DigiCert® DV Certificate Enrollment

Last updated Jan. 17, 2019

DigiCert® DV Certificate Enrollment

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Document creation date: Jan. 17, 2019

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way Ste. 500
Lehi, Utah, 84043
https://www.digicert.com
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

By default, DV certificate products aren't included in your CertCentral account. To get DV certificates added to the SSL/TLS certificate options in your CertCentral account, contact your account representative.

The DV certificate lifecycle includes the following steps:

1. **Order DV certificates**
   RapidSSL and GeoTrust DV certificates are available in CertCentral: RapidSSL Standard DV, RapidSSL Wildcard DV, GeoTrust Standard DV, GeoTrust Wildcard DV, and GeoTrust Cloud DV.
2. **Cancel DV certificate orders**
   When needed, you can cancel a pending DV certificate order, before we issue the certificate.
3. **Check DV certificate order status**
   Check the status of your DV certificate orders.
4. **Complete domain control validation (DCV)**
   Before DigiCert can issue your DV certificate, you must prove control over the domains on the order. Supported DCV methods for DV certificate orders: Email, DNS TXT, and File
5. **Access issued DV certificates**
   To access an issued DV certificate, download it from your CertCentral account. You can also email the certificate from inside your account.
6. **Reissue DV certificates**
   Reissue a DV certificate to replace the existing certificate with a new one that has different information (e.g., SANs, CSR, etc.).
7. **Cancel reissues on DV certificates**
   When needed, you can cancel a pending reissue request on a DV certificate, before we issue the certificate.
8. **Revoke DV certificates**
   When necessary, you can revoke an issued DV certificate. Certificate revocation is a two step process: 1) submit a certificate revocation request and 2) administrator approves the revocation request and DigiCert revokes the certificate.

To download a pdf version of the guide, click CertCentral DV Certificate Enrollment Guide.

Ordering DV Certificates

The certificate lifecycle begins when administrators and users log into their account and request DV certificates for their domains. CertCentral account users can only request the types of certificates that have been authorized for their account (their company/organization).

Prerequisites

Before you can begin ordering DV SSL/TLS certificates, your sales representative must enable DV certificates for your CertCentral account. Then, on the **Product Settings** page (**Settings > Product Settings**), you can enable the DV certificate products (e.g., GeoTrust Standard DV).

Depending on the structure of your account, you may be able to request the following types of DV certificates:

- **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.example.com, example.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

---

- **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 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.example.com, example.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

---

- **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

---

- **GeoTrust Cloud DV**
  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

Order a RapidSSL Standard DV Certificate

Use these instructions to order a RapidSSL Standard DV Certificate.

Info: A Certificate Signing Request (CSR) is required to complete the order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. For information about creating a CSR, see Create a CSR (Certificate Signing Request).
2. **Select the DV Certificate You Want to Order**
   a. In your CertCentral account, in the sidebar menu, click **Request a Certificate** and then under All Products, click **Product Summary**.
   b. On the Request a Certificate page, select **DV Certificates**.
   c. On the DV Certificates tab, select **RapidSSL Standard DV** and then click **Order Now**.
3. **Add Your CSR**
   We take the common name included in your CSR and add it to the **Common Name** field.

   On the Request RapidSSL Standard DV Certificate page, in the Certificate Details section, use one of the options below to add your CSR.

   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box.
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
4. **Common Name**
   When you add the CSR to the order form, we take the common name included in the CSR and add it to the **Common Name** box.

   To add or change the common name, manually enter the domain you want this DV certificate to secure.
5. **Include both www.[your-domain].com and [your-domain].com in the certificate**

   When ordering a RapidSSL Standard DV certificate, we will include [your-domain].com and www.[your-domain].com in your certificate.

   To only secure the version of the domain entered in the **Common Name** box, uncheck **Include both www.[your-domain].com and [your-domain].com in the certificate**.
6. **Validity Period**
   Select a validity period for the certificate.

Info: Industry standards dictate that the maximum validity period for all public SSL/TLS certificates is **2 Years**.

7. **Advanced Certificate Options**

   SHA-256 is the only hash algorithm available for DV certificates.

8. **Select a DCV Method to Prove Control Over Your Domain**

   Before DigiCert can issue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

   In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

   - **DNS TXT (recommended)**
     The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
   - **Email**
     The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
   - **File**
     The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your certificate order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

9. **Select the Language for the DCV Email**

   In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

   Note that this drop-down list only appears when you select **Email** as your DCV method.

10. **Add a Technical Contact**
    Adding a technical contact is optional.

    However, we recommend adding a person we can contact should problems arise with processing the certificate order.

    a. In the Order Details section, under Contacts, in the **Technical Contact** box, click the **Add Contact** link.
    b. In the Add Contact window, provide the contact's information (first and last name, job title, phone, and email) and then click **Submit.**

11. **Notes and Certificate Renewal Message**

Adding notes and a certificate renewal message is optional.

a. Expand **Notes / Renewal Message**.
b. **Comments to Administrator**
   Add a note to the order that only an Administrator can see (e.g., *why the certificate is needed*).
c. **Order Specific Renewal Message**
   Create an order specific renewal message right now.

> **Note:** Comments and renewal messages are not included in the certificate.

12. **Select Payment Method**
    Under **Payment Information**, select a payment method to pay for the certificate:

    a. **Pay with Contract Terms**
       Have a contract and want to use it to pay for the certificate?
       Note: When you have a contract, it is the default payment method.
    b. **Pay with Credit Card**
       Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
    c. **Pay with Account Balance**
       Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
       To deposit funds, click the **Deposit** link.

> **Info:** The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

13. **Certificate Service Agreement**

    Read through the agreement and check **I agree to the Certificate Services Agreement**.

14. When you are finished entering your DV order information, click **Submit Certificate Request**.

Order a RapidSSL Wildcard DV Certificate

Use these instructions to order a RapidSSL Wildcard DV Certificate.

> **Info:** A Certificate Signing Request (CSR) is required to complete the order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. For information about creating a CSR, see Create a CSR (Certificate Signing Request).

2. **Select the DV Certificate You Want to Order**
    a. In your CertCentral account, in the sidebar menu, click **Request a Certificate** and then under All Products, click **Product Summary**.
    b. On the Request a Certificate page, select **DV Certificates**.
    c. On the DV Certificates tab, select **RapidSSL Wildcard DV** and then click **Order Now**.
3. **Add Your CSR**
    We take the common name included in your CSR and add it to the **Common Name** field.
    On the Request RapidSSL Wildcard DV Certificate page, in the Certificate Details section, use one of the options below to add your CSR.
    a. **Click to upload a CSR**
        Click the link to upload your CSR file to the **Add Your CSR** box.
    b. **Paste CSR**
        Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
4. **Common Name**
    When you add the CSR to the order form, we take the common name included in the CSR and add it to the **Common Name** box.

    To add or change the common name, manually enter the domain you want this DV certificate to secure.

Info: Make sure to format the common name correctly (*.example.com).

5. **Include both *.[your-domain].com and [your-domain].com in the certificate**

    When ordering a RapidSSL Wildcard DV certificate, we will include the base domain in your certificate.

    To only secure the wildcard domain entered in the **Common Name** box, uncheck **Include both *.[your-domain].com and [your-domain].com in the certificate**.

6. **Validity Period**
    Select a validity period for the certificate.

Info: Industry standards dictate that the maximum validity period for all public SSL/TLS certificates is **2 Years**.

7. **Advanced Certificate Options**

    SHA-256 is the only hash algorithm available for DV certificates.

8. **Select a DCV Method to Prove Control Over Your Domain**

    Before DigiCert can issue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

- **DNS TXT (recommended)**
  The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
- **Email**
  The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
- **File**
  The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your certificate order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

9. **Select the Language for the DCV Email**

   In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

   Note that this drop-down list only appears when you select **Email** as your DCV method.

10. **Add a Technical Contact**
    Adding a technical contact is optional.

    However, we recommend adding a person we can contact should problems arise with processing the certificate order.

    a. In the Order Details section, under Contacts, in the Technical Contact box, click the **Add Contact** link.
    b. In the Add Contact window, provide the contact's information (first and last name, job title, phone, and email) and then click **Submit.**

11. **Notes and Certificate Renewal Message**
    Adding notes and a certificate renewal message is optional.

    a. Expand **Notes / Renewal Message**.
    b. **Comments to Administrator**
       Add a note to the order that only an Administrator can see (e.g., *why the certificate is needed*).
    c. **Order Specific Renewal Message**
       Create an order specific renewal message right now.

Info: Comments and renewal messages are not included in the certificate.

12. **Select Payment Method**
    Under **Payment Information**, select a payment method to pay for the certificate:
    a. **Pay with Contract Terms**
       Have a contract and want to use it to pay for the certificate?
       Note: When you have a contract, it is the default payment method.
    b. **Pay with Credit Card**
       Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
    c. **Pay with Account Balance**
       Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
       To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

13. **Certificate Service Agreement**
    Read through the agreement and check **I agree to the Certificate Services Agreement**.
14. When you are finished entering your DV order information, click **Submit Certificate Request**.

Order a GeoTrust Standard DV Certificate

Use these instructions to order a GeoTrust Standard DV Certificate.

GeoTrust Standard DV Certificates use Subject Alternative Names (SANs) to let you secure one or up to 250 domains. The base price includes only one Fully Qualified Domain Names (FQDN). Adding SANs to a GeoTrust Standard DV certificate order may incur additional cost.

Info: A Certificate Signing Request (CSR) is required to complete the order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. For information about creating a CSR, see Create a CSR (Certificate Signing Request).
2. **Select the DV Certificate You Want to Order**
   a. In your CertCentral account, in the sidebar menu, click **Request a Certificate** and then under All Products, click **Product Summary**.
   b. On the Request a Certificate page, select **DV Certificates**.
   c. On the DV Certificates tab, select **GeoTrust Standard DV** and then click **Order Now**.

3. **Add Your CSR**
   We take the common name and any SANs included in your CSR and add them to the **Common Name / SANs** field.

   On the Request GeoTrust Standard DV Certificate page, in the Certificate Details section, use one of the options below to add your CSR.

   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box.
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
4. **Common Name / SANs**
   We take the common name and any SANs included in your CSR and add it to the **Common Name / SANs** box.

   Add, remove, and reorder SANs as needed so the certificate will secure the domains that you want.

Note: Base price includes **one** FQDN. Adding SANs to a GeoTrust Standard DV certificate order may incur additional cost.

5. **Validity Period**
   Select a validity period for the certificate.

Info: Industry standards dictate that the maximum validity period for all public SSL/TLS certificates is **2 Years**.

6. **Advanced Certificate Options.**

   SHA-256 is the only hash algorithm available for DV certificates.

7. **Select a DCV Method to Prove Control Over Your Domain**

   Before DigiCert can issue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

   In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

   You must use the selected DCV method to prove control over every domain on the order.

   - **DNS TXT (recommended)**
     The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
   - **Email**
     The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.

- **File**
  The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your certificate order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

8. **Select the Language for the DCV Email**

   In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

   Note that this drop-down list only appears when you select **Email** as your DCV method.

9. **Add a Technical Contact**

   Adding a technical contact is optional.

   However, we recommend adding a person we can contact should problems arise with processing the certificate order.

   a. In the Order Details section, under Contacts, in the Technical Contact box, click the **Add Contact** link.
   b. In the Add Contact window, provide the contact's information (first and last name, job title, phone, and email) and then click **Submit.**

10. **Notes and Certificate Renewal Message**
    Adding notes and a certificate renewal message is optional.

    a. Expand **Notes / Renewal Message**.
    b. **Comments to Administrator**
       Add a note to the order that only an Administrator can see (e.g., *why the certificate is needed*).
    c. **Order Specific Renewal Message**
       Create an order specific renewal message right now.

Note: Comments and renewal messages are not included in the certificate.

11. **Select Payment Method**
    Under **Payment Information**, select a payment method to pay for the certificate:

    a. **Pay with Contract Terms**
       Have a contract and want to use it to pay for the certificate?
       Note: When you have a contract, it is the default payment method.
    b. **Pay with Credit Card**
       Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.

c. **Pay with Account Balance**
Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

12. **Certificate Service Agreement**
Read through the agreement and check **I agree to the Certificate Services Agreement**.
13. When you are finished entering your DV order information, click **Submit Certificate Request**.

Order a GeoTrust Wildcard DV Certificate

Use these instructions to order a GeoTrust Wildcard DV Certificate.

GeoTrust Wildcard DV Certificates use Subject Alternative Names (SANs) to let you secure one or up to 250 domains. The SANs must be a wildcard domain (*.example.com) or based off your listed wildcard domains (mail.example.com).

The base price includes only one Fully Qualified Domain Names (FQDN). Adding SANs to a GeoTrust Wildcard DV certificate order may incur additional cost.

Info: A Certificate Signing Request (CSR) is required to complete the order.

1. **Create a Certificate Signing Request**
To remain secure, certificates must use at least a 2048-bit key size. For information about creating a CSR, see Create a CSR (Certificate Signing Request).
2. **Select the DV Certificate You Want to Order**
    a. In your CertCentral account, in the sidebar menu, click **Request a Certificate** and then under All Products, click **Product Summary**.
    b. On the Request a Certificate page, select **DV Certificates**.
    c. On the DV Certificates tab, select **GeoTrust Wildcard DV** and then click **Order Now**.
3. **Add Your CSR**
We take the common name and any SANs included in your CSR and add them to the **Common Name / SANs** field.
On the **Request GeoTrust Wildcard DV Certificate** page, in the **Certificate Details** section, use one of the options below to add your CSR.
    a. **Click to upload a CSR**
    Click the link to upload your CSR file to the **Add Your CSR** box.
    b. **Paste CSR**
    Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW**

CERTIFICATE REQUEST----- and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.

4. **Common Name / SANs**

   We take the common name and any SANs included in your CSR and add them to the **Common Name / SANs** field.

   Add, remove, and reorder SANs as needed so the certificate will secure the domains that you want.

> **Note:** The SANs must be a wildcard domain (*.example.com) or based off your listed wildcard domains (mail.example.com).

> **Note:** Base price includes **one** FQDN. Adding SANs to a GeoTrust Wildcard DV certificate order may incur additional cost.

5. **Validity Period**

   Select a validity period for the certificate.

> **Info:** Industry standards dictate that the maximum validity period for all public SSL/TLS certificates is **2 Years**.

6. **Advanced Certificate Options**

   SHA-256 is the only hash algorithm available for DV certificates.

7. **Select a DCV Method to Prove Control Over Your Domain**

   Before DigiCert can issue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

   In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

   You must use the selected DCV method to prove control over every domain on the order.

   - **DNS TXT (recommended)**
     The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
   - **Email**
     The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
   - **File**
     The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your certificate order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

8. **Select the Language for the DCV Email**

   In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

   Note that this drop-down list only appears when you select **Email** as your DCV method.

9. **Add a Technical Contact**
   Adding a technical contact is optional.

   However, we recommend adding a person we can contact should problems arise with processing the certificate order.

   a. In the Order Details section, under Contacts, in the Technical Contact box, click the **Add Contact** link.
   b. In the Add Contact window, provide the contact's information (first and last name, job title, phone, and email) and then click **Submit.**

10. **Notes and Certificate Renewal Message**
    Adding notes and a certificate renewal message is optional.

    a. Expand **Notes / Renewal Message**.
    b. **Comments to Administrator**
       Add a note to the order that only an Administrator can see (e.g., *why the certificate is needed*).
    c. **Order Specific Renewal Message**
       Create an order specific renewal message right now.

Note: Comments and renewal messages are not included in the certificate.

11. **Select Payment Method**
    Under **Payment Information**, select a payment method to pay for the certificate:

    a. **Pay with Contract Terms**
       Have a contract and want to use it to pay for the certificate?
       Note: When you have a contract, it is the default payment method.
    b. **Pay with Credit Card**
       Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
    c. **Pay with Account Balance**
       Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
       To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

12. **Certificate Service Agreement**

    Read through the agreement and check **I agree to the Certificate Services Agreement**.

13. When you are finished entering your DV order information, click **Submit Certificate Request**.

Order a GeoTrust Cloud DV Certificate

Use these instructions to order a GeoTrust Cloud DV Certificate.

GeoTrust Cloud DV Certificates use Subject Alternative Names (SANs) to let you secure multiple domains (example.com) and wildcard domains (*.example.com) with one certificate.

The base price includes only one Fully Qualified Domain Names (FQDN). Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost.

Info: A Certificate Signing Request (CSR) is required to complete the order.

1. **Create a Certificate Signing Request**

   To remain secure, certificates must use at least a 2048-bit key size. For information about creating a CSR, see Create a CSR (Certificate Signing Request).

2. **Select the DV Certificate You Want to Order**

   a. In your CertCentral account, in the sidebar menu, click **Request a Certificate** and then under All Products, click **Product Summary**.
   b. On the Request a Certificate page, select **DV Certificates**.
   c. On the DV Certificates tab, select **GeoTrust Cloud DV** and then click **Order Now**.

3. **Add Your CSR**

   We take the common name and any SANs included in your CSR and add them to the **Common Name / SANs** field.

   On the Request GeoTrust Cloud DV Certificate page, in the Certificate Details section, use one of the options below to add your CSR.

   a. **Click to upload a CSR**

      Click the link to upload your CSR file to the **Add Your CSR** box.

   b. **Paste CSR**

      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.

4. **Common Name / SANs**

   We take the common name and SANs included in your CSR and add them to the **Common Name / SANs** field. The SANs can be domains ([yourdomain.com]) and wildcard domains (*.[yourdomain].com).

Add, remove, and reorder SANs as needed so the certificate will secure the domains that you want.

Note: Base price includes **one** FQDN. Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost.

5. **Validity Period**
   Select a validity period for the certificate.

Info: Industry standards dictate that the maximum validity period for all public SSL/TLS certificates is **2 Years**.

6. **Advanced Certificate Options.**

   SHA-256 is the only hash algorithm available for DV certificates.

7. **Select a DCV Method to Prove Control Over Your Domain**

   Before DigiCert can issue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

   In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

   You must use the selected DCV method to prove control over every domain on the order.

   - **DNS TXT (recommended)**
     The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
   - **Email**
     The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
   - **File**
     The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your certificate order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

8. **Select the Language for the DCV Email**

   In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

Note that this drop-down list only appears when you select **Email** as your DCV method.

9. **Add a Technical Contact**
   Adding a technical contact is optional.

   However, we recommend adding a person we can contact should problems arise with processing the certificate order.

   a. In the Order Details section, under Contacts, in the Technical Contact box, click the **Add Contact** link.
   b. In the Add Contact window, provide the contact's information (first and last name, job title, phone, and email) and then click **Submit.**
10. **Notes and Certificate Renewal Message**
    Adding notes and a certificate renewal message is optional.

    a. Expand **Notes / Renewal Message**.
    b. **Comments to Administrator**
       Add a note to the order that only an Administrator can see (e.g., *why the certificate is needed*).
    c. **Order Specific Renewal Message**
       Create an order specific renewal message right now.

Note: Comments and renewal messages are not included in the certificate.

11. **Select Payment Method**
    Under **Payment Information**, select a payment method to pay for the certificate:

    a. **Pay with Contract Terms**
       Have a contract and want to use it to pay for the certificate?
       Note: When you have a contract, it is the default payment method.
    b. **Pay with Credit Card**
       Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
    c. **Pay with Account Balance**
       Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
       To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

12. **Certificate Service Agreement**

    Read through the agreement and check **I agree to the Certificate Services Agreement**.
13. When you are finished entering your DV order information, click **Submit Certificate Request**.

Canceling a DV Certificate Order

Use these instructions to cancel a **pending** DV certificate order.

> **Note:** You can only cancel **pending** certificate orders. Once the order has been issued, you need to revoke the certificate order if it is no longer needed.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the filters and the advanced search features to locate the **pending** DV certificate order you want to cancel.
3. In the Order # column of the certificate order, click the order number link.
4. On the Order details page, in the Certificate Details section, in the **Certificate Actions** drop-down list, select **Cancel Order**.
5. In the Cancel Order window, click **Cancel Order**.

> **Info:** Canceling an order successfully removes it from our system and can't be undone. However, if the certificate ends up being needed, simply place the order again.

6. Congratulations! You have successfully canceled the order.

> **Note:** The canceled order is logged in the **Audit Logs** (in the sidebar menu, click **Account > Audit Logs**).

Domain Control Validation (DCV) Methods

Before DigiCert can issue a certificate, you must prove control over the domains and any SANs (Subject Alternative Names) on the order. We refer to this process as the Domain Control Validation (DCV) process.

DV certificates don't support domain pre-validation. Therefore, each time you order a DV certificate, you must demonstrate control over the domains on the order. After your order has been placed, you need to complete domain validation before DigiCert can issue your DV certificate.

Info: Certificates won't be issued until domain validation is completed

For DV certificates in CertCentral, DigiCert currently supports the following DCV Methods: WHOIS-based Email, Constructed Email, , DNS TXT, and File.

Email Validation

With this validation method, DigiCert sends two sets of DCV emails: WHOIS-based and Constructed. To demonstrate control over the domain, an email recipient follows the instructions in a confirmation email sent for the domain. The confirmation process consists of visiting the link provided in the email and following the instructions on the page.

WHOIS-based Email validation

For the WHOIS-based method, DigiCert sends an authorization email to the registered owners of the public domain as shown in the domain's WHOIS record.

Note: Are you expecting to receive an email at an address published in your domain's WHOIS record? Please verify that your registrar/WHOIS provider has not masked or removed that information. If they are, find out if they provide a way (e.g., anonymized email address, web form) for you to allow CAs to access your domain's WHOIS data.

Constructed Email Validation

For the Constructed Email method, DigiCert sends the authorization email to five constructed email addresses for the domain: admin, administrator, webmaster, hostmaster, and postmaster @[domain_name].

Note: When you register a domain, you must provide identifying and contact information (e.g., administrative and technical contacts). Instead of using a personal email address, you can also use one of the constructed email addresses for your domain (e.g., webmaster@yourdomain.com). Using one of the constructed email addresses allows you to create a "non-expiring" email address that you can add or remove people from when necessary.

If we can't find an MX record for [domain_name], you must use one of the other supported DCV methods to demonstrate your control over the domain.

MX Records (Mail Exchanger Records)

Before we can successfully send an authentication email (DCV Email) to the domain owner (or domain controller), we must verify that an MX record (a resource record in the Domain Name System [DNS]) exists in the DNS records of the recipient's domain name. The presence of valid MX records enables us to send the authentication email.

For example, you want to receive your DCV email at one of the constructed email addresses for example.com, admin@example.com. To successfully send a DCV Email to admin@example.com, we must first find an MX record for said address that identifies the server (e.g., mailhost.example.com) set up to receive the emails destined for admin@example.com

If we find an MX record, we can successfully send a DCV email to admin@example.com. If we don't find an MX record, no DCV email is sent because we cannot identify the proper mail server.

DNS TXT Validation

With this validation method, you add a DigiCert generated random value (provided for the domain in your CertCentral account) to the domain's DNS as a TXT record. When DigiCert does a search for DNS TXT records associated with the domain, we can find a record where the record's value includes the DigiCert random value.

File Validation

With this validation method, you host a file containing a DigiCert generated random value (provided for the domain in your CertCentral account) at a predetermined location on your website: **[domain]/.well-known/pki-validation/fileauth.txt**. Once the file is created and placed on your site, DigiCert visits the specified URL to confirm the presence of our random value.

Use the Email DCV method

Use these instructions to check the status of your DV certificate order and to send or resend the DCV emails.

> **Info:** When ordering your DV certificate, if you chose Email as your DCV method, DigiCert already sent the verification emails. Before resending the DCV emails, make sure to check your inbox and junk/spam folder for emails with the subject **[Action Required] Approve Certificate Request for [yourdomain] {Order #}**.

With the Email validation method, we send two sets of DCV emails: WHOIS-based and Constructed (see Domain Control Validation (DCV) Methods).

To demonstrate control over the domain, an email recipient follows the instructions in a confirmation email sent for the domain. The confirmation process consists of visiting the link provided in the email and following the instructions on the page.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the filters and advanced search features to locate the pending DV certificate order.
3. In the Order # column for the pending certificate order, click the order number link.
4. On the Order # details page, in the Order Status section, check the order's validation status (is the order waiting on domain validation to be completed?).
5. Under You Need To, click the **Prove Control Over Domain** link.
6. In the Prove control of your domain window, complete the following steps to resend the DCV verification email:
    a. In the **DCV verification method** drop-down list, select **Email**.
    b. In the **Send authorization email to** drop-down list, select the email address you want the DCV email sent to.
    Multiple domains on the order:
        i. In the Domain validation must be completed… box, click the **Change email recipients for each domain** link.
        ii. In the Prove control of your domain window, under Send authorization email to, select the email address you want the DCV email to be sent to for each domain.
        Note: To resend/send the DCV email to all email addresses found in the WHOIS record as well as to the constructed emails for the domain, don't select an email address for the domain. When you click **Resend Emails**, we send the emails to all email addresses discovered for the domain.
        iii. Click **Done**.
    c. In the Email language drop-down list, select the language for the email.
    d. In the Email details section, note the subject of the email being sent and the order #.
    Important: The order # in the subject of the email is actually the certificate ID. On the Order

details page, in the Order Details section, the **Certificate ID** is next to DCV method and Requested On.

e. Click **Resend Email**.

7. To locate emails, search your inbox for:

   a. Emails with the subject **[Action Required] Approve Certificate Request for [yourdomain] {Order #}**

   b. Emails with the domain names you are trying to validate on the order.

> **Note:** You may also need to check your junk/spam folder.

8. You can come back and resend the DCV emails as needed.

Use the DNS TXT DCV Method

Use these instructions to check the status of your DV certificate order, and then, to use the DNS TXT DCV method to demonstrate control over the domains on the order.

This validation method lets you demonstrate control over your domains by creating a DNS TXT record containing a DigiCert generated random value (provided for the domain in your CertCentral account).

After you've created the records, DigiCert searches for DNS TXT records on the domains to confirm the presence of your random value.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the filters and advanced search features to locate the pending DV certificate order.
3. In the Order # column for the pending certificate order, click the order number link.
4. On the Order # details page, in the Order Status section, check the order's validation status (is the order waiting on domain validation to be completed?).
5. Under You Need To, click the **Prove Control Over Domain** link.
6. In the Prove control of your domain window, in the **DCV verification method** drop-down list, select **DNS TXT (recommended)**.
7. **Create the DNS TXT record for the domain**

   If your order includes multiple domains, create a DNS TXT record for each domain on the order before running the check.

   a. In the Copy this random valid to paste in your TXT record box, copy your random value. If your order includes multiple domains, add this random value to each domain's DNS TXT record.
   Note: The random value expires after thirty days.

b. Go to your DNS provider's site and create a new TXT record.
c. In the TXT Value field, enter the random value you copied from your CertCentral account.
d. Host field
    i. Base domain (for example, [yourdomain].com)
    Are you validating the base domain? Leave the Host field blank or add the @ symbol (depending on your DNS provider requirements).
    ii. Subdomain (for example, [your.domain].com)
    Are you validating a subdomain? In the Host field, add the subdomain you are validating.
e. In the record type filed (or equivalent), select **TXT**.
f. Select a Time-to-Live (TTL) value or use your DNS provider's default value.
g. Save the record.

Warning: Does your order include multiple domains? Create a DNS TXT record for each domain on the order first -- before you run the check. If any domains are missing a DNS TXT record containing the DigiCert provided random value, the "check" will fail.

8. **Verify the DNS TXT record**
    a. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.
    b. On the Orders page, in the Order # column of the DV certificate order, click the order number link.
    c. On the Order # details page, in the Order Status section, under You Need To, click the **Prove Control Over Domain** link.
    d. In the Prove control of your domain window, click **Check**.
9. Congratulations! You have completed the domain validation for the domains.

Use the File DCV Method

Use these instructions to check the status of your DV certificate order, and then, to use the File DCV method to demonstrate control over the domains on the order.

The File DCV method allows you to demonstrate control over your domain by hosting a .txt file containing a DigiCert generated random value (provided for the domain in your CertCentral account) at a predetermined location on your website.

Once the file is created and placed on your site, DigiCert visits the specified URL to confirm the presence of your random value. Make sure to avoid some of the more common mistakes -- File DCV method common mistakes.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the filters and advanced search features to locate the pending DV certificate order.
3. In the Order # column for the pending certificate order, click the order number link.
4. On the Order # details page, in the Order Status section, check the order's validation status (is the order waiting on domain validation to be completed?).
5. Under You Need To, click the **Prove Control Over Domain** link.
6. In the Prove control of your domain window, in the **DCV verification method** drop-down list, select **File**.
7. **Download your fileauth.txt file**

   Click the **Download fileauth.txt** link.

   If your order includes multiple domains, use this fileauth.txt file for each domain on the certificate order.

Note: The random value in the fileauth.txt file expires after thirty days.

8. **Create the [yourdomain.com]/.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 ***[yourdomain]/.well-known/pki-validation/fileauth.txt***

Info: **Windows-based servers:** The .well-known folder must be created via command line (mkdir .well-known).

Warning: Does your order include multiple domains? Create the .well-known/pki-validation/ directories on the domains and place your fileauth.txt file on them in the specified locations first -- before you run the check. If any domain sites are missing a fileauth.txt file containing the DigiCert provided random value, the "check" will fail.

9. **Verify the fileauth.txt file**
   a. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.
   b. On the Orders page, in the Order # column of the DV certificate order, click the order number link.
   c. On the Order # details page, in the Order Status section, under **Y**ou Need To, click the **Prove Control Over Domain** link.

d. In the Prove control of your domain window, click **Check**.

10. Congratulations! You have completed the domain validation for the domain.

File DCV method common mistakes

To validate your domain using the File 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://[yourdomain.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 reasons the File check fails. The File 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 DigiCert provided URL

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 [yourdomain].com validated, you will use this URL for this domain: http://[yourdomain].com/.well-known/pki-validation/fileauth.txt. Don't place the fileaut.txt file on sub.[yourdomain].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. We are looking for it on [yourdomain].com, the domain from your certificate order.

example.com and www.example.com

If you want DigiCert 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 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 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 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.

Accessing a DV Certificate

After DigiCert issues your DV certificate, you can download it from inside your CertCentral account. You can also email the certificate from your account and select the delivery format: email attachment, plaintext inside the body of the mail, or download link in the body of the email.

Download a DV Certificate

After DigiCert issues your certificate, you may want to download the certificate to your server or workstation, so it can be installed.

1. On the server or workstation where you need to install the certificate, log into your CertCentral account.
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
3. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. In the Order # column, click the **Quick View** link for the DV certificate you want to download.
5. In the **Order** details pane (on the right), in the **Download Certificate As** drop-down list, select the format for your certificate.

   Make sure to note the location where you save the file.

   - **Best format for...**
     Download the certificate in the format recommended for the server software or software that was selected when ordering the certificate.
     Note: If a server platform or software was not specified during the order process, this option is not included in the drop-down list.
   - **.crt (best for Apache/Linux)**
     Download the certificate in a .crt format, best for Apache/Linux platforms.
   - **.p7b (best for Microsoft and Java)**
     Download the certificate in a .p7b format, best for Microsoft and Java platforms.
   - **More Options…**
     Continue to the next step.
6. **More Options**
   a. In the **Download Certificate As** drop-down list, select **More Options** to see more server platforms, file types, and to download a single certificate in the certificate chain.
      i. **Download a combined certificate file**
      In the Download Certificate window, in the Combined Certificate Files section, use one of these options to specify the format for and download your combined certificate file:
         - **Server Platform**
           In the drop-down list, select the server platform (e.g., tomcat) and click **Download**.
         - **File Type**
           In the drop-down list, select the file type (e.g., a single .pem file containing all the certs) and click **Download**.

ii. **Download an individual certificate file (server, intermediate, and Root)**
In the Individual Certificates section, download a single certificate file of any of the certificates you need.
- **Certificate**
Download the DV certificate.
- **Intermediate Certificate**
Download the intermediate certificate that was used to issue your DV certificate.
- **Root Certificate**
Download the root certificate that was used to issue your DV certificate's intermediate certificate.

b. Save the selected certificate file to your server or workstation, making sure to note the location.

Email a DV Certificate from Your CertCentral Account

Use these instructions to email a copy of a DV certificate to specified email addresses. You can also select the delivery format for the certificate: attachment, plaintext, or download link.

> **Note:** When you email a certificate, it is logged as an event in the audit log (in the sidebar menu, click **Account > Audit Logs**).

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. In the Order # column, click the **Quick View** link for the DV certificate you want to send out.
4. In the Order details pane (on the right), click the **Send Certificate** link.
5. In the Send Certificate window, in the Send Certificate To box, type the email addresses for the those you want to receive the certificate (comma separated).
6. Under Send Certificate As, select how you want the DV certificate sent.
   - **Attachment**
   Send the recipients the certificate as an attachment to the email.
   - **Plain Text**
   Send the recipients the certificate as plain text in the body of the email.
   - **Download Link**
   Send the recipients a link to a download page (where they can download the certificate) in the body of the email.

Info: The recipient doesn't need to be a "user" in your CertCentral to access the download page.

7. **Optional: Append custom message**
    a. To add a custom message to the certificate email, check this box.
    b. In the text box, type the message you want included in the email.
8. When you are finished, click **Send Certificate**.

Reissuing DV Certificates

Rapid SSL and GeoTrust DV brand certificates come with unlimited free reissues. Depending on the structure of your account, you may be able to reissue the following types of DV certificates:

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

Some reasons you may reissue your certificate include:

- Lost your private key
- Need to re-key your certificate.
- Need to change the domain on the certificate (for example, from *www.yourname.com* to *secure.yourname.com*).
- Need to add, remove, or change some of the SANs that are listed in your GeoTrust Standard DV Certificate.

Reissue a RapidSSL Standard DV Certificate

Use these instructions to reissue a RapidSSL Standard DV Certificate.

Info: A Certificate Signing Request (CSR) is required to complete the reissue order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. Need help creating a CSR? See Create a CSR (Certificate Signing Request).
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
3. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to find the RapidSSL DV certificate you want to reissue.
4. In the certificate's Order # column, click the **Quick View** link.
5. In the Order details pane (on the right side of the page), click the **Reissue Certificate** link.
6. **Add Your CSR**
   We take the common name included in your CSR and add it to the **Common Name** field.

   On the Reissue Certificate for Order page, use one of the options below to add your CSR.

   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box.
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
7. **Common Name**
   We take the common name included in your CSR and add it to the **Common Name** field.

   To add or change the common name, manually enter the domain you want this DV certificate to secure.

Important: Changing the common name when reissuing a RapidSSL Standard DV Certificate automatically revokes the original certificate and any previous reissues.

8. **Signature Hash**

   SHA-256 is the only signature hash available for DV certificates.
9. **Select a DCV Method to Prove Control Over Your Domain**

   Before DigiCert can reissue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

- **DNS TXT (recommended)**
  The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
- **Email**
  The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
- **File**
  The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your reissue order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

10. **Select the Language for the DCV Email**

    In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

    Note that this drop-down list only appears when you select **Email** as your DCV method.

11. **Reason for Reissue**
    Add a reason for the reissue that only an Administrator can see.

Note: These comments aren't included in the certificate.

12. When you are finished, click **Request Reissue**.

Reissue a RapidSSL Wildcard DV Certificate

Use these instructions to reissue a RapidSSL Standard DV Certificate.

Info: A Certificate Signing Request (CSR) is required to complete the reissue order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. Need help creating a CSR? See Create a CSR (Certificate Signing Request).
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.

3. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to find the RapidSSL DV certificate you want to reissue.
4. In the certificate's Order # column, click the **Quick View** link.
5. In the Order details pane (on the right side of the page), click the **Reissue Certificate** link.
6. **Add Your CSR**
   We take the common name included in your CSR and add it to the **Common Name** field.

   On the Reissue Certificate for Order page, use one of the options below to add your CSR.

   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box.
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
7. **Common Name**
   We take the common name included in your CSR and add it to the **Common Name** field.

   To add or change the common name, manually enter the wildcard domain you want this DV certificate to secure.

Note: Make sure to format the common name correctly (*.example.com)

Important: Changing the common name when reissuing a RapidSSL Wildcard DV Certificate will automatically revoke the original certificate and any previous reissues.

8. **Select Payment Method**
   Did you add SANs to the certificate reissue order? Under **Payment Information**, select a payment method to pay for the certificate.

   If you didn't add SANs, skip to the next step. You won't be charged for your reissue.

   a. **Pay with Contract Terms**
      Have a contract and want to use it to pay for the certificate?
      Note: When you have a contract, it is the default payment method.
   b. **Pay with Credit Card**
      Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
   c. **Pay with Account Balance**
      Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
      To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the reissue form won't be saved.

9. **Signature Hash**

   SHA-256 is the only signature hash available for DV certificates.

10. **Select a DCV Method to Prove Control Over Your Domain**

    Before DigiCert can reissue your DV certificate, you must demonstrate control over the domain on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

    In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domain on the certificate order.

    - **DNS TXT (recommended)**
      The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
    - **Email**
      The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
    - **File**
      The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your reissue order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

11. **Select the Language for the DCV Email**

    In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

    Note that this drop-down list only appears when you select **Email** as your DCV method.

12. **Reason for Reissue**
    Add a reason for the reissue that only an Administrator can see.

Note: These comments aren't included in the certificate.

13. When you are finished, click **Request Reissue**.

Reissue a GeoTrust Standard DV Certificate

Use these instructions to reissue a GeoTrust Standard DV Certificate.

GeoTrust Standard DV Certificates use Subject Alternative Names (SANs) to let you secure one or up to 250 domains. The base price includes only one Fully Qualified Domain Names (FQDN). Adding SANs to a GeoTrust Standard DV certificate order may incur additional cost.

Info: A Certificate Signing Request (CSR) is required to complete the reissue order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. Need help creating a CSR? See Create a CSR (Certificate Signing Request).
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
3. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to find the GeoTrust Standard DV certificate you want to reissue.
4. In the certificate's Order # column, click the **Quick View** link.
5. In the Order details pane (on the right side of the page), click the **Reissue Certificate** link.
6. **Add Your CSR**
   We take the common name and any SANs included in your CSR and add them to the **Common Name** and **Other Hostnames (SANs)** field.

   On the Reissue Certificate for Order page, use one of the options below to add your CSR.

   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box.
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
7. **Common Name**
   We take the common name included in your CSR and add it to the **Common Name** field.

   To add or change the common name, manually enter the domain you want this DV certificate to secure.

Important: Changing the common name when reissuing a GeoTrust Standard DV Certificate automatically revokes the original certificate and any previous reissues unless you add the old common name as a SAN on the reissued certificate. .

8. **Other Hostnames (SANs)**
   We take any SANs included in your CSR and add them to the **Other Hostnames (SANs)** field.

   Add, remove, and reorder SANs as needed so the certificate secures the domains that you want.

   a. **Add SANs**
      In the **Other Hostnames (SANs)** box, enter the additional SANs that you want included in the reissued certificate.

Adding SANs does not revoke the original certificate or previous reissues. However, adding SANs may incur additional charges for the certificate reissue.

b. **Remove SANs**
In the **Other Hostnames (SANs)** box, delete the SANs that you want to exclude in the reissued certificate.

Important: Removing SANs automatically revokes the original certificate or previous reissues.

9. **Select Payment Method**
Did you add SANs to the certificate reissue order? Under **Payment Information**, select a payment method to pay for the certificate.

If you didn't add SANs, skip to the next step. You won't be charged for your reissue.

a. **Pay with Contract Terms**
Have a contract and want to use it to pay for the certificate?
Note: When you have a contract, it is the default payment method.

b. **Pay with Credit Card**
Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.

c. **Pay with Account Balance**
Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

10. **Signature Hash**

SHA-256 is the only signature hash available for DV certificates.

11. **Select a DCV Method to Prove Control Over Your Domain**
Before DigiCert can reissue your DV certificate, you must demonstrate control over the domains on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domains on the certificate order.

You must use the selected DCV method to prove control over every domain on the order.

- **DNS TXT**
The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
- **Email**
The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.

- **File**
  The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your reissue order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

12. **Select the Language for the DCV Email**

    In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

    Note that this drop-down list only appears when you select **Email** as your DCV method.

13. **Reason for Reissue**
    Add a reason for the reissue that only an Administrator can see.

Note: These comments are not included in the certificate.

14. When you are finished, click **Request Reissue**.

Reissue a GeoTrust Wildcard DV Certificate

Use these instructions to reissue a GeoTrust Wildcard DV Certificate.

GeoTrust Wildcard DV Certificates use Subject Alternative Names (SANs) to let you secure one or up to 250 domains. The SANs must be a wildcard domain (*.example.com) or based off your listed wildcard domains (mail.example.com). Adding SANs to a GeoTrust Wildcard DV certificate order may incur additional cost.

Info: A Certificate Signing Request (CSR) is required to complete the reissue order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. Need help creating a CSR? See Create a CSR (Certificate Signing Request).
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
3. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to find the GeoTrust Wildcard DV certificate you want to reissue.
4. In the certificate's Order # column, click the **Quick View** link.
5. In the Order details pane (on the right side of the page), click the **Reissue Certificate** link.

6. **Add Your CSR**
   We take the common name and any SANs included in your CSR and add them to the **Common Name** and **Other Hostnames (SANs)** field.

   On the Reissue Certificate for Order page, use one of the options below to add your CSR.

   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box.
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
7. **Common Name**
   We take the common name included in your CSR and add it to the **Common Name** field.

   To add or change the common name, manually enter the domain you want this DV certificate to secure.

Note: Make sure to format the common name correctly (*.example.com).

Important: Changing the common name when reissuing a GeoTrust Wildcard DV certificate automatically revokes the original certificate and any previous reissues, unless you add the old common name as a SAN on the reissued certificate.

8. **Other Hostnames (SANs)**
   We take any SANs included in your CSR and add them to the **Other Hostnames (SANs)** field.

   Add, remove, and reorder SANs as needed so the certificate secures the domains that you want.

   a. **Add SANs**
      In the **Other Hostnames (SANs)** box, enter the additional SANs that you want included in the reissued certificate.
      Adding SANs does not revoke the original certificate or previous reissues. However, adding SANs may incur additional charges for the certificate reissue.
   b. **Remove SANs**
      In the **Other Hostnames (SANs)** box, delete the SANs that you want to exclude in the reissued certificate.

Note: The SANs must be a wildcard domain (*.example.com) or based off your listed wildcard domains (mail.example.com).

Important: Removing SANs automatically revokes the original certificate or previous reissues.

9. **Select Payment Method**
   Did you add SANs to the certificate reissue order? Under **Payment Information**, select a payment method to pay for the certificate.

If you didn't add SANs, skip to the next step. You won't be charged for your reissue.

a. **Pay with Contract Terms**
   Have a contract and want to use it to pay for the certificate?
   Note: When you have a contract, it is the default payment method.
b. **Pay with Credit Card**
   Don't have a contract or don't want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
c. **Pay with Account Balance**
   Don't have a contract or don't want to use the contract to pay for this certificate? Bill the cost to your account balance.
   To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

10. **Signature Hash**

    SHA-256 is the only signature hash available for DV certificates.

11. **Select a DCV Method to Prove Control Over Your Domain**
    Before DigiCert can reissue your DV certificate, you must demonstrate control over the domains on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

    In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domains on the certificate order.

    You must use the selected DCV method to prove control over every domain on the order.

    - **DNS TXT**
      The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
    - **Email**
      The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
    - **File**
      The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

Note: After submitting your reissue order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

12. **Select the Language for the DCV Email**

    In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

Note that this drop-down list only appears when you select **Email** as your DCV method.

13. **Reason for Reissue**
    Add a reason for the reissue that only an Administrator can see.

> **Note:** These comments are not included in the certificate.

14. When you are finished, click **Request Reissue**.

Reissue a GeoTrust Cloud DV Certificate

Use these instructions to reissue a GeoTrust Cloud DV Certificate.

GeoTrust Cloud DV Certificates use Subject Alternative Names (SANs) to let you secure multiple domains (example.com) and wildcard domains (*.example.com) with one certificate. Adding SANs to a GeoTrust Cloud DV certificate order may incur additional cost.

> **Info:** A Certificate Signing Request (CSR) is required to complete the reissue order.

1. **Create a Certificate Signing Request**
   To remain secure, certificates must use at least a 2048-bit key size. Need help creating a CSR? See Create a CSR (Certificate Signing Request).
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
3. On the Orders page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to find the GeoTrust Wildcard DV certificate you want to reissue.
4. In the certificate's Order # column, click the **Quick View** link.
5. In the Order details pane (on the right side of the page), click the **Reissue Certificate** link.
6. **Add Your CSR**
   We take the common name and any SANs included in your CSR and add them to the **Common Name** and **Other Hostnames (SANs)** field.
   On the Reissue Certificate for Order page, use one of the options below to add your CSR.
   a. **Click to upload a CSR**
      Click the link to upload your CSR file to the **Add Your CSR** box
   b. **Paste CSR**
      Use a text editor to open your CSR file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags and paste it in to the **Add Your CSR** box.
7. **Common Name**
   We take the common name included in your CSR and add it to the **Common Name** field.

To add or change the common name, manually enter the domain you want this DV certificate to secure.

Important: Changing the common name when reissuing a GeoTrust Cloud DV certificate automatically revokes the original certificate and any previous reissues, unless you add the old common name as a SAN on the reissued certificate.

8. **Other Hostnames (SANs)**
   We take any SANs included in your CSR and add them to the **Other Hostnames (SANs)** field.

   Add, remove, and reorder SANs as needed so the certificate secures the domains that you want.

   a. **Add SANs**
      In the **Other Hostnames (SANs)** box, enter the additional SANs that you want included in the reissued certificate.
      Adding SANs does not revoke the original certificate or previous reissues. However, adding SANs may incur additional charges for the certificate reissue.
   b. **Remove SANs**
      In the **Other Hostnames (SANs)** box, delete the SANs that you want to exclude in the reissued certificate.

Important: Removing SANs automatically revokes the original certificate or previous reissues

9. **Select Payment Method**
   Did you add SANs to the certificate reissue order? Under **Payment Information**, select a payment method to pay for the certificate.

   If you didn't add SANs, skip to the next step. You won't be charged for your reissue.

   a. **Pay with Contract Terms**
      Have a contract and want to use it to pay for the certificate?
      Note: When you have a contract, it is the default payment method.
   b. **Pay with Credit Card**
      Don’t have a contract or don’t want to use the contract to pay for this certificate? Use a credit card to pay for the certificate.
   c. **Pay with Account Balance**
      Don’t have a contract or don’t want to use the contract to pay for this certificate? Bill the cost to your account balance.
      To deposit funds, click the **Deposit** link.

Info: The **Deposit** link takes you to another page inside your CertCentral account. Any information entered in the request form will not be saved.

10. **Signature Hash**

    SHA-256 is the only signature hash available for DV certificates.

11. **Select a DCV Method to Prove Control Over Your Domain**
    Before DigiCert can reissue your DV certificate, you must demonstrate control over the domains on your certificate order. To learn more about the available DCV Methods, see Domain Control Validation (DCV) Methods.

    In the **DCV verification method** drop-down list, choose the DCV method you want to use to demonstrate control over the domains on the certificate order.

    You must use the selected DCV method to prove control over every domain on the order.

    - **DNS TXT**
      The DNS TXT DCV method allows you to demonstrate control over the domain on your order by creating a DNS TXT record containing a randomly generated value.
    - **Email**
      The Email DCV method allows an email recipient to demonstrate control over the domain by following the instructions in a confirmation email sent for the domain.
    - **File**
      The File DCV method allows you to demonstrate control over your domain by hosting a fileauth.txt file containing a randomly generated value at a predetermined location on your website.

> **Note:** After submitting your reissue order, you can change the DCV method from the certificate's Order # details page, if needed. (In the sidebar menu, click **Certificates > Orders**. On the Orders page, in the Order # column of the DV certificate order, click the order number link.)

12. **Select the Language for the DCV Email**

    In the **DCV Email Language** drop-down list, select the language you want DCV authentication email to be sent in.

    Note that this drop-down list only appears when you select **Email** as your DCV method.

13. **Reason for Reissue**
    Add a reason for the reissue that only an Administrator can see.

> **Note:** These comments are not included in the certificate.

14. When you are finished, click **Request Reissue**.

Canceling pending reissues on DV Certificates

Use these instructions to cancel a pending reissue on a DV certificate.

Note: You can only cancel pending reissue requests. Once we've issued the certificate, you'll need to revoke the reissued certificate if it is no longer needed.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the filters and the advanced search features to locate the **Reissue Pending** DV certificate request you want to cancel.
3. In the Order # column of the DV certificate order, click its order number link.
4. On the Order details page, in the Certificate Details section, in the **Certificate Actions** drop-down list, select **Cancel Reissue**.
5. In the Cancel Reissue window, click **Cancel Reissue**.

Info: Canceling a reissue on a certificate successfully removes it from our system and can't be undone. However, if the certificate ends up being needed, simply request the reissue again.

6. Congratulations! You have successfully canceled the reissue request.

Note: The canceled reissue request is logged in the **Audit Logs** (in the sidebar menu, click **Account > Audit Logs**).

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 the request and DigiCert revokes the DV certificate.

Submit a Request to Revoke a DV Certificate

Use these instructions to submit a request for revoking a DV Certificate.

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

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the drop-down lists, search box, advanced search features (**Show Advanced Search** link) and column headers to filter the list of certificates.
3. In the Order # column, click the **Quick View** link for the DV certificate you want to revoke.
4. In the Order number details pane (on the right), click the **Revoke Certificate** link.
5. On the Request to Revoke Certificate for Order page, in the Reason for Revocation box, type the reason why you want to revoke the certificate (e.g., certificate no longer needed).
6. Click **Request Revocation**.

   After an account administrator approves your request, DigiCert will revoke the DV certificate.

Approve (or Reject) a Certificate Revocation Request

> **Warning:** Once a certificate is revoked, the process can't be reversed. A revoked DV certificate used on a public site shows trust warnings preventing users from accessing the site.

Use these instructions to approve (or reject) and request to revoke a certificates.

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

1. In your CertCentral account, in the sidebar menu, click **Certificates > Requests**.
2. On the Requests page, in the **Status** drop-down list select **Pending**, in the **Type** drop-down list select **Revoke**, and then click **Go** to see only the certificate request that need administrator approval.
3. In the Order # column, click the Order number link for the DV certificate you want to revoke.
4. In the Order details pane (right side), click **Approve**.

Warning: In the **Approve Request** window, don't click **Approve** unless you are sure that you want to revoke the certificate. The revocation can't be reversed. Any site using this certificate will show trust warnings when users try to access the site.

5. In the **Approve Request** window, in the **Approval Comment** box add a comment about the certificate revocation and then, click **Approve**.
6. DigiCert will now revoke the DV certificate.