6 Updating SSL Order

This is a series of articles dedicated to demonstrating how to get acquainted with Openprovider SSL API methods. If you want to go the beginning of this guide, please navigate to the article "1 How to choose a product".

To get more information about our API in general, please use our documentation portal as your reference.

Using the previous method "5 Retrieving SSL Orders" we successfully retrieved our orders and details.
But what if you want to update the original parameter(s) of an order created but was not yet approved?
There are different cases to use this method:

SSL Order status	What can be updated
PAI	• All fields that are not connected with the product details, e.g. csr, organization_handle, etc. • send start_provision = true if you want to send certificate request to the CA
REQ	domain_validation_methods can be updated, e.g. change method from http to dns
PAI, REQ, ACT	autorenew can be switched on/off

However, for the SSL order in status REQ approver email address value can be modified with the update approver email address method.

Use endpoint path below. Base URL is determined by both the target environment and API version.

```
POST {base_url}/ssl/orders/{id}
```

REQUEST VALUES

Name	Type	Values	Description
id	integer	Mandatory field. Openprovider order ID.	
approver_email	string	Email address.	A valid email address from a pre-approved list. (e.g. admin@example.com).
autorenew	string	on or off	Indicates if the certificate should be automatically renewed (check renew process description for the details).
csr	string	CSR value.	Certificate signing request including information regarding the further certificate.
1. domain_validation_methods	array	Allows to select a specific method for Domain Validation. Hostnames in the array must be equal to hostnames specified in the request (commonName and SANs from the CSR and hostnames).	
1.1 host_name	string	Hostname specified in the request (commonName and SANs from the CSR and hostnames).	
1.2 method	string	• https • dns • email	Mandatory parameter. The validation method (e.g. 'https')

host_names	array	An array of strings.	Array of hostnames. This parameter is optional, and only allowed in combination with a multi domain SSL certificate. If passed, the hostnames in this parameter will override any hostnames in the CSR, except for the common name.
organization_handle	string	Openprovider contact handle.	Internal organization handle stored in resellers profile (e.g. format: XY012345-CC).
signature_hash_algorithm	string	sha1 (deprecated) or sha2 (default)	Deprecated functional, please ignore. Default is: "sha2".
software_id	string	linux or windows.	Certificate software platform. Used if you changed your system configuration from Linux to Windows Server and vice versa.
start_provision	boolean	true or false (default)	If **false** then order won't be sent to CA, it will be in status PAI. To request it use **true** value.
technical_handle	string	Format: "XY012345-CC"	Openprovider technical handle.

REQUEST EXAMPLE

```
curl -X PUT \
 https://api.cte.openprovider.eu/v1beta/ssl/orders/31027 \
 -H 'Authorization: Bearer deb4bf804928981b018caf45c3c4142b' \
 -H 'Content-Type: application/json' \
 -d '{
 "approver_email": "admin@ssl-123-domain.com",
 "autorenew": "on",
 "csr": "-----BEGIN CERTIFICATE REQUEST-----\nMIIDNzCCAh8CAQAwgaUxCzAJBgNVBAYTAk5MMRYwFAYDVQQI
YW5kMQ8wDQYDVQQHEwZIYWFsZW0xGjAYBgNVBAoTEU9wZW5wcm92aWRlciBCLlYu\nMQswCQYDVQQLEwJJVDEbMBkGA1UE
KoZIhvcNAQkBFhhhZG1pbkBzc2wtMTIzLWRvbWFpbi5jb20wggEiMA0GCSqGSIb3\nDQEBAQUAA4IBDwAwggEKAoIBAQD4
```

```
iJXzTda9cIYPjwxduUR7A8EsgxFT/jQ99Gmjyq85liSX45z88eT5a7f84alEfCui\nMzZh9DUK6Y8nigATFnjOohJhkEXX
0ab8PlgOkdphcLUxKOGcpt8xWpzgKpMTJJnmRVkI7rkikYAU7BWxtJ5tcg/lEFcl\nruh/WUxeBH6qJMZ5xHZ2Z1EWLjiV
vTL/8Omo7xDk3vN4nEOAl9cT8gidVHuA+YOLMczLLrhP8LRPAgMBAAGgTDBKBgkq\nhkiG9w0BCQ4xPTA7MAkGA1UdEwQC
Fnd3dy5zc2wtMTIzLWRvbWFpbi5jb20wDQYJKoZIhvcNAQELBQADggEBAJVyt+D8\nBDxcQhuT4kOd8A2u0a+T0PAXX7uJ
1taUMoxlyZuXe38IztCBuUxpKiZz6Ltx5yUrQZaFNNOVsHNjXHe5oajVA1f7dmoI\nIa3E/fpeHpoPzbWdTv1bfMHuAfHI
amGOFSUZoY/HLwfGf1zJMqsF9HEreCVmhWGoIHknzKbIhe7sngzR1We3aafNAUOd\nQ3gov4okpEI8yurKRrGSSo1ZzWqi
4eJiaV7IwubPS78=\n-----END CERTIFICATE REQUEST-----",
 "domain_validation_methods": [
 {
 "host_name": "ssl-123-domain.com",
 "method": "http"
 }
 ],
 "host_names": [
 "ssl-123-domain.com"
 ],
 "organization_handle": "IA900531-NL",
 "signature_hash_algorithm": "sha2",
 "software_id": "windows",
 "start_provision": true,
 "technical_handle": "IA900531-NL"
}'
```


RESPONSE EXAMPLE


```
{
"code": 0,
"data": {
"id": 1
},
"desc": ""
}
```


RESPONSE VALUES

Name	Values	Description
code	API code returned.	**API Result with code returned.** **0 = Sucess with no errors.**
1. data	Update Order Response Data	Response data returned while updating the order.

1.1 id	Digital value usually consists of 6 digits.	Openprovider order ID.
desc	Description text (if presented).	Description (if presented).
maintenance	Boolean parameter: True or False.	The Maintenance: True or False.
2. warnings	An array of warning messages	Warning data returned while updating the order.
2.1 code	Numeric code if warning(s) detected.	Code value (digits).
2.2 data	Warning data values.	Data value returned.
2.3 desc	Description of warnings.	The description value returned.

Now we have updated our order and sent request to te CA (now order status is REQ).

In the next method, we will try "7 Update approver email" cause that help you if you no longer have an access to initial email used when submitted an order in a case if you used email domain validation method.

Revision #9
Created 2026-08-13 10:01:25 UTC by Sarath
Updated 2026-08-24 18:11:10 UTC by Sarath