

5 Retrieving SSL Orders

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 "[4 Creating SSL Order](#)" we created an order with the ID assigned: "1". Using the current method we will retrieve all orders that are assigned with our reseller's account. You can retrieve a full list of certificates you have in a system, either active or not, that have specific handle assigned or (and) by name pattern.

To get orders statuses updates immediately we would recommend you to use our [webhook system](#). Please check input values below.

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

GET [{base_url}](#)/ssl/orders

REQUEST VALUES

Name	Type	Values	Description
limit	integer	Min 0, Max 1000.	A number of records that will be returned in the output.

offset	integer	Min 0, Max ∞.	The argument is used to identify the starting point to return records.
order_by.[parameter] parameter: - common_name - order_date - status - active_date - expiration_date - product_name	string	asc/desc	Sorting order.
common_name_pattern	string	domain name pattern	The pattern of domain common name.
status	string	ACT , PAI , REQ , REJ , FAI , EXP	Current order status.
contact_handle	string	One of the resellers handles (contacts).	Openprovider contact of the person assigned to an order (e.g. XY123456-ZW).

REQUEST EXAMPLE

```
curl -X GET \
'https://api.openprovider.eu/v1beta/ssl/orders?status=PAI&order_by.order_date=asc' \
-H 'Authorization: Bearer ae460da9a7069714b32e29231a6a392c' \
-H 'Content-Type: application/json' \
```

RESPONSE EXAMPLE

```
{
  "code": 0,
  "data": {
    "results": [
      {
        "active_date": "2019-01-01 00:00:01",
        "additional_data": [
          {
            "dns_record": "ssl-123-domain.com",
            "dns_value": "0453ff12343c6d5e24466832668aa13658e5893c917b9486d7c59a5727074c9c",
            "domain": "ssl-123-domain.com",
            "file_contents": "0453ff12343c6d5e24466832668aa13658e5893c917b9486d7c59a5"
```

```
727074c9c",
"file_location": "ssl-123-domain.com/.well-known/pki-validation
/fileauth.txt",
"md5": "73d01a1232214f96ebf08d6f9d0af6f9",
"sha1": "0453ff12343c6d5e24466832668aa13658e5893c917b9486d7c59a5727074c9c",
"sha256": "0453ff12343c6d5e24466832668aa13658e5893c917b9486d7c59a5727074c9
c"
}
],
"administrative_handle": "IA900531-NL",
"autorenew": "off",
"billing_handle": "IA900531-NL",
"brand_name": "RapidSSL",
"certificate": "",
"common_name": "ssl-123-domain.com",
"csr": "-----BEGIN CERTIFICATE REQUEST-----
MIIDNzCCAah8CAQAwgUxGjAIBgNVBAYTAk5MMRYwFAYDVQQLIEw10b29yZC1Ib2xs
YW5kMQ8wDQYDVQQHEwZiYWFsZW9xGjAYBgNVBAoTEU9wZW5wcm92aWRlciBCLlYu
MQswCQYDVQQLLEwJJVDEbMBkGA1UEAxMSc3NsLTEyMy1kb21haW4uY29tMScwJQYJ
KoZiHvcNAQkBFhhG1pbkZzc2wtMTIzLWRvbWVpbj5jb20wgEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwgEKAoIBAQA4t7KW7vJ8Zjw9xZMo1iU4ez7pdPPglmSNNRAK
iJXzTda9cIYPjwxduUR7A8EsgxFT/jQ99Gmjyq85liSX45z88eT5a7f84aEfCui
MzZh9DUK6Y8nigATFnj0ohJhkEXXay8K0fY7/DXD6dSqJYJkhqULedsVB64ofip0
0ab8Plg0kdphcLUxK0Gcpt8xWpZgKpMTJJnmRVkI7rkikYAU7BWxtJ5tcg/LEFcl
ruh/WUxeBH6qJMZ5xHZ2Z1EWLjiVGb6Mw+sYBUky4WDX9xev2wL48dEA3opWR9e
vTL/80mo7xDk3vN4nE0Al9cT8gidVHuA+YOLMcZLLrhP8LRPAgMBAAGgTDBKBgkq
hkiG9w0BCQ4xPTA7MAKGA1UdEwQCAAwCwYDVROPAQDAgXgMCEGA1UdEQQaMBiC
Fnd3dy5zc2wtMTIzLWRvbWVpbj5jb20wDQYJKoZIhvcNAQELBQADggEBAJYvt+D8
BDxcQhuT4k0d8A2u0a+T0PAXX7uJcu1AkJr1gMS6tym118nmjXLilgSsL3IarRq2
1taUMoxlyZuXe38IztCBuUxpKiZz6Ltx5yUrQZaFNN0VsHNjXHe5oajVA1f7dmoI
Ia3E/fpeHpoPzbWdTv1bfMHuAfHIRqVuTHG78T4fJh4JFXfyHfVbLUN5wc9D7oPo
amG0FSUZoY/HLwfGf1zJMqsF9HERECVmhWGoIHknzKbIhe7sngzR1We3aafNAU0d
Q3gov4okpEI8yurKRrGSSo1ZzWqiIew5qEkm6gNGAwVWYgZ0kgadXjJQEBdx6deZ
4eJiaV7IwubPS78=
-----END CERTIFICATE REQUEST-----",
"domain_validation_methods": [
{
"host_name": "ssl-123-domain.com",
"method": "email"
}
],
"domain_validation_statuses": {
"ca_operation": "request",
"ca_order_status": "in_progress",
"ca_status": "requested",
"status": "open"
},
"email_approver": "admin@ssl-123-domain.com",
"email_reissue": "admin@ssl-123-domain.com",
"expiration_date": "2020-01-01 00:00:01",
```

```
"features": "",
"host_names": [
"www.ssl-123-domain.com"
],
"id": 1306772,
"intermediate_certificate": "",
"options": {
"features": ""
},
"order_date": "2019-01-01 00:00:01",
"organization_handle": "TH000001-NL",
"period": 1,
"product_id": 5,
"product_name": "RapidSSL",
"root_certificate": "",
"software": "linux",
"sslinhva_order_id": "11111111-1111-1111-1111-111111111111",
"status": "REQ",
"technical_handle": "IA900531-NL",
"validation_method": "domain",
"vendor_order_id": 123456789,
"vendor_reference_id": 123456789
}
],
"total": 10
},
"desc": ""
}
```

RESPONSE VALUES

Name	Values	Description
code	Result code number.	API Result with code returned. 0 = Success with no errors.
1. data	SSL Orders list data.	Returns results with all required data.
1.1 results	An array of results.	Returns order(s) data.
1.1.1 active data	Date value with date stamp.	Date of order creation.
1.1.2 additional data	Array with additional data.	Useful information with validation values that should be added, file locations, etc.

1.1.1.2.1 dns_record	DNS record .	DNS record should be added to host.
1.1.1.2.2 dns_value	DNS values.	DNS values that should be added to host to process validation (e.g. random text string).
1.1.1.2.3 domain	Domain name as a string.	Domain hostname with what certificate is assigned with.
1.1.1.2.4 file_contents	File contents as a string.	File contents that should be added to the host (an e.g. random string of text).
1.1.1.2.5 file_location	File location as a string.	Indicates a location where the file should be added into an existing host.
1.1.1.2.6 md5	MD5 checksum.	Order MD5 checksum.
1.1.1.2.7 sha1	SHA1 checksum.	Order SHA1 checksum.
1.1.1.2.8 sha256	SHA256 checksum.	Order SHA256 checksum.
1.1.2 administrative_ handle	Openprovider handle .	Administrative handle .
1.1.3 autorenew	"On" or "Off"	If autorenew is enabled or not.
1.1.4 billing_ handle	Openprovider billing handle .	Openprovider handle .
1.1.5 brand_name	Certificate brand name (manufacturer).	Manufacturer string (e.g. Comodo or Symantec).
1.1.6 certificate	Certificate value (string).	Value of certificate.
1.1.7 common_name	Domain common name.	Domain value (e.g. example.com).
1.1.8 csr	CSR value.	CSR value returned.
1.2 domain_validation_methods	An array of SSL Order Domain Validation Methods	
1.2.1 host_name	Domain name.	The hostname of the domain in Openprovider order .
1.2.2 method	Validation method value.	Validation method value (e.g. "https").
1.3 domain_validation_statuses	Set of values returned.	
1.3.1 ca _operation	Returns operation performed in CA . (e.g. "request").	Set of values related to the validation status of your order.
1.3.2 ca _order_status	Certificate Authority order status.	

1.3.3 ca_status	Certificate Authority order operation status.	Current status of order operation processing inside CA . (e.g. "requested").
1.3.4 status	The string value of current status.	Current order status (closed or open).
1.4 email_approver	Email address value.	Email value of approver email.
1.5 email_reissue	Email address value.	Email value of email reissue approver.
1.6 expiration_date	Date of order expiration.	Certificate expiration date (date stamp format).
1.7 features	Product features.	Indicates product features (if presented).
1.8 host_names	An array of strings.	Host names.
1.9 id	Numeric value or Openprovider order ID .	E.g. 1306772.
1.10 intermediate_certificate	Intermediate certificate value as a string.	An intermediate certificate is a certificate that used between the root and end-user certificate.
1.11 options	SSL Order options.	
1.11.1 features	Features of the certificate.	The certificate features an optional parameter (if presented).
1.12 order_date	Date of order creation.	Indicates timestamp when the order was created.
1.13 organization handle	Contact (handle) value from the reseller account.	Openprovider internal technical contact (handle).
1.14 period	Period of a lifetime in years.	1 or 2 years.
1.15 product_id	Openprovider product ID .	Indicates the product ID used.
1.16 product_name	SSL Product name.	Product name (e.g. RapidSSL).
1.17 root_certificate	Root certificate string.	Value of root certificate as a string.
1.18 software	Windows or Linux.	Software used for server: e.g. Windows or Linux.
1.19 sslinhva_order_id	Internal Openprovider value.	Internal system Openprovider value of order.

1.20 status	ACT, PAI, REQ, REJ, FAI, EXP	Current order status. (e.g. ACT=active, PAI=purchased but not requested, REQ=requested but under internal validation, REJ=cancel operation requested for an order, FAI=order cancelled, EXP=expired order).
1.21 technical_ handle	Openprovider internal technical handle (contact).	Handle (contact) internal system value (e.g. "e.g. XY123456-ZW").
1.22 validation_method	Value as a string.	Validation method (e.g. "domain").
1.23 vendor_order_id	Numeric value of internal order ID.	Internal vendor order ID (e.g. "123456789").
1.24 vendor_reference_id	Numeric value of interbal vendor ID.	Internal vendor order ID (e.g. "123456789").
2. total	Numeric value of total results stored in system.	Numeric value returned.
desc	Description value as a string.	Description text returned (if presented).
maintenance	True or False.	The maintenance: True or False.
warnings	An array of warning messages.	An array of boolean and string data returned if Openprovider is under maintenance mode.
2.1 code	Code digits.	Code value (digits).
2.2 data	Data values.	Data value returned.
2.3 desc	Description value.	Description value returned.

After we returned SSL Orders with details we can also [check a single exact order you want.](#)

The next method we would be referring to is "[6 Updating SSL Order](#)" - that will help us to change some details of not yet active order.

Revision #11

Created 2026-08-13 10:01:18 UTC by Sarath

Updated 2026-08-20 19:12:05 UTC by Sarath