CERTCENTRAL API: DV CERTIFICATE ENROLLMENT

Version 1.6

Table of Contents

1 Workflow Overview

The DV certificate API workflow includes the following steps:

1. **Order DV certificate**

   Currently, DV certificates are available from two of our brands:

   - RapidSSL Standard DV
   - RapidSSL Wildcard DV
   - GeoTrust Standard DV
   - GeoTrust Wildcard DV
   - GeoTrust Cloud DV

2. **Cancel DV certificate order**

   If needed, you can cancel a pending DV certificate order. For example, you may discover that a certificate is not needed and want to cancel the order before we issue the DV certificate.

3. **Complete Domain Control Validation (DCV)**

   - **Demonstrate control over the domain**

     Use the Email, DNS TXT, and File Auth DCV methods to demonstrate control over the domain on your DV certificate order.

   - **Verify random value placement**

     Use the *Check DCV* endpoint to validate the domain once the random value is in place (added to the DNS TXT record or placed in the specified location on the web page).

   - **Retrieve the domain emails for a domain**

     Use the Get Domain Control Emails endpoint to retrieve the domain emails for a domain (WHOIS-based and constructed), so that you can see where the DCV emails are sent.

   - **Resend the DCV emails**

     Use the Resend Emails endpoint to resend the Domain Control Validation (DCV) emails for a certificate order.

   - **Generate a new random value**

     Use the DCV Random Value endpoint to generate a new random value for the DNS TXT or File Auth DCV methods.

     Note: Random values expire after 30 days.

- **Change DCV method**

  Use the Change DCV Method endpoint to use a different validation method to demonstrate control over the domain in your pending DV certificate order (for example, to switch from using Email to using the DNS TXT DCV method).

4. **Check order status changes**

   - Check on the status of your DV certificate orders.
   - Enter the time range (in minutes) to check the changes in status of certificates in the last 10 minutes, the last 3 days, etc. (up to a week).

5. **Download issued certificate**

   Download certificate based on the server platform or in a specific certificate format type (Apache, IIS, .p7b, .crt, etc.).

6. **Reissue certificate**

   If needed, reissue a DV certificate. This allows you to replace the existing certificate with a new one that has different information (e.g., common name, CSR, etc.).

   Note: When you reissue a certificate, the original certificate (or previous version of it) is revoked. Additionally, each time you reissue a DV certificate, you must complete domain validation (i.e., demonstrate control over the domain) for the domain on the order/reissue.

7. **Revoke DV certificate**

   When needed, you can revoke an issued DV certificate. For example, you may need to revoke a certificate because the certificate is no longer needed, or because it's been determined that the certificate's private key has been compromised.

   Two step revocation process

   The DV certificate revocation process consists of two steps: 1) Submit a request to revoke a DV certificate and 2) Administrator approves (or rejects) the request, and DigiCert revokes the DV certificate.

   Administrator approval step required

   Once completed, a certificate revocation cannot be reversed. A revoked DV certificate used on a public site shows trust warnings preventing users from accessing the site.

8. **(Optional) View order details**

Once the certificate is issued, you can view the order details to see information about the certificate order.

2 Order a Standard DV Certificate

2.1 Submitting Order - Order Standard DV Certificate

Currently, the *Order Standard DV Certificate* endpoints allow those using the DigiCert Services API to order two types of Standard DV certificates: GeoTrust Standard DV and RapidSSL Standard DV.

- **GeoTrust Standard DV**
  Protect your website with RSA 2048+ encryption or ECC 256+ keys and SHA2-256 signature algorithm.
  - Provides encryption for one domain
  - When you buy www.[yourdomain].com, [yourdomain].com will also be secured -- for free
  - Add SANs to secure multiple domains on one certificate
    (Adding SANs to a GeoTrust Standard DV certificate order may incur additional cost.)
  - Unlimited server license means you can install the certificate on multiple servers at no extra cost
  - Trusted by all major browsers and operating systems
  - Meets and exceeds PCI Compliance requirements for TLS certificates
- **RapidSSL Standard DV**
  Protect your website with RSA 2048+ encryption or ECC 256+ keys and SHA2-256 signature algorithm.
  - Provides encryption for one domain
  - When you buy www.[yourdomain].com, [yourdomain].com will also be secured -- for free
  - Unlimited server license means you can install the certificate on multiple servers at no extra cost
  - Trusted by all major browsers and operating systems
  - Meets and exceeds PCI Compliance requirements for TLS certificates

2.2 Request Endpoint

When using this endpoint, the {product_name_id} must be added to the request URL. Currently, we accept the following values for the Standard DV Certificate product_name_id:

- ssl_dv_rapidssl
- ssl_dv_geotrust

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/{product_name_id}

2.3 Request Body

This endpoint accepts a request body in one of the following formats:

- application/json
- application/xml

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.

- **dcv_emails Parameter**

  This parameter, if included in the request body, is used to specify the email address where the DCV email will be sent to for validating the domain.

  Items to Note:

  - The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

  - We will only send the DCV email to the addresses specified. For example, if you specify john.doe@[domain_name], we will not send DCV emails to any of the constructed email addresses. Or if you specify

admin@[domain.com], we will not send the DCV email to john.doe@[domain_name].

If you do not include this parameter in the request body, we will send emails to any emails address (e.g., administrator and technical contacts) we find in the domain's WHOIS record and to the five constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and postmaster @[domain_name]).

- **locale Parameter**

  This parameter, if included in the request body, is used to determine the language for the Domain Control Validation (DCV) emails.

  If this parameter is not included in the request body, the language for the DCV emails will default to English.

- **SHA256 Signing Algorithm**

  The signature_hash value is not included in a DV certificate request as only SHA256 signature hash is supported for DV certificates.

- **dns_names Parameter**

  The GeoTrust brand offers a single domain DV certificate that can become a multi-domain DV certificate.

  This parameter, if included in your GeoTrust Standard DV certificate request (product_name_id = ssl_dv_geotrust), allows you to list the additional SANs you want included in the certificate.

  Note: Adding SANs to a GeoTrust Standard DV certificate order may incur additional cost.

2.4 JSON Request Parameters

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 FQDNs (up to 250) to be secured in the GeoTrust Standard DV Certificate Adding SANs to a GeoTrust Standard DV certificate

Parameter Name	Required/ Optional	Allowed Values	Default	Description
				order may incur additional cost. **Note:** This parameter will only work for the **ssl_dv_geotrust** product_name_id.
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. If not included in the request, it defaults to other.
id	Required	[int]		The id of the server platform.
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 in section 2.3 Request Body
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters in section 2.3 Request Body.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.

Parameter Name	Required/ Optional	Allowed Values	Default	Description
technical_contact	Optional	[object]		Person we will contact should problems arise with processing the certificate order.
first_name	Required	[string]		First name of the technical contact for the order.
last_name	Required	[string]		Last name of the technical contact for the order.
email	Optional	[string]		Email address at which the technical contact can be reached.
job_title	Optional	[string]		Technical contact's job title.
telephone	Required	[int]		Phone number at which the technical contact can be reached.
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.
dcv_method	Optional	[string]	email	The Domain Control Validation (DCV) method used to demonstrate control of the domain. **dcv_method values:** • email • dns-txt-token • http-token **Note:** If this parameter is not included in the request, it defaults to the email (Email DCV method).

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 to **profile**. Otherwise, it will default to **balance**.
locale	Optional	Reference: Appendix: Locale Type Values		Determines the language for the DCV emails.
alternative_order_id	Optional	[int]		An alternative order id that associates this order to a customer account, id, etc. in your records.
dcv_emails	Optional	[array]		
dns_name	Required	[string]		The domain on the order that you want to validate.
email	Required	[string]		The email address (e.g., john.doe@example.com, hostmaster@example.com) you want us to send the authorization email to. **Note:** The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

2.5 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier.
certificate_id	[int]	Customer order id.

Parameter Name	Data Type	Description
dcv_random_value	[string]	The unique DNS random value used to validate domain control for dns-txt-token and http-token DCV Methods.

2.6 Example Request

Endpoint

When using this endpoint, the {product_name_id} must be added to the request URL. Currently, we accept the following values for product_name_id for Standard DV SSL certificates:

- ssl_dv_rapidssl
- ssl_dv_geotrust

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

Headers

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

Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "example.com",
    "dns_names": [
       "anotherexample.com",
       "secondexample.com",
       "yetanotherexample.com"
    ],
    "csr": "------ [CSR HERE] ------",
    "server_platform": {
      "id": 45
    }
  },
  "validity_years": 2,
  "disable_renewal_notifications": true,
  "technical_contact": {
    "first_name": "Jane",
    "last_name": "Doe",
    "email": "jane.doe@example.com",
    "job_title": "IT Admin",
    "telephone": "555-555-5555"
```

JSON (application/json)

```
  },
  "dcv_method": "email",
  "locale": "en",
  "alternative_order_id": "76ab8",
  "dcv_emails": [
    {
      "dns_name": "example.com",
      "email": "john.doe@example.com"
    }
  ]
}
```

2.7 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

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

Body

JSON (application/json)

Response with email dcv_method:

```
{
    "id": 1234,
    "certificate_id": 4321
}
```

Response with a DCV method that generates a random value (dns-txt-token, http-token):

```
{
    "id": 1234,
    "certificate_id": 4321,
    "dcv_random_value": "icru1984rnekfj"
}
```

3 Order a Wildcard DV Certificate

3.1 Submitting Order - Order Wildcard DV Certificate

Currently, the *Order Wildcard DV Certificate* endpoints allow those using the DigiCert Services API to order two types of Wildcard DV certificates: GeoTrust Wildcard DV and RapidSSL Wildcard DV.

- **GeoTrust Wildcard DV**

Protect your website with RSA 2048+ encryption or ECC 256+ keys and SHA2-256 signature algorithm.

  - Secure your domain and all same level subdomains (*.[yourdomain].com)
  - Also secures the parent domain (*.[yourdomain].com)
  - Add SANs to secure multiple wildcard domains (e.g., *.[yourdomain], *.[seconddomain].com, and *.[thirddomain].com) on one certificate (Adding SANs to a GeoTrust Wildcard DV certificate order may incur additional cost.)
  - Unlimited server license means you can install the certificate on multiple servers at no extra cost
  - Trusted by all major browsers and operating systems
  - Meets and exceeds PCI Compliance requirements for TLS certificates

- **RapidSSL Wildcard DV**
  Protect your website with RSA 2048+ encryption or ECC 256+ keys and SHA2-256 signature algorithm.

  - Secure your domain and all same level subdomains (*.[yourdomain].com)
  - Also secures the parent domain (*.[yourdomain].com)
  - Unlimited server license means you can install the certificate on multiple servers at no extra cost
  - Trusted by all major browsers and operating systems
  - Meets and exceeds PCI Compliance requirements for TLS certificates

3.2 Request Endpoint

When using this endpoint, the {product_name_id} must be added to the request URL. Currently, we accept the following values for the Wildcard DV Certificate product_name_id:

- wildcard_dv_rapidssl
- wildcard_dv_geotrust

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/{product_name_id}

3.3 Request Body

This endpoint accepts a request body in one of the following formats:

- application/json
- application/xml

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.

- **dcv_emails Parameter**

  This parameter, if included in the request body, is used to specify the email address where the DCV email will be sent to for validating the domain.

  Items to Note:

  - The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).
  - We will only send the DCV email to the addresses specified. For example, if you specify john.doe@[domain_name], we will not send DCV emails to any of the constructed email addresses. Or if you specify admin@[domain.com], we will not send the DCV email to john.doe@[domain_name].

  If you do not include this parameter in the request body, we will send emails to any emails address (e.g., administrator and technical contacts) we find in the domain's WHOIS record and to the five constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and postmaster @[domain_name]).

- **locale Parameter**

  This parameter, if included in the request body, is used to determine the language for the Domain Control Validation (DCV) emails.

If this parameter is not included in the request body, the language for the DCV emails will default to English.

- **SHA256 Signing Algorithm**

  The signature_hash value is not included in a DV certificate request as only the SHA256 signature hash is supported for DV certificates.

- **dns_names Parameter**

  The GeoTrust brand offers a Wildcard DV certificate that can become a multi-wildcard-domain DV certificate. What this means is that you can include multiple Wildcard domains (e.g., *.[yourdomain].com, *.[yourdomain1].com, etc.) on the GeoTrust Wildcard DV certificate.

  Note: You can only add Wildcard domains (e.g., *.[yourdomain].com). You cannot add non-Wildcard domains (e.g., ~~[yourdomain].com~~).

  This parameter, if included in your GeoTrust Wildcard DV certificate request (product_name_id = wildcard_dv_geotrust), allows you to list the additional Wildcard SANs you want included in the certificate.

  Note: Adding Wildcard SANs to a GeoTrust Wildcard DV certificate order may incur additional cost.

3.4 JSON Request Parameters

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 (up to 250) to be secured in the GeoTrust Wildcard DV Certificate Adding SANs to a GeoTrust Wildcard DV certificate order may incur additional cost. **Note:** This parameter will only work for the **wildcard_dv_geotrust** product_name_id.
csr	Required	[string]		Certificate Signing Request. To create a CSR

Parameter Name	Required/ Optional	Allowed Values	Default	Description
				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. If not included in the request, it defaults to other.
id	Required	[int]		The id of the server platform.
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 in section 3.3 Request Body
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters in section 3.3 Request Body.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.
technical_contact	Optional	[object]		Person we will contact should problems arise with processing the certificate order.
first_name	Required	[string]		First name of the technical contact for the order.

Parameter Name	Required/ Optional	Allowed Values	Default	Description
last_name	Required	[string]		Last name of the technical contact for the order.
email	Optional	[string]		Email address at which the technical contact can be reached.
job_title	Optional	[string]		Technical contact's job title.
telephone	Required	[int]		Phone number at which the technical contact can be reached.
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.
dcv_method	Optional	[string]	email	The Domain Control Validation (DCV) method used to demonstrate control of the domain. **dcv_method values:** • email • dns-txt-token • http-token **Note:** If this parameter is not included in the request, it defaults to the email (Email DCV method).
payment_method	Optional	balance, card, profile	balance	How to pay for the certificate. If there is a default payment profile, it will default to **profile**. Otherwise, it will default to **balance**.

Parameter Name	Required/ Optional	Allowed Values	Default	Description
locale	Optional	Reference: Appendix: Locale Type Values		Determines the language for the DCV emails.
alternative_order_id	Optional	[int]		An alternative order id that associates this order to a customer account, id, etc. in your records.
dcv_emails	Optional	[array]		
dns_name	Required	[string]		The domain on the order that you want to validate.
email	Required	[string]		The email address (e.g., john.doe@example.com, hostmaster@example.com) you want us to send the authorization email to. **Note:** The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

3.5 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier.
certificate_id	[int]	Customer order id.
dcv_random_value	[string]	The unique DNS random value used to validate domain control for dns-txt-token and http-token DCV Methods.

3.6 Example Request

Endpoint

When using this endpoint, the {product_name_id} must be added to the request URL. Currently, we accept the following values for product_name_id for Wildcard DV SSL certificates:

- wildcard_dv_rapidssl
- wildcard_dv_geotrust

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

Headers

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

Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "*.example.com",
    "dns_names": [
       "*.anotherexample.com",
       "*.secondexample.com",
       "*.thirdexample.com"
    ],
    "csr": "------ [CSR HERE] ------",
    "server_platform": {
      "id": 45
    }
  },
  "validity_years": 2,
  "disable_renewal_notifications": true,
  "technical_contact": {
    "first_name": "Jane",
    "last_name": "Doe",
    "email": "jane.doe@example.com",
    "job_title": "IT Admin",
    "telephone": "555-555-5555"
  },
  "dcv_method": "email",
  "locale": "en",
  "alternative_order_id": "76ab8",
  "dcv_emails": [
    {
      "dns_name": "example.com",
      "email": "john.doe@example.com"
    }
  ]
}
```

3.7 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

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

Body

JSON (application/json)

Response with email dcv_method:

```
{
    "id": 1234,
    "certificate_id": 4321
}
```

Response with a DCV method that generates a random value (dns-txt-token, http-token):

```
{
    "id": 1234,
    "certificate_id": 4321,
    "dcv_random_value": "icru1984rnekfj"
}
```

4 Order a Cloud DV Certificate

4.1 Submitting Order - Order GeoTrust Cloud DV Certificate

Currently, the *Order Cloud DV Certificate* endpoint allows those using the DigiCert Services API to order a GeoTrust Cloud DV Certificate.

GeoTrust Cloud DV Certificates let you secure multiple domains (example.com) and wildcard domains (*.example.com) with one certificate. Ideal for cloud service providers and hosting companies

Protect your website with RSA 2048+ encryption or ECC 256+ keys and SHA2-256 signature algorithm.

- Include a domain or wildcard domain in the common name field
- Add SANs to secure multiple domains and wildcard domains on one certificate (Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost.)
- Unlimited server license means you can install the certificate on multiple servers at no extra cost
- Trusted by all major browsers and operating systems
- Meets and exceeds PCI Compliance requirements for TLS certificates

4.2 Request Endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/cloud_dv_geotrust

4.3 Request Body

This endpoint accepts a request body in these formats:

- application/json
- application/xml

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.

- **dcv_emails Parameter**

  This parameter, if included in the request body, is used to specify the email address where the DCV email will be sent for validating the domain.

  Items to Note:

  - The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).
  - We will only send the DCV email to the addresses specified. For example, if you specify john.doe@[domain_name], we will not send DCV emails to any of the constructed email addresses. Or if you specify

admin@[domain.com], we will not send the DCV email to john.doe@[domain_name].

If you do not include this parameter in the request body, we will send emails to any emails address (e.g., administrator and technical contacts) we find in the domain's WHOIS record and to the five constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and postmaster @[domain_name]).

- **locale Parameter**

  This parameter, if included in the request body, is used to determine the language for the Domain Control Validation (DCV) emails.

  If this parameter is not included in the request body, the language for the DCV emails will default to English.

- **SHA256 Signing Algorithm**

  The signature_hash value is not included in a DV certificate request as only the SHA256 signature hash is supported for DV certificates.

- **dns_names Parameter**

  This parameter allows you to list the additional SANs (domains and wildcard domains) you want included in the certificate.

  Note: Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost.

4.4 JSON Request Parameters

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 (up to 250) to be secured in the GeoTrust Cloud DV Certificate Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost. **Note:** You can use the Cloud DV certificate to secure multiple

Parameter Name	Required/ Optional	Allowed Values	Default	Description
				domains and wildcard domains on one 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. If not included in the request, it defaults to other.
id	Required	[int]		The id of the server platform.
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 in section 4.3 Request Body
validity_days	Optional	[int]		Number of days for which the certificate is valid. See Certificate Validity Parameters in section 4.3 Request Body.
disable_renewal_notifications	Optional	[bool]	false	To turn off renewal notifications for this certificate, you must set this value to **true**.
technical_contact	Optional	[object]		Person we will contact should problems arise with processing the certificate order.

Parameter Name	Required/ Optional	Allowed Values	Default	Description
first_name	Required	[string]		First name of the technical contact for the order.
last_name	Required	[string]		Last name of the technical contact for the order.
email	Optional	[string]		Email address at which the technical contact can be reached.
job_title	Optional	[string]		Technical contact's job title.
telephone	Required	[int]		Phone number at which the technical contact can be reached.
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.
dcv_method	Optional	[string]	email	The Domain Control Validation (DCV) method used to demonstrate control of the domain. **dcv_method values:** • email • dns-txt-token • http-token **Note:** If this parameter is not included in the request, it defaults to the email (Email DCV method).
payment_method	Optional	balance, card, profile	balance	How to pay for the certificate. If there is a default payment profile, it will

Parameter Name	Required/ Optional	Allowed Values	Default	Description
				default to **profile**. Otherwise, it will default to **balance**.
locale	Optional	Reference: Appendix: Locale Type Values		Determines the language for the DCV emails.
alternative_order_id	Optional	[int]		An alternative order id that associates this order to a customer account, id, etc. in your records.
dcv_emails	Optional	[array]		
dns_name	Required	[string]		The domain on the order that you want to validate.
email	Required	[string]		The email address (e.g., john.doe@example.com, hostmaster@example.com) you want us to send the authorization email to. **Note:** The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

4.5 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier.
certificate_id	[int]	Customer order id.
dcv_random_value	[string]	The unique DNS random value used to validate domain control for dns-txt-token and http-token DCV Methods.

4.6 Example Request

Endpoint

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

Headers

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

Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "*.example.com",
    "dns_names": [
       "anotherexample.com",
       "*.secondexample.com",
       "thirdexample.com",
       "*.fourth.example.com"
    ],
    "csr": "------ [CSR HERE] ------",
    "server_platform": {
      "id": 45
    }
  },
  "validity_years": 2,
  "disable_renewal_notifications": true,
  "technical_contact": {
    "first_name": "Jane",
    "last_name": "Doe",
    "email": "jane.doe@example.com",
    "job_title": "IT Admin",
    "telephone": "555-555-5555"
  },
  "dcv_method": "email",
  "locale": "en",
  "alternative_order_id": "76ab8",
  "dcv_emails": [
    {
      "dns_name": "example.com",
      "email": "john.doe@example.com"
    }
  ]
}
```

4.7 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

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

Body

JSON (application/json)

Response with email dcv_method:

```
{
    "id": 1234,
    "certificate_id": 4321
}
```

Response with a DCV method that generates a random value (dns-txt-token, http-token):

```
{
    "id": 1234,
    "certificate_id": 4321,
    "dcv_random_value": "icru1984rnekfj"
}
```

5 Cancel DV Certificate Order

5.1 Cancel a Certificate Order Endpoint

Use the **Cancel a Certificate Order** endpoint update the status of a pending DV certificate order to Canceled (this effectively cancels the order).

Note: Currently, this endpoint only allows you to change the status of the order to **CANCELED**.

5.2 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/order/certificate/{order_id}/status

5.3 Request Body

This endpoint accepts a request body in the following formats:

1. application/json
2. application/xml

5.4 JSON Request Parameters

Parameter Name	Required / Optional	Allowed Values	Default	Description
status	Required	[string]		Changes the status of the DV certificate order to [CANCELED]
note	Required	[string]		Required information about the DV certificate order's status change (i.e., reason for canceling the order) **Note:** This note appears on the email if you choose to set the **send_emails** parameter to **true**.
send_emails	Optional	[bool]	False	Send an email notification of the status change [true|false] **Note:** When set to true, this parameter allows you to send an email (with your note included in it) to the certificate requestor.

5.5 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2/order/certificate/1234/status
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-Type: application/json
Content-Length: 109
```

Body

JSON (application/json)

```
{
  "status": "CANCELED",
  "note": "required note for why the order is being canceled"
}
```

5.6 Example Response

Status Code: 204

When successful, this request returns a 204 OK status.

Body

None

6 Complete Domain Validation

After the order is submitted, you must prove control over the domain on the certificate order before DigiCert can issue the DV certificate. Here are the endpoints that you may need to complete domain validation for a certificate order:

- Get Domain Control Emails
- Resend DCV Emails
- Generate Random Value
- Check DCV
- Change DCV Method

6.1 Get Domain Control Emails

Use the **Get Domain Control Emails** endpoint to retrieve the domain emails for a domain (WHOIS-based and constructed), so that you can see where the DCV emails are sent.

6.1.1 Request Endpoint

Method	URL
GET	https://www.digicert.com/services/v2/domain/{domain_name}/dcv/emails

6.1.2 Request Body

This endpoint accepts a request body in the following formats:

1. application/json
2. application/xml

6.1.3 JSON Response Parameters

Parameter Name	Data Type	Description
name_scope	string	The domain name used to define the scope of the returned email addresses
base_emails	array	List of constructed email addresses for the domain
whois_emails	array	List of email addresses found in the domain's WHOIS record

6.1.4 Example Request

Endpoint

```
GET https://www.digicert.com/services/v2/domain/example.com/dcv/emails
```

Headers

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

Body

None

6.1.5 Example Response

Status Code: 200

When successful, this request returns a 200 OK status

Headers

```
Content-Type: application/json
Content-Length: 100
```

Body

JSON (application/json)

```
{
   "name_scope": "example.com",
   "base_emails": [
      "admin@example.support",
      "webmaster@example.support",
      "postmaster@example.support",
      "hostmaster@example.support",
      "administrator@example.support"
   ],
   "whois_emails": [
      "jaden.doe@digicert.com",
      "liam.tribel@digicert.com"
   ]
}
```

6.2 Resend DCV Emails

Use the **Resend Emails** endpoint to resend the Domain Control Validation (DCV) emails for a certificate order.

6.2.1 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/order/certificate/{order_id}/resend-emails

6.2.2 Request Body

This endpoint accepts a request body in the following formats:

1. application/json
2. application/xml

6.2.3 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2 /order/certificate/12345/resend-emails
```

Headers

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

6.2.4 Example Response

Status Code: 204

When successful, this request returns a 204 OK status.

Body

None

6.3 Generate Random Value

Use the **DCV Random Value** endpoint to generate a random value for the DNS TXT or File Auth DCV methods.

Note: Random values expire after 30 days.

6.3.1 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/order/certificate/{order_id}/dcv-random-value

6.3.2 Request Body

This endpoint accepts a request body in the following formats:

1. application/json
2. application/xml

6.3.3 JSON Response Parameters

Parameter Name	Data Type	Description
dcv_random_value	[string]	The random value that will be used to validate the domain for dns-txt-token and http-token DCV methods. This string is only returned when one of those DCV methods is used.

6.3.4 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2 /order/certificate/ 12345/dcv-random-value
```

Headers

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

Body

None

6.3.5 Example Response

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: application/json
Content-Length: 37
```

Body

JSON (application/json)

```
{
      "dcv_random_value": "fjqr7th5ds"
}
```

6.4 Check DCV

The Email DCV method is completed automatically when the email recipient clicks the link provided in the confirmation email sent for the domain.

For the DCV methods that require a random value (DNS TXT and File Auth), proof of control over the domain is completed using the **Check DCV** endpoint.

Use the **Check DCV** endpoint on pending DV certificate orders to complete Domain Control Validation (DCV) for a domain once the random value for dns-txt-token or http-token is in place(in the domain's DNS TXT record, or on the web page in the specified location, etc.).

6.4.1 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/order/certificate/{order_id}/check-dcv

6.4.2 Request Body

This endpoint accepts a request body in the following formats:

1. application/json
2. application/xml

6.4.3 JSON Response Parameters

Parameter Name	Data Type	Description
order_status	[string]	The status of the order statuses: • issued • pending
certificate_id	[int]	The certificate's identifier
dcv_status	[string]	The status of the DCV approval check: • valid • pending

6.4.4 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2 /order/certificate /12345/check-dcv
```

Headers

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

Body

None

6.4.5 Example Response

The response will include the order status and more detailed domain validation status.

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: application/json
Content-Length: 81
```

Body

JSON (application/json)

```
{
      "order_status": "pending",
      "certificate_id": 4321,
      "dcv_status": "valid"
}
```

6.5 Change Domain Control Validation (DCV) Method

Use the **Change DCV Method** endpoint to use a different validation method to demonstrate control over the domain in your pending DV certificate order (i.e., switch from using Email to DNS TXT DCV method).

6.5.1 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/order/certificate/{order_id}/dcv-method

6.5.2 Request Body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

6.5.3 JSON Request Parameters

Parameter Name	Required/ Optional	Allowed Values	Default	Description
dcv_method	Required	[string]		The name of the Domain Control Validation Method you want to use to validate the domain on your certificate order.

Parameter Name	Required/ Optional	Allowed Values	Default	Description
				dcv_method values: • email • dns-txt-token • http-token

6.5.4 JSON Response Parameters

The parameters in this table only apply the dns-txt-token and http-token DCV methods.

Parameter Name	Data Type	Description
dcv-random-value	[string]	The unique random value that will be used to prove control over the domain (i.e., placed in a DNS TXT record or on your web page in specified location). This string is only returned when one of those DCV methods is used.

6.5.5 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2 /order/certificate/ 12345/dcv-method
```

Headers

```
X-DC-DEVKEY:{api_key}
Content-Type: application/json
Content-Length: 26
```

Body

JSON (application/json)

email

```
{
      "dcv_method": "email"
{
```

dns-txt-token

```
{
      "dcv_method": "dns-txt-token"
{
```

http-token

```
{
```

JSON (application/json)

```
{
      "dcv_method": "http-token"
```

6.5.6 Example Responses

1. email Method

Status Code: 204

When successful, this request returns a 204 OK status.

Headers

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

Body

None

2. dns-txt-token and http-token DCV Methods

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: application/json
Content-Length: 37
```

Body

Both dns-txt-token and http-token return the same type of response that includes the random value needed to demonstrate control over the domain in your DV certificate order.

JSON (application/json)

```
{
      "dcv_random_value": "kfjadkjg2345"
}
```

7 Check Order Status Changes

7.1 Get Order Status Changes

Use the **Get Order Status Changes** endpoint to check on the status of all your certificate orders within a specified time range up to a week.

7.2 Request Endpoint

Enter the time range (in minutes) to check the changes in status of certificates in the last 10 minutes, the last 3 days, etc. (up to a week).

Note: Maximum time range is 1 week (10080 minutes).

We recommend adding 5 seconds to your time range to adjust for the time it takes to process and return the response.

Method	URL
GET	https://www.digicert.com/services/v2/order/certificate/status-changes?minutes={time_in_minutes}&seconds={time_in_seconds}

7.3 JSON Response Parameters

Parameter Name	Data Type	Description
order_id	[int]	The order's identifier
certificate_id	[int]	The certificate's identifier
status	[string]	Statuses: • pending • issued • revoked

7.4 Example Request

Endpoint

```
GET https://www.digicert.com/services/v2/order/certificate/status-changes?minutes=10&seconds=5
```

Headers

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

Body

None

7.5 Example Response

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: application/json
Content-Length: 181
```

Body

JSON (application/json)

```
{
    "orders": [
        {
            "order_id": 10,
            "certificate_id": 1,
            "status": "pending"
        },
        {
            "order_id": 11,
            "certificate_id": 2,
            "status": "issued"
        },
        {
            "order_id": 12,
            "certificate_id": 3,
            "status": "issued"
        }
    ]
}
```

8 Download Issued Certificate

8.1 Download a Certificate Endpoint

Use the **Download Certificate** endpoint to download a DV Certificate file from an order. By default, it uses the platform specified in the order.

8.1.1 Request Endpoint

Method	URL
GET	https://www.digicert.com/services/v2/certificate/{certificate_id}/download/platform

8.1.2 Example Request

Endpoint

```
GET https://www.digicert.com/services/v2/certificate/4321/download/platform
```

Headers

```
X-DC-DEVKEY:{api_key}
```

```
Accept: */*
```

Body

None

8.1.3 Example Response

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: */*
Content-Length: 108
```

Body

The certificate file is returned in the preferred format for the platform specified in the order (.pem, .p7b, .crt, etc.).

8.2 Download a Certificate by Platform

Use the **Download Certificate by Platform** endpoint to download a DV certificate file from an order using the platform specified in the request URL. A list of supported formats and platforms can be found in the Appendix: Certificate Formats.

8.2.1 Request Endpoint

Method	URL
GET	https://www.digicert.com/services/v2/certificate/{certificate_id}/download/platform/{platform_id}

8.2.2 Example Request

Endpoint

```
GET
https://www.digicert.com/services/v2/certificate/4321/download/platform/apache
```

Headers

```
X-DC-DEVKEY:{api_key}
Accept: */*
```

Body

None

8.2.3 Example Response

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: */*
Content-Length: 81
```

Body

The certificate file is returned in the preferred format for the platform specified (.pem, .p7b, .crt, etc.).

8.3 Download a Certificate by Format

Use the **Download Certificate by Format** endpoint to download a DV certificate file from an order using the format specified in the request URL for the platform specified in the order. A list of supported formats and platforms can be found in the Appendix: Certificate Formats.

8.3.1 Request Endpoint

Method	URL
GET	https://www.digicert.com/services/v2/certificate/{certificate_id}/download/format/{format_type}

8.3.2 Example Request

Endpoint

```
GET
https://www.digicert.com/services/v2/certificate/4321/download/format/p7b
```

Headers

```
X-DC-DEVKEY:{api_key}
Accept: */*
```

Body

None

8.3.3 Example Response

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: */*
Content-Length: 69
```

Body

The Certificate file is returned in the specified format (.pem, .p7b, .crt, etc.).

9 Reissue a Standard DV Certificate Order

If needed, you can use the **Reissue** endpoint to reissue your Standard DV certificate. This allows you to replace the existing certificate with a new one that has different information (e.g., common name, CSR, etc.).

9.1 Request Endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/{order_id}/reissue

9.2 Request Body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

Items to note about the request body parameters and DV certificate reissues:

- **Original certificate is revoked**

  When you reissue a certificate, the original certificate (or previous version of it) is revoked.

- **Technical contact**

  If you added a technical contact in the original order, that contact will be used for all subsequent reissues.

- **Complete Domain Control Validation (DCV)**

  Each time you reissue a DV certificate, you must complete domain validation (i.e., demonstrate control over the domain) for the domain on the order/reissue using one of the supported DCV methods. See Appendix: DCV Method Values.

- **dcv_emails Parameter**

  This parameter, if included in the request body, is used to specify the email address where the DCV email will be sent to for validating the domain.

  Items to Note:

- The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).
- We will only send the DCV email to the addresses specified. For example, if you specify john.doe@[domain_name], we will not send DCV emails to any of the constructed email addresses. Or if you specify admin@[domain.com], we will not send the DCV email to john.doe@[domain_name].

If you do not include this parameter in the request body, we will send emails to any emails address (e.g., administrator and technical contacts) we find in the domain's WHOIS record and to the five constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and postmaster @[domain_name]).

- **locale Parameter**

  This parameter, if included in the request body, is used to determine the language for the Domain Control Validation (DCV) emails.

  If this parameter is not included in the request body, the language for the DCV emails will default to English.

- **SHA256 Signing Algorithm**

  The signature_hash value is not included in a DV certificate request because only SHA256 is supported for DV certificates.

- **dns_names Parameter**

  The GeoTrust brand offers a single domain DV certificate that can become a multi-domain DV certificate.

  This parameter, if included in your GeoTrust Standard DV certificate reissue request, allows you to list the additional SANs you want included in the reissued certificate.

  Note: Adding SANs to a GeoTrust Standard DV certificate reissue may incur additional cost.

9.3 JSON Request Parameters

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_name	Optional	[array]		Additional FQDNs (up to 250) to be secured in the GeoTrust Standard DV certificate reissue. Adding SANs to a GeoTrust Standard DV certificate reissue may incur additional cost. **Note:** This parameter will only work for GeoTrust Standard DV Certificates.
csr	Required	[string]		Certificate Signing Request. To create a CSR from your server, visit the DigiCert Website (https://www.digicert.com/csr-creation.htm).
dcv_method	Optional	[string]	email	The Domain Control Validation (DCV) method used to show control of the domain. **dcv_method values:** • email • dns-txt-token • http-token **Note:** If this parameter is not included in the request, it defaults to email (Email DCV method).
server_platform	Optional	Reference: Server Platforms	-1	The server platform type. If not included in the request, it defaults to **Other**.
id	Required	[int]		The id of the server platform
locale	Optional	Reference: Locale Type Values		Determines the language for the DCV emails.

Parameter Name	Required/ Optional	Allowed Values	Default	Description
dcv_emails	Optional	[array]		
dns_name	Required	[string]		The domain on the order that you want to validate.
email	Required	[string]		The email address (e.g., john.doe@example.com, hostmaster@example.com) you want us to send the authorization email to. **Note:** The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

9.4 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier.
certificate_id	[int]	Customer order id.
dcv_random_value	[string]	The unique DNS random value used to validate domain control for dns-txt-token and http-token DCV Methods.

9.5 Example Request

Endpoint

```
POST https:/www.digicert.com/services/v2/order/certificate/12345/reissue
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-Type: application/json
Content-Length: 203
```

Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "example.com",
    "dns_names": [
      "anotherexample.com",
      "secondexample.com"
    ],
    "csr": "------ [CSR HERE] ------"
  }
}
```

9.6 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-Type: application/json
Content-Length: 55
```

Body

JSON (application/json)

```
{
    "id": 1234,
    "certificate_id": 4321,
    "dcv_random_value": "7mx003lr9900"
}
```

10 Reissue a Wildcard DV Certificate Order

If needed, you can use the **Reissue** endpoint to reissue your Wildcard DV certificate. This allows you to replace the existing certificate with a new one that has different information (e.g., common name, CSR, etc.).

10.1 Request Endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/{order_id}/reissue

10.2 Request Body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

Items to note about the request body parameters and DV certificate reissues:

- **Original certificate is revoked**

  When you reissue a certificate, the original certificate (or previous version of it) is revoked.

- **Technical contact**

  If you added a technical contact in the original order, that contact will be used for all subsequent reissues.

- **Complete Domain Control Validation (DCV)**

  Each time you reissue a DV certificate, you must complete domain validation (i.e., demonstrate control over the domain) for the domain on the order/reissue using one of the supported DCV methods. See Appendix: DCV Method Values.

- **dcv_emails Parameter**

  This parameter, if included in the request body, is used to specify the email address where the DCV email will be sent to for validating the domain.

  Items to Note:

  - The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).
  - We will only send the DCV email to the addresses specified. For example, if you specify john.doe@[domain_name], we will not send DCV emails to any of the constructed email addresses. Or if you specify admin@[domain.com], we will not send the DCV email to john.doe@[domain_name].

  If you do not include this parameter in the request body, we will send emails to any emails address (e.g., administrator and technical contacts) we find in the domain's WHOIS record and to the five constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and postmaster @[domain_name]).

- **locale Parameter**

  This parameter, if included in the request body, is used to determine the language for the Domain Control Validation (DCV) emails.

  If this parameter is not included in the request body, the language for the DCV emails will default to English.

- **SHA256 Signing Algorithm**

  The signature_hash value is not included in a DV certificate request because only SHA256 is supported for DV certificates.

- **dns_names Parameter**

  The GeoTrust brand offers a Wildcard DV certificate that can become a multi-wildcard-domain DV certificate. What this means is that you can include multiple Wildcard domains (e.g., *.[yourdomain].com, *.[anotherdomain].com, etc.) on the GeoTrust Wildcard DV certificate.

  Note: You can only add Wildcard domains (e.g., *.[yourdomain].com). You cannot add non-Wildcard domains (e.g., ~~[yourdomain].com~~).

  This parameter, if included in your GeoTrust Wildcard DV certificate request (product_name_id = wildcard_dv_geotrust), allows you to list the additional Wildcard SANs you want included in the certificate.

  Note: Adding Wildcard SANs to a GeoTrust Wildcard DV certificate order may incur additional cost.

10.3 JSON Request Parameters

Parameter Name	Required/ Optional	Allowed Values	Default	Description
certificate	Required	[object]		
common_name	Required	[string]		The name to be secured in the certificate
dns_name	Optional	[array]		Additional names (up to 250) to be secured in the GeoTrust Wildcard DV Certificate Adding SANs to a GeoTrust Wildcard DV certificate order may incur additional cost. **Note:** This parameter will only work for GeoTrust Wildcard DV Certificates.
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
dcv_method	Optional	[string]	email	The Domain Control Validation (DCV) method used to show control of the domain. **dcv_method values:** • email • dns-txt-token • http-token **Note:** If this parameter is not included in the request, it defaults to email (Email DCV method).
server_platform	Optional	Reference: Server Platforms	-1	The server platform type. If not included in the request, it defaults to **Other**.
id	Required	[int]		The id of the server platform
locale	Optional	Reference: Locale Type Values		Determines the language for the DCV emails.
dcv_emails	Optional	[array]		
dns_name	Required	[string]		The domain on the order that you want to validate.
email	Required	[string]		The email address (e.g., john.doe@example.com, hostmaster@example.com) you want us to send the authorization email to. **Note:** The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

10.4 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier.
certificate_id	[int]	Customer order id.
dcv_random_value	[string]	The unique DNS random value used to validate domain control for dns-txt-token and http-token DCV Methods.

10.5 Example Request

Endpoint

```
POST https:/www.digicert.com/services/v2/order/certificate/12345/reissue
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-Type: application/json
Content-Length: 203
```

Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "*.example.com",
    "dns_names": [
      "*.anotherexample.com",
      "*.secondexample.com"
    ],
    "csr": "------ [CSR HERE] ------"
  }
}
```

10.6 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-Type: application/json
Content-Length: 55
```

Body

JSON (application/json)

```
{
    "id": 1234,
    "certificate_id": 4321,
    "dcv_random_value": "7mx003lr9900"
}
```

11 Reissue a Cloud DV Certificate Order

If needed, you can use the **Reissue** endpoint to reissue your GeoTrust Cloud DV Certificate. This allows you to replace the existing certificate with a new one that has different information (e.g., common name, CSR, etc.).

11.1 Request Endpoint

Method	URL
POST	https://www.digicert.com/services/v2/order/certificate/{order_id}/reissue

11.2 Request Body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

Items to note about the request body parameters and DV certificate reissues:

- **Original certificate is revoked**

  When you reissue a certificate, the original certificate (or previous version of it) is revoked.

- **Technical contact**

  If you added a technical contact in the original order, that contact will be used for all subsequent reissues.

- **Complete Domain Control Validation (DCV)**

  Each time you reissue a DV certificate, you must complete domain validation (i.e., demonstrate control over the domain) for the domain on the order/reissue using one of the supported DCV methods. See Appendix: DCV Method Values.

- **dcv_emails Parameter**

  This parameter, if included in the request body, is used to specify the email address where the DCV email will be sent to for validating the domain.

Items to Note:

- The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).
- We will only send the DCV email to the addresses specified. For example, if you specify john.doe@[domain_name], we will not send DCV emails to any of the constructed email addresses. Or if you specify admin@[domain.com], we will not send the DCV email to john.doe@[domain_name].

If you do not include this parameter in the request body, we will send emails to any emails address (e.g., administrator and technical contacts) we find in the domain's WHOIS record and to the five constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and postmaster @[domain_name]).

- **locale Parameter**

  This parameter, if included in the request body, is used to determine the language for the Domain Control Validation (DCV) emails.

  If this parameter is not included in the request body, the language for the DCV emails will default to English.

- **SHA256 Signing Algorithm**

  The signature_hash value is not included in a DV certificate request because only SHA256 is supported for DV certificates.

- **dns_names Parameter**

  This parameter allows you to list the additional SANs (domains and wildcard domains) you want included in the certificate.

  Note: Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost.

11.3 JSON Request Parameters

Parameter Name	Required/ Optional	Allowed Values	Default	Description
certificate	Required	[object]		
common_name	Required	[string]		The name to be secured in the certificate

Parameter Name	Required/ Optional	Allowed Values	Default	Description
dns_name	Optional	[array]		Additional names (up to 250) to be secured in the GeoTrust Cloud DV Certificate Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost. **Note:** You can use the Cloud DV certificate to secure multiple domains and wildcard domains on one 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).
dcv_method	Optional	[string]	email	The Domain Control Validation (DCV) method used to show control of the domain. **dcv_method values:** • email • dns-txt-token • http-token **Note:** If this parameter is not included in the request, it defaults to email (Email DCV method).
server_platform	Optional	Reference: Server Platforms	-1	The server platform type. If not included in the request, it defaults to **Other**.
id	Required	[int]		The id of the server platform
locale	Optional	Reference: Locale Type Values		Determines the language for the DCV emails.
dcv_emails	Optional	[array]		

Parameter Name	Required/ Optional	Allowed Values	Default	Description
dns_name	Required	[string]		The domain on the order that you want to validate.
email	Required	[string]		The email address (e.g., john.doe@example.com, hostmaster@example.com) you want us to send the authorization email to. **Note:** The email address must be specified in the domain's WHOIS record or be one of the constructed email addresses for the domain (admin, administrator, webmaster, hostmaster, and/or postmaster @[domain_name]).

11.4 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier.
certificate_id	[int]	Customer order id.
dcv_random_value	[string]	The unique DNS random value used to validate domain control for dns-txt-token and http-token DCV Methods.

11.5 Example Request

Endpoint

```
POST https:/www.digicert.com/services/v2/order/certificate/12345/reissue
```

Headers

```
X-DC-DEVKEY: {api_key}
Content-Type: application/json
Content-Length: 203
```

Body

JSON (application/json)

```
{
  "certificate": {
    "common_name": "*.example.com",
    "dns_names": [
       "anotherexample.com",
       "*.secondexample.com",
       "thirdexample.com",
       "*.fourth.example.com"
    ],
    "csr": "------ [CSR HERE] ------"
  }
}
```

11.6 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-Type: application/json
Content-Length: 55
```

Body

JSON (application/json)

```
{
    "id": 1234,
    "certificate_id": 4321,
    "dcv_random_value": "7mx003lr9900"
}
```

12 Revoke an Issued DV Certificate

When needed, you can revoke an issued DV certificate. For example, you may need to revoke a certificate because the certificate is no longer needed, or because it's been determined that the certificate's private key has been compromised.

Two step revocation process

The DV certificate revocation process consists of two steps: 1) Submit a request to revoke a DV certificate and 2) An administrator approves (or rejects) the request and DigiCert revokes the DV certificate.

12.1 Submit a Request to Revoke an Issued DV Certificate

Use the Revoke a Certificate endpoint to submit a request to revoke an issued DV certificate.

Note: Before DigiCert can revoke the certificate, an account administrator must first approve the revocation request.

12.1.1 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/certificate/{certificate_id}/revoke

12.1.2 Request Body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

12.1.3 JSON Request Parameters

Parameter Name	Required / Optional	Allowed Values	Default	Description
comments	Optional	[string]		Comments about this revocation request that the approver will see

12.1.4 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	
date	[ISO 8601]	Date will be returned in the UT time zone, formatted in ISO 8601
type	[string]	Example type: revoke
status	[string]	Statuses: submitted, pending, approved, rejected
requestor	[object]	The user who make the request to have the DV certificate revoked
id	[int]	The user's identifier
first_name	[string]	The user's first name
last_name	[string]	The user's last name
email	[string]	The user's email address
Order	[object]	
id	[int]	The order's identifier

Parameter Name	Data Type	Description
container	[object]	
id	[int]	The container's identifier
comments	[string]	

12.1.5 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2/certificate/4321/revoke
```

Headers

```
X-DC-DEVKEY:{api_key}
Content-Type: application/json
Content-Length: 46
```

Body

JSON (application/json)

```
{
   "comments": "I no longer need this certificate."
}
```

12.1.6 Example Response

Status Code: 201

When successful, this request returns a 201 OK status.

Headers

```
Content-Type: application/json
Content-Length: 242
```

Body

JSON (application/json)

```
{
  "id": 4321,
  "date": "2016-02-10T17:06:15+00:00",
  "type": "revoke",
  "status": "submitted",
  "requester": {
    "id": 1234,
    "first_name": "Jane",
    "last_name": "Doe",
    "email": "jane.doe@example.com"
  },
  "order": {
     "id": 1111,
     "container": {
        "id": 2222
  },
  "comments": "I no longer need this certificate."
}
```

12.2 Approve a Revocation Request and Revoke an Issued DV Certificate

Use the **Update Request Status** endpoint to approve (or reject) a submitted DV certificate revocation request.

After someone submits a request to have a DV certificate revoked, an administrator must approve the revocation request. Once the request is approved, DigiCert can revoke the issued certificate.

Caution: Once completed, a certificate revocation cannot be reversed. A revoked DV certificate used on a public site shows trust warnings preventing users from accessing the site.

12.2.1 Request Endpoint

Method	URL
PUT	https://www.digicert.com/services/v2/request/{request_Id}/status

12.2.2 Request Body

This endpoint accepts a request body in the following formats:

- application/json
- application/xml

12.2.3 JSON Request Parameters

Parameter Name	Required / Optional	Allowed Values	Default	Description
status	Required	[string]		Statuses: submitted, pending, approved, reject
processor_comment	Optional	[string]		

12.2.4 Example Request

Endpoint

```
PUT https://www.digicert.com/services/v2/request/4321/status
```

Headers

```
X-DC-DEVKEY:{api_key}
Content-Type: application/json
Content-Length: 74
```

Body

JSON (application/json)

```
{
   "status": "approved",
   "process_comments": "Your certificate will be revoked."
}
```

12.2.5 Example Response

Status Code: 204

When successful, this request returns a 204 OK status.

Body

None

13 View Order Details

Use **View Order Details** endpoint to retrieve and view the details of a DV certificate order.

13.1 Request Endpoint

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

13.2 JSON Response Parameters

Parameter Name	Data Type	Description
id	[int]	The order's identifier
certificate	[object]	
id	[int]	The certificate's identifier
common_name	[string]	The name to be secured in the certificate
dns_names	[array]	Additional names in the certificate.
date_created	[ISO 8601 date]	Date will be returned in UTC time zone and formatted in ISO 8601.
valid_from	[date]	Date will be returned in format YYYY-MM-DD.
valid_till	[date]	Date will be returned in format YYYY-MM-DD.
csr	[string]	The certificate signing request (CSR) used to order the certificate.
signature_hash	[string]	The certificate's signing algorithm hash, for DV certificates only sha256 is supported.
key_size	[int]	
status	[string]	Order statuses include: pending, rejected, processing, issued, revoked, canceled, and needs_csr
is_renewal	[bool]	Identifies the order as a renewal or new order. true: order is a renewal. false: order is new.
is_renewed	[bool]	Identifies whether this order has been renewed. True: order was renewed False: order was not renewed.

Parameter Name	Data Type	Description
renewed_order_id	[int]	If this order is a renewal of a previous order, returns the previous order's id in this parameter
date_created	[ISO 8601 date]	Date will be returned in UTC time zone and formatted in ISO 8601.
disable_renewal_notifications	[bool]	If this is true, then no renewal notifications will be sent for the certificate.
container	[object]	
id	[int]	The container's identifier
name	[string]	The container's name
product	[object]	
name_id	[string]	Reference: Appendix: Product Display Name Values
name	[string]	The product's display name. Reference: Appendix: Product Display Name Values
type	[string]	type: ssl_certificate
disable_renewal_notifications	[bool]	If this is true, then no renewal notifications will be sent for the certificate.
technical_contact	[object]	
first_name	[string]	The technical contact's first name
last_name	[string]	The technical contact's last name
email	[string]	The technical contact's email address
job_title	Optional	[string]
telephone	[string]	The technical contact's telephone number

Parameter Name	Data Type	Description
user	[object]	
id	[int]	The user's identifier
first_name	[string]	The user's first name
last_name	[string]	The user's last name
email	[string]	The user's email address
receipt_id	[int]	The receipt id
allow_duplicates	[bool]	Whether or not the order allows duplicate certificates true: allows duplicate certificates false: does not allow duplicate certificates
payment_method	[string]	How to pay for the certificate. If there is a default payment profile, it will default to **profile**. Otherwise it'll default to **balance**. **payment_methods values:** • balance • card • profile
disable_ct	[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.
dcv_method	[string]	The Domain Control Validation (DCV) method used to show control of the domain. **dcv_method values:** • email

Parameter Name	Data Type	Description
		• dns-txt-token • http-token
alternative_order_id	[int]	An alternative order id that associates this order to a customer account, id, etc. in your records.
product_name_id	[string]	The certificate's product identifier: **product_name_id values:** • ssl_dv_geotrust • ssl_dv_rapidssl

13.3 Example Request

Endpoint

```
GET https://www.digicert.com/services/v2/order/certificate/4321
```

Headers

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

Body

None

13.4 Example Response

Status Code: 200

When successful, this request returns a 200 OK status.

Headers

```
Content-Type: application/json
Content-Length: 2342
```

Body

JSON (application/json)

```
{
    "id": 3093202,
    "certificate": {
        "id": 3464629,
```

JSON (application/json)


```
        "common_name": "example.com",
        "dns_names": [
            "anotherexample.com",
            "secondexample.com"
        ],
        "date_created": "2018-06-20T13:57:37+00:00",
        "valid_from": "2018-06-20",
        "csr": " ----- [CSR HERE] -----",
        "signature_hash": "sha256",
        "key_size": 2048
    },
    "status": "pending",
    "is_renewed": false,
    "date_created": "2018-06-20T13:57:37+00:00",
    "validity_years": 2,
    "container": {
        "id": 938,
        "name": "My Company, Inc."
    },
    "product": {
        "name_id": "ssl_dv_rapidssl",
        "name": "RapidSSL Standard DV",
        "type": "dv_ssl_certificate"
    },
    "technical_contact": {
        "first_name": "Jane",
        "last_name": "Doe",
        "telephone": "555-555-5555"
    },
    "user": {
        "id": 1542,
        "first_name": "John",
        "last_name": "Doe",
        "email": "john.doe@example.com"
    },
    "allow_duplicates": false,
    "is_out_of_contract": true,
    "payment_method": "balance",
    "product_name_id": "ssl_dv_rapidssl",
    "disable_issuance_email": false,
    "disable_ct": false,
    "dcv_method": "email",
    "alternative_order_id": "1212"
}
```


14 Appendix: Server Platform IDs

Server Platform	ID
Apache	2
BEA Weblogic 8 & 9	42

Server Platform	ID
Barracuda	41
Bea Weblogic 7 and older	29
Cisco	30
Citrix (Other)	39
Citrix Access Essentials	46
Citrix Access Gateway 4.x	50
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

Server Platform	ID
Microsoft IIS 8	67
Microsoft Live Communications Server 2005	37
Microsoft Lync Server 2010	59
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

15 Appendix: DCV Method Values

email (default)
http-token
dns-txt-token

16 Appendix: Locale Type Values

en - English (default)
de – German
fr - French
it - Italian
es - Spanish
pt - Portuguese
jp - Japanese
zh_cn – Simplified Chinese
zh_tw – Traditional Chinese
kr – Korean
ru – Russian

17 Appendix: Certificate Format Values

Certificate Format	Description
p7b	A p7b bundle of all the certificates (primary, intermediate, and root) in a .p7b file.
cer	A p7b bundle of all the certificates (primary, intermediate, and root)with a .cer extension.
pem_all	A single .pem file containing all the certificates (primary, intermediate, and root).
pem_noroot	A single .pem file containing the primary and intermediate certificates.
pem_nointermediate	A single .pem file containing only the primary certificate.
default_cer	Individual .crt files (primary, intermediate, and root) with a .cer extension (zipped).
default_pem	Individual .crt files (primary, intermediate, and root) with a .pem extension (zipped).
Default	Individual .crt files (primary, intermediate, and root) with a .crt extension (zipped).
apache	Separate primary and intermediate .crt files (zipped)

18 Appendix: Product Display Name Values

Name ID	Display Name
ssl_dv_rapidssl	RapidSSL Standard DV
wildcard_dv_rapidssl	RapidSSL Wildcard DV
ssl_dv_geotrust	GeoTrust Standard DV
wildcard_dv_geotrust	GeoTrust Wildcard DV
cloud_dv_geotrust	GeoTrust Cloud DV

19 Appendix: Use dns-txt-token to Validate a Domain

The DNS TXT DCV method (dns-txt-token) allows you to demonstrate control over a domain on your DV certificate order by creating a DNS TXT record containing a randomly generated value. Once the DNS TXT record is created, you can use the Check DCV endpoint to confirm presence of the random value in your domain's DNS records and complete domain control validation.

How to Use the DNS TXT DCV Method for a Domain

1. There are three ways a random value can be generated for use to demonstrate control over your domain:
    - Using the **Order Standard DV Certificate** endpoint (one-time random value generation).
    - Using the **Change DCV Method** endpoint (one-time random value generation).
    - Using the **Generate Random Value** endpoint (regenerate random value as needed).

      Note: The unique random value expires after thirty days.
2. **Create Your DNS TXT Record:**
    a. Go to your DNS provider's site and create a new TXT record.
    b. In the **TXT Value** field, paste the randomly generated value.
    c. **Host** field
        - Base Domain

          If you are validating the base domain, leave the **Host** field blank, or use the @ symbol (depending on your DNS provider requirements).

- Subdomain

  In the **Host** field, enter the subdomain that you are validating.

d. In the record type field (or equivalent), select **TXT**.

e. Select a Time-to-Live (TTL) value or use your DNS provider's default value.

f. Save the record.

3. Once the DNS TXT record is created, use the **Check DCV** endpoint to confirm the presence of the random value.

20 Appendix: Use http-token to Validate a Domain

The File Auth DCV method (http-token) allows you to demonstrate control over your domain by hosting a .txt file containing a randomly generated value at a predetermined location on your website. Make sure to avoid some of the more Common Mistakes.

Once the .txt file is created and placed on your site, you can use the Check DCV endpoint to confirm presence of the random value at the specified URL and complete domain control validation.

How to Use the File Auth DCV Method for a Domain

1. There are three ways a random value can be generated for use to demonstrate control over your domain:

   - Using the **Order Standard DV Certificate** endpoint (one-time random value generation).
   - Using the **Change DCV Method** endpoint (one-time random value generation).
   - Using the **Generate Random Value** endpoint (regenerate random value as needed).

     Note: The unique random value expires after thirty days.

2. **Create Your fileauth.txt File:**

   a. Open a text editor (such as Notepad) and paste in the random value for the domain.

   b. Save the file as fileauth.txt file.

3. **Create the .well-known/pki-validation/ Directory**

Create the .well-known/pki-validation/ directory on your site and place your fileauth.txt file in it. You need to make the file available at ***[domain name]/.well-known/pki-validation/fileauth.txt***

Note: On Windows-based servers, the .well-known folder must be created via command line (mkdir .well-known).

4. Once the fileauth.txt file containing the random value has been added to your website at ***[domain name]/.well-known/pki-validation/fileauth.txt***, use the **Check DCV** endpoint to confirm the presence of the random value on your website.

Common Mistakes

To validate your domain using the File Auth DCV method, you need two items: 1) a random value (provided by DigiCert), and 2) the URL or location where you need to place the fileauth.txt file containing the random value on your website (e.g., http://example.com]/.well-known/pki-validation/fileauth.txt).

The URL (http://[yourdomain.com]/.well-known/pki-validation/fileauth.txt) does two things:

- It contains the FQDN (fully qualified domain name) of the domain you want us to validate.
- It tells us where to look so that we can find the fileauth.txt file you add the generated random value to.

Below are some of the more common issues we run into when troubleshooting the reason File Auth checks fail. The File Auth DCV process was designed to keep an unauthorized individual from using a domain they do control to validate and get a certificate for a domain they don't control, such as one of yours.

Don't Modify the URL Provided

If you modify the URL in any way (change to the FQDN, capitalize a lowercase letter, forget to add a period, etc.), we won't find the fileauth.txt file with our generated random value in it.

For example, with this URL: [http://yourdomain.com]/.well-known/pki-validation/fileauth.txt, **don't** add **www** to it ([http://]~~www~~.yourdomain.com]/.well-known/pki-validation/fileauth.txt) or capitalize a letter that wasn't capitalized in the original URL ([http://[yourdomain.com]/.well-known/~~PKI~~-validation/fileauth.txt).

Don't Place the fileauth.txt File on a Different Domain or Subdomain

To complete domain control validation for yourdomain.com, place the fileauth.txt file on the exact domain you want validated; the one on your certificate order. We won't look at

a different domain or subdomain to find the random value. We only look at the domain you want validated (i.e., the domain on your certificate order).

For example, if you need example.com validated so that you can request SSL/TLS certificates for it, you will use this URL for this domain - http://example.com/.well-known/pki-validation/fileauth.txt. Don't place the fileaut.txt file on sub.example.com or modify the URL and place it on yourotherdomain.com - it won't work. We can't find the fileaut.txt file on these domains - only on example.com.

example.com and www.example.com

If you want us to validate www.example.com and examle.com, place the fileauth.txt file on example.com. This validates both example.com and www.example.com. We won't look at www.example.com to find the fileauth.txt file.

Free Base Domain SAN

If you received a free base domain SAN on your SSL/TLS certificate, make sure to place the fileauth.txt file on the base domain. We need to validate the domain on the SSL/TLS certificate order.

Don't Include Any Additional Content in the fileauth.txt File

When you create the fileauth.txt file, copy the DigiCert provided random value and paste it in the file. Don't add the word "token", "value" or any other text.

Because we only read the first 2kb of the fileauth.txt file, additional text blocks us from validating your control over the domain.

Don't Place the fileauth.txt File on a Page with Multiple Redirects

When using the File Auth method for domain validation, the fileauth.txt file may be placed on a page that contains up to one redirect. With a single redirect, we are still able to locate the fileauth.txt file and verify your control over the domain.

For example, you need a certificate for http://example.com, but the page redirects to https://www.example.com. That's okay. You can place the fileauth.txt file on the http://example.com page. We will still be able to follow the single redirect to validate your control over http://example.com.

However, if you place the fileauth.txt file on a page with multiple redirects, we won't be able to locate the file. Multiple redirects block us from locating the fileauth.txt file and validating your control over the domain.

For example, you need a certificate for http://multiple-redirect.com, but the page redirects to https://www.multiple-redirect.com and then redirects again to https://www.single-redirect.com. In this case, you must still place the fileauth.txt file on the http://multiple-redirect.com page. However, you will need to disable the second

redirect (https://www.single-redirect.com) long enough for us to locate the fileauth.txt and validate your control over http://multiple-redirect.com.

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