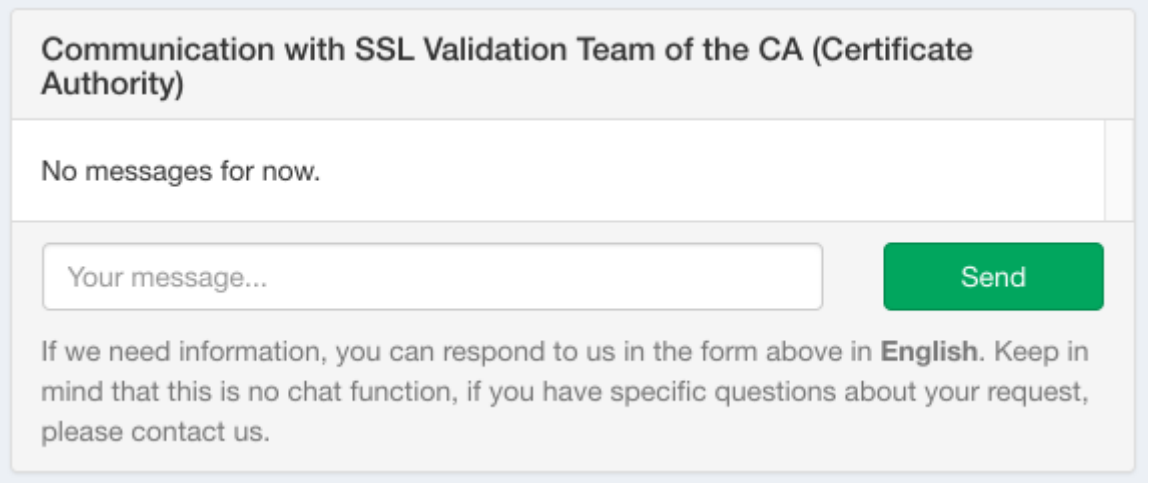


You may have missed the message from Certificate Authority (Sectigo)

Sectigo (CA) will validate your SSL request. In case there is an issue with the details, they will inform you via the CHAT window on the detail page of the SSL.
Examples:

1. The company is registered with a different name or different address in the company registration database and does not match the used handle.
2. During the phone validation, the person who answered was not aware of the order and rejected the validation.
3. There is a CAA record in your zone which prohibits the validation.

You can reply to Sectigo, but keep in mind, this is not a realtime chat.
This CHAT is only operational from the moment the SSL request is "pending" and will be closed once the SSL is issued. When the SSL has the status "open" the CHAT can not be used yet.



CAA record is prohibiting the validation

During a mandatory check of the CAA record for the (sub)domain it gives a DNS server error. In case a CAA is used in the zone, it must permit Sectigo to issue certificates for your domain.

There are 4 options that could solve the issue, before the certificate can be issued.

1: Ensure that the DNS server gives a correct NSEC / NSEC3 signed response that no CAA records exist.

2: Add a CAA record that approves issuance by Sectigo;

```
CAA 0 issue "sectigo.com"

CAA 0 issuewild “sectigo.com”

CAA 0 issuemail “sectigo.com”
```

Options:
issue: Explicitly authorizes a single certificate authority to issue a certificate (any type) for the hostname.
issuewild: Authorization to issue certificates that specify a wildcard domain.
Please note: "**issuewild**" properties take precedence over issue properties when specified.

CAA for S/MIME involves checking the “**issuemail**” properties of the RRSet, whereas for SSL, it involves checking the “**issue**” and “**issuewild**” properties.

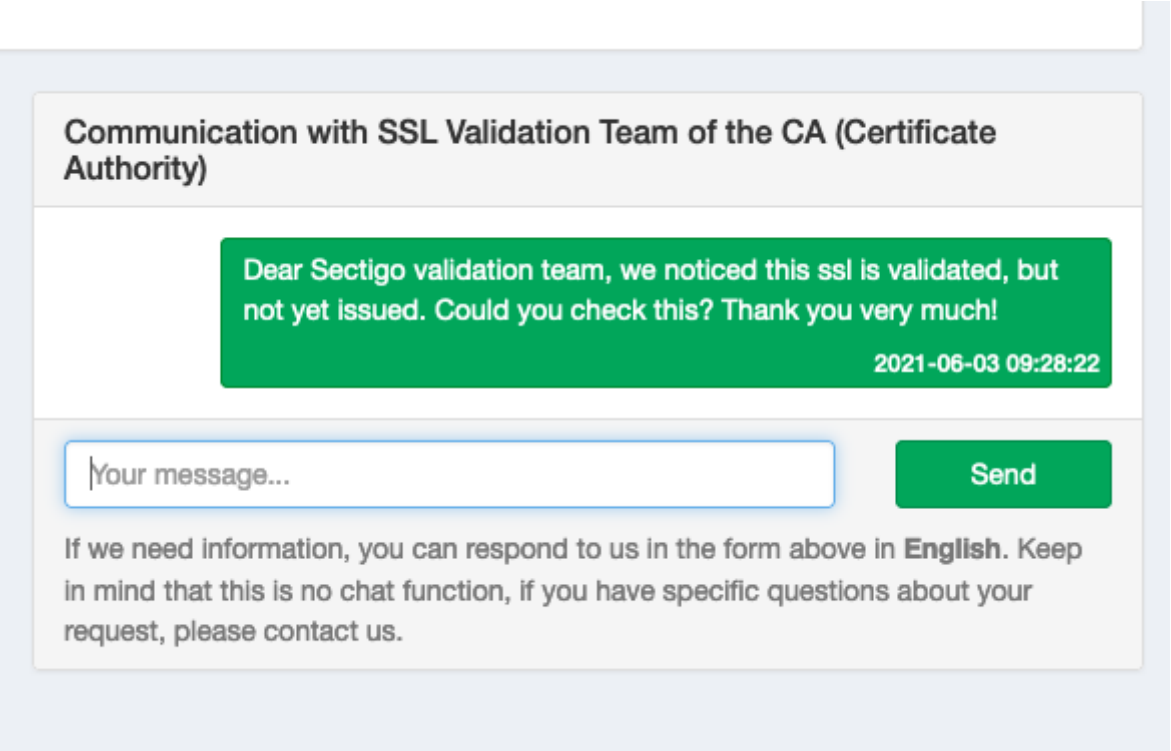
3: Fix the failure in the DNS response.

4: Disable DNSSEC on the domain(s).

- # CA stopped doing AUTOMATIC CHECKS

Sectigo does automated checks with a frequency of 15 minutes for a limited time period from the time when the certificate is REQUESTED.

At some point, Sectigo stops doing these automated checks on a frequent basis and limit the amount of checks they are preforming. This can delay the issuing of an "older" certificate.
In case a validation was stuck and fixed by the requester, inform Sectigo via the CHAT and ask them to continue the validation. This is not a realtime chat but it will trigger Sectigo to check the case manually.



- ## Contact Handle information incomplete or invalid

This is the most important part when you request a SSL Certificate, the contact information for the certificate. The order will be created based on the handle which you select during the order creation. Make sure this handle contains is complete and valid. In case of a OV or EV order, the contact person mentioned in this handle will be contacted.
A handle containing:

Firstname: Domain
Lastname: Administration

can therefore not be used for a SSL request as this validation will fail.

We advise to always check the handle which you are going to use if the information and contact person mentioned are still valid. In case the information is outdated, please create a new handle select this one.