SECTIGO

FORMERLY COMODO CA

AutoApplyOrder API

Version 2.1

2019

https://secure.trust-provider.com/products/!AutoApplyOrder

One API for Multiple Products – product implementation has never been easier

Our new, single API – AutoApplyOrder – makes requesting not only our range of SSL certificates, but also new products such as CodeGuard, HackerGuardian PCI Compliance, VPN and easier than ever. This single API reduces product implementation from weeks or months to hours or even minutes.

For existing Sectigo Partners

AutoApplyOrder is fully backward-compatible with AutoApplySSL, accepting all the same parameters and able to request all the same certificates.
Changing to AutoApplyOrder is a simple case of changing the API endpoint URL – all the parameters, values and authentication remain the same, and you'll now have the ability to request a range of new Sectigo products with simple, minor changes to the API call.

For assistance with this or any API please contact: *partnerapisupport@sectigo.com*

Version History

2.0. Added: Support of license products and bundling options by adding CodeGuard and HackerGuardian to AutoApplyOrder
Various modifications and simplifications of some parameters and values
Added a contents section and sections covering examples, push notification
Version history prior to 2.0 was removed – please refer to AutoApplySSL API documentation for historical version information

Contents

1. Request

Required variables are in **bold**.
Optional variables are in *italics*.

Variable Name (case insensitive)	Type	Max. Length	Allowed Values	Description
loginName	string	**64** chars		Account Username (case sensitive)
loginPassword	string	**128** chars		Account Password (case sensitive)
product	string	**64** chars	This parameter is a comma-separated string of integers. There MUST be exactly ONE of the following certificate values specified: **PositiveSSL:** **291** = PositiveSSL Trial DV **287** = PositiveSSL DV **289** = PositiveSSL Wildcard DV **279** = PositiveSSL Multi-Domain DV **556** = PositiveSSL EV **557** = PositiveSSL EV Multi-Domain **InstantSSL:** **330** = InstantSSL DV **331** = InstantSSL Wildcard DV **7** = InstantSSL OV **35** = InstantSSL OV Wildcard **361** = InstantSSL UCC OV **567** = InstantSSL EV **568** = InstantSSL EV Multi-Domain **EnterpriseSSL:** **63** = EnterpriseSSL OV **64** = EnterpriseSSL Pro OV **65** = EnterpriseSSL Pro Wildcard OV **335** = EnterpriseSSL Pro Multi-Domain OV **562** = EnterpriseSSL Pro EV **563** = EnterpriseSSL Pro EV Multi-Domain **SectigoSSL:** **488** = SectigoSSL DV **489** = SectigoSSL Wildcard DV **492** = SectigoSSL UCC DV **316** = SectigoSSL OV **322** = SectigoSSL OV Wildcard **583** = SectigoSSL OV Multi Domain	Product(s) required

			337 = SectigoSSL EV **410** = SectigoSSL EV Multi-Domain EV **TrustLogo** **36** = EV or OV TrustLogo *Add this value to any OV or EV product code, separated by a comma, such as:* 316,36 *to include a Trustlogo on a 'SectigoSSL OV' certificate.* **CodeGuard Products:** **703** = Sectigo CodeGuard (Small Business) **702** = Sectigo CodeGuard (Company) **701** = Sectigo CodeGuard (Professional) **700** = Sectigo CodeGuard (Personal) **HackerGuardian Products (Pairs):** **586** = Sectigo HackerGuardian Control Center Lite **587** = Sectigo HackerGuardian Vulnerability Scanning and Assessment Service (Lite) **346** = HackerGuardian PCI Scan Control Center **329** = HackerGuardian Vulnerability Scanning and Assessment Service (Basic) **349** = HackerGuardian PCI Scan Control Center Enterprise **259** = HackerGuardian Vulnerability Scanning and Assessment Service (Medium Volume) **HackerGuardian Additional IP pack for all HG packages:** **356** = HackerGuardian Additional IP Addresses Pack	
days	integer		For certificate products: **30, 90, 365, 730** *Note: 'years' parameter is deprecated in favour of 'days'*	Validity Period (in days)
serverSoftware	integer		**2** = Apache **10** = Java-based servers **14** = Microsoft IIS 5.x to 6.x **35** = Microsoft IIS 7.x and later **36** = nginx **18** = Oracle **30** = Plesk **31** = WHM/cPanel **-1** = OTHER *Note: This parameter does not directly affect the certificate content. Please use '-1' as the default option.*	
domainNames (only relevant for Multi-Domain SSL Certificates and Unified Communications Certificates)	string	**32767** chars	A comma-separated (or whitespace-separated) list of Domain Names / IP Addresses to be placed into the EV Multi-Domain SSL Certificate, Multi-Domain SSL Certificate or Unified Communications Certificate. If the CSR's Subject Alternative Name extension... i) includes 1 or more Domain Names, and this "domainNames" parameter is *omitted*, then the Domain Names from the CSR will be *used*. ii) includes 1 or more Domain Names, and this "domainNames" parameter is *specified*, then the Domain Names from the CSR will be *ignored*. iii) is not present, or is present but includes 0 Domain Names, then this "domainNames" parameter *must be present*. **NOTE**: commas and/or whitespace may need to be manually URL-encoded (e.g. %2C for a comma), depending on whether or not the calling environment does this automatically.	List of Domain Names
primaryDomainName (only relevant for Multi-Domain SSL Certificates and Unified Communications Certificates)	string	**64** chars	One of the Domain Names listed in "domainNames", which should appear as the first Common Name in the Subject DN of the resulting EV Multi-Domain SSL Certificate, Multi-Domain SSL Certificate or Unified Communications Certificate. For Multi-Domain Certificates: If this parameter is omitted, the Common Names will be listed in alphabetical order within the certificate. For Unified Communications Certificates: If this parameter is omitted, then the value of the CSR's Common Name will be used as the primary domain name instead.	Primary Domain Name
maxSubjectCNs (optional for Multi-Domain SSL Certificates; ignored for all other certificate types)	integer		If omitted, all of the Domain Names listed in "domainNames" will be included as Common Names in the Subject DN of the resulting EV Multi-Domain SSL Certificate or Multi-Domain SSL Certificate. If **1**, there will only be 1 Common Name in the resulting certificate. This will have the value provided by "primaryDomainName" (so, in this case, "primaryDomainName" must have a value). If **0**, no Common Names will be included in the resulting certificate. Note that all of the Domain Names listed in "domainNames" will always be included as dnsName components of the Subject Alternative Name extension in the resulting Multi-Domain SSL Certificate or EV Multi-Domain SSL Certificate. This parameter need not be specified for Unified Communications Certificates, since UCCs always have "maxSubjectCNs" set to 1.	Number of CNs
csr	string	**32767** chars	***Version:* 0** ***Subject:***	Certificate Signing Request

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>
The fields may be in any order (although multiple street addresses, if present, should be in the correct order).
MUST include these fields:
<table>
<tr><th>OID</th><th>Description</th><th>Supported ASN.1 Type(s)</th><th>Max. Length</th></tr>
<tr><td>2.5.4.3</td><td>Common Name
(MUST contain the Fully-Qualified Domain Name)</td><td>DirectoryString</td><td>64 chars</td></tr>
</table>
MAY include these fields:
<table>
<tr><th>OID</th><th>Description</th><th>Supported ASN.1 Type(s)</th><th>Max. Length</th></tr>
<tr><td>2.5.4.10</td><td>Organization Name</td><td>DirectoryString</td><td>64 chars</td></tr>
<tr><td>2.5.4.11</td><td>Organizational Unit Name</td><td>DirectoryString</td><td>64 chars</td></tr>
<tr><td>2.5.4.18</td><td>Post Office Box</td><td>DirectoryString</td><td>40 chars</td></tr>
<tr><td>2.5.4.9</td><td>Street Address 1</td><td>DirectoryString</td><td>128 chars</td></tr>
<tr><td>2.5.4.9</td><td>Street Address 2</td><td>DirectoryString</td><td>128 chars</td></tr>
<tr><td>2.5.4.9</td><td>Street Address 3</td><td>DirectoryString</td><td>128 chars</td></tr>
<tr><td>2.5.4.7</td><td>Locality Name</td><td>DirectoryString</td><td>128 chars</td></tr>
<tr><td>2.5.4.8</td><td>State or Province Name</td><td>DirectoryString</td><td>128 chars</td></tr>
<tr><td>2.5.4.17</td><td>Postal Code</td><td>DirectoryString</td><td>40 chars</td></tr>
<tr><td>2.5.4.6</td><td>Country Name
(ISO3166 2-character code)</td><td>PrintableString</td><td>2 chars</td></tr>
</table>
Note: DirectoryString is a choice of PrintableString, TeletexString, BMPString, UniversalString (ASCII only) or UTF8String.
Any other fields MAY be present but will be ignored.
Subject Public Key Info:
RSA: OID = rsaEncryption (PKCS#1); Size = 2048 to 8192 bits.
ECC: OID = id-ecPublicKey (RFC3279); Curve = P-256, P-384 or P-521.
Attributes:
Any attributes MAY be present but will be ignored.
Signature Algorithm:
md5WithRSAEncryption (PKCS#1)
or sha1WithRSAEncryption (PKCS#1)
or sha224WithRSAEncryption (PKCS#1)
or sha256WithRSAEncryption (PKCS#1)
or sha384WithRSAEncryption (PKCS#1)
or sha512WithRSAEncryption (PKCS#1)
or ecdsa-with-SHA1 (RFC3279)
or ecdsa-with-SHA224 (RFC5758)
or ecdsa-with-SHA256 (RFC5758)
or ecdsa-with-SHA384 (RFC5758)
or ecdsa-with-SHA512 (RFC5758)

For the HTTP_CSR_HASH, and CNAME_CSR_HASH dcvMethods we have introduced support for Request Tokens as defined in the CABF Baseline Requirements (version 1.4.1 or later) and in the manner described in Sectigo's 'Domain Control Validation' document (version 1.09 or later).

From 20th July 2017, the use of unique Request Tokens, the new /.well-known/pki-validation path, and the underscore prepended to the NAME for the CNAME will be required for the HTTP_CSR_HASH and CNAME_CSR_HASH dcvMethods.

Request tokens may be ensured to be unique by:

1) Generating a new CSR each time;

2) Provide a previously used CSR and omit the uniqueValue.
Sectigo will generate a uniqueValue and this will be returned;
or
3) Passing in the uniqueValue variable (see below) in addition to the CSR.
This will allow the re-use of a CSR.
</td>
<td>(Base-64 encoded, with or without the -----BEGIN xxxxx----- and -----END xxxxx----- header and footer)</td>
</tr>
<tr>
<td>uniqueValue</td>
<td>string</td>
<td>20 chars</td>
<td>
An alphanumeric value.

This uniqueValue is incorporated into the Request Token used with the HTTP_CSR_HASH, and CNAME_CSR_HASH dcvMethods.

This uniqueValue is used to ensure that the Request Token for this certificate is unique.
Request Tokens are as defined in the CABF Baseline Requirements (version 1.4.1 or later) and used in the manner described in Sectigo's 'Domain Control Validation' document (version 1.09 or later)

If this uniqueValue parameter is omitted, and if the same CSR has previously been passed to Sectigo as part of a certificate order,
Sectigo will generate a uniqueValue and return it in the response from this API call.

If this uniqueValue parameter is provided, and if the same CSR has previously been passed to Sectigo as part of a certificate order,
an error code (-55) will be returned if you are attempting to re-use the same combination of CSR and uniqueValue.
</td>
<td></td>
</tr>
<tr>
<td>prioritiseCSRValues</td>
<td>char</td>
<td>1 char</td>
<td>
Y or N.

If omitted, it's value defaults to Y.
</td>
<td>This specifies which values to use if there are duplicates (e.g. if a Postal Code is specified</td>
</tr>
</table>

				in both the CSR and as a separate variable).
organizationName *organizationName (if there is an Organization Name in the CSR)*	string	**64** chars	If an Organization Name is specified here and **prioritiseCSRValues** is set to **N**, this value will be used instead of the Organization Name in the CSR.	Organization Name
organizationalUnitName	string	**64** chars	If an Organizational Unit Name is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Organizational Unit Name (e.g. Company Department)
postOfficeBox	string	**40** chars	If a Post Office Box is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Post Office Box
streetAddress1 *streetAddress1 (if there is a Street Address in the CSR)*	string	**128** chars	If a Street Address is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Street Address 1
streetAddress2	string	**128** chars	If a second Street Address is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Street Address 2
streetAddress3	string	**128** chars	If a third Street Address is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Street Address 3
localityName *localityName (if there is a Locality Name in the CSR)*	string	**128** chars	If a Locality Name is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Locality Name
stateOrProvinceName *stateOrProvinceName (if there is a State or Province Name in the CSR)*	string	**128** chars	If a State or Province Name is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	State or Province Name
postalCode *postalCode (if there is a Postal Code in the CSR)*	string	**40** chars	If a Postal Code is specified here and in the **csr**, **prioritiseCSRValues** indicates which value will be used.	Postal Code
countryName *countryName (if there is a Country Name in the CSR)*	string	**2** chars	If a Country Name is specified here and **prioritiseCSRValues** is set to **N**, this value will be used instead of the Country Name in the CSR.	Country Name (ISO3166 2-character country code)

dunsNumber	string	**20** chars		DUN and Bradstreet Number
companyNumber	string	**25** chars		Company Registration Number
joiLocalityName	string	**128** chars	Only for EV Certificates: The City or Town (if any) in which the company is incorporated or registered.	Jurisdiction of Incorporation: Locality
joiStateOrProvinceName	string	**128** chars	Only for EV Certificates: The State or Province (if any) in which the company is incorporated or registered.	Jurisdiction of Incorporation: State
joiCountryName **joiCountryName** (for EV Certificate orders)	string	**2** chars	Only for EV Certificates: The Country in which the company is incorporated or registered.	Jurisdiction of Incorporation: Country
dateOfIncorporation	string	**10** chars	Only for EV Certificates: The date of incorporation (YYYY-MM-DD) of the company. This is useful information for Validation purposes.	Date of Incorporation
assumedName	string	**64** chars	Only for EV Certificates: The d/b/a (does business as) name (if any) for the company.	d/b/a Name
businessCategory	char	**1** char	**b** = Private Organization. **c** = Government Entity. **d** = Business Entity.	Business Category (see Clause 5 of the EV Guidelines V1.0)
emailAddress	string	**255** chars	If specified, the certificate will be emailed to this email address rather than the applicant's admin email address. If the value specified is "none", no certificate issuance email will be sent at all (this is probably only useful if you intend to collect the certificate with CollectSSL).	Alternative issuance email address
validationEmailAddress	string	**255** chars	If specified, Comodo will validate that this is the email address of the end customer. Sectigo will not send any emails to this email address; instead Sectigo will trust you, the Partner, to forward emails to this end customer as appropriate.	Validation Email Address
contactEmailAddress	string	**255** chars	If specified, this email address will be the only email address that Sectigo Validation Staff will correspond with during the processing of this order.	Contact Email Address
dcvMethod	string	**32** chars	Selected method for Domain Control Validation. Permitted values are: **EMAIL** **HTTP_CSR_HASH** **CNAME_CSR_HASH** **IP_ADDRESS_PRE** (If omitted, the default value is "EMAIL"). For more information, see the "Domain Control Validation" document (version 1.09 or later).	Domain Control Validation Method
dcvEmailAddress (only relevant for single-domain SSL certificates)	string	**255** chars	If specified, this email address must be an acceptable email address with which to perform Domain Control Validation (DCV) for this certificate. See the documentation for the GetDCVEmailAddressList API for more information. Alternative DCV mechanisms are now available. See the "Domain Control Validation" document for full details.	Domain Control Validation Email Address
dcvEmailAddresses (only relevant for Multi-Domain SSL Certificates and Unified Communications Certificates)	string	**32767** chars	A comma (or white-space)-separated list of DCV Email Addresses to be used to perform Domain Control Validation for each domain in this certificate. The order in which these email addresses are listed must be exactly the same as the order of the domain names in the certificate request (see 'domainNames' variable, above). Alternative DCV mechanisms are now available – see the "Domain Control Validation" document for full details. You can pass the following values for each domain: **HTTPCSRHASH** or **CNAMECSRHASH** or **IPADDRESSPRE** You can use one of the following magic tokens if all the domains in the order are to be set to the same alternative DCV method: **ALLHTTPCSRHASH** or **ALLCNAMECSRHASH** or **ALLIPADDRESSPRE** **Note:** The magic token must be the only value passed to the parameter for it to work. If this parameter is specified, "validationTokens" should not be specified.	List of DCV Email Addresses
dcvTemplateID	integer		An account can contain multiple DCV templates (in different languages, for example). Please contact Support for the DCV template	If specified, this overrides Sectigo's default choice of DCV email template to be used to validate this certificate. Talk to your account manager if you would like to set up one or more of your own DCV email templates that can be referenced by this parameter

validationTokens (only relevant for Multi-Domain SSL Certificates and Unified Communications Certificates)	string	**32767** chars	A comma (or white-space)-separated list of DCV Email Addresses to be used to perform Domain Control Validation for each domain in this certificate. The order in which these email addresses are listed must be exactly the same as the order of the domain names in the certificate request (see 'domainNames' variable, above). Alternative DCV mechanisms are now available – see the "Domain Control Validation" document for full details. You can pass the following values for each domain: **HTTPCSRHASH** or **CNAMECSRHASH** or **IPADDRESSPRE** You can use one of the following magic tokens if all the domains in the order are to be set to the same alternative DCV method: **ALLHTTPCSRHASH** or **ALLCNAMECSRHASH** or **ALLIPADDRESSPRE** **Note:** The magic token must be the only value passed to the parameter for it to work. If this parameter is specified, "dcvEmailAddresses" should not be specified.	List of Validation Tokens
caCertificateID	integer		If specified, this overrides Sectigo's default choice of CA certificate/key to be used to issue this certificate. This functionality is only available by special agreement with Sectigo.	Use particular CA certificate/key
isCustomerValidated	char	**1** char	**N**	
showCertificateID	char	**1** char	**Y** or **N**. If omitted, it's value defaults to **N**.	If this value is set to **Y**, the certificateID of the SSL certificate generated by the order is also part of the resultSet.
foreignOrderNumber	char	**64** characters	This identifier can be returned by some of our other APIs to aid in integration with partner systems.	An identifier for this order.
checkFONIsUnique	char	**1** char	**Y** or **N**.	If **Y**, the "foreignOrderNumber" parameter (if specified) must have **not** already been used for any order placed by this account.
responseFormat	char	**1** char	**0** = New-line delimited parameters. **1** = URL-encoded parameters. If omitted, its value defaults to **0**.	Explained in sections 2 and 3 below.
test	char	**1** char	**Y** or **N**.	If **Y** (or **y**), the account will not be charged and the order will be processed as a test order. If omitted, its value defaults to **N**.
idaEmailAddress	string	**255** chars	An Email Address to add to IdAuthority, for display in TrustLogo popups. (Only applicable if a TrustLogo is being ordered).	An Email Address to add to IdAuthority.
idaTelephoneNumber	string	**32** chars	A Telephone Number to add to IdAuthority, for display in TrustLogo popups. (Only applicable if a TrustLogo is being ordered)	A Telephone Number to add to IdAuthority.
idaFaxNumber	string	**32** chars	A Fax Number to add to IdAuthority, for display in TrustLogo popups. (Only applicable if a TrustLogo is being ordered)	An Fax Number to add to IdAuthority.
appRepForename (only relevant for OV and EV Certificates)	string	**64** chars	Required when Sectigo will perform the Organizational callback.	Applicant Representative's Name to be used for callback.
appRepSurname (only relevant for OV and EV Certificates)	string	**64** chars	Required when Sectigo will perform the Organizational callback.	Applicant Representative's Name to be used for callback.
appRepEmailAddress (only relevant for OV and EV Certificates)	string	**255** chars	Required when Sectigo will perform the Organizational callback.	Applicant Representative's email address to be used with callback.
appRepTelephone (only relevant for OV and EV Certificates)	string	**32** chars	Required when Sectigo will perform the Organizational callback.	Applicant Representative's phone number for callback.
appRepTitle (only relevant for OV and EV Certificates)	string	**64** chars		Applicant Representative's title to be used for callback.
appRepFax (only relevant for OV and EV Certificates)	string	**32** chars		Applicant Representative's fax number to be used for callback.
appRepOrganization Name (only relevant for OV and EV Certificates)	string	**255** chars	**DO NOT** specify this field unless the Applicant Representative's Organization Name/Address details are different to the Organization Name/Address details that have been requested to appear in the certificate.	Applicant Representative's Organization Name
appRepOrganizationalUnitName (only relevant for OV and EV Certificates)	string	**64** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's Organizational Unit Name
appRepStreetAddress1 (only relevant for OV and EV Certificates)	string	**128** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's street address 1

appRepStreetAddress2 (only relevant for OV and EV Certificates)	string	**128** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's street address 2
appRepStreetAddress3 (only relevant for OV and EV Certificates)	string	**128** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's street address 3
appRepPostOfficeBox (only relevant for OV and EV Certificates)	string	**128** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's post office box #
appRepLocalityName (only relevant for OV and EV Certificates)	string	**128** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's locality name
appRepStateOr ProvinceName (only relevant for OV and EV Certificates)	string	**128** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's state
appRepPostalCode (only relevant for OV and EV Certificates)	string	**40** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's Zip
appRepCountryName (only relevant for OV and EV Certificates)	char	**2** chars	If *appRepOrganizationName* is not specified, then this field is ignored.	Applicant Representative's country code (ISO3166 2-character country code)
callbackMethod	char	**1** char	**T** = The *appRepTelephone* number will be called to communicate a callback verification code which will be used to confirm the identity of the Applicant Representative. **L** = A letter, containing a callback verification code, will be posted to the Applicant Representative.	Callback method for verification of Applicant Representative's identity
isAppRepValidated	char	**1** char	**Y** = The Partner Reseller has verified that the Applicant Representative's contact details are legitimate, using a data source other than the Applicant. (Only Partner Resellers with sufficient RA privileges may specify **Y**). **N** = Sectigo will verify the Applicant Representative's contact details before performing the callback using the method specified by *callbackMethod*.	Who will verify the Applicant Representative's contact details before the callback is performed?
isCallbackCompleted	char	**1** char	**Y** = The Partner has completed the callback and verified the identity of the Applicant Representative. (Only Partner Resellers with sufficient RA privileges may specify **Y**. If *isCallbackCompleted=Y* is specified, then *isAppRepValidated=Y* must also be specified). **N** = Sectigo will perform the callback using the method specified by *callbackMethod*.	Who will perform the callback?
showCertificateState	char	1 char	**Y** or **N**.	If this value is set to **Y**, the state of the SSL certificate generated by the order is also part of the resultSet.
omitAdditionalFQDN (only relevant for single-domain SSL certificates)	char	1 char	**N** = Sectigo will add an additional FQDN, either for www.<*domain*> (if the certificate was requested for <*domain*>) or for <*domain*> (if the certificate was requested for www.<*domain*>). **Y** = An additional FQDN will not be added.	If omitted, its value defaults to **N**.
appRepLoginName	64 chars		Required for HackerGuardian license account	
IP Addresses	integer		Sectigo HackerGuardian Additional IP Addresses Pack (example: 'product=356&IP%20Addresses=5') For HG additional IP Addresses Pack available values are 1,5,10,50,100,500,1000	
Domains	integer		Number of domains to order CodeGuard product to choose plan you need to mention number of domains available values are: 1,12,25,100	

2. Response (when *responseFormat=0*, the default)

2.1 MIME Type and first line

Line	Possible Value(s)
Mime-Type	text/plain
Line 1: *Status Code* NOTE: Whether **0** or **1** is returned for Successful orders depends on how your account is configured with Sectigo. Usually, you will take payment from your customer and Sectigo will debit your account funds when you place the order. However, in special circumstances it can be arranged for Sectigo to take payment from your customer on your behalf.	**1** = Successful, Payment Required **0** = Successful **-1** = Request was not made over https! **-2** = '*xxxx*' is an unrecognised argument! **-3** = The '*xxxx*' argument is missing! **-4** = The value of the '*xxxx*' argument is invalid! **-5** = The CSR's Common Name may NOT contain a wildcard! **-6** = The CSR's Common Name MUST contain ONE wildcard! **-7** = '*xx*' is not a valid ISO-3166 country! **-8** = The CSR is missing a required field! **-9** = The CSR is not valid Base-64 data! **-10** = The CSR cannot be decoded! **-11** = The CSR uses an unsupported algorithm! **-12** = The CSR has an invalid signature! **-13** = The CSR uses an unsupported key size! **-14** = An unknown error occurred! **-15** = Not enough credit! **-16** = Permission denied! Contact Sectigo Support to have your account enabled for the !AutoApplyOrder API. **-17** = Request used GET rather than POST! **-18** = The CSR's Common Name may not be a Fully-Qualified Domain Name! **-19** = The CSR's Common Name may not be an Internet-accessible IP Address! **-35** = The CSR's Common Name may not be an IP Address! **-40** = The CSR uses a key that is believed to have been compromised! **-55** = This Request Token is not unique!

Note: We reserve the right to define additional error codes/messages in the future.

2.2.1 If *Status Code* < 0

Line	Possible Value(s)
Line 2: *Error Message*	See *Status Code* Possible Value(s)

2.2.2 If *Status Code* >= 0

Line	Possible Value(s)
Line 2: *Order Number*	Integer
Line 3: *(If Status Code = 0): Amount Debited* *(If Status Code = 1): Amount Required (not including UK VAT, if required)*	Amount, in your account's native currency, without a currency symbol (e.g. $)
Line 4: *Expected Delivery Time*	This value can be ignored and has been deprecated.
Line 5: *SSL Certificate ID* (up to 16 digits; only returned if *showCertificateID=Y*)	The internal Certificate ID of the SSL certificate purchased by this order. **240** – this order is for an EV Certificate. The validation process generally takes a lot longer for EV, compared to other SSL Certificates.
Line 5 or 6: *SSL Certificate State* (only returned if *showCertificateState=Y*)	The status of the SSL certificate purchased by this order.
Line 5, 6 or 7: *Unique Value* (only returned if a uniqueValue parameter was passed in to this API, or if a uniqueValue has been generated by Sectigo for this order)	A unique alphanumeric value up to 20 characters long.

3. Response (when *responseFormat=1*)

Most of Sectigo's newer APIs always use URL-encoding for responses. !AutoApplyOrder can now be instructed to return responses in the same format, simply by specifying *responseFormat=1* in the request.

3.1 MIME Type

Line	Possible Value(s)
Mime-Type	application/x-www-form-urlencoded

3.2 Parameters

bold when always present.
italic when not always present.

Name	Possible Value(s)
errorCode	An integer (see section 2.1 - "Status Code" - for the possible values).
errorMessage	A string (see section 2.1 - "Status Code" - for the possible values). This parameter is not present when *errorCode=0*.
orderNumber	An integer. This parameter is only present when *errorCode=0*.
totalCost	Amount, in your account's native currency, without a currency symbol (e.g. $). This parameter is only present when *errorCode=0*.
expectedDeliveryTime	Expected number of hours before this order will be completed (0, 1, 24, 48 or 240). This parameter is only present when *errorCode=0*.
certificateID	The internal Certificate ID of the SSL certificate purchased by this order. This parameter is only present when *showCertificateID=Y* and *errorCode=0*.
certificateStatus	The status of the SSL certificate purchased by this order. This parameter is only present when *showCertificateState=Y* and *errorCode=0.*
uniqueValue	A unique alphanumeric value up to 20 characters long. Only returned if a uniqueValue parameter was passed in to this API, or if a uniqueValue has been generated by Sectigo for this order.

4. Parameters for new products available with !AutoApplyOrder

4.1 CodeGuard

Parameter	Possible Value(s)
days	Integer
years	Integer
appRepEmailAddress	String
appRepForename	String, not required
appRepSurname	String, not required
Domains	Integer

4.2 HackerGuardian

Name	Possible Value(s)
days	Integer
years	Integer
appRepLoginName	String
"IP Addresses"	Integer
organizationName	String

5. Example API Calls

5.1 DV certificate

Request

Parameter	Value	Details
loginName	*mypartnerusername*	
loginPassword	*th15ISNOTas3ns!blePassW0rd!*	
isCustomerValidated	*N*	Required
serverSoftware	*-1*	Required, used ‘OTHER’
days	*365*	365 days = 1 year
product	*488*	Code for SectigoSSL DV single cert
csr	*<full base64 encoded CSR>*	CSR for ‘sectigo.com’
dcvEmailAddress	*admin@sectigo.com*	Acceptable email address for DCV

Response

Output	Details
0	Successful!
123456789	Sectigo OrderNumber
35.00	Amount debited to account - $35.00
1	(Ignore, deprecated ‘Estimated Delivery Time’)
ImWhh1J1	(Optional) A ‘uniqueValue’ returned as one was not provided and the CSR has been re-used.

5.2 OV Multi-Domain Certificate

Request

Parameter	Value	Details
loginName	*mypartnerusername*	
loginPassword	*th15ISNOTas3ns!blePassW0rd!*	
isCustomerValidated	*N*	Required
serverSoftware	*-1*	Required, used ‘OTHER’
days	*730*	730 days = 2 years
product	*583*	Code for SectigoSSL OV MDC cert
appRepEmailAddress	*seniorstaffmember@sectigo.com*	Email address of the customer to action the callback
organizationName	*Sectigo*	Company name and information
streetAddress1	*5 Becker Farm Road*	
localityName	*Roseland*	
stateOrProvinceName	*NJ*	
countryName	*US*	ISO-3166 2-letter country code for United States
potsalCode	*07068*	
csr	*<full base64 encoded CSR>*	CSR for ‘sectigo.com’
domainNames	*sectigo.com,www.sectigo.com,secure.sectigo.com*	List of FQDNs
primaryDomainName	*sectigo.com*	Name for the Subject CN
validationTokens	*ALLCNAMECSRHASH*	Single token indicating all names to be DCV’d by DNS method

Response

Output	Details
0	Successful!
987654321	Sectigo OrderNumber
210.00	Amount debited to account - $210.00
1	(Ignore, deprecated ‘Estimated Delivery Time’)

5.2 EV Certificate

Request

Parameter	Value	Details
loginName	*mypartnerusername*	
loginPassword	*th15ISNOTas3ns!blePassW0rd!*	
isCustomerValidated	*N*	Required
serverSoftware	*-1*	Required, used 'OTHER'
days	*365*	365 days = 1 year
product	*562*	Code for EnterpriseSSL EV Pro certificate
appRepEmailAddress	*seniorstaffmember@sectigo.com*	Email address of the customer to action the callback
appRepForename	*John*	Name of representative of organisation
appRepSurname	*Smith*	
organizationName	*Sectigo*	Company name and information
streetAddress1	*5 Becker Farm Road*	
localityName	*Roseland*	
stateOrProvinceName	*NJ*	
countryName	*US*	ISO-3166 2-letter country code for United States
potsalCode	*07068*	
csr	*<full base64 encoded CSR>*	CSR for 'sectigo.com'
domainNames	*sectigo.com,www.sectigo.com,secure.sectigo.com*	List of FQDNs
primaryDomainName	*sectigo.com*	Name for the Subject CN
validationTokens	*ALLCNAMECSRHASH*	Single token indicating all names to be DCV'd by DNS method

Response

Output	Details
0	Successful!
987654321	Sectigo OrderNumber
210.00	Amount debited to account - $210.00
1	(Ignore, deprecated 'Estimated Delivery Time')

5.3 Product Bundle - DV certificate and Personal CodeGuard Account

Request

Parameter	Value	Details
loginName	*mypartnerusername*	
loginPassword	*th15ISNOTas3ns!blePassW0rd!*	
isCustomerValidated	*N*	Required
serverSoftware	*-1*	Required, used 'OTHER'
days	*365*	365 days = 1 year
product	*488,700*	Code for SectigoSSL DV single cert and CodeGuard Personal
csr	*<full base64 encoded CSR>*	CSR for 'sectigo.com'
dcvEmailAddress	*admin@sectigo.com*	Acceptable email address for DCV
appRepEmailAddress	*John.Doe@sectigo.com*	Email address for CodeGuard account delivery
domains	*1*	Number of domains for CodeGuard account

Response

Output	Details
0	Successful!
123458975	Sectigo OrderNumber
85.00	Amount debited to account - $85.00
1	(Ignore, deprecated 'Estimated Delivery Time')

5.4 Product Bundle - EV Certificate and

Request

Parameter	Value	Details
loginName	*mypartnerusername*	
loginPassword	*th15ISNOTas3ns!blePassW0rd!*	
isCustomerValidated	*N*	Required
serverSoftware	*-1*	Required, used 'OTHER'
days	*365*	365 days = 1 year
product	*562,346*	Code for EnterpriseSSL EV Pro certificate and HackerGuardian PCI Scan Control Centre
appRepEmailAddress	*seniorstaffmember@sectigo.com*	Email address of the customer to action the callback
appRepForename	*John*	Name of representative of organisation
appRepSurname	*Smith*	
organizationName	*Sectigo*	Company name and information
streetAddress1	*5 Becker Farm Road*	
localityName	*Roseland*	
stateOrProvinceName	*NJ*	
countryName	*US*	ISO-3166 2-letter country code for United States
potsalCode	*07068*	
csr	*<full base64 encoded CSR>*	CSR for 'sectigo.com'
domainNames	*sectigo.com,www.sectigo.com,secure.sectigo.com*	List of FQDNs
primaryDomainName	*sectigo.com*	Name for the Subject CN
validationTokens	*ALLCNAMECSRHASH*	Single token indicating all names to be DCV'd by DNS method
appRepLoginName	*sectigoHGusername*	Username to create for the HackerGuardian service

Response

Output	Details
0	Successful!
987654321	Sectigo OrderNumber
210.00	Amount debited to account - $210.00
1	(Ignore, deprecated 'Estimated Delivery Time')

6. Push Notification / Webhook API

Sectigo has the ability to 'push' information about issued certificates to your system when the certificates are signed.
The signed certificate and certificate chain can optionally also be pushed to your system.

This 'push' mechanism allows us to notify you when your certificates change status or are signed and available. The signed certificate itself can also optionally be included along with the certificate chain, or you can choose not to have the certificate sent and use the status push to trigger a call to the CollectSSL API.

This system helps alleviate the requirement for frequent polling of order status.

Notes:

- Changes in state are communicated, when triggered by completion of various actions – e.g. DCV completed, OV or EV validation completed.
- We only push the details of signed **SSL (server) certificates**. Client/email and code signing certificates are not supported at this time.
- There is a 'failed' status that can be pushed. It should never occur. Please handle this error, but we would suggest notifying your Account Manager if this occurs.
- You should ensure that the endpoint URL to which we call is available as much as possible. Should there be a problem communicating the call to your system, we will log as a failure within our system. The call will be attempted **three (3)** times only. A 'failure' can be defined as: a network connectivity issue; verification failure of your SSL certificate; an authentication failure (if provided); a protocol error or server-issued error (HTTP error codes).
- While this system alleviates the need for frequent polling of CollectSSL for status, we understand it does not remove it altogether. We advise that if you do wish to continue with polling for status of your certificate orders you do so **no more frequently than once every 3 hours**.
- If you choose to have the signed certificate and chain pushed, our system will make a **POST** call instead of **GET** – including for status changes without certificates attached.
- The *reason* in a 'failed' status (code 3) could include:
  CAA: Not authorized to issue - the CAA DNS record does not authorise us to issue.
- For use of the *verificationCode* – this applies to both OV and EV certificates.

  OV Callback Link:
  *https://secure.trust-provider.com/products/EnterCallbackCode?orderNumber=**{orderNumber}**&code2=**{verificationCode}***

  EV Click-through and Callback Link:
  *https://secure.trust-provider.com/products/ExecuteAgreementsWithCode?orderNumber**={orderNumber}**&code2=**{verificationCode}***

Setup:
To setup the certificate issuance push, you should setup a system to receive HTTP or HTTPS calls.

The system should accept all the parameters from the IP listed below. You do not need to utilise both orderNumber and certificateID unless you wish to.

The URL must be visible on the public internet, although you may wish to add IP-restrictions to only allow the call to be made from our system.

'Basic Authentication' is supported.

Call Information:
Sectigo will make a call to a URL which you delegate.

WITHOUT certificate push:
These parameters will be passed as a HTTP(S) GET to your URL, as follows:

Parameter	Type	Description	Example
orderNumber	string	Sectigo order number.	1234567repl#1
certificateID	integer	Sectigo certificate ID.	1234567890
Status	string	Certificate status.	issued
statusCode	integer	Certificate status as an integer value.	6
statusDesc	string	Brief description of the status.	Valid
verificationCode	string	Will be present just for statuses (verified and click-through)	mdtBfVzq0MIaiGg8

WITH certificate push:
The above parameters are sent, with two additions. All parameters are POSTed to your URL.

Parameter	Type	Description	Example
certificate	string	PEM (Base64 with PEM headers) encoded certificate.	
caCertificate	string	PEM encoded certificate chain.	

A list of the 'status', 'statusCode' and 'statusDesc' parameters:

statusCode	status	statusDesc
6	issued	Valid
9	issued	Issued but not yet collected
8	revoked	Revoked
14	replaced	Replaced
12	awaitingbrandvalidation	Awaiting Validation (Brand)
5	failed	POST-SIGN FAILED
3	failed	PRE-SIGN FAILED: *reason*
7	rejected	Rejected: *reason*
Any of above depending on certificate state	verified	Phone number verified
Any of above depending on certificate state	click-through	EV click-through e-mail sent

The call will be made from:

91.199.212.132

Once you have your endpoint URL setup, please contact your Account Manager or *partnerapisupport@sectigo.com* with both your account number or username and the URL (including basic authentication credentials if necessary).

Please also specify if you wish to have the signed certificate and chain pushed or not.