CERTCENTRAL API: SECURE SITE PRODUCTS

Version 1.1

Table of Contents

1 Workflow overview

DigiCert brings its new Secure Site products to CertCentral. This introduces five new endpoints into the API ecosystem.

1. **Order a Secure Site product**
    a. Secure Site product line: DigiCert includes five types of certificates
        - Secure Site SSL
        - Secure Site Multi-Domain SSL
        - Secure Site Wildcard SSL
        - Secure Site EV SSL
        - Secure Site EV Multi-Domain SSL

        See Appendix: Secure Site products available in CertCentral.

    b. All Secure Site certificates come with the following benefits:
        - **Priority validation** – Secure Site certificate orders are automatically placed at the top of our validation queues allowing our validation agents to respond to these orders first.
        - **Priority support** – Secure Site certificates come with access to a “priority” support queue allowing our support agents to respond to your needs first.
        - **Two premium site seals** – Included with every Secure Site certificate are the two most recognized trust marks on the web: DigiCert and Norton Secured. Pick the premium site seal you want to use to display proof of trust on your site.
        - **Industry-leading warranties** – Secure Site certificates include warranties to protect you and your customers: a $1.75M Netsure Protection Warranty for your business and an industry-best $2M aggregate Relying Party Warranty for your customers.
2. **Get your premium site seal**
    a. Get your site seal "hash"

        Each site seal is tied to a specific certificate order. The site seal will only display properly on domains included in the certificate order.

        Before you begin using your site seal, you need to get the hash for the certificate. The hash ties the site seal to the domains on the certificate allowing the site seal to work on those domains.

        Note: The site seal "hash" is a prerequisite for emailing the site seal code. Without the "hash", the email with the site seal code can't be sent.

b. **Email your site seal code**

To access your site seal code so that you can display the site seal on your site, you need to email the site seal code to yourself or another recipient.

2 Submitting orders – order Secure Site SSL Certificate

Use this endpoint to order a Secure Site SSL Certificate

2.1 Request endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certifcate/ssl_securesite

2.2 Request body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

2.3 JSON request parameters

Items to note about the request body parameters:

- **Certificate Validity Parameters**

  When ordering a certificate, you are required to specify the certificate validity period. You can use any of these parameters to determine how long a certificate will be valid.

  Parameter Priority Note: If you accidently include more than one of these parameters in your certificate request, we prioritize the parameters as follows: custom_expiration_date > validity_days > validity_years.

  - validity_years

    Specify the number of years you want the certificate to be valid for.

  - custom_expiration_date

    Specify the date on which you want the certificate to expire.

  - validity_days

    Specify the number of days you want the certificate to be valid for.

Parameter name	Required / optional	Allowed values	Default	Description
certificate	Required	[object]		

Parameter name	Required / optional	Allowed values	Default	Description
common_name	Required	[string]		The name to be secured in the certificate.
csr	Required	[string]		Certificate Signing Request To create a CSR from your server, visit the DigiCert Website (https://www.digicert.com/csr-creation.htm).
organization_units	Optional	[array]	[blank]	The OU (organization unit) field in the certificate.
server_platform	Optional	Reference: Appendix: Server Platform IDs	-1	The server platform type you plan to install the SSL/TLS certificate on. If not included in the request, it defaults to OTHER.
id	Required	[int]		The id for the server platform.
signature_hash	Required	sha256 sha384 sha512 ecc256 ecc384		The certificate's signing algorithm hash.
profile_option	Optional	[string]	[blank]	Some custom modifications to the resulting certificate are managed through certificate profiles. Do you have custom certificate profiles enabled on your account? Then, you can pass a certificate profile name through this parameter.

Parameter name	Required / optional	Allowed values	Default	Description
				For more information about custom certificate profiles please contact your DigiCert account manager.
organization	Required	[object]		
id	Required	[int]		The organization's identifier.
validity_years	Required	[int]		Number of years for which the certificate is valid.
custom_expiration_date	Optional	[date]		Date on which the certificate expires. Required Date format: YYYY-MM-DD. See Certificate Validity Parameters.
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters.
comments	Optional	[string]	[string]	Comments about this certificate request the approver will see.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.
renewal_of_order_id	Optional	[int]		Is this order a renewal of a previous order? Then add the previous order's id to this parameter.

Parameter name	Required / optional	Allowed values	Default	Description
payment_method	Optional	balance card profile	balance	How to pay for the certificate. If there is a default payment profile, it will default **profile**. Otherwise, it will default to **balance**.
disable_ct	Optional	[bool]		To set disable_ct, your account must first be configured to allow per-cert CT logging. If disable_ct is true, it will turn off public CT logging for an order. Unless otherwise specified, the default for an order is false and the order will be logged to public CT logs.

2.4 JSON response parameters

Parameter name	Data type	Description
id	[int]	The order's identifier.
requests	[array]	
id	[int]	
status	[string]	Certificate order statuses: pending, approved, rejected.

2.5 Example request

Endpoint

```
POST https://www.digicert.com/services/v2/order/certificate/ssl_securesite
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-type: application/json
Content-length: 662
```

Body

JSON (application/json)

```
{
    "certificate": {
        "common_name": "example.com",
        "csr": "------ [CSR HERE] ------",
        "organization_units": [
            "Dev-ops"
        ],
        "server_platform": {
            "id": 45
        },
        "signature_hash": "sha256",
        "profile_option": "some_ssl_profile"
    },
    "organization": {
        "id": 111
    },
    "validity_years": 2,
    "custom_expiration_date": "2018-11-20",
    "comments": "Comments for the approver",
    "disable_renewal_notifications": false,
    "renewal_of_order_id": 222,
    "payment_method": "balance",
    "disable_ct": false
}
```

2.6 Example response

Status code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-type: application/json
Content-length: 84
```

Body

JSON (application/json)

```
{
    "id": 12345,
    "requests": [
        {
            "id": 54321,
            "status": "pending"
        }
    ]
}
```

3 Submitting orders – order Secure Site Multi-Domain SSL Certificate

Use this endpoint to order a Secure Site Multi-Domain SSL Certificate

3.1 Request endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certifcate/ssl_securesite_multi_domain

3.2 Request body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

3.3 JSON request parameters

Items to note about the request body parameters:

- **Certificate Validity Parameters**

  When ordering a certificate, you are required to specify the certificate validity period. You can use any of these parameters to determine how long a certificate will be valid.

  Parameter Priority Note: If you accidently include more than one of these parameters in your certificate request, we prioritize the parameters as follows: custom_expiration_date > validity_days > validity_years.

    - validity_years

Specify the number of years you want the certificate to be valid for.

- custom_expiration_date

  Specify the date on which you want the certificate to expire.

- validity_days

  Specify the number of days you want the certificate to be valid for.

Parameter name	Required / optional	Allowed values	Default	Description
certificate	Required	[object]		
common_name	Required	[string]		The name to be secured in the certificate.
dns_names	Optional	[array]		Additional names to be secured in the certificate. Adding SANs to a certificate order may incur additional cost.
csr	Required	[string]		Certificate Signing Request To create a CSR from your server, visit the DigiCert Website (https://www.digicert.com/csr-creation.htm).
organization_units	Optional	[array]	[blank]	The OU (organization unit) field in the certificate.
server_platform	Optional	Reference: Appendix: Server Platform IDs	-1	The server platform type you plan to install the SSL/TLS certificate on. If not included in the request, it defaults to OTHER.
id	Required	[int]		The id for the server platform.

Parameter name	Required / optional	Allowed values	Default	Description
signature_hash	Required	sha256 sha384 sha512 ecc256 ecc384		The certificate's signing algorithm hash.
profile_option	Optional	[string]	[blank]	Some custom modifications to the resulting certificate are managed through certificate profiles. Do you have custom certificate profiles enabled on your account? Then, you can pass a certificate profile name through this parameter. For more information about custom certificate profiles please contact your DigiCert account manager.
organization	Required	[object]		
id	Required	[int]		The organization's identifier.
validity_years	Required	[int]		Number of years for which the certificate is valid.
custom_expiration_date	Optional	[date]		Date on which the certificate expires. Required Date format: YYYY-MM-DD. See Certificate Validity Parameters.
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters.

Parameter name	Required / optional	Allowed values	Default	Description
comments	Optional	[string]	[string]	Comments about this certificate request the approver will see.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.
renewal_of_order_id	Optional	[int]		Is this order a renewal of a previous order? Then add the previous order's id to this parameter.
payment_method	Optional	balance card profile	balance	How to pay for the certificate. If there is a default payment profile, it will default **profile**. Otherwise, it will default to **balance**.
disable_ct	Optional	[bool]		To set disable_ct, your account must first be configured to allow per-cert CT logging. If disable_ct is true, it will turn off public CT logging for an order. Unless otherwise specified, the default for an order is false and the order will be logged to public CT logs.

3.4 JSON response parameters

Parameter name	Data type	Description
id	[int]	The order's identifier.
requests	[array]	

id	[int]	
status	[string]	Certificate order statuses: pending, approved, rejected.

3.5 Example request

Endpoint

```
POST
https://www.digicert.com/services/v2/order/certificate/ssl_securesite_multi_domain
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-type: application/json
Content-length: 662
```

Body

JSON (application/json)

```
{
    "certificate": {
        "common_name": "example.com",
        "dns_names": [
            "secondexample.com",
            "thirdexample.com",
            "fourthexample.com"
        ],
        "csr": "------ [CSR HERE] ------",
        "organization_units": [
            "Dev-ops"
        ],
        "server_platform": {
            "id": 45
        },
        "signature_hash": "sha256",
        "profile_option": "some_ssl_profile"
    },
    "organization": {
        "id": 111
    },
    "validity_years": 2,
    "custom_expiration_date": "2018-11-20",
```

JSON (application/json)


```
    "comments": "Comments for the approver",
    "disable_renewal_notifications": false,
    "renewal_of_order_id": 222,
    "payment_method": "balance",
    "disable_ct": false
}
```


3.6 Example response

Status code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-type: application/json
Content-length: 84
```

Body

JSON (application/json)


```
{
    "id": 12345,
    "requests": [
        {
            "id": 54321,
            "status": "pending"
        }
    ]
}
```


4 Submitting orders – order Secure Site Wildcard SSL Certificate

Use this endpoint to order a Secure Site Wildcard SSL Certificate

4.1 Request endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certifcate/ssl_securesite_wildcard

4.2 Request body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

4.3 JSON request parameters

Items to note about the request body parameters:

- **Certificate Validity Parameters**

  When ordering a certificate, you are required to specify the certificate validity period. You can use any of these parameters to determine how long a certificate will be valid.

  Parameter Priority Note: If you accidently include more than one of these parameters in your certificate request, we prioritize the parameters as follows: custom_expiration_date > validity_days > validity_years.

  - validity_years

    Specify the number of years you want the certificate to be valid for.

  - custom_expiration_date

    Specify the date on which you want the certificate to expire.

  - validity_days

    Specify the number of days you want the certificate to be valid for.

Parameter name	Required / optional	Allowed values	Default	Description
certificate	Required	[object]		
common_name	Required	[string]		The name to be secured in the certificate.
dns_names	Optional	[array]		Additional names to be secured in the certificate. SANs must be a wildcard domain (for example, *.yourdomain.com) or based off of your listed wildcard domains. For example, if one of your

Parameter name	Required / optional	Allowed values	Default	Description
				wildcard domains is *.example.com, then you may use www.example.com or www.app.example.com. Adding wildcards SANs to a certificate order may incur additional cost.
csr	Required	[string]		Certificate Signing Request To create a CSR from your server, visit the DigiCert Website (https://www.digicert.com/csr-creation.htm).
organization_units	Optional	[array]	[blank]	The OU (organization unit) field in the certificate.
server_platform	Optional	Reference: Appendix: Server Platform IDs	-1	The server platform type you plan to install the SSL/TLS certificate on. If not included in the request, it defaults to OTHER.
id	Required	[int]		The id for the server platform.
signature_hash	Required	sha256 sha384 sha512 ecc256 ecc384		The certificate's signing algorithm hash.
profile_option	Optional	[string]	[blank]	Some custom modifications to the resulting certificate are

Parameter name	Required / optional	Allowed values	Default	Description
				managed through certificate profiles. Do you have custom certificate profiles enabled on your account? Then, you can pass a certificate profile name through this parameter. For more information about custom certificate profiles please contact your DigiCert account manager.
organization	Required	[object]		
id	Required	[int]		The organization's identifier.
validity_years	Required	[int]		Number of years for which the certificate is valid.
custom_expiration_date	Optional	[date]		Date on which the certificate expires. Required Date format: YYYY-MM-DD. See Certificate Validity Parameters.
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters.
comments	Optional	[string]	[string]	Comments about this certificate request the approver will see.

Parameter name	Required / optional	Allowed values	Default	Description
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.
renewal_of_order_id	Optional	[int]		Is this order a renewal of a previous order? Then add the previous order's id to this parameter.
payment_method	Optional	balance card profile	balance	How to pay for the certificate. If there is a default payment profile, it will default **profile**. Otherwise, it will default to **balance**.
disable_ct	Optional	[bool]		To set disable_ct, your account must first be configured to allow per-cert CT logging. If disable_ct is true, it will turn off public CT logging for an order. Unless otherwise specified, the default for an order is false and the order will be logged to public CT logs.

4.4 JSON response parameters

Parameter name	Data type	Description
id	[int]	The order's identifier.
requests	[array]	

Parameter name	Data type	Description
id	[int]	
status	[string]	Certificate order statuses: pending, approved, rejected.

4.5 Example request

Endpoint

```
POST https://www.digicert.com/services/v2/order/certificate/ssl_securesite_wildcard
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-type: application/json
Content-length: 662
```

Body

JSON (application/json)

```
{
    "certificate": {
        "common_name": "*.example.com",
        "dns_names": [
            "www.second.example.com",
            "*.yourdomain.com",
            "second.yourdomain.com"
        ],
        "csr": "------ [CSR HERE] ------",
        "organization_units": [
            "Dev-ops"
        ],
        "server_platform": {
            "id": 45
        },
        "signature_hash": "sha256",
        "profile_option": "some_ssl_profile"
    },
    "organization": {
        "id": 111
    },
    "validity_years": 2,
```

JSON (application/json)

```
    "custom_expiration_date": "2018-11-20",
    "comments": "Comments for the approver",
    "disable_renewal_notifications": false,
    "renewal_of_order_id": 222,
    "payment_method": "balance",
    "disable_ct": false
}
```

4.6 Example response

Status code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-type: application/json
Content-length: 84
```

Body

JSON (application/json)

```
{
    "id": 12345,
    "requests": [
        {
            "id": 54321,
            "status": "pending"
        }
    ]
}
```

5 Submitting orders – order Secure Site EV SSL Certificate

Use this endpoint to order a Secure Site EV SSL Certificate

5.1 Request endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certifcate/ssl_ev_securesite

5.2 Request body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

5.3 JSON request parameters

Items to note about the request body parameters:

- **Certificate Validity Parameters**

  When ordering a certificate, you are required to specify the certificate validity period. You can use any of these parameters to determine how long a certificate will be valid.

  Parameter Priority Note: If you accidently include more than one of these parameters in your certificate request, we prioritize the parameters as follows: custom_expiration_date > validity_days > validity_years.

  - validity_years

    Specify the number of years you want the certificate to be valid for.

  - custom_expiration_date

    Specify the date on which you want the certificate to expire.

  - validity_days

    Specify the number of days you want the certificate to be valid for.

Parameter name	Required / optional	Allowed values	Default	Description
certificate	Required	[object]		
common_name	Required	[string]		The name to be secured in the certificate.
csr	Required	[string]		Certificate Signing Request To create a CSR from your server, visit the DigiCert Website (https://www.digicert.com/csr-creation.htm).

Parameter name	Required / optional	Allowed values	Default	Description
organization_units	Optional	[array]	[blank]	The OU (organization unit) field in the certificate.
server_platform	Optional	Reference: Appendix: Server Platform IDs	-1	The server platform type you plan to install the SSL/TLS certificate on. If not included in the request, it defaults to OTHER.
id	Required	[int]		The id for the server platform.
signature_hash	Required	sha256 sha384 sha512 ecc256 ecc384		The certificate's signing algorithm hash.
profile_option	Optional	[string]	[blank]	Some custom modifications to the resulting certificate are managed through certificate profiles. Do you have custom certificate profiles enabled on your account? Then, you can pass a certificate profile name through this parameter. For more information about custom certificate profiles please contact your DigiCert account manager.
organization	Required	[object]		
id	Required	[int]		The organization's identifier.

Parameter name	Required / optional	Allowed values	Default	Description
validity_years	Required	[int]		Number of years for which the certificate is valid.
custom_expiration_date	Optional	[date]		Date on which the certificate expires. Required Date format: YYYY-MM-DD. See Certificate Validity Parameters.
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters.
comments	Optional	[string]	[string]	Comments about this certificate request the approver will see.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.
renewal_of_order_id	Optional	[int]		Is this order a renewal of a previous order? Then add the previous order's id to this parameter.
payment_method	Optional	balance card profile	balance	How to pay for the certificate. If there is a default payment profile, it will default **profile**. Otherwise, it will default to **balance**.
disable_ct	Optional	[bool]		To set disable_ct, your account must first be

Parameter name	Required / optional	Allowed values	Default	Description
				configured to allow per-cert CT logging. If disable_ct is true, it will turn off public CT logging for an order. Unless otherwise specified, the default for an order is false and the order will be logged to public CT logs.

5.4 JSON response parameters

Parameter name	Data type	Description
id	[int]	The order's identifier.
requests	[array]	
id	[int]	
status	[string]	Certificate order statuses: pending, approved, rejected.

5.5 Example request

Endpoint

```
POST https://www.digicert.com/services/v2/order/certificate/ssl_ev_securesite
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-type: application/json
Content-length: 662
```

Body

JSON (application/json)

```
{
    "certificate": {
```

JSON (application/json)

```
        "common_name": "example.com",
        "csr": "------ [CSR HERE] ------",
        "organization_units": [
            "Dev-ops"
        ],
        "server_platform": {
            "id": 45
        },
        "signature_hash": "sha256",
    },
    "organization": {
        "id": 111
    },
    "validity_years": 2,
    "custom_expiration_date": "2018-11-21",
    "comments": "Comments for the approver",
    "disable_renewal_notifications": false,
    "renewal_of_order_id": 222,
    "disable_ct": false
}
```

5.6 Example response

Status code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-type: application/json
Content-length: 84
```

Body

JSON (application/json)

```
{
    "id": 12345,
    "requests": [
        {
            "id": 54321,
            "status": "pending"
        }
    ]
}
```

6 Submitting orders – order Secure Site EV Multi-Domain SSL Certificate

Use this endpoint to order a Secure Site EV Multi-Domain SSL Certificate

6.1 Request endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certifcate/ssl_ev_securesite_multi_domain

6.2 Request body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

6.3 JSON request parameters

Items to note about the request body parameters:

- **Certificate Validity Parameters**

  When ordering a certificate, you are required to specify the certificate validity period. You can use any of these parameters to determine how long a certificate will be valid.

  Parameter Priority Note: If you accidently include more than one of these parameters in your certificate request, we prioritize the parameters as follows: custom_expiration_date > validity_days > validity_years.

  - validity_years

    Specify the number of years you want the certificate to be valid for.

  - custom_expiration_date

    Specify the date on which you want the certificate to expire.

  - validity_days

    Specify the number of days you want the certificate to be valid for.

Parameter name	Required / optional	Allowed values	Default	Description
certificate	Required	[object]		

Parameter name	Required / optional	Allowed values	Default	Description
common_name	Required	[string]		The name to be secured in the certificate.
dns_names	Optional	[array]		Additional names to be secured in the certificate. Adding SANs to a certificate order may incur additional cost.
csr	Required	[string]		Certificate Signing Request To create a CSR from your server, visit the DigiCert Website (https://www.digicert.com/csr-creation.htm).
organization_units	Optional	[array]	[blank]	The OU (organization unit) field in the certificate.
server_platform	Optional	Reference: Appendix: Server Platform IDs	-1	The server platform type you plan to install the SSL/TLS certificate on. If not included in the request, it defaults to OTHER.
id	Required	[int]		The id for the server platform.
signature_hash	Required	sha256 sha384 sha512 ecc256 ecc384		The certificate's signing algorithm hash.
profile_option	Optional	[string]	[blank]	Some custom modifications to the resulting certificate are

Parameter name	Required / optional	Allowed values	Default	Description
				managed through certificate profiles. Do you have custom certificate profiles enabled on your account? Then, you can pass a certificate profile name through this parameter. For more information about custom certificate profiles please contact your DigiCert account manager.
organization	Required	[object]		
id	Required	[int]		The organization's identifier.
validity_years	Required	[int]		Number of years for which the certificate is valid.
custom_expiration_date	Optional	[date]		Date on which the certificate expires. Required Date format: YYYY-MM-DD. See Certificate Validity Parameters.
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters.
comments	Optional	[string]	[string]	Comments about this certificate request the approver will see.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this

Parameter name	Required / optional	Allowed values	Default	Description
				certificate, you must set this value to **true**.
renewal_of_order_id	Optional	[int]		Is this order a renewal of a previous order? Then add the previous order's id to this parameter.
payment_method	Optional	balance card profile	balance	How to pay for the certificate. If there is a default payment profile, it will default **profile**. Otherwise, it will default to **balance**.
disable_ct	Optional	[bool]		To set disable_ct, your account must first be configured to allow per-cert CT logging. If disable_ct is true, it will turn off public CT logging for an order. Unless otherwise specified, the default for an order is false and the order will be logged to public CT logs.

6.4 JSON response parameters

Parameter name	Data type	Description
id	[int]	The order's identifier.
requests	[array]	
id	[int]	

status	[string]	Certificate order statuses: pending, approved, rejected.

6.5 Example request

Endpoint

```
POST
https://www.digicert.com/services/v2/order/certificate/ssl_securesite_multi_domain
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-type: application/json
Content-length: 662
```

Body

JSON (application/json)

```
{
    "certificate": {
        "common_name": "example.com",
        "dns_names": [
            "secondexample.com",
            "thirdexample.com",
            "fourthexample.com"
        ],
        "csr": "------ [CSR HERE] ------",
        "organization_units": [
            "Dev-ops"
        ],
        "server_platform": {
            "id": 45
        },
        "signature_hash": "sha256",
        "profile_option": "some_ssl_profile"
    },
    "organization": {
        "id": 111
    },
    "validity_years": 2,
    "custom_expiration_date": "2018-11-20",
    "comments": "Comments for the approver",
    "disable_renewal_notifications": false,
```

JSON (application/json)

```
    "renewal_of_order_id": 222,
    "payment_method": "balance",
    "disable_ct": false
}
```

6.6 Example response

Status code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-type: application/json
Content-length: 84
```

Body

JSON (application/json)

```
{
    "id": 12345,
    "requests": [
        {
            "id": 54321,
            "status": "pending"
        }
    ]
}
```

7 Get site seal "hash"

Use this endpoint to get the "hash" for your site seal. The same "hash" can be used to get the code for all site seals (types, sizes, colors, etc.). For example, the same "hash" can be used the get the site seal code for a DigiCert and a Norton Site Seal.

7.1 Request endpoint

When using this endpoint, the "{order_id}" must be included in the URL. The site seal "hash" is tied to a specific certificate order. Your site seal is only valid on domains included in that order.

Method	URL
GET	https://www.digicert.com/services/v2/order/certificate/{order_id}/site-seal

7.2 Example request

Endpoint

```
GET https://www.digicert.com/services/v2/order/certificate/12345/site-seal
```

Headers

```
X-DC-DEVKEY: {api_key}
Accept: application/json
```

Body

None

7.3 Example response

Status Code

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: application/json
Content-Length: 78
```

Body

JSON (application/json)

```
{
   "seal_hash": "aBcD1234e"
}
```

8 Email site seal code

Use this endpoint to send an email that contains the site seal code. Placing this code on your page, allows you to display the selected site seal (DigiCert or Norton) on your site.

For information about installing your site seal, see the Install Your Site Seals site page.

8.1 Request endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/{order_id}/site-seal/email-seal

8.2 Request body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

Items to note about the request body parameters:

- **seal_hash**

  The same hash is used to get code for both site seals (DigiCert and Norton) in any size, color, or language for the specified certificate order.

- **seal_number**

  This parameter determines which site seal design you get back in the email. See Appendix: Site seal design values and preview.

- **seal_size**

  This parameter determines the size of the site seal you get back in the email. There are three site seal sizes: small, medium (standard), or large. See Appendix: Site seal size values and dimensions.

- **seal_color**

  This parameter determines the color of the text (SSL Certificates) that falls outside of the seal design (SSL Certificates). See Appendix: Site seal text color values and preview.

- **seal_language**

  This parameter determines the default language for the site seal pop-up content. Once it opens, the user can pick a different supported language for the pop-up. See Appendix: Seal pop-up window language type values.

8.3 JSON request parameters

Parameter name	Required / optional	Allowed values	Default	Description
seal_hash	Required	[string]		The site seal hash tied to the certificate order you are requesting the site seal code for **Note:** The hash must match the hash on the certificate order

Parameter name	Required / optional	Allowed values	Default	Description
seal_number	Required	Reference: Appendix: Site seal design values and preview		The seal number for the site seal design you want to use (DigiCert or Norton site seal) **seal_number values:** • 3 • 15 **Note:** Use 3 to get the DigiCert site seal and 15 to get the Norton site seal.
seal_size	Required	Reference: Appendix: Site seal size values and dimensions		Determines the size of the chosen site seal **seal_size values:** • s • m • l
seal_color	Required	Reference: Appendix: Site seal text color values and preview	white	Determines the text color of the wording that falls outside the site seal design (SSL Certificates) **seal_color values:** • white • black
seal_language	Required	Reference: Appendix: Seal pop-up window language type values	en	Determines the default language for the site seal pop-up

8.4 Example request

Endpoint

```
POST https://www.digicert.com/services/v2/order/certificate/{order_id}/site-seal/email-seal
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-Type: application/json
Content-Length: 662
```

Body

JSON (application/json)

```
{
      "seal_hash": "aBcD1234e",
      "seal_number": 5,
      "seal_size": "m",
      "seal_color": "white",
      "seal_language": "fr"
}
```

8.5 Example Response

Status Code: 204

When successful, this request returns a 204 OK status.

Body

None

9 Appendix: Server Platform IDs

Server Platform	ID
Apache	2
BEA Weblogic 8 & 9	42
Barracuda	41
Bea Weblogic 7 and older	29
Cisco	30
Citrix (Other)	39
Citrix Access Essentials	46
Citrix Access Gateway 4.x	50

Server Platform	ID
Citrix Access Gateway 5.x and higher	58
F5 Big-IP	31
F5 FirePass	32
IBM HTTP Server	7
Java Web Server (Javasoft / Sun)	10
Juniper	33
Lighttpd	44
Lotus Domino	11
Mac OS X Server	49
Microsoft Exchange Server 2003	47
Microsoft Exchange Server 2007	36
Microsoft Exchange Server 2010	48
Microsoft Exchange Server 2013	68
Microsoft Exchange Server 2016	71
Microsoft Forefront Unified Access Gateway	66
Microsoft IIS 1.x to 4.x	13
Microsoft IIS 10	70
Microsoft IIS 5 or 6	14
Microsoft IIS 7	40
Microsoft IIS 8	67
Microsoft Live Communications Server 2005	37
Microsoft Lync Server 2010	59

Server Platform	ID
Microsoft Lync Server 2013	69
Microsoft OCS R2	60
Microsoft Office Communications Server 2007	38
Microsoft Small Business Server 2008 & 2011	62
Netscape Enterprise Server	15
Netscape iPlanet	9
Novell NetWare	17
Novell iChain	65
OTHER (default)	-1
Oracle	18
Qmail	34
SunOne	35
Tomcat	24
WebStar	26
Zeus Web Server	28
cPanel	43
nginx	45

10 Appendix: Site seal design values and preview

Value	Seal design and preview
3	DigiCert site seal 
15	Norton site seal 

11 Appendix: Site seal size values and dimensions

Seal Design	Size value and dimensions
DigiCert	• **s** - 80 x 47px • **m** - 100 x 59px • **l** - 130 x 76px.
Norton	• **s** - 110 x 63px • **m** - 133 x 78px • **l** - 177 x 98px.

12 Appendix: Site seal text color values and preview

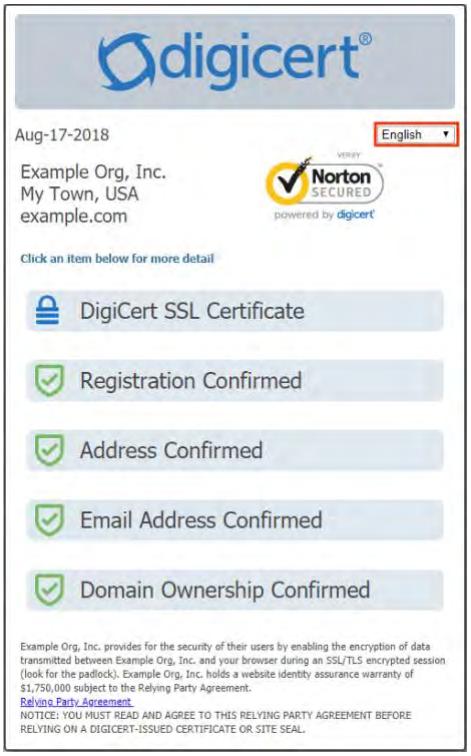
Value	Preview
white	DigiCert site seal used for this example Affected text: "SSL Certificates" (below the seal image) 
black	Norton site seal used for this example Affected text: "SSL Certificates" (below the seal image) 

13 Appendix: Seal pop-up window language type values

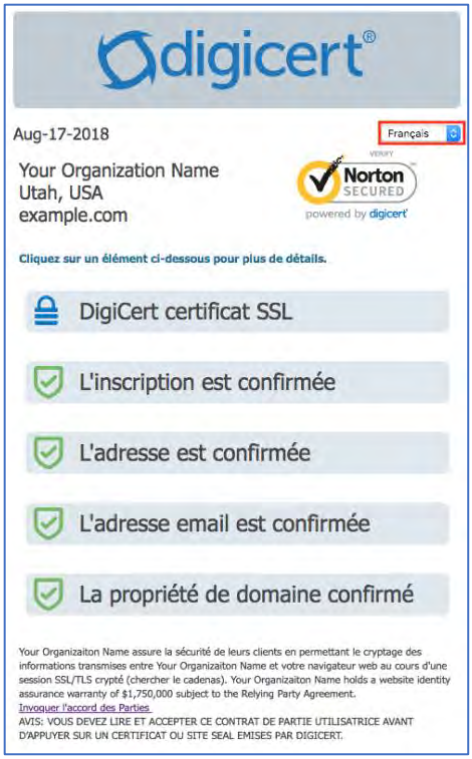
Value	Language
en	English (default language)
es	Spanish
fr	French
ja	Japanese
pt	Portuguese

13.1 Pop-up default language examples

1. DigiCert site seal pop-up with default language set to English



2. Norton site seal pop-up with the default language set to French



14 Appendix: Secure Site products available in CertCentral

1. **Secure Site SSL**

   Secure Site SSL Certificates protect your website or email traffic with industrial-strength 2048-bit encryption.

   - Provides encryption and authentication for one domain
   - When you buy www.example.com, example.com is also secured for free
   - Comes with unlimited free reissues for the life of the certificate
   - No licensing fees – Install the certificate on multiple servers at no extra cost
   - Trusted by all major browsers and operating systems
   - Meets PCI requirements for credit card transaction security
   - Comes with automated authenticity checks

2. **Secure Site Multi-Domain SSL**

   Secure Site Multi-Domain SSL certificates use Subject Alternative names (SANs) to secure multiple sites (that is, fully qualified domain names) with one certificate.

   - Includes 4 fully qualified domain names (FQDNs) in the base price
   - Lets you secure up to 250 websites (FQDNs) on one certificate
   - No licensing fees – Install the certificate on multiple servers at no extra cost
   - Comes with unlimited free reissues for the life of the certificate.
   - Trusted by all major browsers and operating systems
   - Meets PCI requirements for credit card transaction security
   - Comes with automated authenticity checks

3. **Secure Site Wildcard SSL**

   Secure Site Wildcard SSL Certificates secures unlimited servers with one certificate (*.example.com).

   - Includes 1 wildcard domain in the base price
   - Lets you secure a domain and all its first-level subdomains (*.example.com)
   - Also secures the base domain for free (for example, *.yourdomain.com secures yourdomain.com)
   - Add SANs to secure multiple wildcard domains on one certificate (for example, *.example.com, *.secondexample.com, and *.thirdexample.com)
   - Lets you secure up to 250 wildcard domains on one certificate
   - No licensing fees – Install the certificate on multiple servers at no extra cost

- Comes with unlimited free reissues for the life of the certificate
- Trusted by all major browsers and operating systems
- Meets PCI requirements for credit card transaction security
- Comes with automated authenticity checks

4. **Secure Site EV SSL**

   Secure Site Extended Validation (EV) SSL Certificates protect your most valuable assets–your customers and your brand–from phishing scams and online fraud.

   - Provides your customers proof that they can confidently interact with your site when sharing sensitive information (such as credit card numbers and personal information)
   - Converts visitors into sales, increasing revenue
   - Provides encryption and authentication for one domain
   - When you buy www.example.com, example.com is also secured for free.
   - Comes with unlimited free reissues for the life of the certificate
   - No licensing fees – Install the certificate on multiple servers at no extra cost
   - Trusted by all major browsers and operating systems
   - Meets PCI requirements for credit card transaction security
   - Comes with automated authenticity checks

5. **Secure Site EV Multi-Domain SSL**

   Secure Site Extended Validation (EV) Multi-Domain SSL Certificates protect your most valuable assets–your customers and your brand–from phishing scams and online fraud. These certificates use Subject Alternative Names (SANs) to secure multiple sites (fully qualified domain names) with one certificate.

   - Gives you the flexibility of a SANs certificate as well as the additional security and user confidence benefits from Extended Validation
   - Secure multiple sites (fully qualified domain names) with one certificate
   - Includes 3 FQDNs in the base price
   - Lets you secure up to 250 websites (FQDNs) on one certificate
   - Provides your customers proof that they can confidently interact with your site when sharing sensitive information (such as credit card numbers and personal information)
   - Converts visitors into sales, increasing revenue
   - No licensing fees – Install the certificate on multiple servers at no extra cost
   - Comes with unlimited free reissues for the life of the certificate.
   - Trusted by all major browsers and operating systems
   - Meets PCI requirements for credit card transaction security

- Comes with automated authenticity checks

About DigiCert

DigiCert is a premier provider of security solutions and certificate management tools. We have earned our reputation as the security industry leader by building innovative solutions for SSL Certificate management and emerging markets.

DIGICERT
2801 NORTH THANKSGIVING WAY STE. 500
LEHI, UTAH 84043
PHONE: 801.701.9690
EMAIL: SALES@DIGICERT.COM