Advanced CertCentral® Getting Started Guide

Version 9.2

Table of Contents

1 CertCentral User Roles and Account Access

The CertCentral account has two categories, four roles, and three subroles that can be used for setting up user account permissions. The two categories are Unrestricted and Restricted. The four roles are Administrator, User, Finance Manager, and Manager. The three subroles are EV Verified User, CS Verified User, and EV CS Verified User.

1.1 Unrestricted versus Restricted

Users in your CertCentral account fall into two categories: unrestricted and restricted.

The restricted and unrestricted categories are only relevant if you have divisions within your CertCentral account. If you are using divisions in your account, then you need to decide if a user should have access to all divisions, just some, or just one.

- **Unrestricted User:** Can access all the divisions within your account.
- **Restricted User:** Can only access the divisions to which you assign them.

If you do not use divisions within your account, then all users are unrestricted.

1.2 Roles and Account Access

Account administrators do not assign individual permissions to a user. Instead, they assign each user a role. The role assigned to the user determines which account features they can access.

Administrator:

Unrestricted Administrator: Has full CertCentral account access with permissions to do the following:

- They can access and manage Certificate Inspector.
- They can manage divisions (create and edit) and account users (create, delete, and edit).
- They can manage organization (add new organizations), domains (add or deactivate), guest requests, and API access.
- They can view all certificate requests and certificate orders, can request certificates, can approve certificate requests, and can run orders reports.
- They can manage account finance settings and finances (view balance history, run spending reports, deposit funds, etc.).
- They can manage account settings (including authentication settings, IP access restrictions, and product restrictions), audit settings, and audit logs.

Restricted Administrator: Has full access to the division(s) to which they are assigned. Has permissions to do the following:

- They can access and manage Certificate Inspector.
- They can manage their division(s) (edit).

	• They can manage their division users (create, delete, and edit). • They can view domains assigned to their division(s) and can manage guest requests and API access. • They can view their division certificate requests and certificate orders, can request certificates, can approve certificate requests, and can run orders reports. • They can manage their division finances (view balance history, run spending reports, deposit funds, etc.). **All Administrators**: By default, they do not have permissions to approve EV Certificate, EV Code Signing Certificate, or Code Signing Certificate requests. To approve these types of request, the administrator must be assigned the appropriate subroles.
Standard User:	**Unrestricted User:** Account users who can do the following: • They can request certificates. • They can monitor certificate requests and orders (their own and others). • A manager or administrator must approve changes. **Restricted User:** Limited division user who can do the following: • They can request certificates only for the division(s) to which they are assigned. • They can monitor certificate requests and orders (their own and others) for the division(s) to which they are assigned. • A manager or administrator must approve changes.
Limited User: You can remove permission from the **Standard** user role to create a second user role: **Limited User**. *(Standard User + Limit to placing and managing their own orders)*	**Unrestricted User:** Limited account users who can do the following: • They can request certificates. • They can monitor their own certificate requests and orders. • A manager or administrator must approve changes. **Restricted User:** Limited division user who can do the following: • They can request certificates only for the division(s) to which they are assigned. • They can monitor their own certificate requests and orders. • A manager or administrator must approve changes.

Finance Manager:	**Unrestricted Finance Manager:** Limited account users whose primary role is to manage account finances. They can do the following: • They can view balance history, spending reports, and account pricing. • They can manage purchase orders and deposit funds. • They can manage order reports. • They can request certificates. • They can monitor their own certificate requests and orders. **Restricted Finance Manager:** Limited division users whose primary role is to manage their division finances. They can do the following: • They can view their division's balance history, spending reports, and account pricing. • They can manage their division's purchase orders and deposit funds. • They can manage their division's order reports. • They can request certificates for the division(s) to which they are assigned. • They can monitor their own certificate requests and orders.
Manager:	**Unrestricted Manager:** Limited account users whose primary role is to help manage the account. They can do the following: • They can access and manage Certificate Inspector. • They can view divisions and manage account users (edit). • They can view organizations and manage domains (add or deactivate). • They can view all certificate requests and certificate orders, can request certificates, can approve certificate requests, and can run orders reports. • They can manage account finance settings and finances (view balance history, run spending reports, deposit funds, etc.). • They can manage audit settings and audit logs. **Restricted Manager:** Limited division users whose primary role is to help manage their division(s). They can do the following: • They can access and manage Certificate Inspector. • They can view divisions and manage account users (edit).

- They can view their division's certificate requests and certificate orders, can request certificates, can approve certificate requests, and can run orders reports.
- They can manage division finances (view balance history, run spending reports, deposit funds, etc.).

All Managers: By default, they do not have permissions to approve EV Certificate, EV Code Signing Certificate, or Code Signing Certificate requests. To approve these types of request, the manager must be assigned the appropriate subroles.

1.3 Subroles

As part of the certificate approval process, the CertCentral account has three subroles that you must add to the appropriate user so that Extended Validation, Code Signing, and Extended Validation Code Signing Certificate requests can be approved.

EV Verified User:	EV Verified Users can approve certificate request for EV SSL and EV Multi-Domain Certificates. For a user to be an EV Verified User, they must be an administrator or a manager and must have a phone number and job title.
CS Verified User:	CS Verified Users can approve certificate request for Code Signing Certificates. For a user to be a CS Verified User, they must be an administrator or a manager and must have a phone number and job title.
EV CS Verified User:	EV CS Verified Users can approve certificate request for EV Code Signing Certificates. For a user to be an EV CS Verified User, they must be an administrator or a manager and must have a phone number and job title.

2 CertCentral Language Preferences

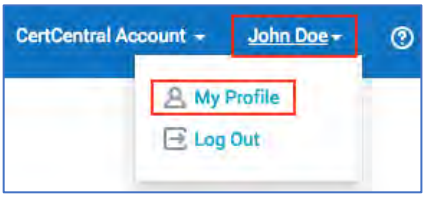
Language support allows you to change and save your CertCentral platform language preference.

Currently, CertCentral supports the following languages:

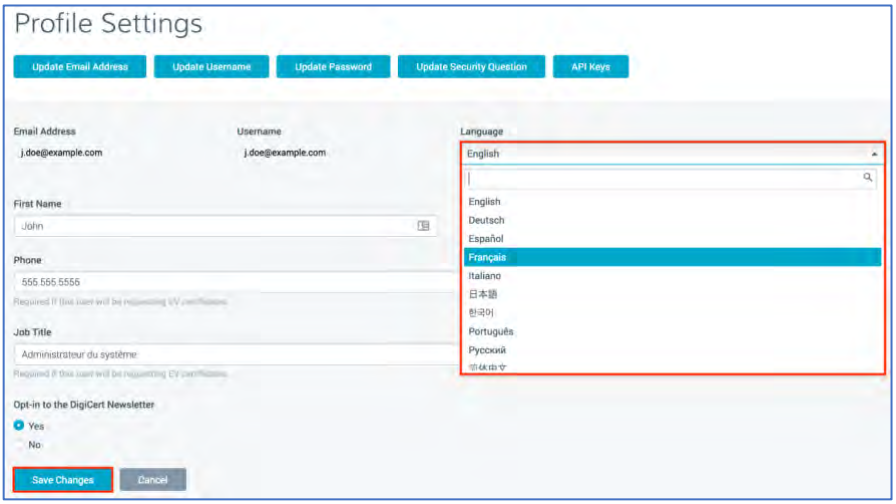
- Deutsch
- Español
- Français
- Italiano
- 日本語
- 한국어
- Português
- Русский
- 简体中文
- 繁體中文
- English

2.1 How to Change Your Account Language Preference

1. In your CertCentral account, in the **"your name"** drop-down list, select **My Profile**.



2. On the **Profile Settings** page, in the **Language** drop-down list, select the language preference for your account.



3. Click **Save Changes**.

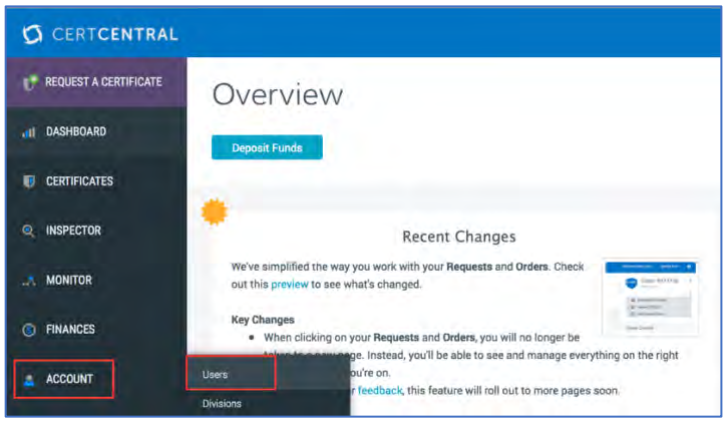
   The language in your CertCentral should now be the same as the one you selected.

3 Manage Users

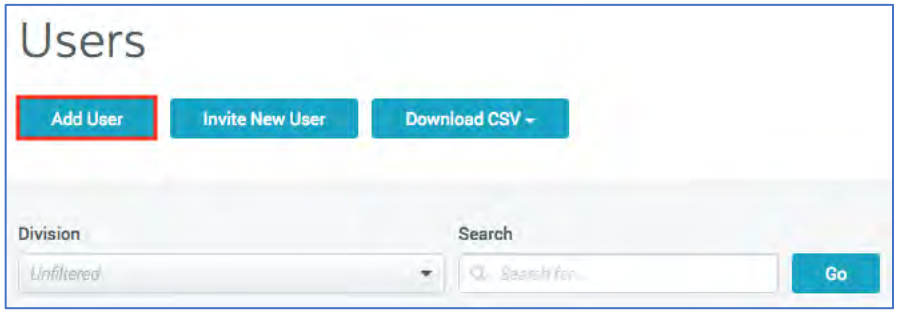
3.1 How to Add a New User to Your CertCentral Account

Use these instructions to add a user to your CertCentral account.

1. In your CertCentral account, in the sidebar menu, click **Account > Users**.



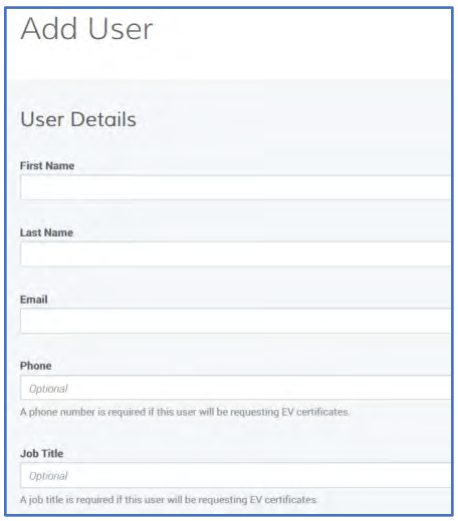
2. On the **Users** page, click **Add User**.



3. On the **Add User** page, in the **User Details** section, provide the following user information:

First Name:	Type the user's first name.
Last Name:	Type the user's last name.
Email:	Type an email address at which the user can be contacted. The user will be sent an email with instructions for creating a password for and logging into their account.
Phone:	Type a phone number at which the user can be reached. A phone number is only required if the user will be an **EV Verified User**, an **EV CS Verified User**, and/or a **CS Verified User**. (See 1.3 Subroles.)

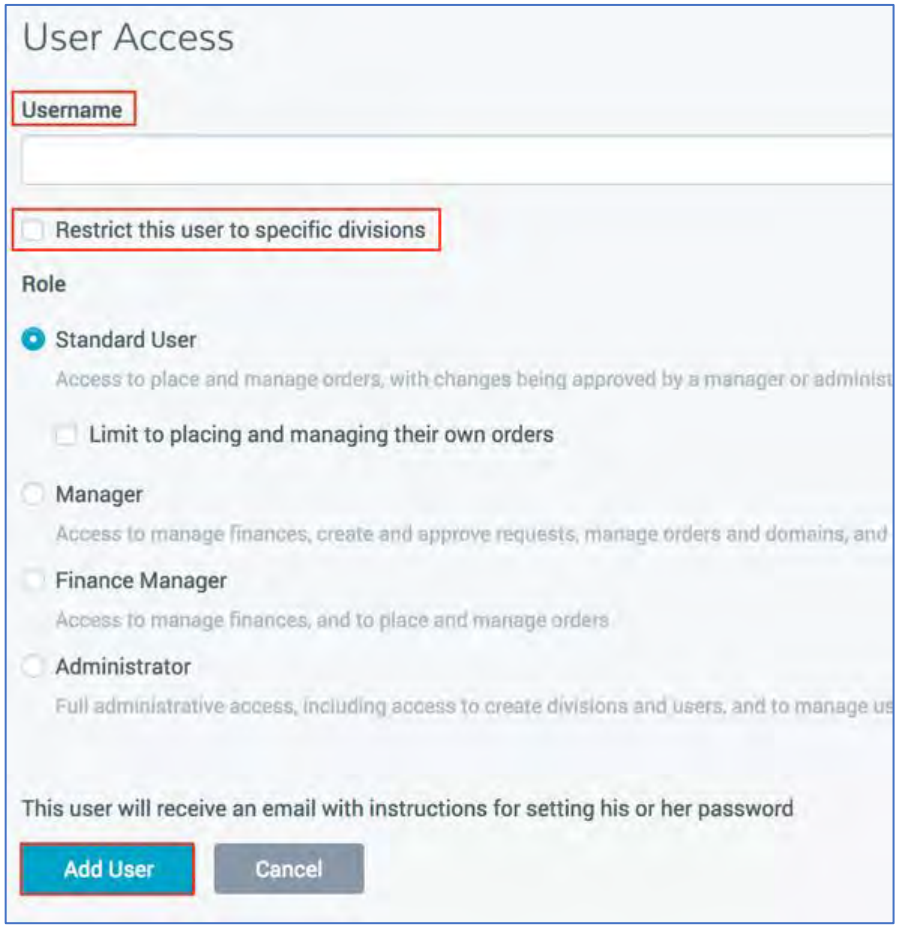
Job Title:	Type the user's job title. A job title is only required if the user will be an **EV Verified User**, an **EV CS Verified User**, and/or a **CS Verified User**. (See 1.3 Subroles.)



4. In the **User Access** section, assign the user a role and configure their division access – if applicable:

Username:	The entry in the **Email** box auto populates this box. You can type a different username for the user, but we don't recommend it Although you can create a unique username for each user, we recommend using their email address (e.g., *john @example.com*).
Restrict this user to specific divisions	Check this box if you want to restrict the role to specific divisions. (See 1.1 Unrestricted versus Restricted.) **Note:** This option only appears if you are using divisions within your CertCentral account.
User is restricted to the following divisions	In the drop-down list, select the divisions to which the role is restricted (assigned). **Note:** This drop-down list only appears if you check **Restrict this user to specific divisions**.
Role:	Select a role for the new user: **Administrator**, **Standard User**, **Finance Manager**, or **Manager**. (See 1.2 Roles and Account Access.)

Limit to placing and managing their own orders	To create a **Limited User** role, select **Standard User** and check this box.



5. When you are finished, click **Add User**.

   The newly added user will receive an email with instructions for setting up their account credentials (password, security question, etc.) so they can log in to their CertCentral account.

3.2 How to Resend the "DigiCert User Account Created - Action Required" Email

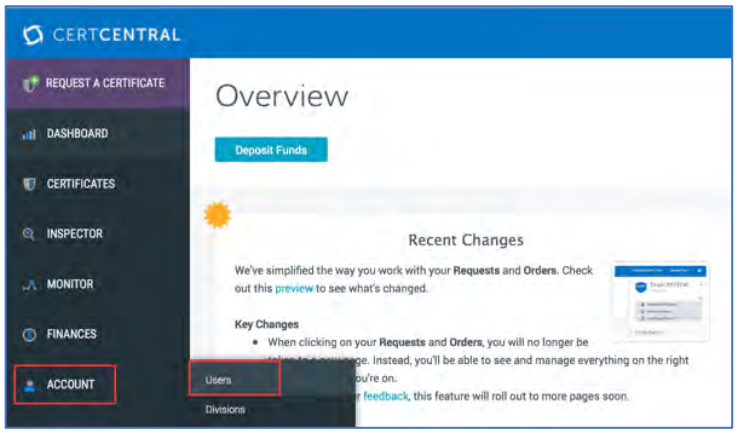
Use these instructions to resend the DigiCert User Account Created - Action Required" Email to a newly added account user.

If a newly added user deletes or loses the **DigiCert User Account Created - Action Required** email before their password is created, you can resend the email.

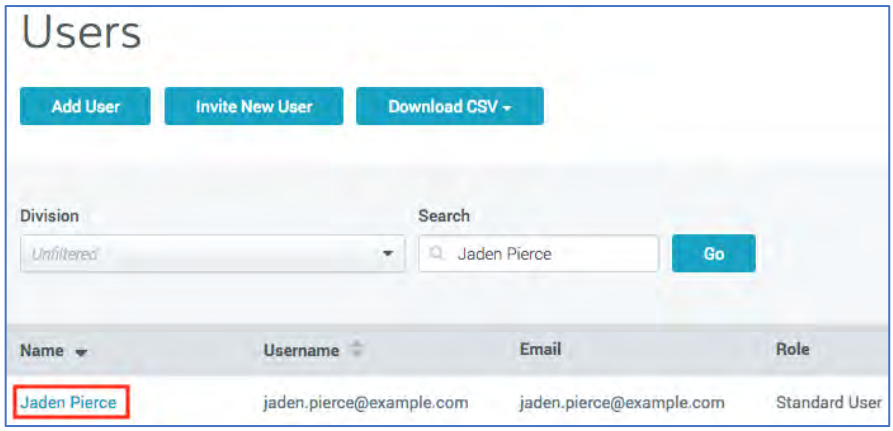
As soon as you resend the **DigiCert User Account Created - Action Required** email, the old link expires and cannot be used to create a password. If the expired link is used, the following message is displayed:

"The emailed link is invalid or has expired. Try resetting your password or try logging in to resolve the issue."

1. In your CertCentral account, in the sidebar menu, click **Account > Users**.



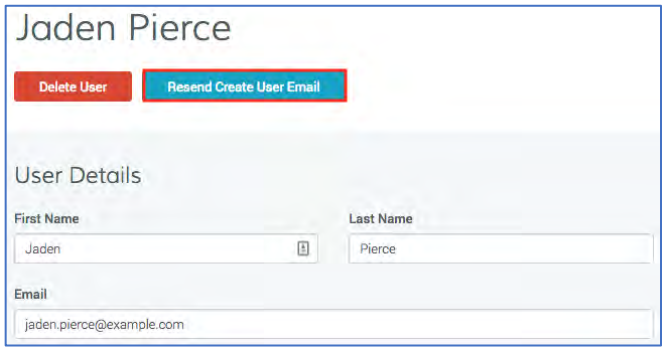
2. On the **Users** page, use the search features to locate the user that you need to resend the **DigiCert User Account Created - Action Required** email to.



3. In the **Name** column, click the **"User's Name"** link

4. On the **"User's Name"** page, click **Resend Create User Email**.

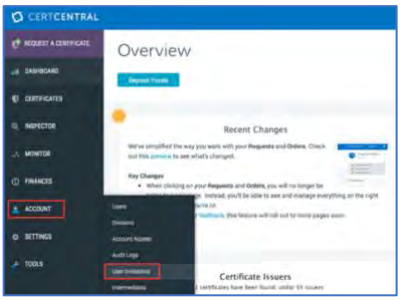
   This resends the **DigiCert User Account Created - Action Required** email to the user with a new link to create a password for logging in to their account.



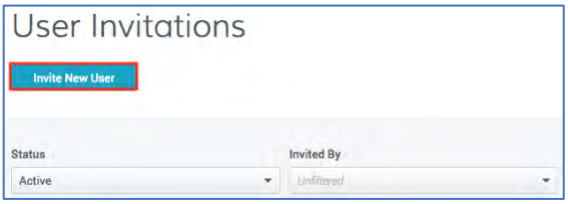
3.3 How to Invite New Users to Join Your CertCentral Account

Use these instructions to send an email inviting a new user to set up their account themselves. Once the account is set up, you will need to go to the **User Invitations** page (**Account > User Invitations**) and approve/activate the new user account request.

1. In your CertCentral account, in the sidebar menu, click **Account > User Invitations**.

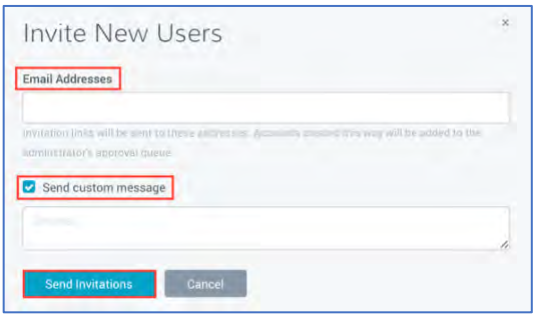


2. On the **User Invitations** page, click **Invite New User**.



3. In the **Invite New Users** window, provide the following information, as needed:

Email Addresses	In the box, type the email addresses (comma separated) of the new users who you want to invite to join your account.
Send custom message	1. To add a custom email message, check the check box. 2. In the box that appears, type the message you want to include in the new account invitee email.



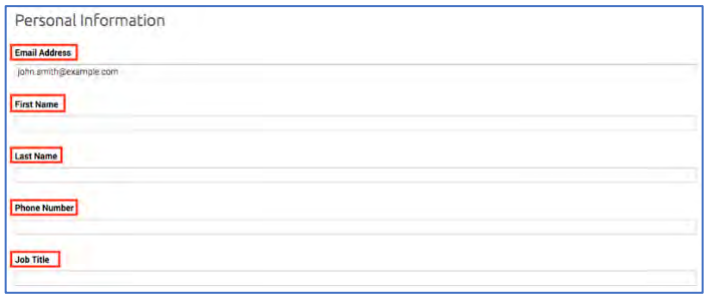
4. When you are finished, click **Send Invitations**.

   The newly invited user will be sent the **Please create your user login for DigiCert CertCentral** email that contains links that will let them create their user profile.

3.4 How to Create Your New User (Invitee) Account

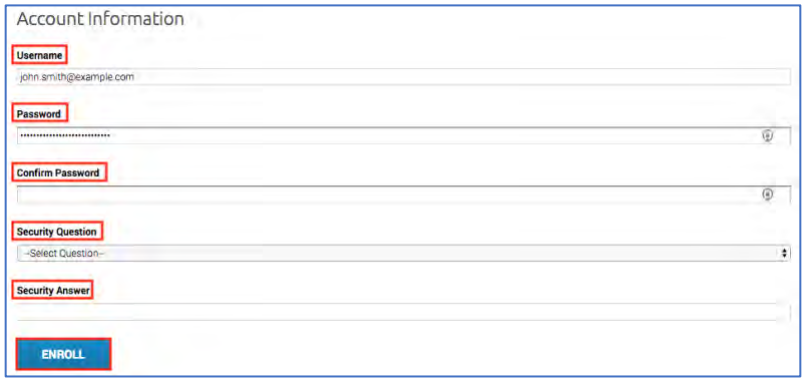
1. In your email account inbox, locate the **Please create your user account for DigiCert CertCentral** email and click the link provided to create your account user profile.

2. On the **Create CertCentral User** page, under **Personal Information**, provide this information: **Email Address**, **First Name**, **Last Name**, **Phone Number**, and **Job Title**.



3. Under **Account information**, configure your account credentials:

Username	Create a username per your company's policy (for example they may want you to use your email address as your username).
Password/Confirm Password	Create and confirm the password you want to use to log into your account.
Security Question/Security Answer	Select a security question and then answer it.



4. When you are finished, click **Enroll**.

   You should receive a ***Your request has been received*** email, which lets you know that your account request has been sent to the account administrator for approval

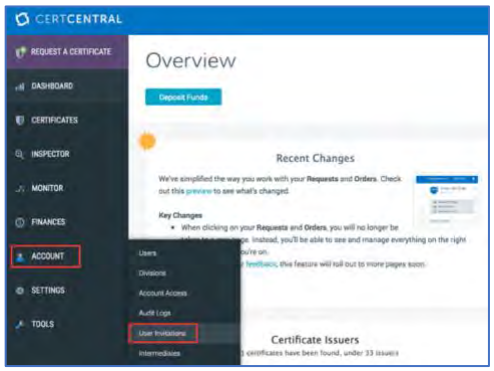
   You cannot log into your account until your account administrator approves the request. Then, you will receive an email notifying you (**User account for "User Name" has been approved**) that your request has been approved.

3.5 How to Approve/Activate an Invitee's Account

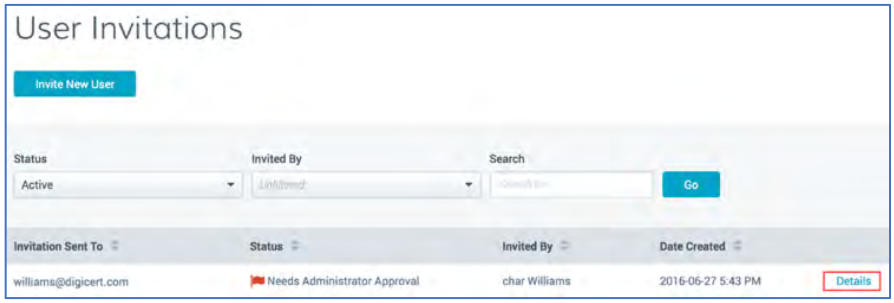
User these instructions to finish configuring an invitee's user account.

After you receive the ***"CertCentral user invite accepted"*** email, you can approve/activate the account, so the new user can log in to their CertCentral account.

1. In your CertCentral account, in the sidebar menu, click **Account > User Invitations**.



2. On the **User Invitations** page, user the filters and column headers to locate the new user account you want to approve/activate.



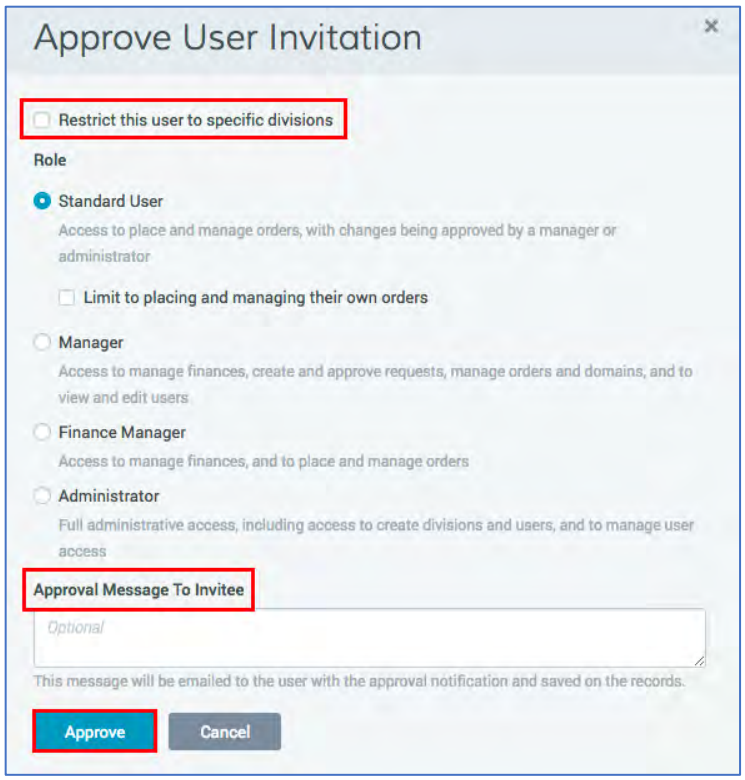
3. In the user's row, next to **Date Created**, click the **Details** link.

4. On the **User Invitation to** page, review the information the invitee provided and click **Approve**.

5. In the **Approve User Invitation** window, configure the user's role and account access:

Restrict this user to specific divisions	Check this box if you want to restrict the user to specific divisions. (See 1.1 Unrestricted versus Restricted.) **Note:** This option only appears if you are using divisions within your CertCentral account.

User is restricted to the following divisions	In the drop-down list, select the divisions to which the user is restricted (assigned). **Note:** This drop-down list only appears if you check **Restrict this user to specific divisions**.
Role	Select a role for the new user: **Administrator**, **Standard User**, **Finance Manager**, or **Manager**. (See 1.2 Roles and Account Access.)
Limit to placing and managing their own orders	To create a **Limited User** role, select **Standard User** and check this box.
Approval Message to Invitee	Enter a message to be included in the approval email.



6. When you are finished, click **Approve**.

   Congratulations! You've added the new user to your account (**Account > Users**). The new user will receive an email (**User account for "User Name" has been approved**) with a link that takes them to the account login page.

3.6 How to Unlock a "Locked" Account

Use theses instructions to unlock your account due to excessive log in failures or for other security reasons.

1. If you are locked out of your CertCentral account, contact DigiCert so we can unlock the account.

    - **Contact your DigiCert account representative**
    - **Contact the DigiCert Support Team**

      Phone: 1-801-701-9600
      Email: support@digicert.com
      Live Chat: www.digicert.com

3.7 Manage API Keys

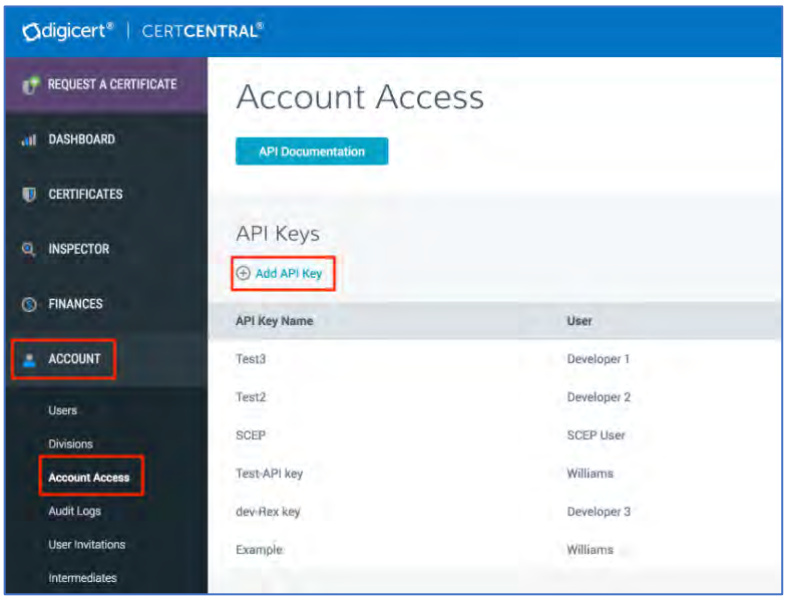
The DigiCert Services API allows you to create your own version of the platform with your organization's branding to seamlessly integrate with existing CertCentral features.

To take advantage of all the CertCentral functionality and benefits while controlling how the platform looks and feels for your users, you need to issue developer API keys. The DigiCert Services API requires a DigiCert Developer API key. This key will be included in the header as part of each request.

3.7.1 (Admins and Managers only) How to Issue an API Key

Use these instructions to create an API Key for a user in your CertCentral account.

1. In your CertCentral account, in the sidebar menu, click **Account > Account Access**.

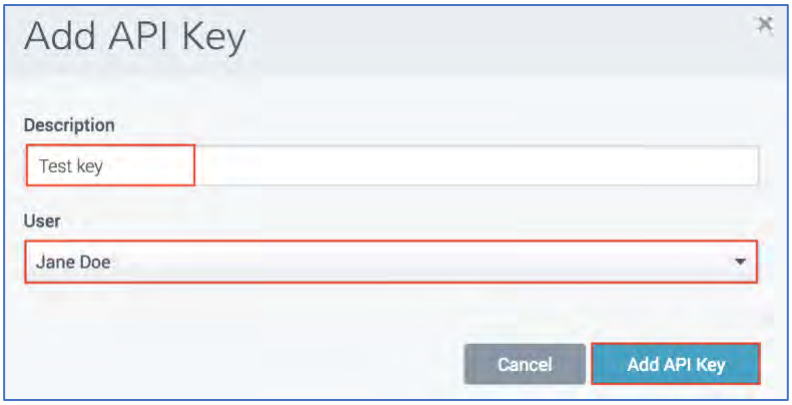


2. On the **Account Access** page, under **API Keys**, click **Add API Key**.

3. Next, open a text editor (such as Notepad).

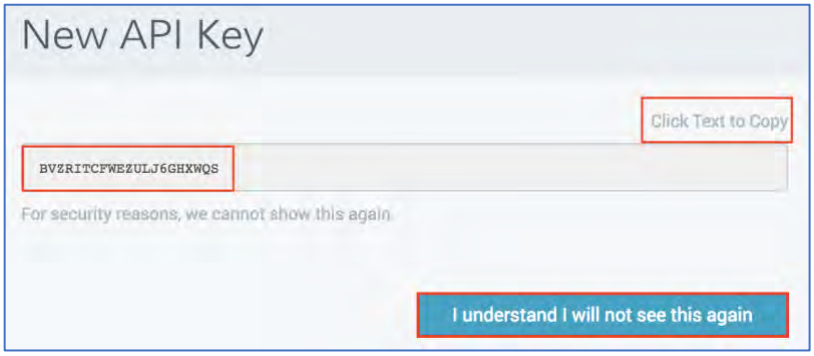
4. In the **Add API Key** window, provide the following API key information:

Description	Type a description/name for the API key.
User	In the drop-down list, select the user to whom you want to assign the API key.



5. When you are done, click **Add API Key**.
6. In the **New API Key** window, above ***"For security reasons, we cannot show this again."***, click on your API key (e.g., *ERKW3MYURGX98IDLN*) to copy it and then paste it in to your text editor.

   CAUTION: Do not close the **New API Key** window until you have saved a copy of the API key. If you close the window without recording your new API key, you will not be able to retrieve it. You will need to revoke the API key that you just created and create a new one.

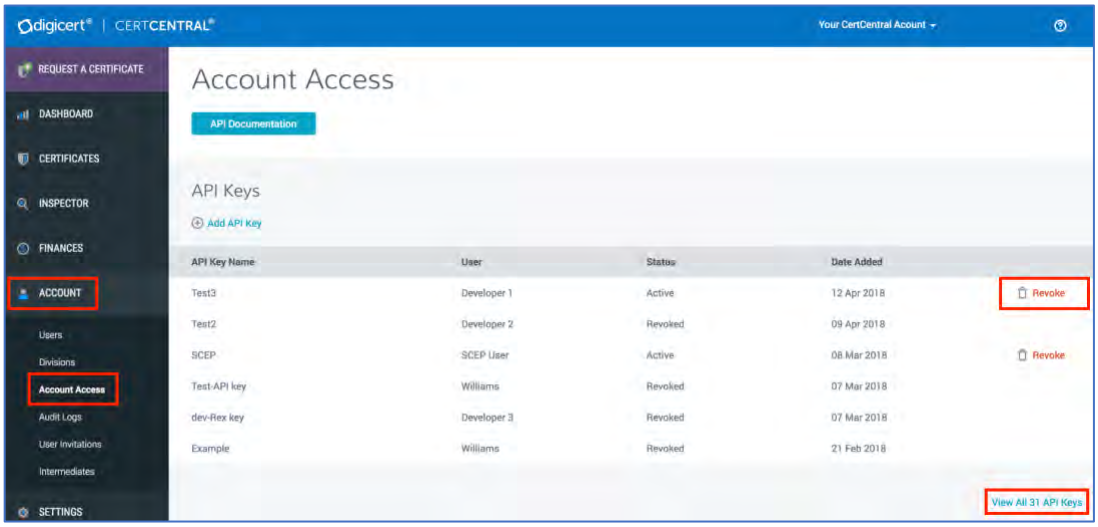


7. Save your text editor document, making sure to note its location.
8. In the **New API Key** window, once you have saved a copy of your API key, click **I understand I will not see this again**.

3.7.2 (Admins and Managers only) How to Revoke an API Key

Use these instructions to revoke an unneeded API key. Note that revoking an API key permanently disables access for those using it.

1. In your CertCentral account, in the sidebar menu, click **Account > Account Access**.



2. On the **Account Access** page, under **API Keys**, to the right of the API key that you need to revoke, click **Revoke**.

   API Key not listed on Account Access page (more than 10 API keys)

   a. If you don't see the key listed on this page, in the bottom right corner below the list of keys, click **View All "#" API Keys**.

      Note: The **View All "#" API Keys** link only appears if you have issued more than 10 API keys.

   b. On the **API Keys** page, to the right of the API key that you need to revoke, click **Revoke**.

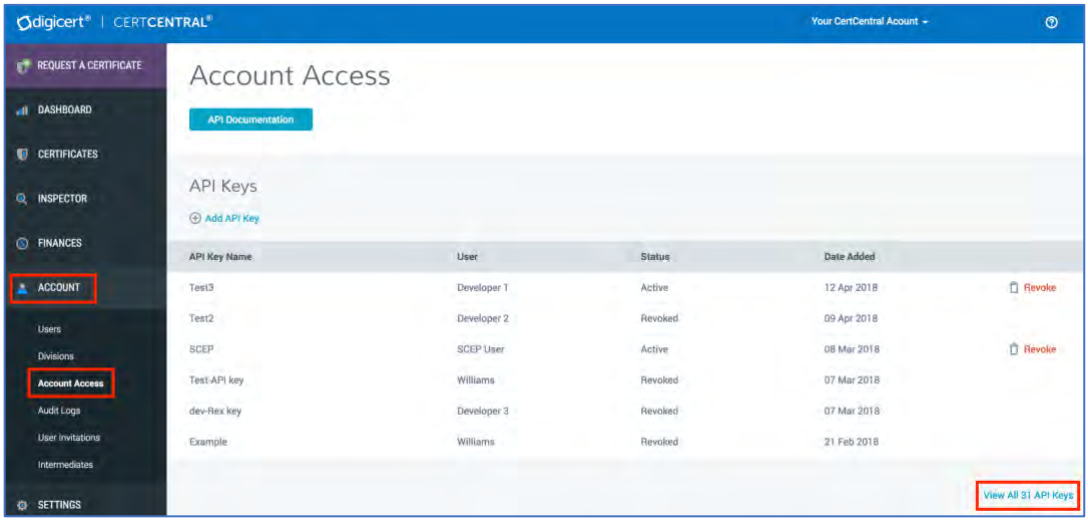
3. In the **Revoke API Key** window, under the ***"Are you sure you want to permanently revoke the API key 'API key Name' for 'User Name'?"*** message, click **Revoke**.

   CAUTION: In the **Revoke API Key** window, do not click **Revoke**, unless you are ***sure*** that you want to permanently revoke the API key. Revoking an API key permanently disables access for anyone who is using it.

3.7.3 (Admins and Managers only) How to View API Keys and API Key Users

Use these instructions to view all the API keys created (active and revoked) for your CertCentral account.

1. In your CertCentral account, in the sidebar menu, click **Account > Account Access**.



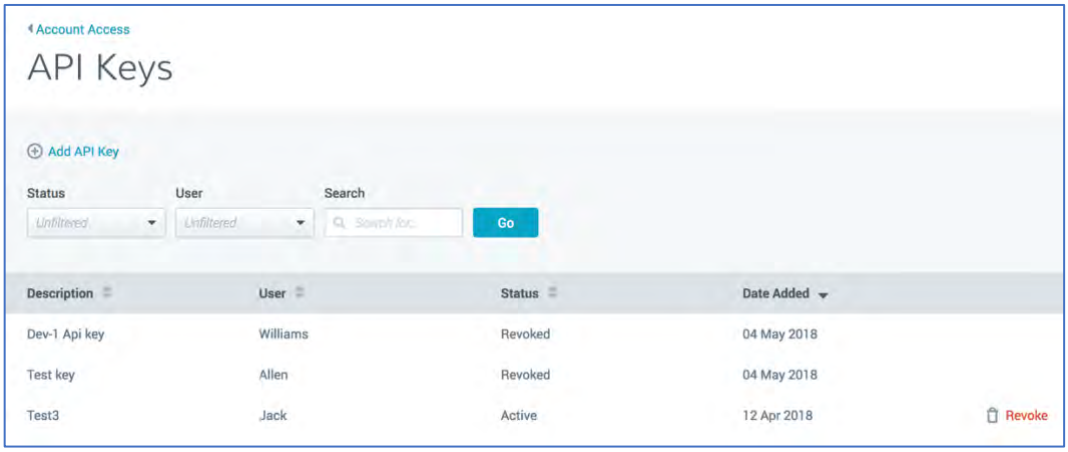
2. On the **Account Access** page, under **API keys**, you can view all or some of the API keys that you have issued.

3. When you have more then 10 API Keys,

   a. To see all your API keys, in the bottom right corner, below the list of keys, click **View All "#" API Keys**.

      Note: The **View All "#" API Keys** link only appears if you have issued more than 10 API keys.

   b. On the **API Keys** page, all keys are listed**.**



4. Use the drop-down list, search box, and column headers to locate specific keys.

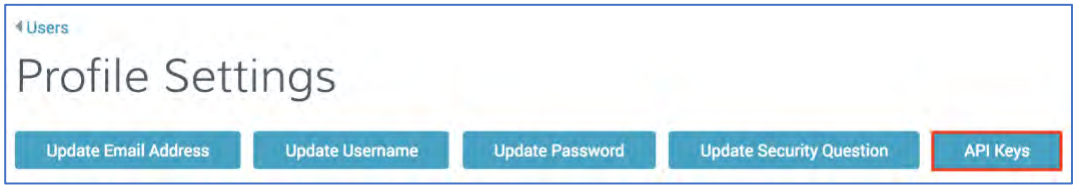
3.7.4 (All Users) How to Issue Your Own API Key

Use these instructions to create your own API Key.

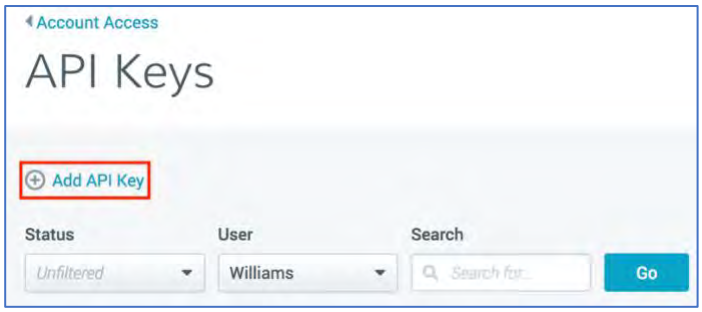
Rather than creating all the API keys yourself, CertCentral account Users (administrators and user) can issue their own API Keys through the user's **Profile Settings**.

1. In your CertCentral account, in top right corner, in the **"User Name"** drop-down list, select **My Profile**.

2. On the **Profile Settings** page, click **API Keys**.

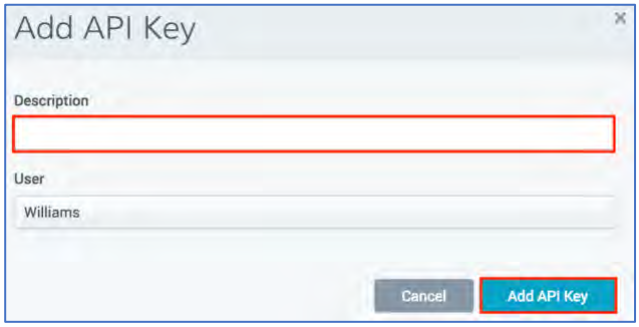


3. On the **API Keys** page, click **+Add API Key**.



4. Next, open a text editor (such as Notepad).

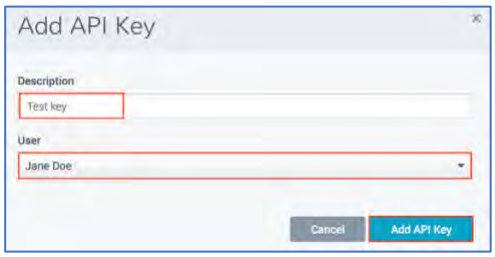
5. In the **Add API Key** window, under **Description**, type a description/name for the API key.



5.a Step for Admins Only:

The **User** drop-down list appears in the administrator's UI only.

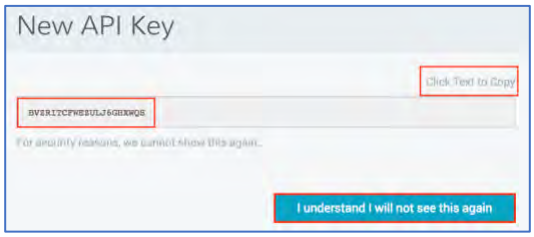
In **User** the drop-down list, select yourself.



6. When you are done, click **Add API Key**.

7. In the **New API Key** window, above ***"For security reasons, we cannot show this again."***, click on your API key (e.g., *ERKW3MYURGX98IDLN*) to copy it and then paste it in to your text editor.

   CAUTION: Do not close the **New API Key** window until you have saved a copy of the API key. If you close the window without recording your new API key, you will not be able to retrieve it. You will need to revoke the API key that you just created and create a new one.



8. Save your text editor document, making sure to note its location.

9. In the **New API Key** window, once you have saved a copy of your API key, click **I understand I will not see this again**.

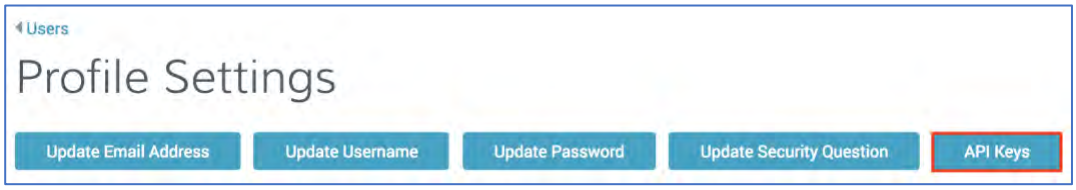
3.7.5 (All Users) How to Revoke Your Own API Key

Use these instructions to revoke your, no longer needed, API Key.

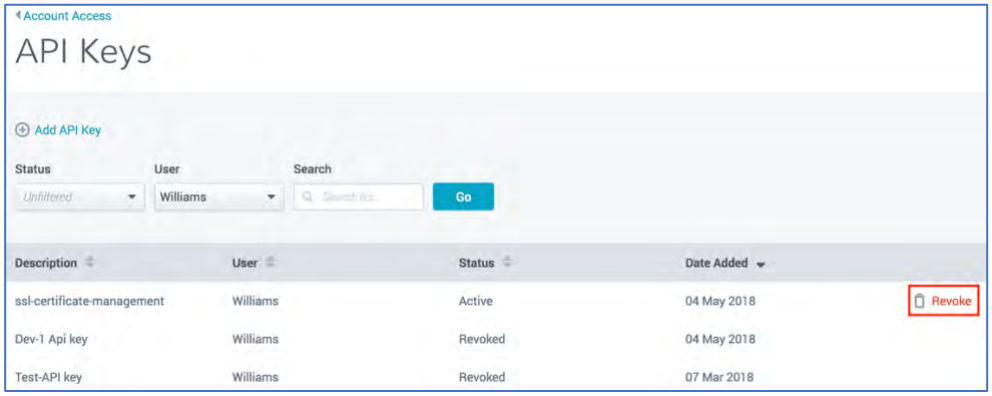
Users (users and administrators) can revoke the API Keys that they created for themselves through the user's **Profile Settings**. Note that revoking an API key permanently disables access for those using it.

1. In your CertCentral account, in top right corner, in the **"User Name"** drop-down list, select **My Profile**.

2. On the **Profile Settings** page, click **API Keys**.



3. On the **API Keys** page, to the right of the API key that you need to revoke, click **Revoke**.



4. In the **Revoke API Key** window, under the ***"Are you sure you want to permanently revoke the API key 'API key Name' for 'User Name'?"*** message, click **Revoke**.

CAUTION: In the **Revoke API Key** window, do not click **Revoke**, unless you are ***sure*** that you want to permanently revoke the API key. Revoking an API key permanently disables access for anyone who is using it.

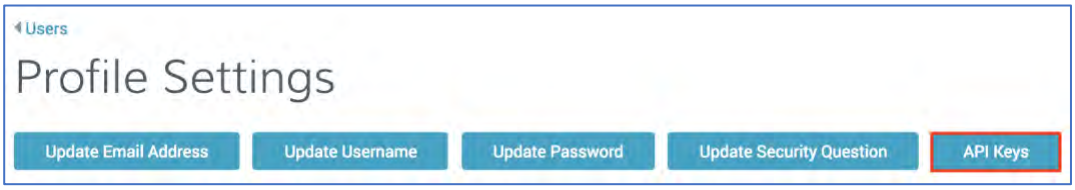
3.7.6 (All Users) How to View Your API Keys

Use these instructions to view the API keys that you created for yourself

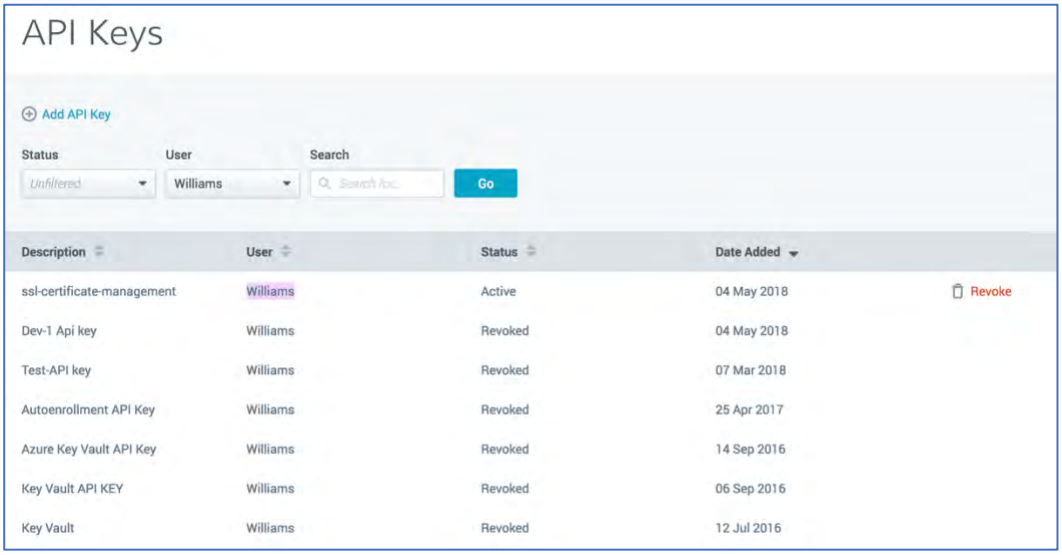
Users (users and admins) can use this instruction to view the API keys they issued to themselves.

1. In your account, in top right corner, in the **"User Name"** drop-down list, select **My Profile**.

2. On the **Profile Settings** page, click **API Keys**.



3. On the **API Keys** page, all keys are listed**.**



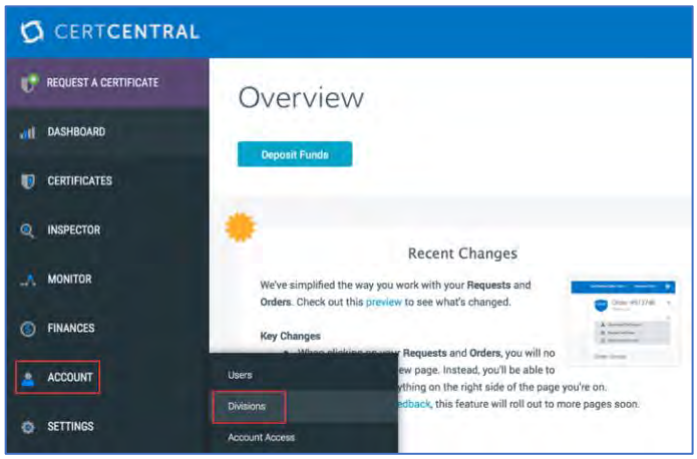
4. Use the drop-down list, search box, and column headers to locate specific keys.

4 Division Management

4.1 How to Create a Division

Use these instructions to create a division in your CertCentral account.

1. In your CertCentral account, in the sidebar menu, click **Account > Divisions**.



2. On the **Divisions** page, click **New Division**.

3. On the **New Division** page, provide the information needed to create the division:

***Name:**	Type the Division name.
Description:	Type a brief description that provides basic information about the Division.
Send request renewal notifications to	Enter the email addresses for those you want to receive request renewal notifications (comma separated).
Users restricted to this division:	In the drop-down list, select any users that you want to restrict (assign) to the division. **Note:** Users can be restricted (assigned) to multiple divisions. User not restricted to a division can access all division.
***Certificates can be ordered for:**	**1. All organizations** Select this option to allow the division to request certificates for all organizations.

	2. Specific Organizations Select this option to restrict the division to specific organizations. In the drop-down list, select the specific organizations.
***Certificates can be ordered for:**	**1. All domains** Select this option to allow the division to request certificates for all domains. **2. Specific Domains** Select this option to restrict the division to specific domains. In the box provided, enter the domains in a comma-separated list.

4. When you are finished, click **Save Division**.

5 Organization and Domain Management

5.1 Validation Process

Before DigiCert can issue any type of certificate, the certificate order must first go through a validation process. For OV and EV TLS/SSL, Private SSL, Code Signing, and Document Signing certificate orders, the certificate's validation process includes organization validation, including verifying the organization contact. For certificates that are issued to a domain (TLS/SSL and some client certificates), the certificate order process includes domain validation.

To quicken the certificate issuance process, you'll want to submit your organizations and domains for pre-validation. Once you've completed pre-validation, future certificate issuance and renewals for those domains and organizations can be done almost immediately.

5.2 Organization Validation

To validate an organization, DigiCert firsts verifies that the organization requesting a certificate is in good standing. This can include confirming good standing and active registration in corporate registries. It can also include verifying that the organization is not listed in any fraud, phishing, or government restricted entities and anti-terrorism databases.

Additionally, we verify that the organization requesting a certificate is, in fact, the organization to which the certificate will be issued. This step includes verifying the organization contact.

5.3 Domain Validation

The aim of DigiCert's domain validation process is to ensure that the organization requesting a certificate does in fact have authority to request a certificate for the domain in question.

Domain validation can include emails or phone calls to the contacts listed in a domain's WHOIS record, as well as emails to default administrative addresses at the domain. For example, we may send an authorization email to administrator@domain.com or webmaster@domain.com but would not send an authorization email to tech@domain.com. See Domain Pre-Validation: Domain Control Validation (DCV) Methods.

5.4 Manage Organizations

Adding organizations to your CertCentral account and getting them pre-validated is a prerequisite for getting your domains pre-validated. Pre-validating organizations quickens the certificate issuance process.

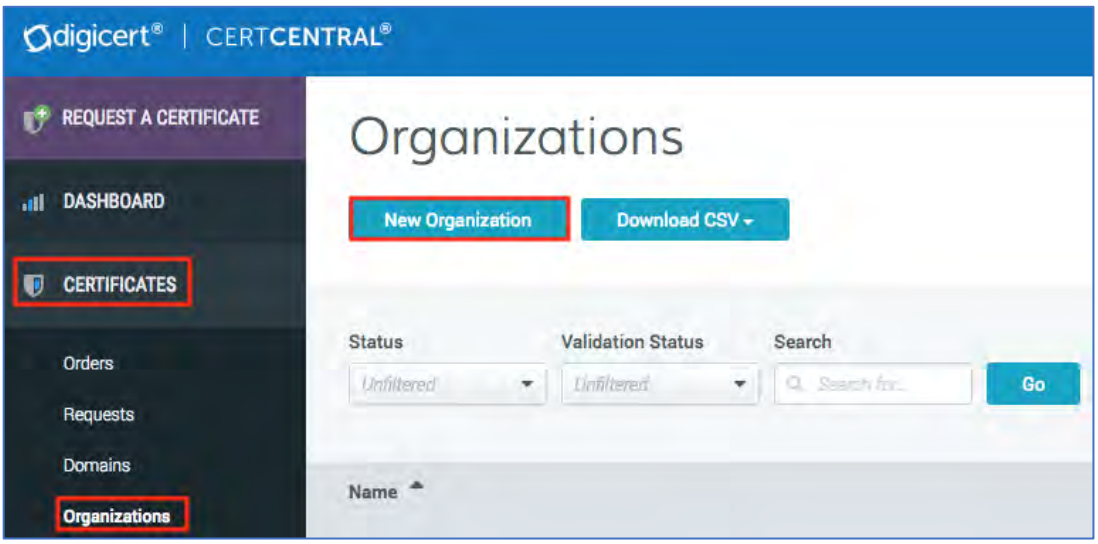
Managing organizations typically involves adding an organization, submitting it for validation. You can also deactivate a no longer needed organization.

Note: When you deactivate an organization, you remove it from all selection lists when ordering new certificates. You also hide it from the list of active organizations. Deactivating an organization also deactivates any domains validated for this organization.

5.4.1 How to Add an Organization

Use these instructions to add an organization to your CertCentral account.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Organizations**.

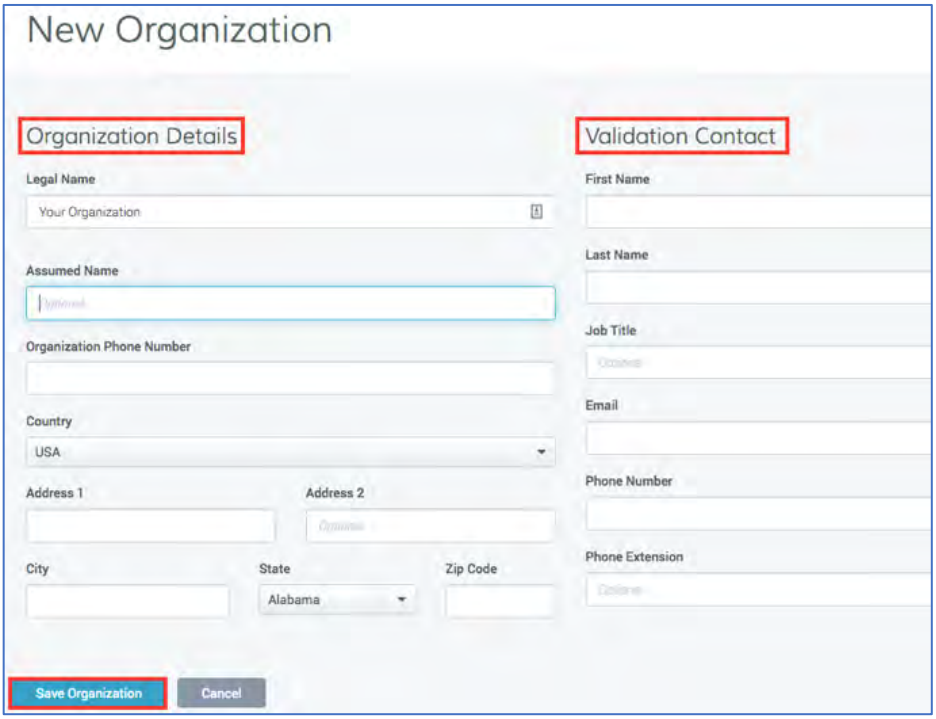


2. On the **Organizations** page, click **New Organization**.

3. On the **New Organization** page, under **Organization Details**, enter the specified organization information:

Legal Name	Enter the organization's legally registered name.
Assumed Name	If your organization has a DBA name (doing business as name), and you want to appear on the certificates, enter it here. If not, leave this box blank.
Organization Phone Number	Enter a phone number at which the organization can be contacted.
Country	In the drop-down list, select the country where the organization is legally located.
Address 1	Enter the address where the organization is legally located.
Address 2	Enter a second address, if applicable.
City	Enter the city where the organization is legally located.
State / Province / Territory/ Region / County:	Enter the state, province, territory, region, or county where the organization is legally located.

Zip Code/ Postal Code	Enter the zip or postal code for the organization's location.



4. Under **Validation Contact**, provide the following contact information:

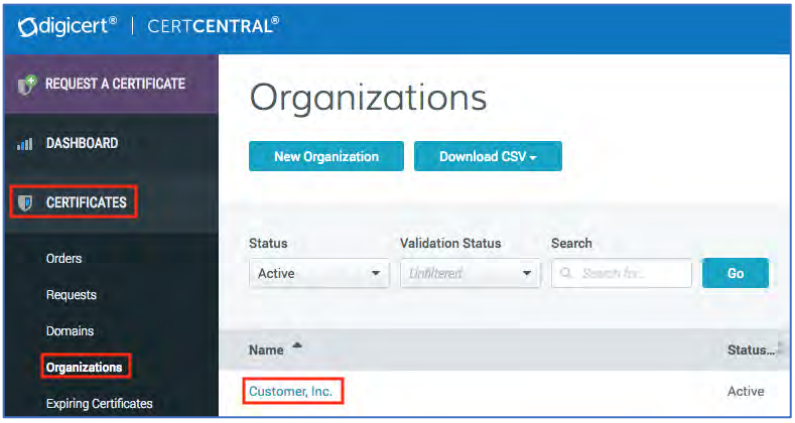
First Name	Enter the contacts first name.
Last Name	Enter the contacts last name.
Job Title	Enter the contacts job title.
Email	Enter an email address at which the contact can be reached.
Phone Number	Enter a phone number at which the contact can be reached.
Phone Extension	Enter the contact's extension, if applicable.

5. When you are finished, click **Save Organization**.

5.4.2 How to Submit an Organization for Validation

After you add your organizations, you can submit then for validation and authorize them for specific types of certificates. When ordering SSL Certificates, this authorization makes domain validation quicker because the organization part of the domain validation process is already completed.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Organizations**.

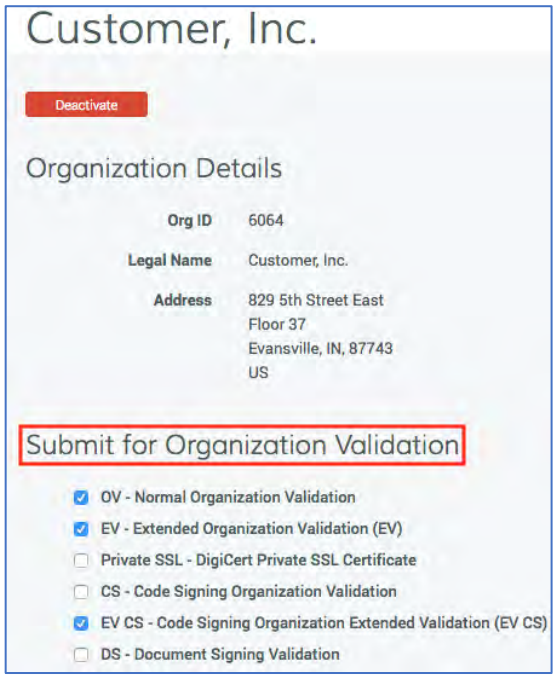


2. On the **Organizations** page, use the drop-down list, search box, and column headers to filter the list of organizations.

3. Click the **"Organization's Name"** link of the organization that you want to submit for validation and authorize for certificates.

4. On the **"Organization's Name"** page, in the **Submit Organization for Validation** section, select the validation types (certificates) for which DigiCert must validate the organization.

   - **OV - Normal Organization Validation**
   - **EV - Extended Organization Validation (EV)***
   - **Private SSL - DigiCert Private SSL Certificate**
   - **CS - Code Signing Organization Validation***
   - **EV CS - Code Signing Organization Extended Validation (EV CS)***
   - **DS – Document Signing Validation**



5. **Add verified contact (EV / EV CS and CS)**

*If the organization validations you chose don't require verified users, skip to step 7.

When you submit orders for EV TLS/SSL, Code Signing, and EV Code Signing certificate orders, we must contact the "verified" contact as part of the organization validation process. However, before we can reach out to the verified contact, we must first validate the contact.

During the organization pre-validation process, you can also submit the organization's verified contacts to be pre-validated. This quickens the certificate issuance process for EV TLS/SSL, Code Signing, and EV Code Signing certificates. Because we've already validated the contact, all we do is contact them and get their order approval.

- If you selected **EV - Extended Organization Validation (EV)**, you must select an organization contact to be designated as an EV verified contact.
- If you selected **EV CS - Code Organization Extended Validation (EV CS)**, you must select an organization contact to be designated as an EV CS verified contact.
- If you selected **CS - Code Signing Organization Validation**, you must select an organization contact to be designated as an CS verified contact.

Only an EV/EV CS verified user can approve Extended Validation (EV) and EV Code Signing Certificate requests. Only a CS verified user can approve Code Signing Certificate requests.

Feature Note:

If you've enabled the **Allow non-DigiCert users to be used as verified contacts** feature (see Enable Adding non-CertCentral Account Users as Verified Contacts), you will see two options: **Existing Contact** and **New Contact**. The **Existing Contact** option lets you assign a CertCentral user as the verified EV contact. The **New Contact** option lets you enter information for a non-CertCentral account user. Use option 1 or 2.

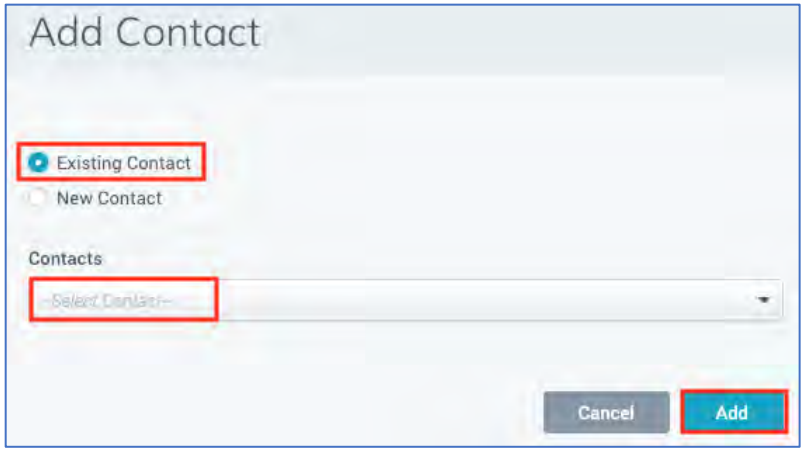
If you haven't enabled this feature, you won't see any options. You can only add account users as verified EV contacts. Use Option 1.

To add an EV, CS, and EV CS verified contact, complete one of the options below. Note that you can add multiple verified contacts.

Option 1: Add an existing CertCentral account user as a verified contact

a. Under **Organization Contacts**, click the **Add Contact** link.

b. In the **Add Contact** window, select **Existing Contact**.



c. In the **Contacts** drop-down list, select verified contact.

   Is the contact you selected missing a **Job Title** or a **Phone** number? Then, you need to add the missing information. For example, if the contact has a job title but no phone number, you will only need to add the phone number.

   i. In the **Job Title** box, enter the contact's job title.

   ii. In the **Phone** box, enter the contact's phone number (and **Ext**).

   When adding **Job Title** and/or **Phone** for an existing contact, the user profile will be updated with the new information.

d. Click **Add**.

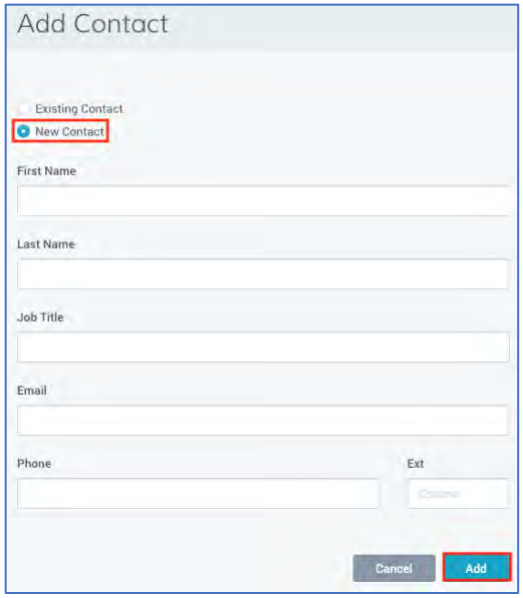
e. To add another verified contact, click the **Add Contact** link.

Option 2: Add a non-CertCentral account user as a verified contact

By default, the **Allow non-CertCentral account users to be used as verified contacts** feature is disabled for a CertCentral account. You can activate this feature on the **Division Preferences** page (**Settings > Preferences**). See Enable Adding non-CertCentral Account Users as Verified Contacts.

a. Under **Organization Contacts**, click the **Add Contact** link.

b. In the **Add Contact** window, select **New Contact**.



c. Add the contact's **First Name**, **Last Name**, and **Job Title**.

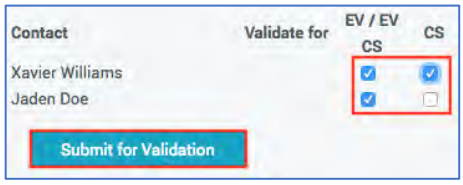
d. Next, add an **Email** address and **Phone** number at which the contact can be contacted for verifying a certificate order.

e. When you are done, click **Add**.

f. To add another verified contact, click the **Add Contact** link.

6. After adding the verified contacts, you can add (check) or remove (uncheck) the types of certificates they can approve (**EV / EV CS** or **CS**).

   Note: After you've submitted a contact as a verified contact for a certificate type (**EV/EV CS** or **CS**), you can't remove it.



7. When you are finished, click **Submit for Validation**.

   DigiCert will now validate the organization for the validation types that you selected and if necessary, the EV/EV CS and CS verified users that you selected.

5.4.3 Enable Adding non-CertCentral Account Users as Verified Contacts

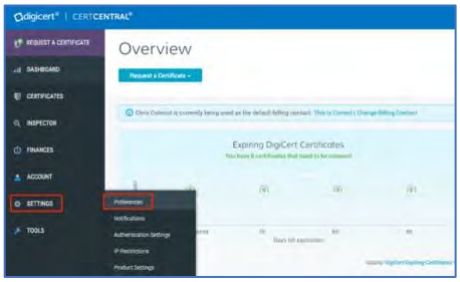
By default, when submitting an organization for EV SSL and EV Code Signing validation or when ordering an EV SSL certificate, you are only able to choose CertCentral account users as verified contacts. However, there are situations where you need someone to be a verified contact, but you don't want to add them to your account just so they can approve EV SSL and EV Code Signing requests.

Use these instructions to allow non-CertCentral account users to be added as EV verified contacts when submitting organizations for EV SSL or EV Code Signing validation and when ordering an EV SSL certificate.

Note: This feature will be added to guest URL EV SSL certificate order forms too.

If you want to limit who can add non-CertCentral account users as verified contacts, see Limit Who Can Add New Contacts from Request Forms.

1. In your CertCentral account, in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, at the bottom of the page, expand **Advanced Settings**.

3. In the **Verified Contacts** section, check **Allow non-DigiCert users to be used as verified contacts**.
4. Scroll to the bottom of the page and click **Save Settings**.
5. Congratulations!

   The next time someone submits an organization for EV validation, or someone orders an EV SSL certificate from inside their account or from a guest URL, they will be able to add a non-CertCentral account user as a verified contact.

5.5 Managing Domains

After you've submitted your organizations for pre-validation, you can begin submitting domains for pre-validation and the type of authorization for which the domain should be validated.

5.5.1 Domain Pre-Validation: 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.

CertCentral features a domain pre-validation process that allows you to pre-validate your domains before you begin ordering certificates for them. We recommend submitting your domains (and organizations) for pre-validation. Taking care of the validation ahead of time means certificates can be issued immediately. When validation can't be done ahead of time, see 5.7 Domain Validation (Pending Order): Domain Control Validation (DCV) Methods.

In CertCentral, DigiCert currently supports the following DCV Methods: WHOIS-based Email, Constructed Email, DNS CNAME, DNS TXT, and HTTP Practical Demonstration.

Email Validation (Default DCV Method)

By default, when you add domains to your account for pre-validation, 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 CNAME Validation

With this validation method, you add a DigiCert generated token (provided for the domain in your CertCentral account) to the domain's DNS as a CNAME record. Then you add dcv.digicert.com as the CNAME target.

DNS TXT Validation

With this validation method, you add a DigiCert generated token (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 verification token.

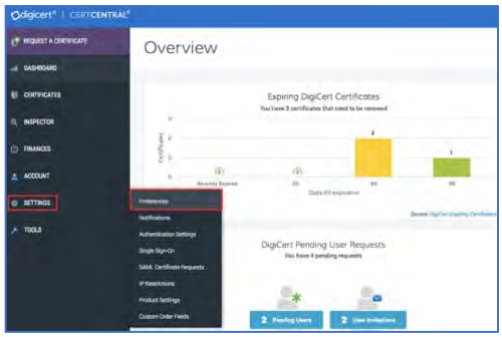
HTTP Practical Demonstration Validation

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

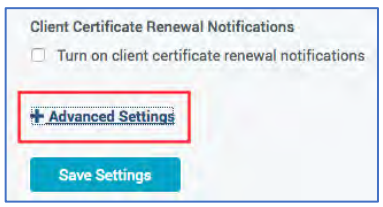
5.5.2 How to Hide Alternative Domain Control Validation (DCV) Methods

If you prefer, you can hide all or specific alternative DCV methods enabled for your account. Note that you cannot hide the email validation method.

1. In your CertCentral account, in the sidebar menu, click **Settings > Preferences**.

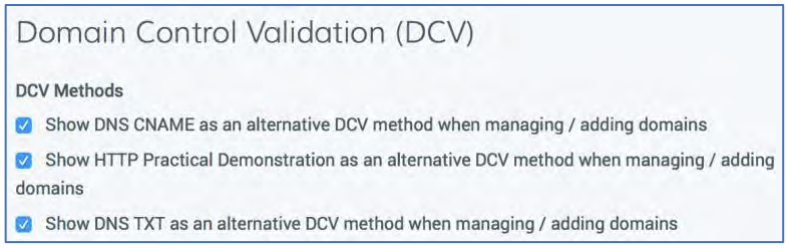


2. On the **Division Preferences** page, at the bottom of the page, click **+ Advanced Settings**.



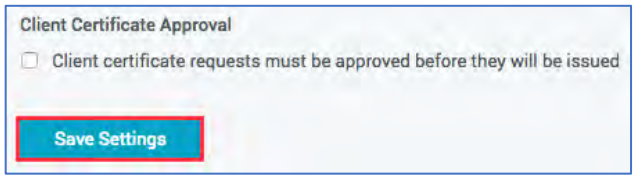
3. In the **Domain Control Validation (DCV)** section, under **DCV Methods**, uncheck the alternative DCV methods that you wish to remove as an option when adding domains for pre-validation:

    - **Show DNS CNAME as an alternative DCV method when managing / adding domains**.
      To demonstrate control over the domain, you add a DigiCert generated token (provided for the domain in your CertCentral account) to the domain's DNS as a CNAME record.
    - **Show HTTP Practical Demonstration as an alternative DCV method when managing / adding domains**
      To demonstrate control over the domain, you host a file containing a DigiCert generated token (provided for the domain in your CertCentral account) at a predetermined location on your website ([domain]/.well-know/pki-validation/[filename].txt).
    - **Show DNS TXT as an alternative DCV method when managing / adding domains**
      To demonstrate control over the domain, you add a DigiCert generated token (provided for the domain in your CertCentral account) to the domain's DNS as a TXT record.



4. At the bottom of the page, click **Save Settings**.

    The next time you add domains for pre-validation or edit a domain, you should no longer see the alternative method(s) that you unchecked.



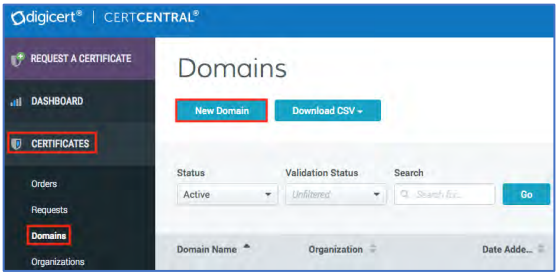
5.5.3 How to Add a Domain, Authorize the Domain for Certificates, and Use Verification Email as the DCV Method

Use these instructions to add and authorize a domain for TLS/SSL certificates and to select the Verification Email as the DCV method you want to use to complete its domain validation.

Validation Note: Before you can pre-validate a domain for TLS/SSL validation, you must first submit the organization to be pre-validated. Additionally, if you want the domain to be used for OV, EV, and/or Private SSL certificates, you must submit its organization for those matching validation types.

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. See Domain Pre-Validation: Domain Control Validation (DCV) Methods.

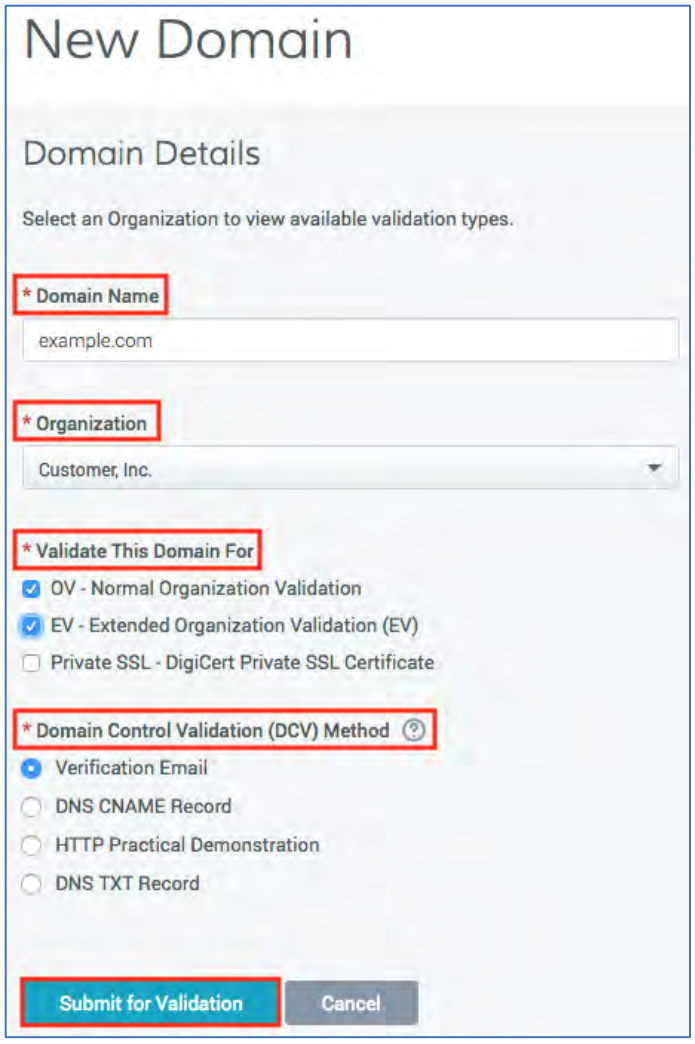
1. In your CertCentral account, in the sidebar menu, click **Certificates > Domains**.



2. On the **Domains** page, click **New Domain**.

3. On the **New Domain** page, under **Domain Details**, enter the following information:

    a. ***Domain Name**
    Enter the domain name the certificates for it will secure (for example, *yourdomain.com*).



    b. ***Organization**
    In the drop-down list, select the organization you want to assign the domain to.

4. Under ***Validate This Domain For**, check the validation types you want the domain validated for.

   - **OV - Normal Organization Validation**
     Use this option so you can order Standard SSL, Secure Site SSL, Wildcard SSL, Secure Site Wildcard SSL, Multi-Domain SSL, and Secure Site Multi-Domain SSL Certificates for this domain.
   - **EV - Extended Organization Validation (EV)**
     Use this option so you can order EV SSL, Secure Site EV SSL, EV Multi-Domain SSL, and Secure Site EV Multi-Domain SSL Certificates for this domain.
   - **Private SSL - DigiCert Private SSL Certificate**
     Use this option so you can order Private SSL certificates for this domain.

5. Under ***Domain Control Validation (DCV) Method**, select **Verification Email**.

   To demonstrate control over the domain, an email recipient follows the instructions in a confirmation email sent for the domain.

6. When you are finished, click **Submit for Validation**.

   DigiCert now sends two sets of DCV emails: WHOIS-based and Constructed.

5.5.4 How to Add a Domain, Authorize the Domain for Certificates, and Use DNS CNAME Record as the DCV Method

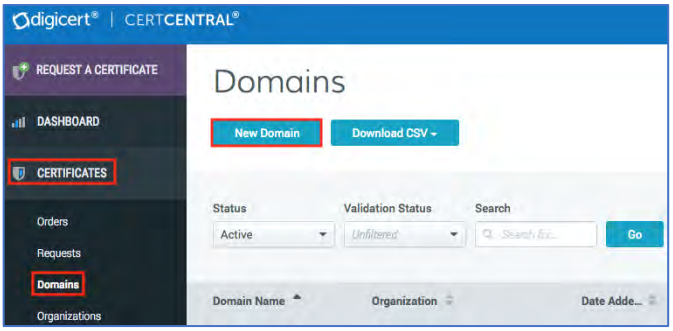
Use these instructions to add and authorize a domain for TLS/SSL certificates. Then, use the DNS CNAME Record DCV method to demonstrate control over the domain in your CertCentral account.

Validation Note: Before you can pre-validate a domain for TLS/SSL validation, you must first submit the organization to be pre-validated. Additionally, if you want the domain to be used for OV, EV, and/or Private SSL certificates, you must submit its organization for those matching validation types.

This validation method allows you to demonstrate control over your domain by creating a DNS CNAME record containing a randomly generated token. The CNAME record is used to point token.domain to DigiCert (*dcv.digicert.com*).

Step I: Add and Authorize a Domain For TLS/SSL Certificates

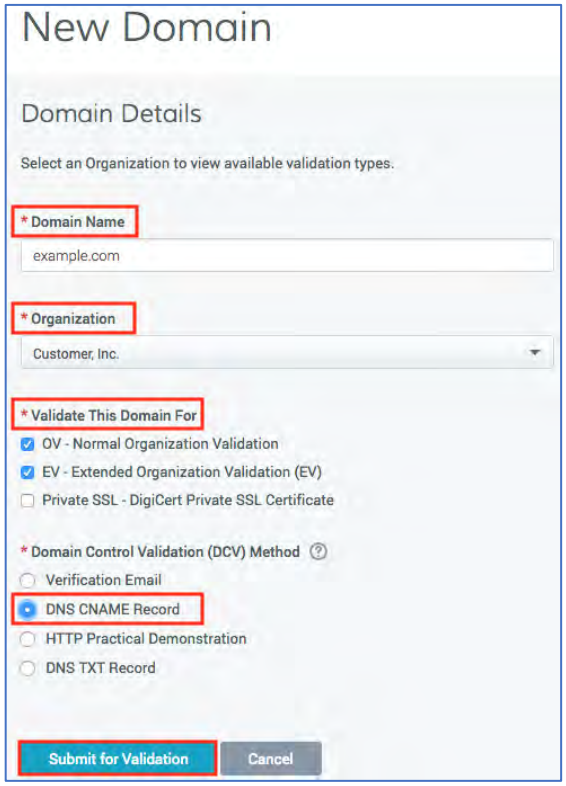
1. In your CertCentral account, in the sidebar menu, click **Certificates > Domains**.



2. On the **Domains** page, click **New Domain**.

3. On the **New Domain** page, under **Domain Details**, enter the following domain information:

    a. ***Domain Name**
    In the box, enter the domain name the certificates for it will secure (for example, *yourdomain.com*).



    b. ***Organization**
    In the drop-down list, select the organization you want to assign the domain to.

4. Under ***Validate This Domain For**, check the validation types you want the domain validated for:

    - **OV - Normal Organization Validation**
    Use this option so you can order Standard SSL, Secure Site SSL, Wildcard SSL, Secure Site Wildcard SSL, Multi-Domain SSL, and Secure Site Multi-Domain SSL Certificates for this domain.

    - **EV - Extended Organization Validation (EV)**
    Use this option so you can order EV SSL, Secure Site EV SSL, EV Multi-Domain SSL, and Secure Site EV Multi-Domain SSL Certificates for this domain.

    - **Private SSL - DigiCert Private SSL Certificate**
    Use this option so you can order Private SSL certificates for this domain.

5. Under ***Domain Control Validation (DCV) Method**, select **DNS CNAME** Record.

    Note: The default DCV method is **Verification Email**.

6. When you are finished, click **Submit for Validation**.

Step II: Use DNS CNAME Record to Demonstrate Control Over the Domain

7. **Create the DNS CNAME Record:**

    a. Under **User Actions**, in the **Your unique verification token** box, copy your verification token.

    To copy the value to your clipboard, single click in the text field.

    Note: The unique verification token expires after thirty days. To generate a new token, click the **Generate New Token** link.

    b. Go to your DNS provider's site and create a new CNAME record.

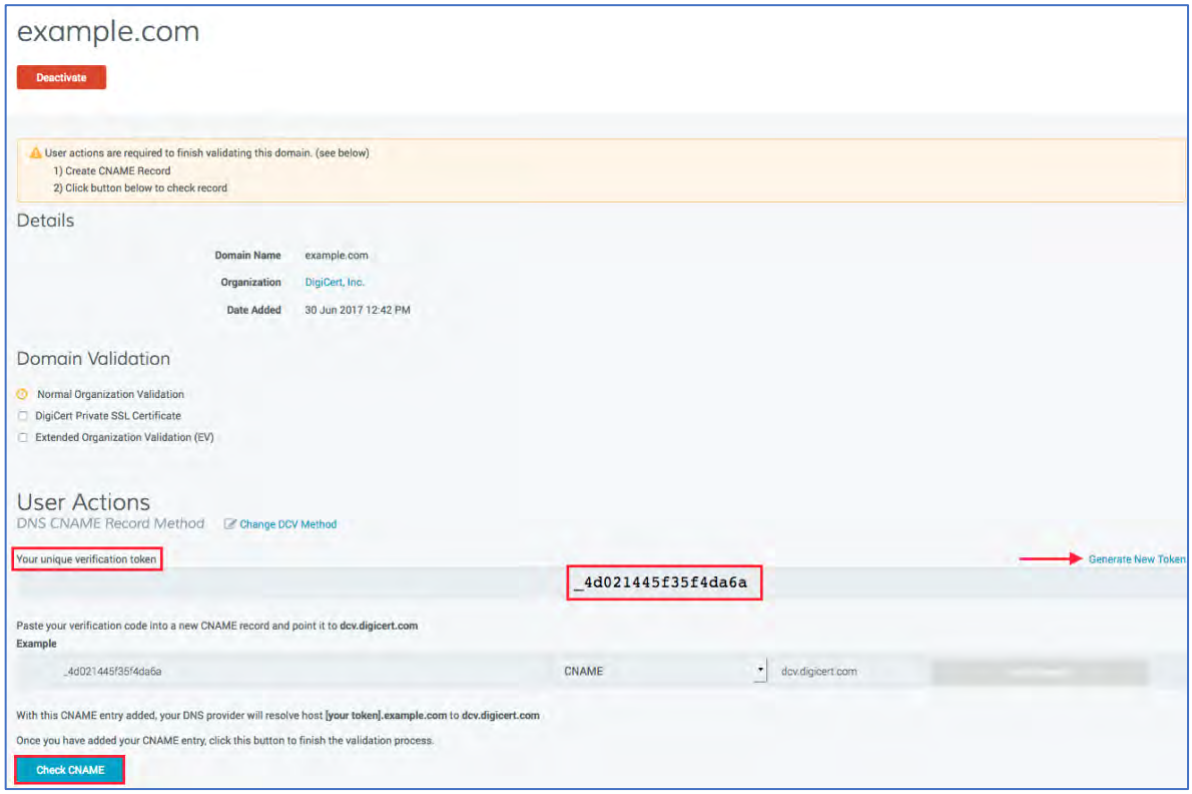
    c. In the hostname field (or equivalent), paste the verification token that you copied from your DigiCert account.

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

    e. In the target host field (or equivalent), enter ***dcv.digicert.com*** (this points the CNAME record to dcv.digicert.com).

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

    g. Save the record.



8. **Verify the DNS CNAME Record:**

    a. In your CertCentral account, in the sidebar menu click **Certificates > Domains**.

    b. On the **Domains** page, in the **Domain Name** column, click ***"Domain Name"*** link for the domain.

    c. On the ***"Domain Name"*** page, at the bottom of the page, click **Check CNAME**.

    You have successfully verified the CNAME.

5.5.5 How to Add a Domain, Authorize the Domain for Certificates, and Use DNS TXT as the Validation Method

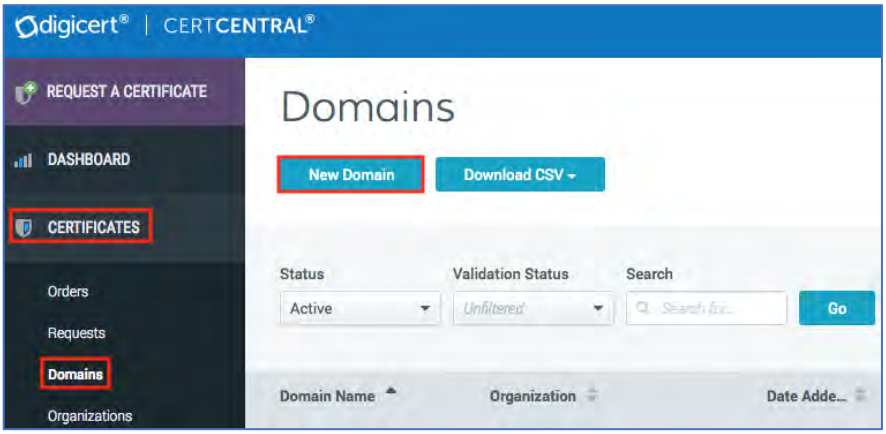
Use these instructions to add and authorize a domain for TLS/SSL certificates. Then, use the DNS TXT Record DCV method to demonstrate control over the domain in your CertCentral account.

Validation Note: Before you can pre-validate a domain for TLS/SSL validation, you must first submit the organization to be pre-validated. Additionally, if you want the domain to be used for OV, EV, and/or Private SSL certificates, you must submit its organization for those matching validation types.

This validation method allows you to demonstrate control over your domain by creating a DNS TXT record containing a randomly generated token as the value. Once the DNS TXT record is created, DigiCert searches the domain's DNS records to confirm the presence of your verification token.

Step I: Add and Authorize a Domain For TLS/SSL Certificates

1. In your CertCentral account, in the sidebar menu, click **Certificates > Domains**.

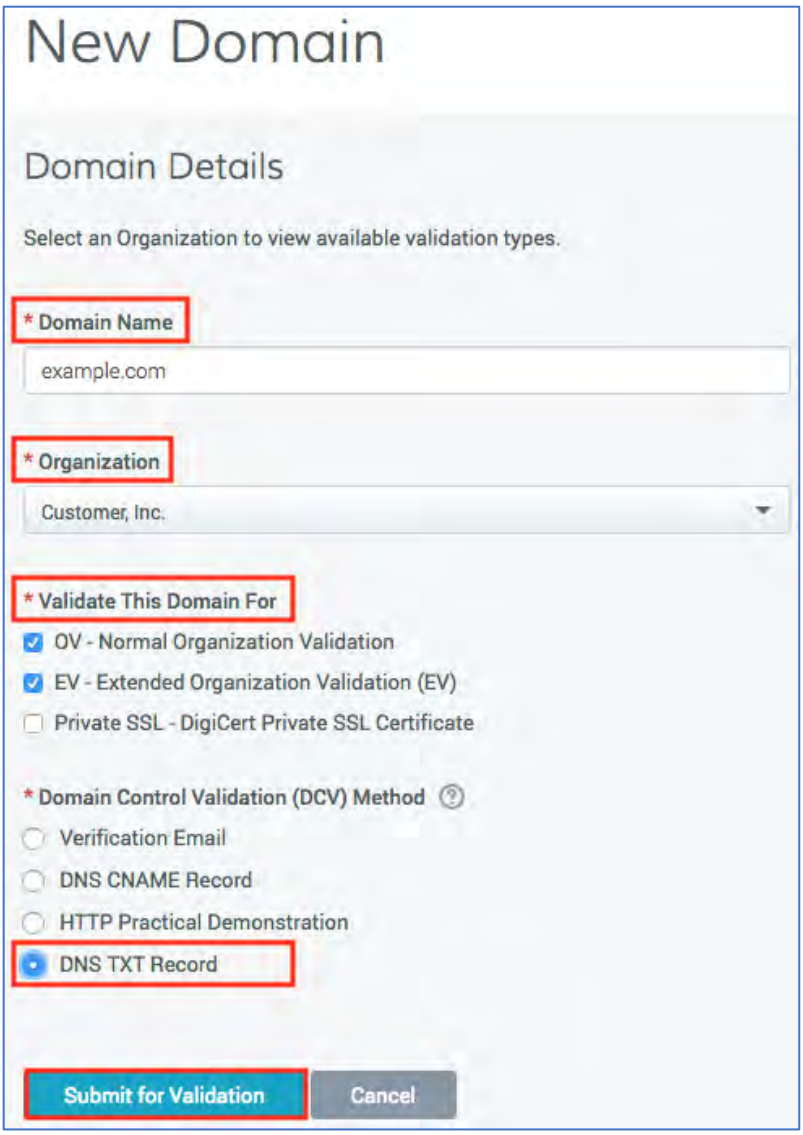


2. On the **Domains** page, click **New Domain**.

3. On the **New Domain** page, under **Domain Details**, enter the following domain information:

    a. ***Domain Name**
    In the box, enter the domain name the certificates for it will secure for example, *yourdomain.com*).

    b. ***Organization**
    In the drop-down list, select the organization you want to assign the domain to.



4. Under ***Validate This Domain For**, check the validation types you want the domain validated for:

   - **OV - Normal Organization Validation**
     Use this option so you can order Standard SSL, Secure Site SSL, Wildcard SSL, Secure Site Wildcard SSL, Multi-Domain SSL, and Secure Site Multi-Domain SSL Certificates for this domain.
   - **EV - Extended Organization Validation (EV)**
     Use this option so you can order EV SSL, Secure Site EV SSL, EV Multi-Domain SSL, and Secure Site EV Multi-Domain SSL Certificates for this domain.
   - **Private SSL - DigiCert Private SSL Certificate**
     Use this option so you can order Private SSL certificates for this domain.

5. Under ***Domain Control Validation (DCV) Method**, select **DNS TXT Record**.

   Note: The default DCV method is by verification email.

6. When you are finished, click **Submit for Validation**.

Step II: Use DNS TXT Record to Demonstrate Control Over the Domain

7. **Create Your DNS TXT Record:**

    a. Under **User Actions**, in the **Your unique verification token** box, copy your verification token.

    To copy the value to your clipboard, single click in the text field.

    Note: The unique verification token expires after thirty days. To generate a new token, click the **Generate New Token** link.

    b. Go to your DNS provider's site and create a new TXT record.

    c. In the **TXT Value** field, paste your verification code you copied from your CertCentral account.

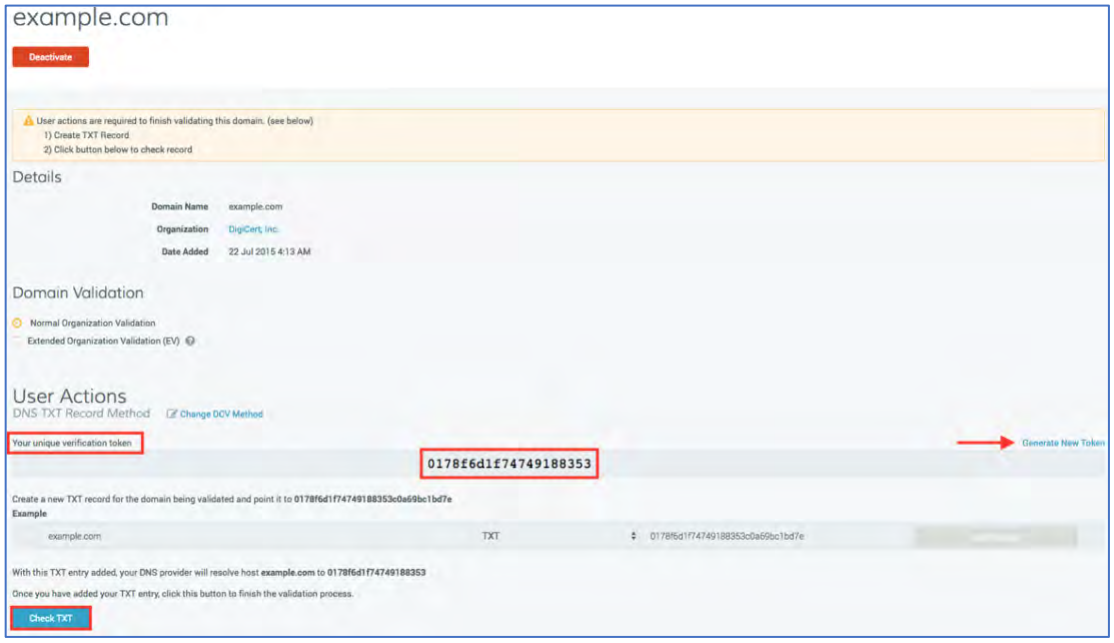
    d. **Host** field

    - **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.

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

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

    g. Save the record.



8. **Verify the DNS TXT Record:**

    a. In your CertCentral account, in the sidebar menu, click **Certificates > Domains**.

    b. On the **Domains** page, in the **Domain Name** column, click ***"Domain Name"*** link for the domain.

    c. On the ***"Domain Name"*** page (e.g., *example.com*), at the bottom of the page, click **Check TXT**.

    You have successfully verified the TXT record.

5.5.6 How to Add a Domain, Authorize the Domain for Certificates, and Use HTTP Practical Demonstration as the Validation Method

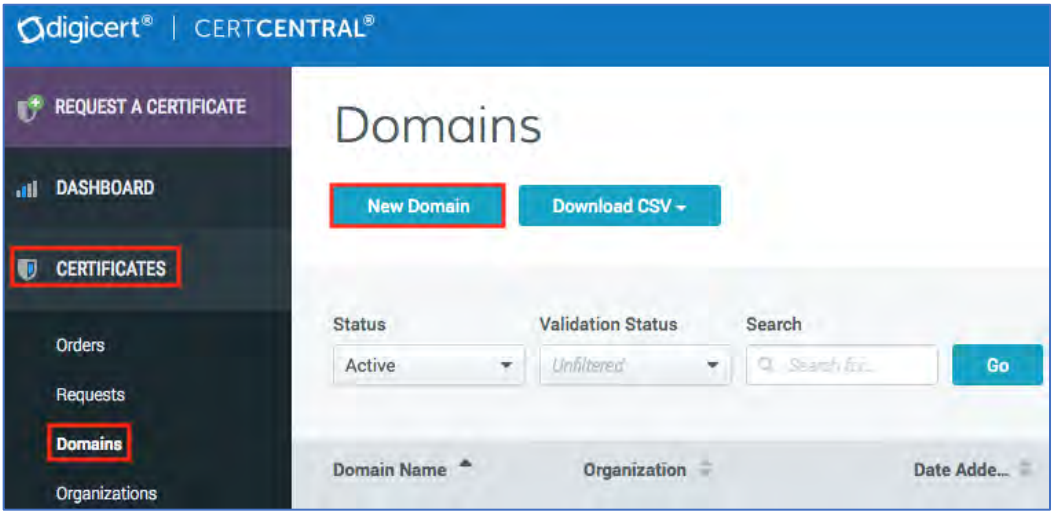
Use these instructions to add and authorize a domain for TLS/SSL certificates. Then, use the HTTP Practical Demonstration DCV method to demonstrate control over the domain in your CertCentral account.

Validation Note: Before you can pre-validate a domain for TLS/SSL validation, you must first submit the organization to be pre-validated. Additionally, if you want the domain to be used for OV, EV, and/or Private SSL certificates, you must submit its organization for those matching validation types.

This validation method allows you to demonstrate control over your domain by hosting a .txt file containing a randomly generated token value 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 verification token. Make sure to avoid some of the more Common Mistakes: HTTP Practical Demonstration DCV Method.

Step I: Add and Authorize a Domain for TLS/SSL Certificate

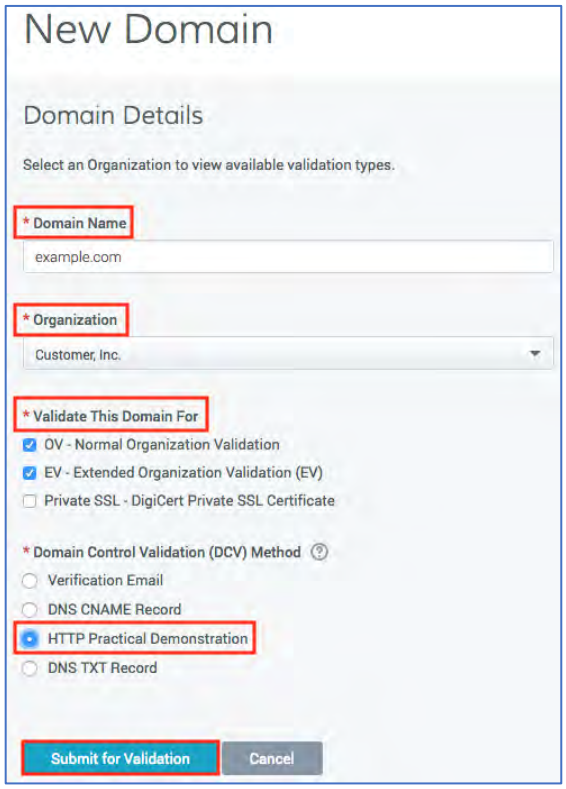
1. In your CertCentral account, in the sidebar menu, click **Certificates > Domains**.



2. On the **Domains** page, click **New Domain**.

3. On the **New Domain** page, under **Domain Details**, enter the following domain information:

a. ***Domain Name**
In the box, enter the domain name the certificates for it will secure (for example, *yourdomain.com*).



b. ***Organization**

In the drop-down list, select the organization you want to assign the domain to.

4. Under ***Validate This Domain For**, check the validation types for which the domain must be validated.

   - **OV - Normal Organization Validation**
     Use this option so you can order Standard SSL, Secure Site SSL, Wildcard SSL, Secure Site Wildcard SSL, Multi-Domain SSL, and Secure Site Multi-Domain SSL Certificates for this domain.
   - **EV - Extended Organization Validation (EV)**
     Use this option so you can order EV SSL, Secure Site EV SSL, EV Multi-Domain SSL, and Secure Site EV Multi-Domain SSL Certificates for this domain.
   - **Private SSL - DigiCert Private SSL Certificate**
     Use this option so you can order Private SSL certificates for this domain.

5. Under ***Domain Control Validation (DCV) Method**, select **HTTP Practical Demonstration**.

   Note: The default DCV method is by verification email.

6. When you are finished, click **Submit for Validation**.

Step II: Use HTTP Practical Demonstration to Demonstrate Control Over the Domain

7. **Create Your .txt File:**

    a. Under **User Actions**, in the **Your unique verification token** box, copy your verification token.

    To copy the value to your clipboard, single click in the text field.

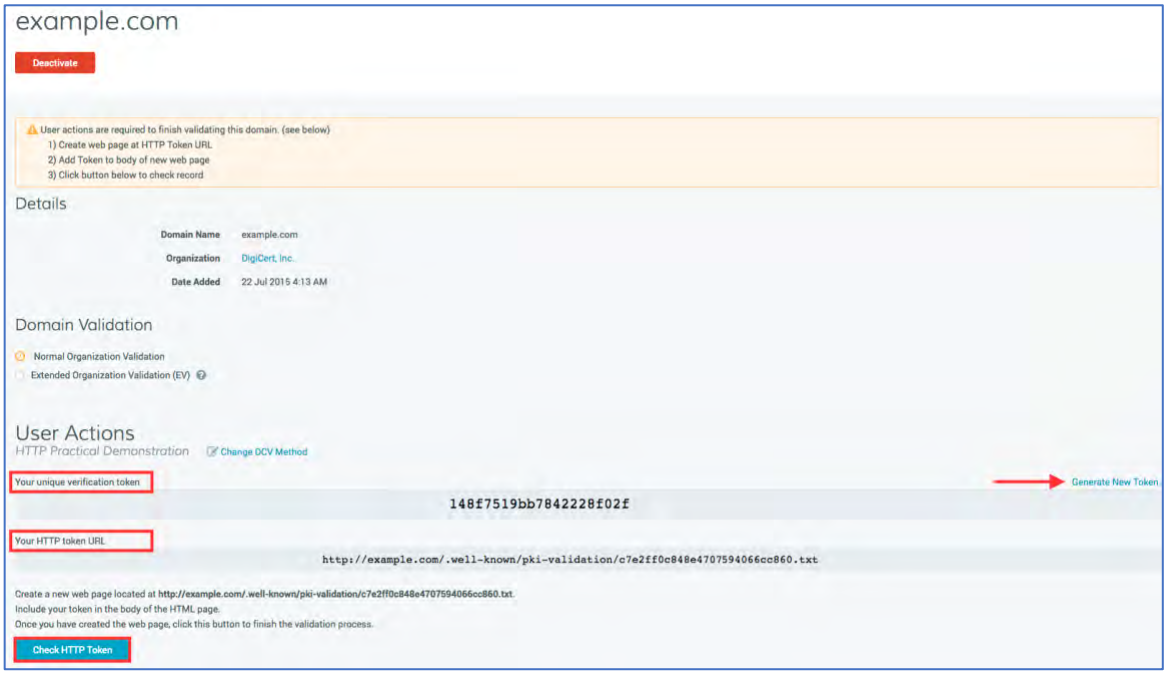
    Note: The unique verification token expires after thirty days. To generate a new token, click the **Generate New Token** link.

    b. Open a text editor (such as Notepad) and paste in **Your unique verification token**.

    c. In **Your HTTP token URL**, the string after **pki-validation/** is the name of your .txt file.

    For example, if **Your HTTP token URL** is **http://example.com/.well-known/pki-validation/c7e2ff0c848e4707594066cc860.txt**, then, your file name is **c7e2ff0c848e4707594066cc860.txt**

    d. Save the .txt file from under this name (for example, **c7e2ff0c848e4707594066cc860.txt**).



8. **Create the .well-known/pki-validation/ Directory:**

Create the **.well-known/pki-validation/** directory on your site and place your .txt file in it.

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

9. **Verify the HTTP Token**.

    a. In your CertCentral account, in the sidebar menu, click **Certificates > Domains**.

    b. On the **Domains** page, in the **Domain Name** column, click ***"Domain Name"*** link for the domain.

    c. On the ***"Domain Name"*** page (e.g., *example.com*), at the bottom of the page, click **Check HTTP Token**.

    You have successfully verified your URL (web page).

10. **Troubleshooting Tips:**

    Verify the URL matches exactly

    Make sure that the URL for your web page matches the DigiCert provided URL.

    - http://***YourDomain.com***/.well-known/pki-validation/**[filename].txt**

    Where **YourDomain.com** matches the domain that you are validating and **[filename].txt** matches the unique hash provided by DigiCert under **Your HTTP token URL** (for example, **c7e2ff0c848e4707594066cc860**.txt).

    Important: If you are missing a **period**, a number, or a letter, validation cannot be completed.

5.5.7 Common Mistakes: HTTP Practical Demonstration DCV Method

To validate your domain using the HTTP Practical Demonstration DCV method, DigiCert provides you with a URL and a token value. The URL 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 verificationtoken.txt you add the generated random value to.

Below are some of the more common issues we run into when troubleshooting the reason HTTP Practical Demonstration checks fail. The HTTP Practical Demonstration 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 verificationtoken.txt file with our generated random value in it.

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

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

To complete domain control validation for yourdomain.com, place the verificationtoken.txt file on the exact domain you want validated; the one we generate the URL for. We won't look at a different domain or subdomain to find our random token. We only look at the domain you want validated (such as the domain on your certificate order).

For example, if you need yourdomain.com validated so that you can request TLS/SSL certificates for it, we generate a URL for this domain – [http://yourdomain.com]/.well-known/pki-validation/verificationtoken.txt. Don't place the verificationtoken.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 verificationtoken.txt file on these domains – only on yourdomain.com.

yourdomain.com and www.yourdomain.com

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

Free Base Domain SAN

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

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

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

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

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

When using the HTTP Practical Demonstration method for domain validation, the verificationtoken.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 verificationtoken.txt file and verify your control over the domain.

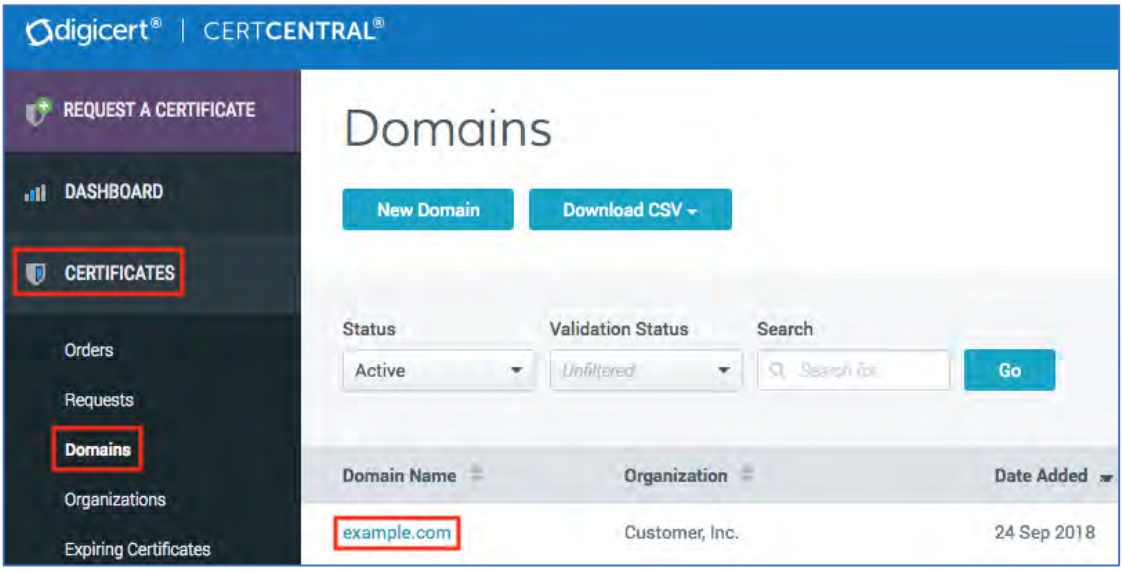
For example, you need a certificate for http://example.com, but the page redirects to https://www.example.com. That's okay. You can place the verificationtoken.txt file on the http://example.com page. We will still be able to follow the single redirect to validate your control over http://example.com.

However, if you place the verificationtoken.txt file on a page with multiple redirects, we won't be able to locate the file. Multiple redirects block us from locating the verificationtoken.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 verificationtoken.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 verificationtoken.txt and validate your control over http://multiple-redirect.com.

5.5.8 How to Change a Domain's Domain Control Validation (DCV) Method

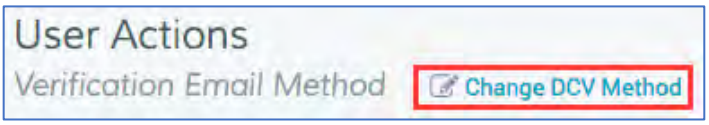
1. In your account, in the sidebar menu, click **Certificates > Domains**.



2. On the **Domains** page, use the drop-down lists, search box, and column headers to filter the list of domains.

3. In the **Domain Name** column, click the ***"Domain name"*** link for the domain with DCV method you need to change.

4. On the ***"Domain name"*** page, in the **User Actions** section, click **Change DCV Method**.



5. In the **Change DCV Method** window, under ***Domain Control Validation (DCV) Method**, select the DCV method you want to use to complete the validation for the domain.

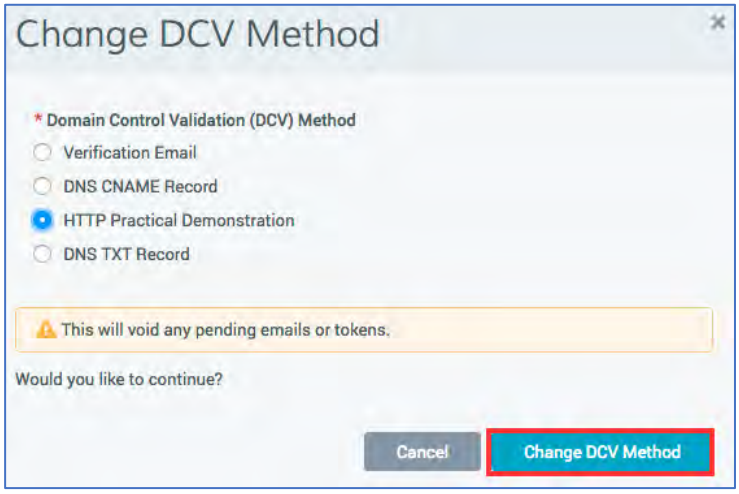
   If you change the DCV method for a domain that is pending validation, you will void any pending verification emails or unique verification tokens.

   - **Verification Email**
     To demonstrate control over the domain, an email recipient follows the instructions in a confirmation email sent for the domain.

- **DNS CNAME Record**
  To demonstrate control over the domain, you add a DigiCert generated token (provided for the domain in your CertCentral account) to the domain's DNS as a CNAME record.

- **HTTP Practical Demonstration**
  To demonstrate control over the domain, you host a file containing a DigiCert generated token (provided for the domain in your CertCentral account) at a predetermined location on your website ([domain]/.well-know/pki-validation/[filename].txt).

- **DNS TXT Record**
  To demonstrate control over the domain, you add a DigiCert generated token (provided for the domain in your CertCentral account) to the domain's DNS as a TXT record.



6. When you are finished, click **Change DCV Method**.

5.6 Domain Validation (Pending Order): 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.

CertCentral features a domain pre-validation process that allows you to pre-validate your domains before you begin ordering certificates for them (see Domain Pre-Validation: Domain Control Validation (DCV) Methods). However, sometimes certificates are needed for domains that haven't been pre-validated.

CertCentral allows you to submit orders for non-validated domains. After your order has been placed, you will need to complete domain validation on pending orders for non-validated domains submitted during the order process.

Note: Certificates will not be issued until domain validation is completed. Taking care of the validation ahead of time means certificates can be issued immediately.

In CertCentral, DigiCert currently supports the following DCV Methods: WHOIS-based Email, Constructed Email, DNS CNAME, DNS TXT, and HTTP Practical Demonstration.

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 CNAME Validation

With this validation method, you add a DigiCert generated token (provided for the domain in your CertCentral account) to the domain's DNS as a CNAME record. Then you add dcv.digicert.com as the CNAME target.

DNS TXT Validation

With this validation method, you add a DigiCert generated token (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 verification token.

HTTP Practical Demonstration Validation

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

5.6.1 Domain Validation (Pending Order): Use the Verification Email DCV Method

Use these instructions to check the status of your TLS/SSL certificate order and use the Verification Email DCV method to demonstrate control over a domain on the order.

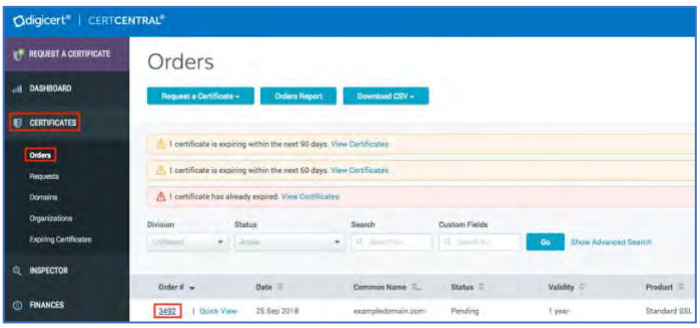
Note: Submitting domains for validation during the order process means certificates will not be issued until domain validation is completed. For immediate certificate issuance, submit domains for pre-validation when possible.

With the Email 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.

Step 1: Check the Status of Your Pending Order

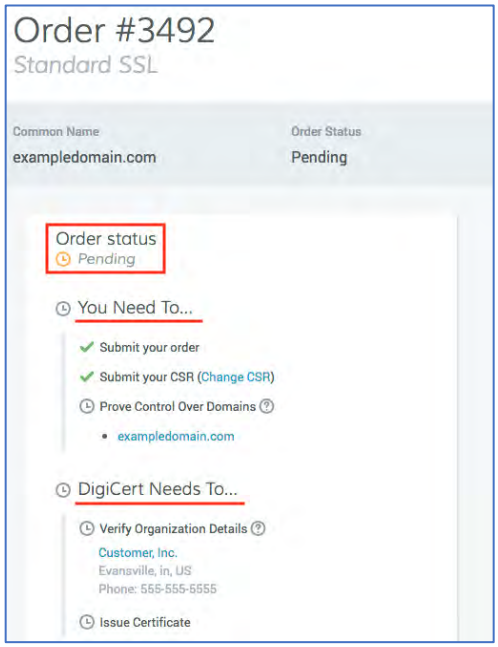
After you've ordered an TLS/SSL certificate, you can visit the certificate's **Order#** details page to see its validation status. You can also see if the order is waiting on domain or organization validation to be completed before it can be issued.

1. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.



2. On the **Orders** page, use the filters and advanced search features to locate the pending certificate order you want to view.
3. In the **Order#** column of the certificate order, click the order number link.
4. On the **Order#** details page, in the **Order status** section, you can check the order's validation status (for example, is the order waiting on domain or organization validation to be completed).

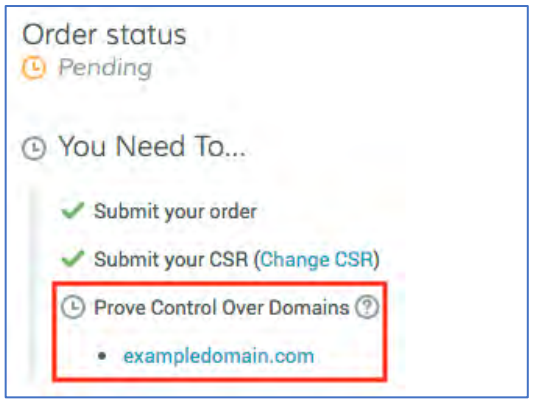
   Note: After validation is completed (domains and organization), the **Order status** section no longer appears on the **Order#** details page.



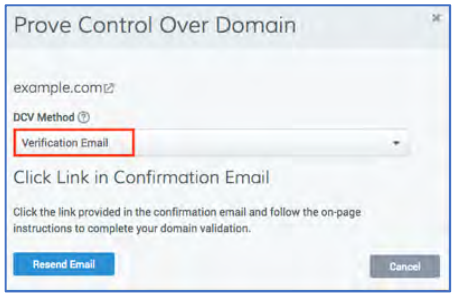
Step 2: Send the DCV Emails

5. On the **Order#** details page, in the **Order status** section, under **You Need To**, locate the domain pending validation and click the domain link.

   Note: When you have multiple domains (SANs) on your order, each one will be listed. Those with a checkmark next to them are validated. Those with a clock icon next to them are pending validation.



6. In the **Prove Control Over Domain** window, in the **DCV Method** drop-down list, select **Verification Email**.



7. We will now search for your domain's WHOIS record and any MX records and send the DCV email to the discovered/verified addresses.

8. To locate emails, search your inbox for emails from validation@digicert.com and for the domain names you are trying to validate. Note that you may also need to check your junk/spam folder.

9. You can come back and resend the DCV emails if needed.

5.6.2 Domain Validation (Pending Order): Use the DNS CNAME Record DCV Method

Use these instructions to check the status of your TLS/SSL certificate order and use the DNS CNAME Record DCV method to demonstrate control over a domain on the order.

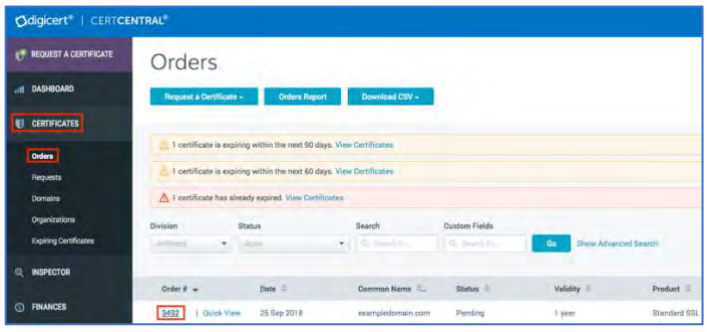
Note: Submitting domains for validation during the order process means certificates will not be issued until domain validation is completed. For immediate certificate issuance, submit domains for pre-validation when possible.

This validation method allows you to demonstrate control over your domain by creating a DNS CNAME record containing a randomly generated token. The CNAME record is used to point *token.domain* to DigiCert (*dcv.digicert.com*).

Step 1: Check the Status of Your Pending Order

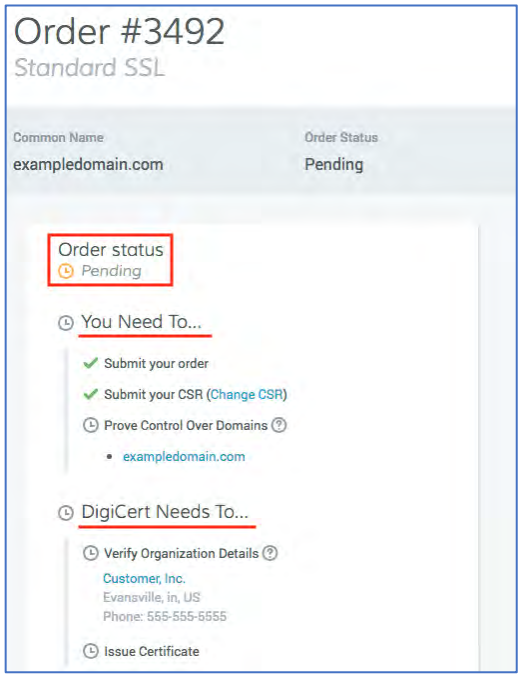
After you've ordered a TLS/SSL certificate, you can visit the certificate's **Order#** details page to see its validation status. You can also see if the order is waiting on domain or organization validation to be completed before it can be issued.

1. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.



2. On the **Orders** page, use the filters and advanced search features to locate the pending certificate order you want to view.
3. In the **Order#** column of the certificate order, click the order number link.
4. On the **Order#** details page, in the **Order status** section, you can check the order's validation status (for example, is the order waiting on domain or organization validation to be completed).

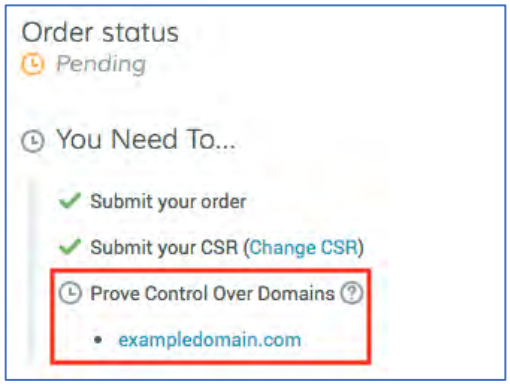
   Note: After validation is completed (domains and organization), the **Order status** section no longer appears on the **Order#** details page.



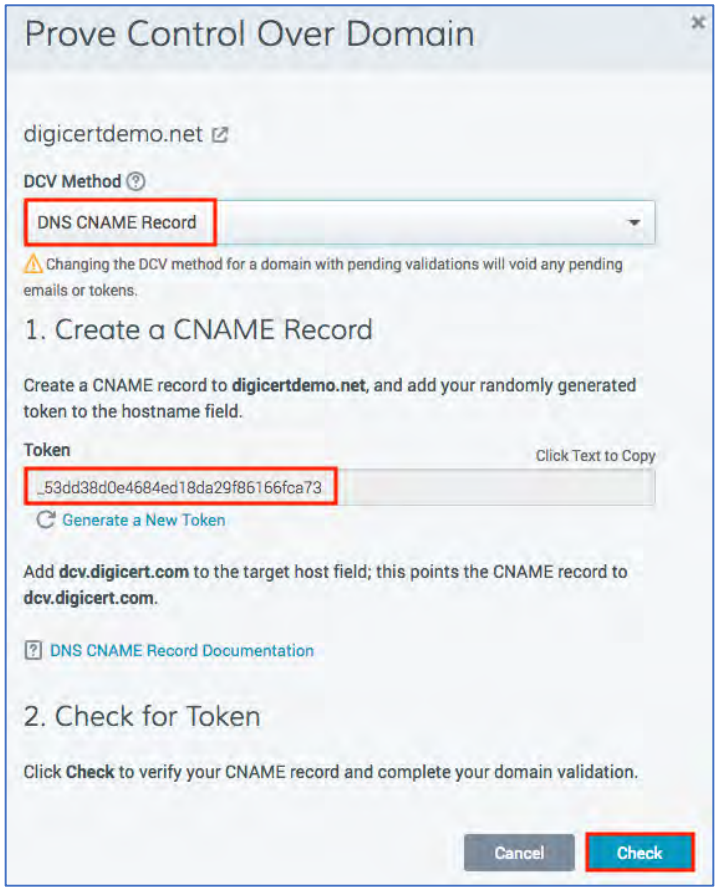
Step II: Use DNS CNAME Record to Demonstrate Control Over the Domain

5. On the **Order#** details page, in the **Order status** section, under **You Need To**, locate the domain pending validation and click the domain link.

   Note: When you have multiple domains (SANs) on your order, each one will be listed. Those with a checkmark next to them are validated. Those with a clock icon next to them are pending validation.



6. In the **Prove Control Over Domain** window, in the **DCV Method** drop-down list, select **DNS CNAME Record**.



7. **Create the DNS CNAME Record:**

    a. In the **Token** box, copy your unique token.

    To copy the value to your clipboard, single click in the text field.

    Note: The unique token expires after thirty days. To generate a new token, click the **Generate a New Token** link.

    b. Go to your DNS provider's site and create a new CNAME record.

    c. In the hostname field (or equivalent), paste the unique token that you copied from your DigiCert account.

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

    e. In the target host field (or equivalent), enter ***dcv.digicert.com*** (this points the CNAME record to dcv.digicert.com).

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

    g. Save the record.

8. **Verify the DNS CNAME Record:**

    a. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.

    b. On the **Orders** page, in the **Order#** column of the certificate order, click the order number link.

    c. On the **Order #** details page, in the **Order status** section, under **You Need To**, locate the domain and click the domain link.

    d. In the **Prove Control Over Domain** window, under **2. Check for Token** click **Check**.

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

5.6.3 Domain Validation (Pending Order): Use the DNS TXT Record DCV Method

Use these instructions to check the status of your TLS/SSL certificate order and use the DNS TXT Record DCV method to demonstrate control over a domain on the order.

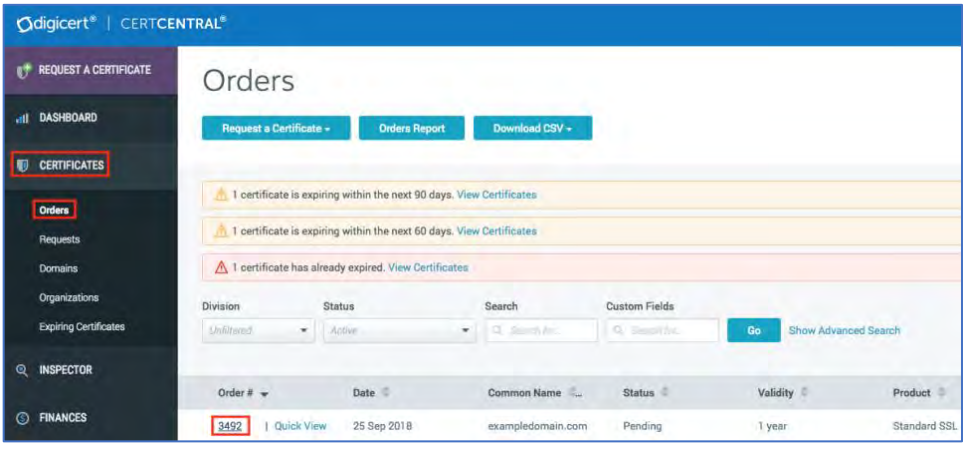
Note: Submitting domains for validation during the order process means certificates will not be issued until domain validation is completed. For immediate certificate issuance, submit domains for pre-validation when possible.

This validation method allows you to demonstrate control over your domain by creating a DNS TXT record containing a randomly generated token as the value. Once the DNS TXT record is created, DigiCert searches the domain's DNS records to confirm the presence of your verification token.

Step 1: Check the Status of Your Pending Order

After you've ordered a TLS/SSL certificate, you can visit the certificate's **Order#** details page to see its validation status. You can also see if the order is waiting on domain or organization validation to be completed before it can be issued.

1. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.

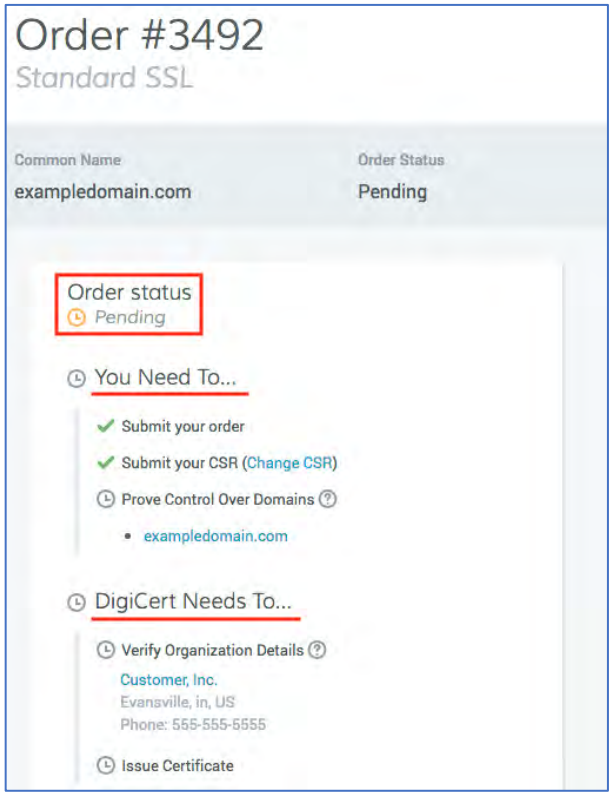


2. On the **Orders** page, use the filters and advanced search features to locate the pending certificate order you want to view.

3. In the **Order#** column of the certificate order, click the order number link.

4. On the **Order#** details page, in the **Order status** section, you can check the order's validation status (for example, is the order waiting on domain or organization validation to be completed).

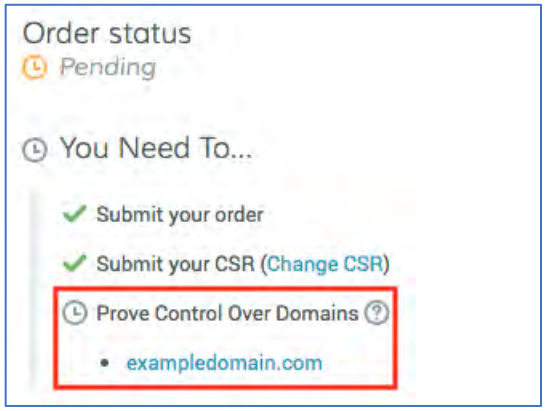
   Note: After validation is completed (domains and organization), the **Order status** section no longer appears on the **Order#** details page.



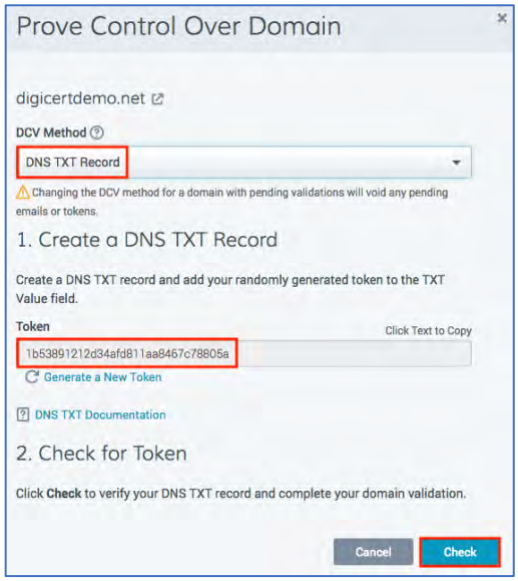
Step II: Use DNS TXT Record to Demonstrate Control Over the Domain

5. On the **Order#** details page, in the **Order status** section, under **You Need To**, locate the domain pending validation and click the domain link.

   Note: When you have multiple domains (SANs) on your order, each one will be listed. Those with a checkmark next to them are validated. Those with a clock icon next to them are pending validation.



6. In the **Prove Control Over Domain** window, in the **DCV Method** drop-down list, select **DNS TXT Record**.



7. **Create the DNS TXT Record:**

    a. In the **Token** box, copy your unique token.

    To copy the value to your clipboard, single click in the text field.

    Note: The unique token expires after thirty days. To generate a new token, click the **Generate a New Token** link.

    b. Go to your DNS provider's site and create a new TXT record.

    c. In the **TXT Value** field, paste the unique token that you copied from your DigiCert account.

    d. **Host** field

        i. Base Domain (e.g., example.com)

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

        ii. Subdomain (e.g., my.example.com)

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

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

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

    g. Save the record.

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 certificate order, click the order number link.

c. On the **Order#** details page, in the **Order status** section, under **You Need To**, locate the domain and click the domain link.

d. In the **Prove Control Over Domain** window, under **2. Check for Token** click **Check**.

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

5.6.4 Domain Validation (Pending Order): Use the HTTP Practical Demonstration DCV Method

Use these instructions to check the status of your TLS/SSL certificate order and use the HTTP Practical Demonstration DCV method to demonstrate control over a domain on the order.

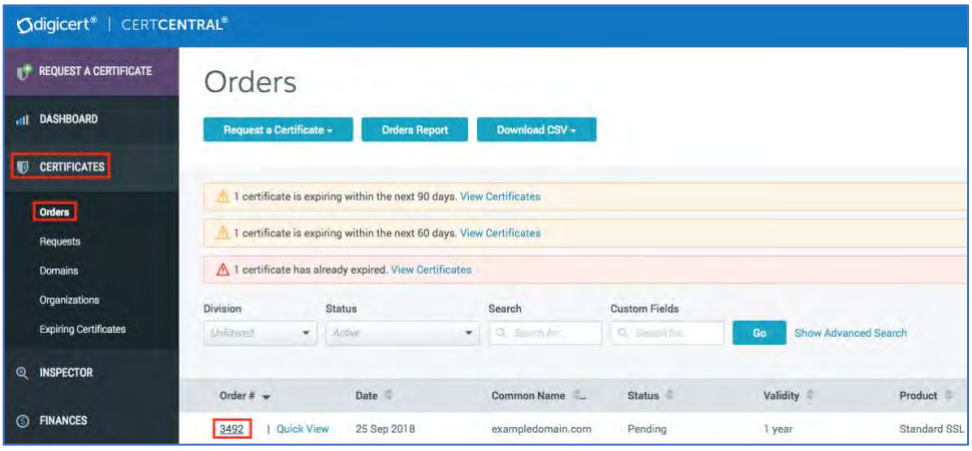
Note: Submitting domains for validation during the order process means certificates will not be issued until domain validation is completed. For immediate certificate issuance, submit domains for pre-validation when possible.

This validation method allows you to demonstrate control over your domain by hosting a .txt file containing a randomly generated token value 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 verification token. Make sure to avoid some of the more Common Mistakes: HTTP Practical Demonstration DCV Method.

Step 1: Check the Status of Your Pending Order

After you've ordered a TLS/SSL certificate, you can visit the certificate's **Order#** details page to see its validation status. You can also see if the order is waiting on domain or organization validation to be completed before it can be issued.

1. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.

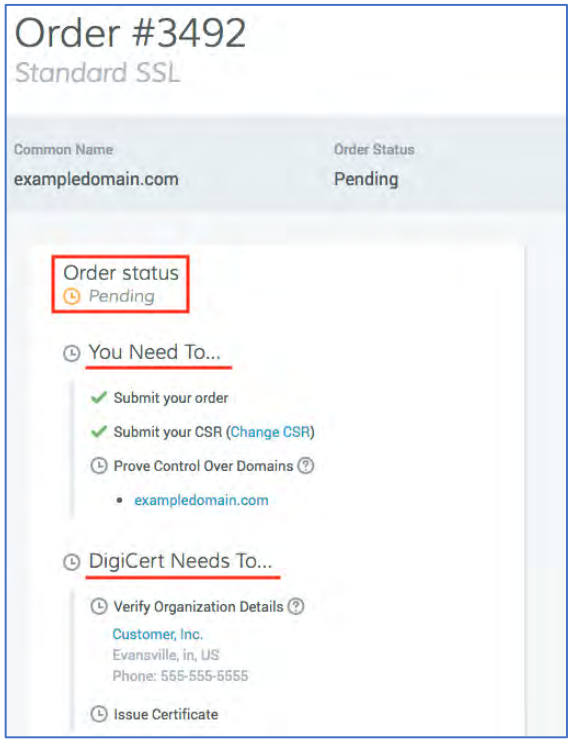


2. On the **Orders** page, use the filters and advanced search features to locate the pending certificate order you want to view.

3. In the **Order#** column of the certificate order, click the order number link.

4. On the **Order#** details page, in the **Order status** section, you can check the order's validation status (for example, is the order waiting on domain or organization validation to be completed).

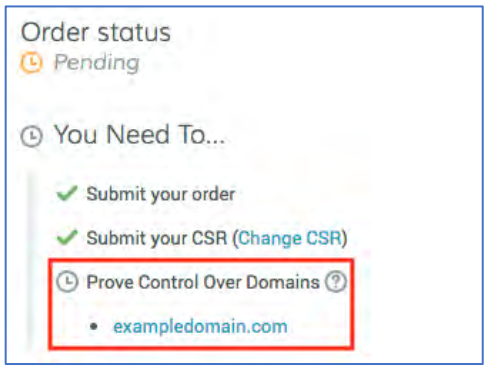
   Note: After validation is completed (domains and organization), the **Order status** section no longer appears on the **Order#** details page.



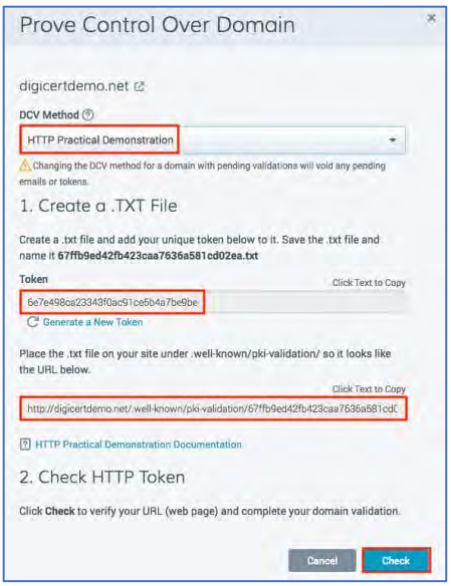
Step II: Use HTTP Practical Demonstration to Demonstrate Control Over the Domain

5. On the **Order#** details page, in the **Order status** section, under **You Need To**, locate the domain pending validation and click the domain link.

   Note: When you have multiple domains (SANs) on your order, each one will be listed. Those with a checkmark next to them are validated. Those with a clock icon next to them are pending validation.



6. In the **Prove Control Over Domain** window, in the **DCV Method** drop-down list, select **HTTP Practical Demonstration.**



7. **Create Your .txt File:**

    a. In the **Token** box, copy your unique token.

    To copy the value to your clipboard, single click in the text field.

    Note: The unique token expires after thirty days. To generate a new token, click the **Generate a New Token** link.

    b. Open a text editor (such as Notepad) and paste in your unique **Token**.

    c. In your HTTP practical demonstration URL, the string after **pki-validation/** is the name of your txt file.

    For example, if your HTTP practical demonstration URL is http://example.com/.well-known/pki-validation/c7e2ff0c848e4707594066cc860.txt, then, your file name is c7e2ff0c848e4707594066cc860.txt.

    d. Save the .txt file you created under this name (for example, *c7e2ff0c848e4707594066cc860.txt*).

8. **Create the .well-known/pki-validation Directory:**

    Create the **.well-known/pki-validation/** directory on your site and place your .txt file in it.

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

9. **Verify the HTTP Token:**

    a. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.

    b. On the **Orders** page, in the **Order#** column of the certificate order, click the order number link.

c. On the **Order#** details page, in the **Order status** section, under **You Need To**, locate the domain and click the domain link.

d. In the **Prove Control Over Domain** window, under **2. Check HTTP Token**, click **Check**.

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

Troubleshooting Tips:

Verify the URL matches exactly

a. Make sure that the URL for your web page matches the DigiCert provided URL.

   http://**YourDomain.com**/.well-known/pki-validation/**[filename].txt**

b. Where **YourDomain.com** matches the domain that you are validating and **[filename].txt** matches the unique hash provided by DigiCert under **Your HTTP token URL** (for example, **c7e2ff0c848e4707594066cc860.txt**).

c. **Important:**

   If you are missing a period, a number, or a letter, validation cannot be completed.

5.7 DNS CAA Resource Record Check

As of September 8, 2017, Certificate Authorities (CAs) are required to check, process, and abide by a domain's DNS Certification Authority Authorization (CAA) resource records (RRs) before a certificate can be issued to the requestor.

Note: A CAA resource record is **NOT REQUIRED** for DigiCert to issue certificates for your domains. The information provided concerning these records is only important **if you already have** CAA resource records set up for any of your domains or **if you would like to add** CAA resource records for your domains.

Prior to issuing a certificate, a CA checks the CAA RRs to establish whether they can issue a certificate for a domain. A CA can issue a certificate for a domain if **one** of the following conditions is met:

- There is no record for the domain
- There is a record for the domain authorizing the CA to issue that type of certificate for the domain

If you have or are planning to create DNS CAA RRs for your domain(s), it's important to make sure your records are up-to-date and accurate. At DigiCert, we recommend checking your existing DNS CAA RRs for your domain(s) to verify that you have the necessary records for each CA authorized to issue certificates for each domain. We also recommend that those creating new DNS CAA RRs understand how the process works, so you don't accidentally prevent a CA from issuing a certificate that's needed ASAP.

For more information, please visit **DNS CAA Resource Record Check** (https://www.digicert.com/dns-caa-rr-check.htm).

6 Certificate Management

6.1 Publicly Trusted Certificates – Data Entries that Violate Industry Standards

Baseline requirements and RFC 5280 Violations

For publicly trusted certificates, industry standards (baseline requirements and RFC 5280) require data entries meet certain criteria. Violating these standards when ordering a certificate prevents a Certificate Authority (CA) from issuing the certificate.

6.1.1 Sixty-Four Maximum Character Limit Violation

For publicly trusted certificates, we cannot allow these values (data entries) to exceed the 64-maximum character limit, including spaces:

- **Common Name**
  We cannot allow the common name value to exceed the 64-character limit. However, the subject alternative names (SANs) value does not have the same character length restrictions as the common name value. The SANs included in a certificate order (for example, in a Multi-Domain SSL Certificate order) can be greater than 64 characters.
- **Organization**
  Does the organization include an assumed name? And, you are planning to validate that organization for extended validation (EV) certificates?
  Then, make sure the organization name + assumed name values do not exceed 64 characters, including spaces.
- **Street 1**
- **Street 2**
- **City**
- **State**
- **Postal Code**

6.1.2 Organization Unit Value Violation

For publicly trusted certificates, the organization unit value is not a required value (field). According to baseline requirements, Certificate Authorities (CAs) are only required to validate the organization unit value, when a value is provided. If you leave this field blank (do not provide an organization unit value), CAs are instructed not to include the field in the certificate.

Baseline requirements also prohibit this value from being or appearing to be "junk" data or indicators of non-applicability (na, ?, etc.), which helps keep certificates smaller. By keeping certificates smaller, this ensures TLS remains accessible to a greater range of users and site operators.

The list below contains some of the characters that if entered by themselves in the organization unit field do not represent a valid organization unit value.

- "-" (Hyphen)
- " " (Space)
- "." (Period)

- "?" (Question mark)
- "na" (Not applicable)
- "NA" (Not applicable)

Note that if you only put a hyphen in the organization unit field, a CA will be unable to validate the value. However, if you enter an organization name that includes a hyphen in it (for example, Dev-Ops), this hyphen does not prevent a CA from validating your organization unit value.

6.1.3 Use of Underscores Violation

For publicly trusted certificates, we can no longer allow use of underscores (_) in:

- Subject Common Name
- Subject Alternative Name (SAN)

As of October 1, 2018, we can only issue certificates for domains and subdomains using:

- Lowercase letters a–z
- Uppercase letters A–Z
- Digits 0–9
- Special characters: period (.) and hyphen (-)

Important: Currently, you can include underscores in other certificate values, such as organization unit and organization names. However, the use of the underscore in these values is being reevaluated. Industry standards may change and require you to remove the underscores from those values too.

7 Customize Your Certificate Request Forms

7.1 Managing Custom Order Form Fields

CertCentral allows you to add custom fields to your certificate order forms. The custom field metadata can be used to search or sort a set of certificate orders that match the metadata search criteria.

***Note:** The **Custom Fields** feature is turned off by default. To enable this feature for your CertCentral account, please contact your DigiCert account representative.

Once this feature has been enabled for your CertCentral account, the **Custom Order Fields** menu option is added to the sidebar menu under **Settings** (**Settings > Custom Order Fields**).

7.1.1 Custom Order Forms Fields Features

Apply to Future and Present Requests

When you add custom order form fields, the field is also added to pending requests. If the field is required, the pending requests cannot be approved until the field is completed.

Apply to Entire Account

When you add custom order form fields, the fields are applied to the order forms for the entire account. Custom order form fields cannot be set per Division.

Apply to All Certificate Types

When you create custom order form fields, the fields are added to the order forms for all certificate types (SSL, Client, Code Signing, etc.). You cannot add a custom order form field to the order forms for only SSL certificate types, etc.

Apply to Guest URLs

When you add custom order form fields, these fields are added to the certificates ordered from directly inside your CertCentral account as well as from any guest URLs you have sent out.

Different Types to Choose From

When you create custom order form fields, different types of fields can be added such as single line and multiple line text boxes, email address and email address list boxes, etc.

Required or Optional

When you add custom order form fields, you can make them required or optional. Required fields must be completed before the order can be approved. Optional fields can be left blank.

Deactivated or Activated

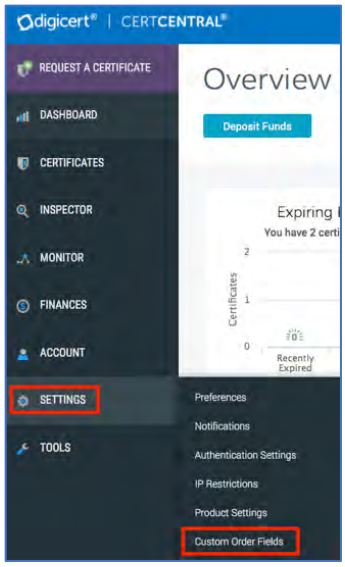
After you have added a custom order form field, you can deactivate (remove) and activate (add back) the field as needed. Fields that you deactivate are removed from pending requests but not from issued orders.

Fields that you activate are added to pending requests. If the field is required, it must be completed before the request can be approved.

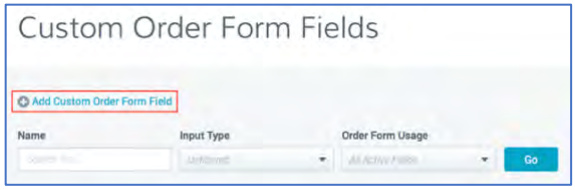
7.1.2 How to Add a Custom Field to Your Request Forms

Use these instructions to add customer fields to you certificate order forms.

1. In your CertCentral account, in the sidebar menu, click **Settings > Custom Order Fields**.

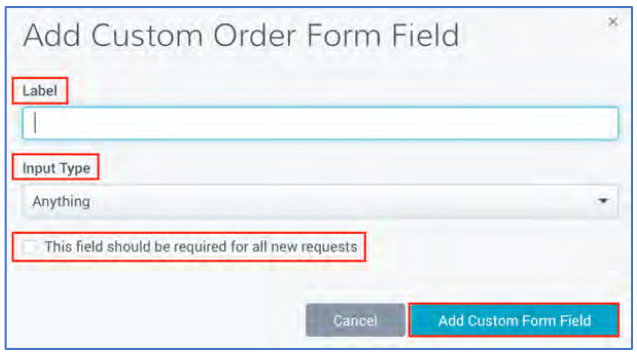


2. On the **Custom Order Form Fields** page, click the **Add Custom Order Form Field** link.



3. In the **Add Custom Order Form Field** window, do the following:

Label	In the box, type a name/label for the field (i.e., *Direct Report's Email Address*).
Input Type	In the drop-down list, select an input type for the field (i.e., *email address*). Input Types: • **Anything:** Single line text box • **Text:** Multiline text box • **Integer:** Number box (limited to non-decimal whole numbers) • **Email Address:** Single email address box • **Email Address List:** Multiple email address box
This field should be required for all new requests	If you want the field to be completed before the request can be submitted (or approved for pending requests), check this box. **Note:** If you don't check this box, the field appears on the order form with the word optional in the box. The requestor does not need to complete the box for the request to be submitted (or approved for pending requests).



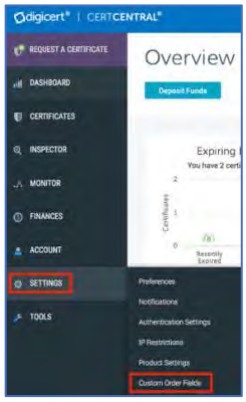
4. When you are finished, click **Add Custom Form Field**.

   The custom field affects all future orders and current pending requests. If the field is required, the field must be completed before the pending requests can be approved.

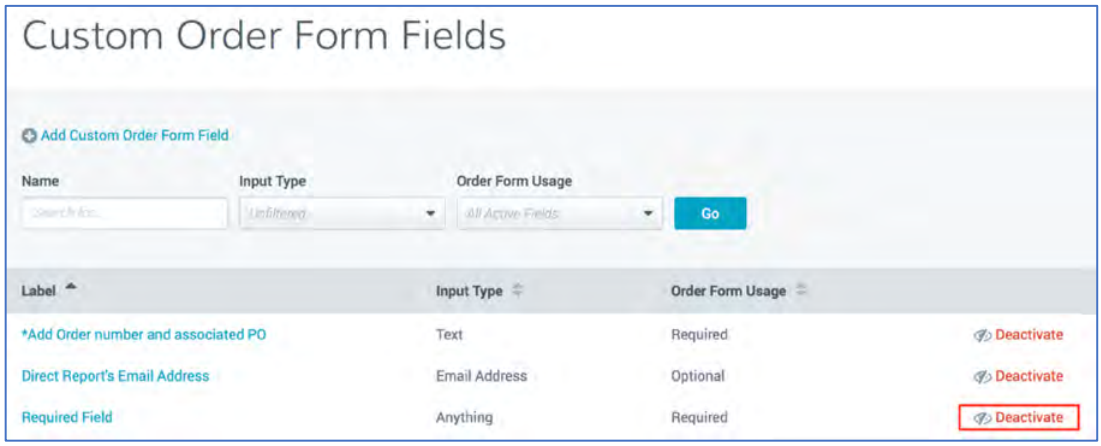
7.1.3 How to Deactivate a Custom Order Form Field

Use these instructions to deactivate a customer order form field so it no longer appears on your certificate request forms. If you want to use the field again, you can reactivate.

1. In your CertCentral account, in the sidebar menu, click **Setting > Custom Order Fields**.

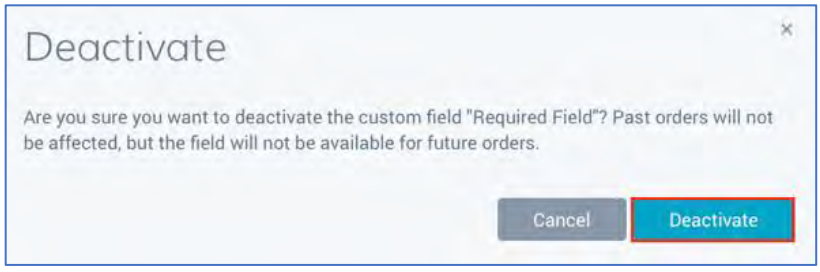


2. On the **Custom Order Form Fields** page, use the filters and column headers to locate the order form field (**Label**) you want to deactivate and then click **Deactivate**.



3. In the **Deactivate** window, click **Deactivate**.

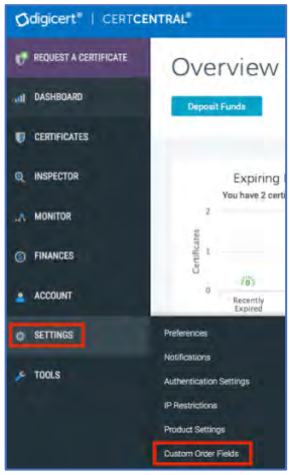
   Note: Deactivating the field does not affect past certificate orders.



7.1.4 How to Activate a Custom Order Form Field

Use these instructions to reactivate a customer order form field.

1. In your CertCentral account, in the sidebar menu, click **Settings > Custom Order Fields**.

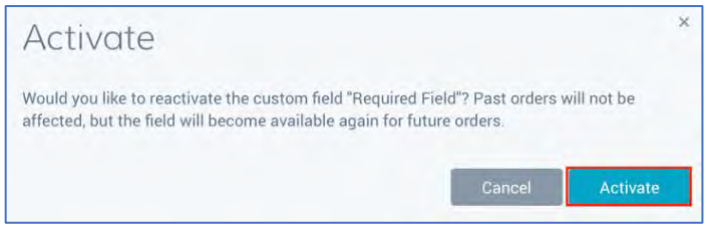


2. On the **Custom Order Form Fields** page, in the **Order Form Usage** drop-down list, select **Inactive** and then click **Go**.

3. Locate the custom field you want to reactivate and then click **Activate**.

4. In the **Activate** window, click **Activate**.

   Note: Activating the field does not affect past certificate orders.



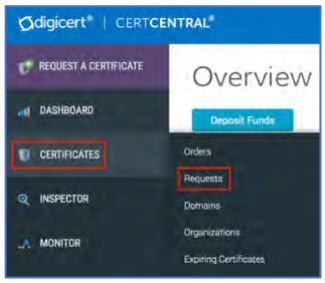
7.1.5 Pending Requests: How to Complete Required and Optional Custom Fields

Use these instructions to complete require and optional fields activated for certificates waiting for administrator approval.

When a required custom field is added after a certificate request has been submitted but before the request has been approved, the newly added required custom field must be completed before the request can be approved.

While you are completing the required fields, you can also complete any optional fields that were added after you submitted your request.

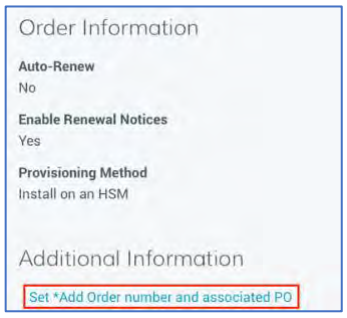
1. In your CertCentral account, in the sidebar menu, click **Certificates > Requests**.



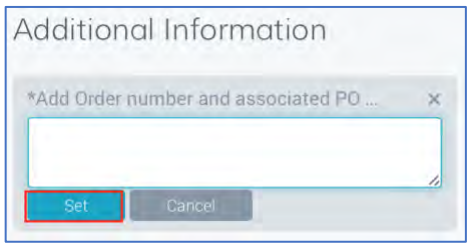
2. On the **Requests** page, in the **Status** drop-down list, select **Pending** and click **Go**.

3. Locate the pending request that needs to have its custom required fields completed and then, click the requests **Order #** link.

4. In the **Order #** details pane (on the right), under **Additional Information**, click the required field link (i.e., *Set *Add Order number and associate PO*).



5. In the custom order field, type the necessary information and click **Set**.

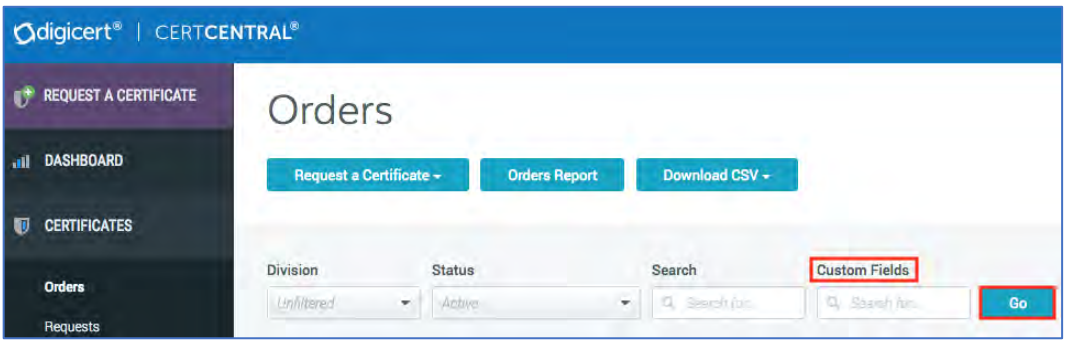


6. Repeat the previous step for each additional required and optional field.

7.1.6 How to Use Your Custom Fields to Search for Specific Orders

Use these instructions to search for orders using custom field data.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



2. On the **Orders** page, in the **Custom Fields** search box, type in a custom value entered in any of your custom order form fields (e.g., email address, number, etc.) and click **Go**.

3. The list of orders should now be populated with the orders that contain the custom field value you just entered along with a list of custom fields (required and optional) in that order.

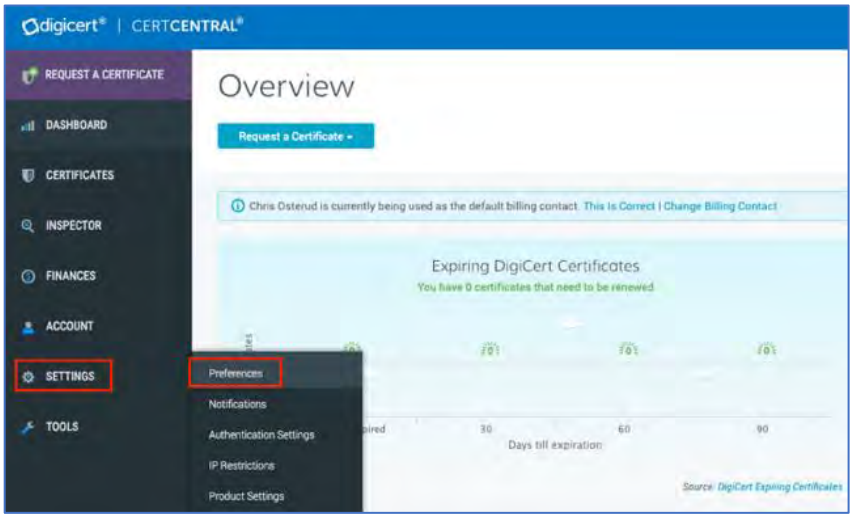
7.2 Limit Who Can Add New Organizations from Request Forms

By default, when ordering a TLS certificate (Standard SSL, EV SSL, etc.) from inside your account or from a guest URL, users can add either an existing organization or a new organization (name, address, etc.).

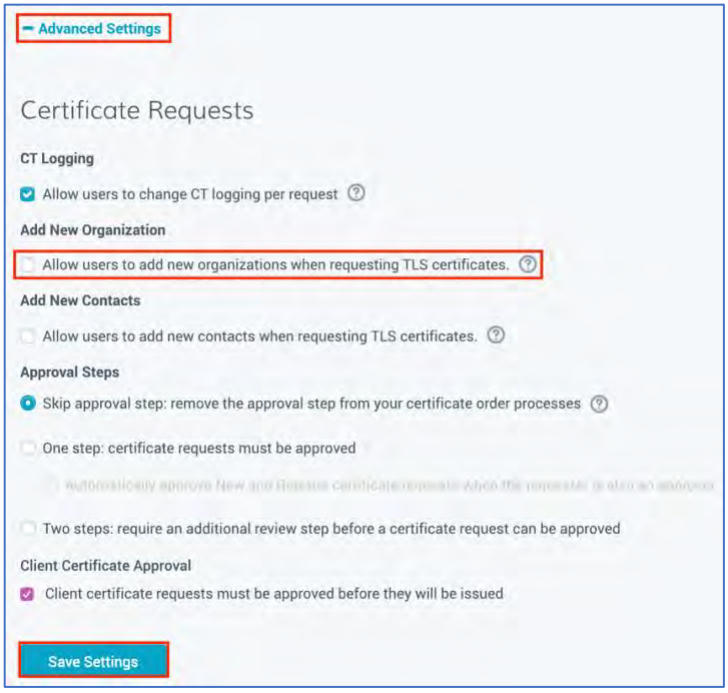
Use these instructions to disable the **Add New Organization** feature for the Standard User, Finance Manager, and Limited User roles when ordering a TLS certificate (OV and EV) and to remove it from the guest URL certificate order forms. This change does not remove the ability to add an existing organization to an order as this is required for all OV and EV TLS certificate orders.

Note: Administrator and Manager roles retain the ability to add new organizations whether this feature is enabled or disabled.

1. In your CertCentral account, in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, at the bottom of the page, expand **Advanced Settings**.



3. In the **Certificate Requests** section, under **Add New Organization**, uncheck **Allow users to add new organizations when requesting TLS certificates**.
4. At the bottom of the page, click **Save Settings**.
5. Congratulations!

   The next time a standard user, finance manager, and limited user orders a TLS certificate from inside their account or anyone from a guest URL, they will only be able to add an existing organization to their order.

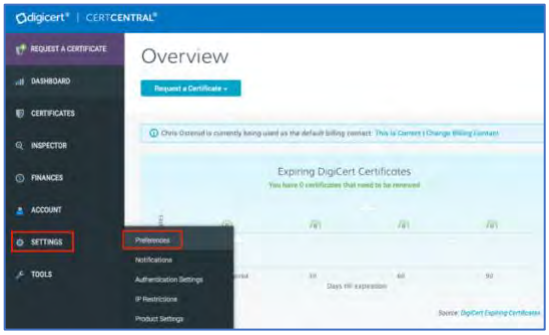
7.3 Limit Who Can Add New Contacts from Request Forms

By default, when you enable the **Allow non-DigiCert users to be used as verified contacts** feature, you also allow all users to add new non-CertCentral account users as verified contacts when ordering an EV TLS certificate from inside your account or from guest URLs. SeeEnable Adding non-CertCentral Account Users as Verified Contacts.

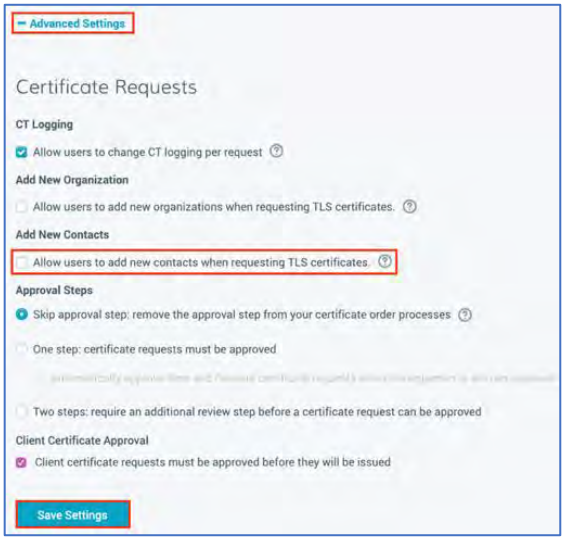
Use these instructions to disable the **Add New Contact** feature for the Standard User, Finance Manager, and Limited User roles when ordering an EV TLS certificate and to remove it from the guest URL certificate order forms. This change does not remove the ability to add an existing contact to an order as this is required for EV TLS certificate orders.

Note: Administrator and Manager roles retain the ability to add new contacts whether this feature is enabled or disabled. This feature does not affect the **Organizations** page as only standard users, finance managers, and limited users don't have permissions to access this page in their accounts.

1. In your account, in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, at the bottom of the page, expand **Advanced Settings**.



3. In the **Certificate Requests** section, under **Add New Organization**, uncheck **Allow users to add new contacts when requesting TLS certificates**.

4. At the bottom of the page, click **Save Settings**.

5. Congratulations!

   The next time a standard user, finance manager, and limited user orders a TLS certificate from inside their account or anyone from a guest URL, they will only be able to add an existing verified contact to their order.

7.4 Requesting TLS/SSL Certificates

The TLS/SSL certificate lifecycle begins when administrators and users log into their account and request certificates for their assigned domains.

The process for requesting any of the available TLS/SSL Certificates is the same:

- Create your Certificate Signing Request (CSR).
- Fill out the request form. The form for requesting each type of SSL Certificate is similar.
- Wait for approval.

CertCentral account users can only request the types of certificates that have been authorized for their organization and the domains assigned to their account and/or division.

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

- **Business TLS/SSL**
  Secure Site EV Multi-Domain SSL, Secure Site EV SSL, Secure Site Multi-Domain SSL, Secure Site SSL, and Secure Site Wildcard SSL
- **Basic TLS/SSL Certificates**
  EV Multi-Domain, EV SSL, Multi-Domain SSL, Standard SSL, and Wildcard SSL
- **Grid Certificates**
  Grid Premium, Grid Robot Email, Grid Robot FQDN, Grid Robot Name, Grid Host SSL, and Grid Host Multi-Domain SSL
- **Client Certificates**
  Digital Signature Plus, Email Security Plus, and Premium
- **Code Signing Certificates**
  Code Signing and EV Code Signing
- **Document Signing Certificates**
  Document Signing - Organization (2000) and Document Signing - Organization (5000)

7.4.1 How to Request an SSL or EV SSL Certificate

Use these instructions to order a Secure Site SSL, Secure Site EV SSL, Standard SSL, and EV SSL Certificates.

The major difference between the EV SSL and SSL certificate issuance process is the degree of organization verification (validation) DigiCert does for the certificate type. See SSL Certificate Validation Process from DigiCert.

Depending on your organizations policies and how your CertCentral account is set up, you may need administrator approval before your order is submitted. After approval, your order will be submitted to DigiCert, so we can complete your order and issue your certificate.

Request an SSL or EV SSL certificate

When ordering an EV SSL certificate, you will need to add a verified contact. This step is not required for ordering an SSL certificate.

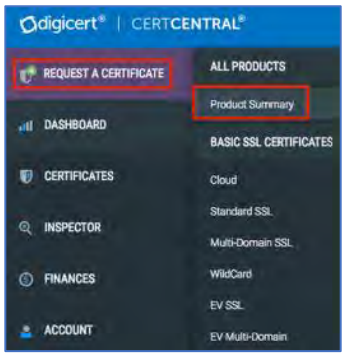
f. **Create your CSR.**

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

g. In your CertCentral account, use one of these options to access the certificate's order page:

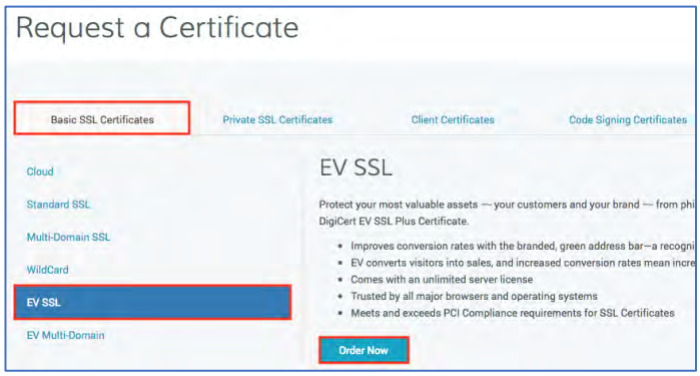
i. **Option 1: Not sure which certificate you want**

i. In the sidebar menu, hover over **Request a Certificate** and then under **All Products**, click **Product Summary**.



ii. On the **Request a Certificate** page, look over the certificate options and select the certificate you want to order.

- On the **Business SSL Certificates** tab, select **Secure Site SSL** or **Secure Site EV SSL** and then, click **Order Now**.
- On the **Basic SSL Certificates** tab, select **Standard SSL** or **EV SSL** and then, click **Order Now**.



ii. **Option 2: Know which certificate you want**

In the sidebar menu, hover over **Request a Certificate** and then select the certificate you want to order.

- Under **Business SSL Certificates**, click **Secure Site SSL** or **Secure Site EV SSL.**
- Under **Basic SSL Certificates**, click **Standard SSL** or **EV SSL**.

h. **Add your CSR**

We use information included in your CSR to populate corresponding values in the order form: Common Name, Organization Unit, and Organization. If any of this information is not included in the CSR, the field in the form is left blank.

Note: Add your CSR before you start filling out the order form. Adding the CSR after will overwrite or delete information from the specified fields in the form (such as the **Organization Unit** field).

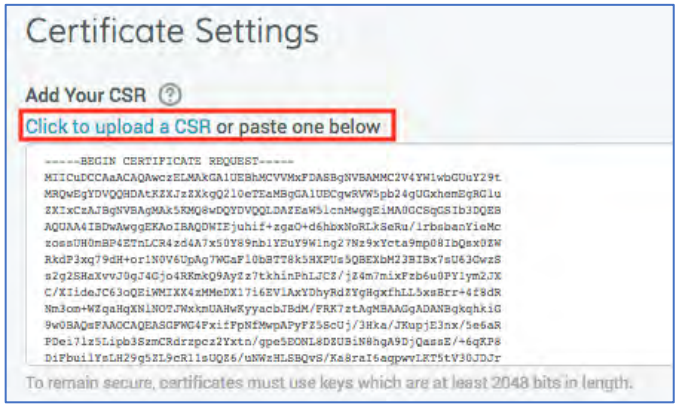
On the **Request "Certificate Name"** page, under **Certificate Settings**, in the **Add Your CSR** box, use one of these options to add your CSR:

- **Upload your CSR**

  Click the **Click to upload a CSR** link to browse for, select, and open your CSR file.

- **Paste your 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.



i. **Common Name**

After adding your CSR to the order form, we populate the **Common Name** box with the common name from the CSR.

To add the common name yourself, use one of these options:

- **Add a recently created domain**

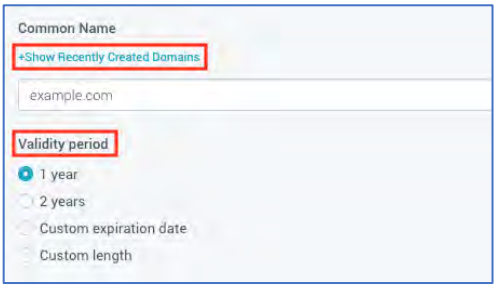
  Under **Common Name**, expand **Show Recently Created Domains** and select one of the available (pre-validated) domains.

- **Add a new domain**

  When adding a new domain, you will need to complete domain validation (demonstrate control over the domain) before we can issue your certificate. See Domain Validation (Pending Order): Domain Control Validation (DCV) Methods.

  Under **Common Name**, in the **Common Name** box, type the domain that you want to secure.

When adding a new domain, certificate issuance may take a bit longer while we validate the domain.



j. **Validity Period***

Select a validity period for the certificate: **1 year**, **2 years**, **Custom expiration date**, or **Custom length**.

***Custom validity periods**

- Certificate pricing is prorated to match the custom certificate length.
- Certificate validity can't exceed the industry allowed maximum lifecycle period for the certificate. For example, you can't set a 900-day validity period for a certificate.

k. **Additional Certificate Options**

Expand **Additional Certificate Options** and provide the information below as needed:

i. **Signature Hash**

In the drop-down list, select a signature hash.

Note: We recommend using the default signature hash (for example, *SHA-256*).

ii. **Server Platform**

In the drop-down list, select the server on which the CSR was generated.

iii. **Organization Unit(s)**

You can leave this box blank. Adding an organization unit (OU) for which the certificate and domain will be used is not required. However, if you include OUs in your order, DigiCert will need to validate them before we can issue your certificate.

If your CSR includes an OU, we populate the **Organization Unit** box in the order form with that OU information. If you want to use a different OU than the one included in your CSR, click the delete icon (trash can) and add a different one.

To add the OU yourself, in **the Organization Unit** box, enter the OU.

iv. **Auto-Renew**

To set up automatic renewal for this certificate, check **Auto-renew order 30 days before expiration**.

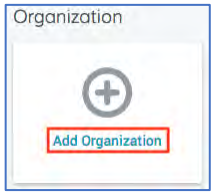
With auto renew enabled, a new certificate order will be automatically submitted when this order nears its expiration date. If your certificate still has time remaining before it expires, DigiCert adds the remaining time from your current certificate to your new certificate (up to 825 days – approximately 27 months).

Important: **Auto-Renew** can't be used with credit card payments. To automatically renew a certificate, the order must be charged to account balance. You can configure the finance settings for your account on the **Finance Settings** page (in the sidebar menu, click **Finances > Settings**).

l. **Organization**

To add an organization, click **Add Organization** and complete one of the options below.

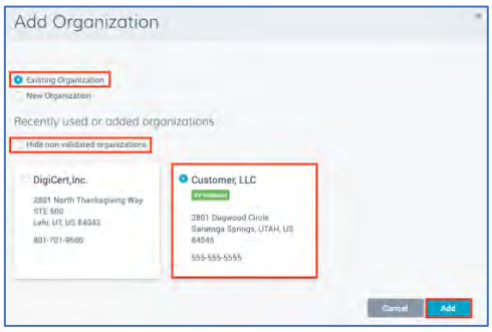
Note: Depending on how your account is configured, you may not be able to use **Option 2: Add a new organization**.



Option 1: Add an existing organization

If your CSR includes an organization currently used in your account, we populate the **Organization** card in the order form with the organization information. If you want to use a different organization than the one included in your CSR, click the delete icon (trash can) and add a different one.

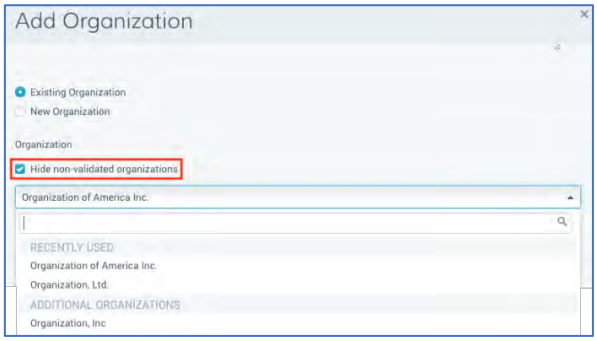
i. In the **Add Organization** window, select **Existing Organization**.



ii. To see only a list of fully validated organizations, check **Hide non-validated organizations**.

iii. Select one of the available organizations.

If have more than nine organizations in your account, use the **Organization** drop-down list to select an organization.

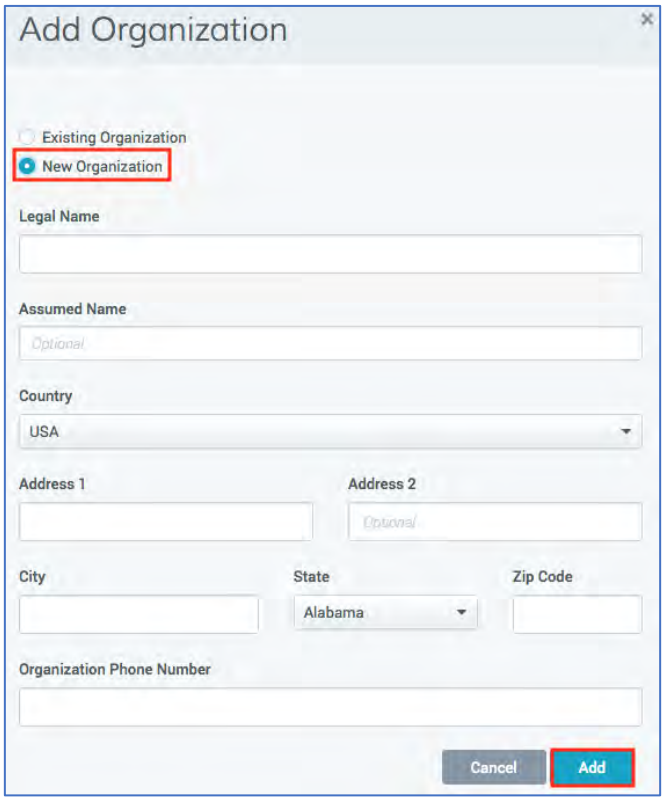


iv. Click **Add**.

Option 2: Add a new organization

When adding a new organization, we will need to validate the organization before we can issue your certificate. Also, when you add a new organization, you, the requestor, becomes the organization contact for the newly added organization.

a. In the **Add Organization** window, select **New Organization**.



b. Add these organization details:

i. **Legal Name**

Enter the organization's legally registered name.

ii. **Assumed Name**

Does your organization have a DBA name (doing business as name) that you want to appear on the certificate?

Yes – Enter it here
No – Leave this box blank.

iii. **Country**

In the drop-down list, select the country where the organization is legally located.

iv. **Address 1**

Enter the address where the organization is legally located.

v. **Address 2**

Does the organization have a second address that you need to include?

Yes – Enter it here.
No – Leave this box blank.

vi. **City**

Enter the city where the organization is legally located.

vii. **State / Province / Territory/ Region / County**

Enter the state, province, territory, region, or county where the organization is legally located.

viii. **Zip / Postal Code**

Enter the zip or postal code for the organization’s location.

ix. **Organization Phone Number**

Enter a phone number at which the organization can be contacted.

v. When you are finished, click **Add**.

m. **Contacts**

When ordering an EV SSL or Secure Site SSL Certificate, you need to add a verified EV Contact.

Note: **Contacts** does not appear on the Standard SSL or Secure Site SSL Certificate request form.

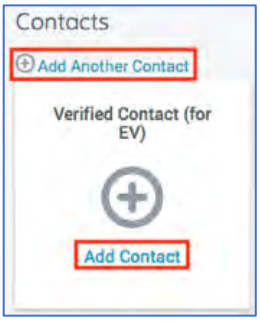
EV Verified Users can approve certificate requests for EV SSL Certificates. For a user to be an EV Verified User, they must have a phone number and job title.

Feature Note:

If you've enabled the **Allow non-DigiCert users to be used as verified contacts** feature, you will see two options: **Existing Contact** and **New Contact**. The **Existing Contact** option lets you assign a CertCentral user as the verified EV contact. The **New Contact** option lets you enter information for a non-CertCentral account user. Use option 1 or 2.

If you haven't enabled this feature, you won't see any options. You can only add account users as verified EV contacts. Use Option 1.

To add a verified EV contact, under **Contacts**, click **Add Contact** and complete one of the options below.

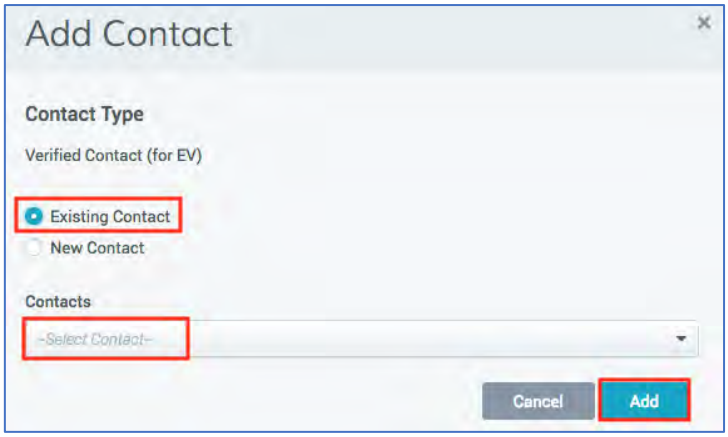


Option 1: Add an existing contact

If your CSR includes an organization currently used in your account and this same organization already has assigned EV verified contacts, the **Verified Contact (for EV)** cards are populated with their information (name, title, email, and phone number).

If you want to use a different EV verified contact, click the delete icon (trash can) and add a different one.

i. In the **Add Contact** window, select **Existing Contact**.



ii. In the **Contacts** drop-down list, select a verified contact for EV.

Is the contact you selected missing a **Job Title** or a **Phone** number? Then, you need to add the missing information. For example, if the contact has a job title but no phone number, you will only need to add the phone number.

i. In the **Job Title** box, enter the contact's job title.

ii. In the **Phone** box, enter the contact's phone number (and **Ext**).

When adding **Job Title** and/or **Phone** for an existing contact, the user profile will be updated with the new information.

iii. Click **Add**.

iv. To add another verified contact, click **Add Another Contact** and repeat the previous steps as needed.

Option 2: Add New Contact

a. In the **Add Contact** window, select **New Contact**.

b. Add the contact's **First Name**, **Last Name**, and **Job Title**.

c. Next, add an **Email** address and **Phone** number at which the contact can be contacted for verifying an EV SSL Certificate request.

d. When you are finished, click **Add**.

e. To add another verified contact, click **Add Another Contact** and repeat the previous steps as needed.

n. **Additional Order Options**

Expand **Additional Order Options** and enter the information below as needed. None of this information is required.

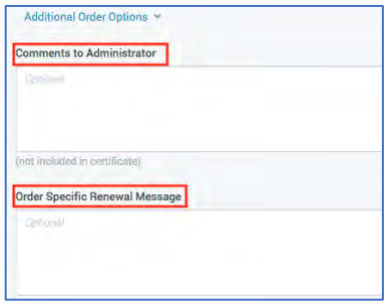
- **Comments to Administrator**

  Enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc.

  Note: These comments are not included in the certificate.

- **Order Specific Renewal Message:**

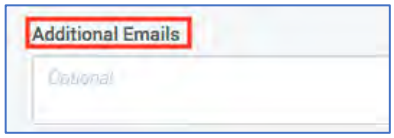
  To create a renewal message for this certificate right now, type a renewal message with information that might be relevant to the certificate's renewal.



o. **Additional Emails**

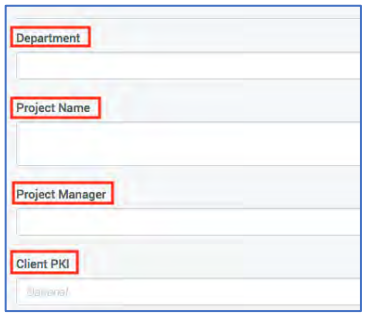
In the box, enter the email addresses (comma separated) for the people you want to receive the certificate notification emails, such as certificate issuance, duplicate certificate, certificate renewals, etc.

Note: The recipients cannot manage the order, just receive certificate related emails.



p. **Customized Fields**

If your company/organization has added any custom fields to your certificate request form, enter the additional information, required and optional.

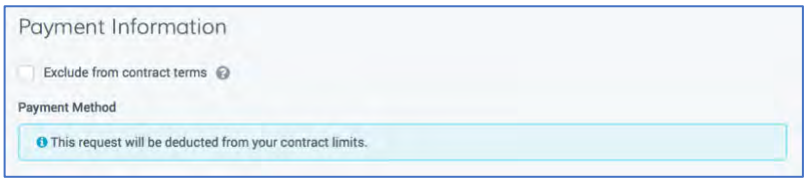


q. Under **Payment Information**, use one of the following options to pay for the certificate:

   a. **Pay with Contract Terms**

Do you have a contract and want to use it to pay for the certificate request? Then, continue to step 13.

Note: When you have a contract, it is the default payment method.

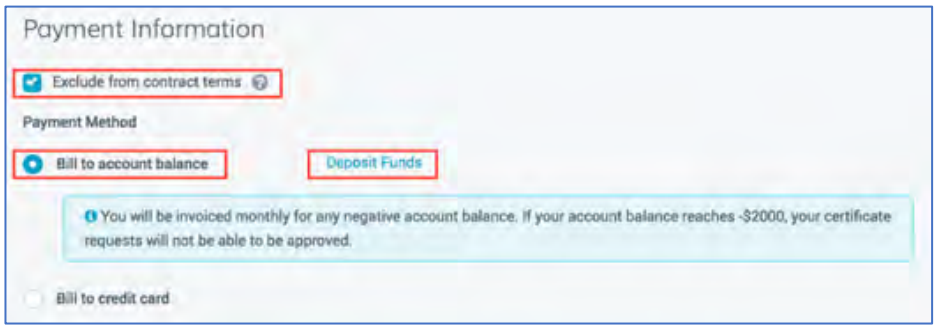


b. **Exclude from Contract Terms and Pay with Account Balance**

   i. Check **Exclude from contract terms**

   ii. Select **Bill to account balance**.

   Note: If you need to deposit funds before continuing with the certificate order, click the **Deposit** link. Be aware that when you click the link you are taken to another page inside CertCentral, and the information that you have entered about the certificate is not saved.



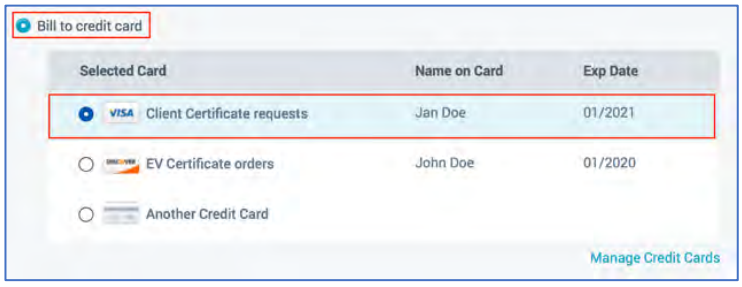
c. **Exclude from Contract Terms and Pay with Credit Card**

   i. Check **Exclude from contract terms**.

   ii. Select **Bill to credit card** and then do one of the following options:

   1. **Use One of the Credit Cards Listed**

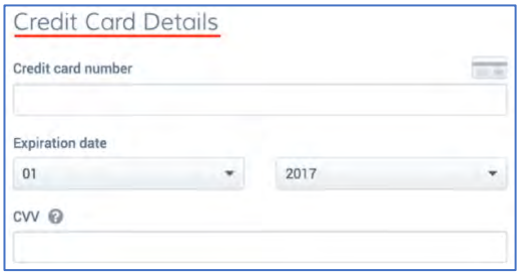
      Under **Selected Card**, select one of the available cards.



   2. **Add a Different Credit Card**

a. Under **Selected Card**, select **Another Credit Card**.

b. Under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



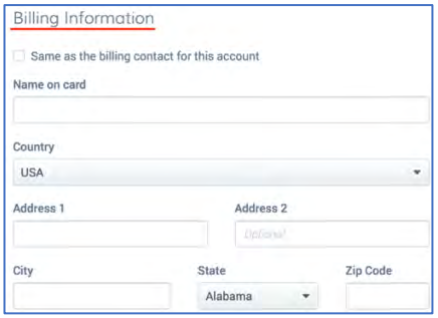
c. Then, under **Billing Information**, use one of these options to add the billing contact information:

Use account's billing contact information

To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.

Add your billing information

Type your billing information (Name on card, Country, etc.).



d. Under **Credit Card Options**, save or don't save your credit card information:

Do Not Save the Credit Card

Uncheck **Save this credit card**.

The credit card will not be added to your account. If you want to use the credit card again, you will need to reenter its information in your account.

Save the Credit Card

To Save the Credit Card do 1 or more of the following tasks:

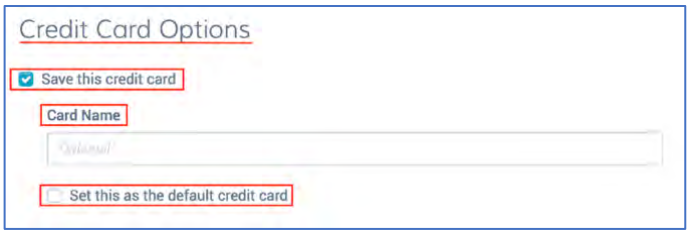
1) Check **Save this credit card**.

2) (Optional) Under **Card Name**, type a name for the credit card that will be helpful when using or identifying the card (i.e., *Pay Account Balance*).

   Note: If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*).

3) (Optional) If you want to use this credit card as the default credit card for your account, check **Set this as the default credit card**.

   Note: This option does not appear when adding your first credit card. The first credit card added to your account is automatically set as the default credit card.



r. Under **Certificate Services Agreement**, read through the agreement, making sure you understand it and then, check **I agree to the Certificate Services Agreement above**.

s. When you are finished, click **Submit Certificate Request**.

- On the **Certificate Requests** page (**Certificates > Requests**), your certificate should be listed with the *status* of **Pending**.
- Standard SSL – Before the certificate can be issued, an administrator may need to approve the certificate request.
- EV SSL – Before the certificate can be issued an EV Certificate approver may need to approve the certificate request.

- When an approval is required, the administrator or EV verified contact is sent an email informing them that they need to approve the certificate request.

7.4.2 How to Request a Wildcard Certificate

Use these instructions to order a Secure Site Wildcard SSL and Wildcard SSL Certificates. Depending on your organization policies and how your CertCentral account is set up, you may need administrator approval before your order is submitted. After approval, your order will be submitted to DigiCert, so we can complete your order and issue your certificate.

Request a Wildcard Certificate

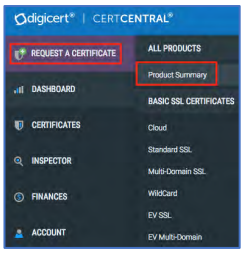
1. Create your CSR.

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

2. In your CertCentral account, do one of the following:

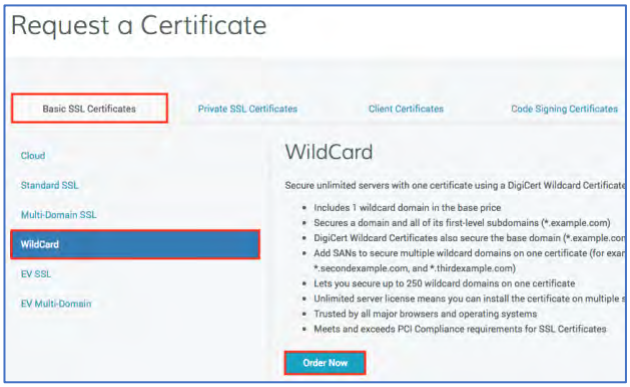
   a. **Option 1: Not sure which certificate you want**

      i. In the sidebar menu, hover over **Request a Certificate** and then under **All Products**, click **Product Summary**.



      ii. On the **Request a Certificate** page, look over the certificate options and select the certificate you want to order.

         - On the **Business SSL Certificates** tab, select **Secure Site Wildcard** and then, click **Order Now**.
         - On the **Basic SSL Certificates** tab, select **Wildcard SSL** and then, click **Order Now**.



b. **Option 2: Know which certificate you want**

In the sidebar menu, hover over **Request a Certificate** and then select the certificate you want to order.

a. Under **Business SSL Certificates**, click **Secure Site Wildcard SSL.**

b. Under **Basic SSL Certificates**, click **Wildcard SSL**.

3. **Add your CSR**

We use information included in your CSR to populate corresponding values in the order form: Common Name, Other Hostnames (SANs), Organization Unit, and Organization. If any of this information is not included in the CSR, the field in the form is left blank.

Note: Add your CSR before you start filling out the order form. Adding the CSR after will overwrite or delete information from the specified fields in the form (such as the **Organization Unit** field).

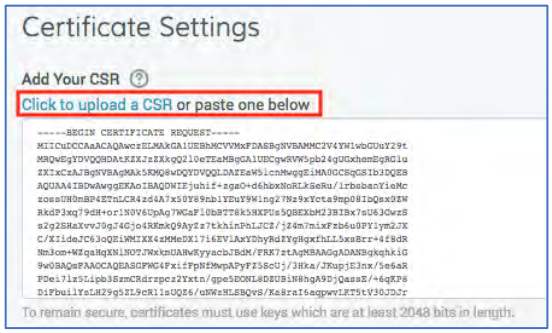
On the **Request "Certificate Name"** page, under **Certificate Settings**, in the **Add Your CSR** box, use one of these options to add your CSR:

- **Upload your CSR**

  Click the **Click to upload a CSR** link to browse for, select, and open your CSR file.

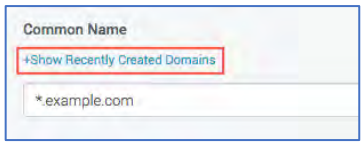
- **Paste your CSR**

  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**

After adding your CSR, we populate the **Common Name** box with the common name from the CSR.



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

To add the common name yourself, use one of these options:

- Add a recently created domain

  Under **Common Name**, expand **Show Recently Created Domains** and select an available (pre-validated) domain.

  Because you are ordering a wildcard certificate, make sure to format the common name correctly (*.example.com).

- Add a new domain

  When adding a new domain, you will need to complete domain validation (demonstrate control over the domain) before we can issue your certificate. See Domain Validation (Pending Order): Domain Control Validation (DCV) Methods.

  Under **Common Name**, in the **Common Name** box, type the domain that you want to secure.

  Because you are ordering a wildcard certificate, make sure to format the common name correctly (*.example.com).

  When adding a new domain, certificate issuance may take a bit longer while we validate the domain.

5. **Other Hostnames (SANs)**

   After adding your CSR, we populate the **Other Hostnames (SANs)** box with the SANs included in the CSR. You can still remove or add additional SANs as needed.

   - **Single wildcard domain certificate**

     In the **Other Hostnames (SANs)** box, enter the subdomain(s) that you want your Wildcard Certificate to secure. Note that the SANs names must be a subdomain of the specified common name. For example, if **.yourdomain.com* is the common name, you can use *www.yourdomain.com*, *www.app.yourdomain.com*, and *mail.yourdomain.com* as SANs.

   - **Multiple-wildcard-domain certificate**

     In the **Other Hostnames (SANs)** box, enter the wildcard domains and subdomains that you want to secure. The SANs must be a wildcard domain (for example, *.yourdomain.com) or based off your listed wildcard domains. For example, if one of your wildcard domains is

*.yourdomain.com, then you can add the SANs www.yourdomain.com or www.app.yourdomain.com to your certificate order.

Subdomains Note:

By default, Wildcard Certificates only secure a specific subdomain level. If your certificate is for **.yourdomain.com*, it will secure subdomains of the same level automatically, which means under most circumstances you *don't* need to enter in *secure.yourdomain.com* to use the certificate for that FQDN.

To secure subdomains on different levels (e.g., *test.secure.yourdomain.com* and *six.test.secure.yourdomain.com*) request a duplicate certificate. Since these subdomains are not on the same level as the wildcard (*) character, you must manually add them as SANs to the certificate. Requesting multiple duplicate certificates allows you to secure additional subdomains without invalidating the previous certificates.

6. **Validity Period***

   Select a validity period for the certificate: **1 year**, **2 years**, **Custom expiration date**, or **Custom length**.

   ***Custom validity periods**

   - Certificate pricing is prorated to match the custom certificate length.
   - Certificate validity can't exceed the industry allowed maximum lifecycle period for the certificate. For example, you can't set a 900-day validity period for a certificate.

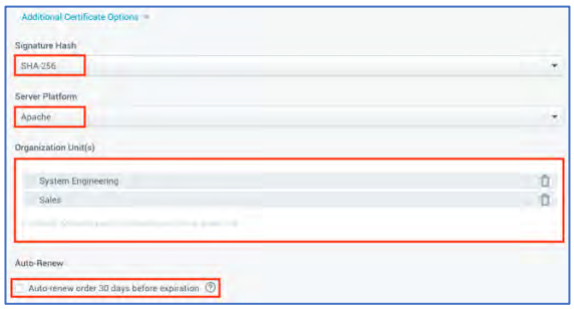
7. **Additional Certificate Options**

   Expand **Additional Certificate Options**, and provide this information as needed (some information is required; other information is optional):

a. **Signature Hash**

We recommend using the default signature hash (for example, *SHA-256*).

In the drop-down list, select a signature hash.



b. **Server Platform**

In the drop-down list, select the server on which the CSR was generated.

c. **Organization Unit(s)**

You can leave this box blank. Adding an organization unit (OU) for which the certificate and domain will be used is not required. However, if you include OUs in your order, DigiCert will need to validate them before we can issue your certificate.

If your CSR includes an OU, we populate the **Organization Unit** box in the order form with that OU information. If you want to use a different OU than the one included in your CSR, click the delete icon (trash can) and add a different one.

To add the OU yourself, in **the Organization Unit** box, enter the OU.

d. **Auto-Renew**

To set up automatic renewal for this certificate, check **Auto-renew order 30 days before expiration**.

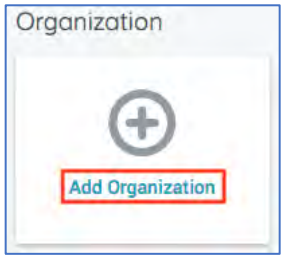
With auto renew enabled, a new certificate order will be automatically submitted when this order nears its expiration date. If your certificate still has time remaining before it expires, DigiCert adds the remaining time from your current certificate to your new certificate (up to 825 days – approximately 27 months).

Important: **Auto-Renew** can't be used with credit card payments. To automatically renew a certificate, the order must be charged to account balance. You can configure the finance settings for your account on the **Finance Settings** page (in the sidebar menu, click **Finances > Settings**).

8. **Organization**

To add an organization, click **Add Organization** and complete one of the options below.

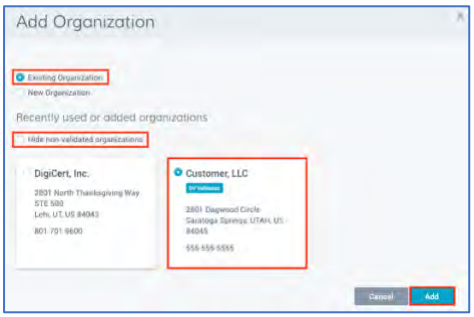
Note: Depending on how your account is configured, you may not be able to use **Option 2: Add a new organization**.



Option 1: Add an existing organization

If your CSR includes an organization currently used in your account, we populate the **Organization** card in the order form with the organization information. If you want to use a different organization than the one included in your CSR, click the delete icon (trash can) and add a different one.

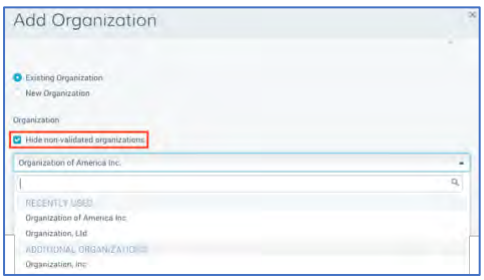
a. In the **Add Organization** window, select **Existing Organization**.



b. To see only a list of fully validated organizations, check **Hide non-validated organizations**.

c. Select one of the available organizations.

   If have more than nine organizations in your account, use the **Organization** drop-down list to select an organization.

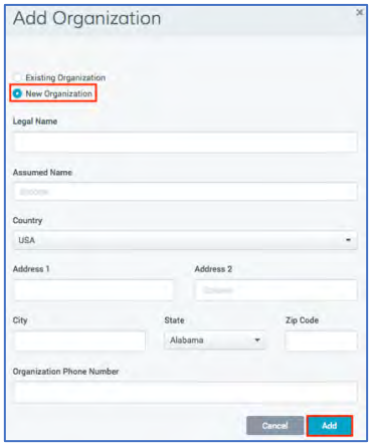


d. Click **Add**.

Option 2: Add a new organization

When adding a new organization, we will need to validate the organization before we can issue your certificate. Also, when you add a new organization, you, the requestor, becomes the organization contact for the newly added organization.

a. In the **Add Organization** window, select **New Organization**.



b. Add these organization details:

i. **Legal Name**

Enter the organization's legally registered name.

ii. **Assumed Name**

Does your organization have a DBA name (doing business as name) that you want to appear on the certificate?

Yes – Enter it here
No – Leave this box blank.

iii. **Country**

In the drop-down list, select the country where the organization is legally located.

iv. **Address 1**

Enter the address where the organization is legally located.

v. **Address 2**

Does the organization have a second address that you need to include?

Yes – Enter it here.
No – Leave this box blank.

vi. **City**

Enter the city where the organization is legally located.

vii. **State / Province / Territory/ Region / County**

Enter the state, province, territory, region, or county where the organization is legally located.

viii. **Zip / Postal Code**

Enter the zip or postal code for the organization's location.

ix. **Organization Phone Number**

Enter a phone number at which the organization can be contacted.

e. When you are finished, click **Add**.

9. **Additional Order Options**

Expand **Additional Order Options** and enter the information below as needed. None of this information is required.

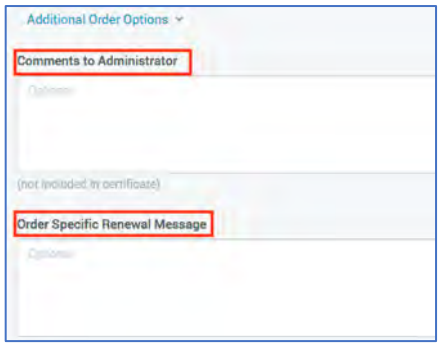
- **Comments to Administrator**

  Enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc.

  Note: These comments are not included in the certificate.

- **Order Specific Renewal Message:**

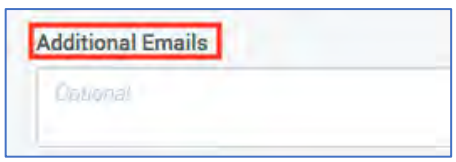
  To create a renewal message for this certificate right now, type a renewal message with information that might be relevant to the certificate's renewal.



10. **Additional Emails**

In the box, enter the email addresses (comma separated) for the people you want to receive the certificate notification emails, such as certificate issuance, duplicate certificate, certificate renewals, etc.

Note: The recipients cannot manage the order, just receive certificate related emails.



11. **Customized Fields**

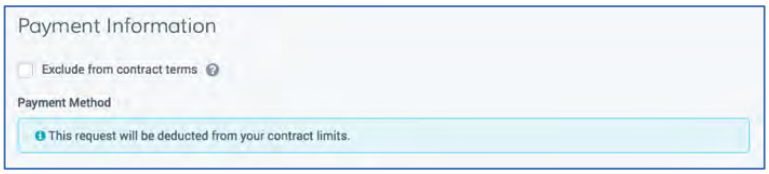
    If your company/organization has added any custom fields to your certificate request form, enter the additional information, required and optional.

12. Under **Payment Information**, use one of the following options to pay for the certificate:

    a. **Pay with Contract Terms**

    If you have a contract and want to use it to pay for the certificate request, continue to step 13.

    Note: If you have a contract, it is the default payment method.



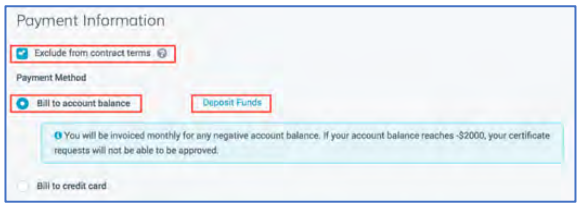
    b. **Exclude from Contract Terms and Pay with Account Balance**

    If you don't want to or can't use your contract terms to pay for the certificate, you can pay for the certificate by billing it to your account.

        i. Check **Exclude from contract terms**

        ii. Select **Bill to account balance**.

        Note: If you need to deposit funds before continuing with the certificate order, click the **Deposit** link. Be aware that when you click the link you are taken to another page inside CertCentral, and the information that you have entered about the certificate is not saved.



c. **Exclude from Contract Terms and Pay with Credit Card**

If you don't want to or can't use your contract terms to pay for the certificate, you can pay for the certificate by billing it to a credit card.

i. Check **Exclude from contract terms**.

ii. Select **Bill to credit card** and then do one of the following options:

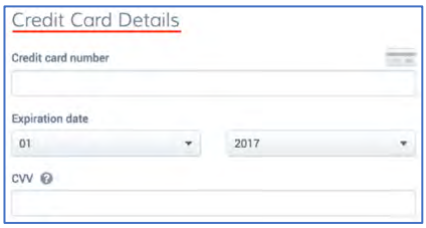
1. **Use One of the Credit Cards Listed**

Under **Selected Card**, select one of the available cards.

2. **Add a Different Credit Card**

a. Under **Selected Card**, select **Another Credit Card**.

b. Under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



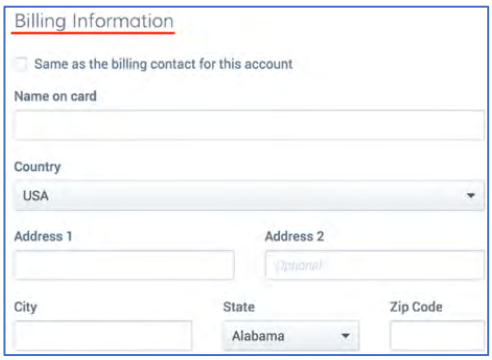
c. Then, under **Billing Information**, use one of the following options add the billing contact information:

Use account's billing contact information

To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.

Add your billing information

Type your billing information (i.e., *Name on card, Country, etc.*).



d. Under **Credit Card Options**, save or don't save your credit card information:

Do Not Save the Credit Card

Uncheck **Save this credit card**.

The credit card will not be added to your account. If you want to use the credit card again, you will need to reenter its information in your account.

Save the Credit Card

To Save the Credit Card do 1 or more of the following tasks:

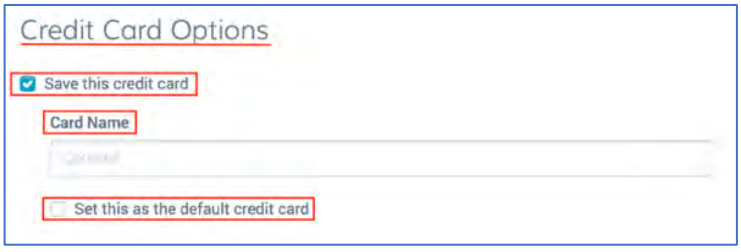
1) Check **Save this credit card**.

2) (Optional) Under **Card Name**, type a name for the credit card that will be helpful when using or identifying the card (i.e., *Pay Account Balance*).

Note: If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*).

3) (Optional) If you want to use this credit card as the default credit card for your account, check **Set this as the default credit card**.

Note: This option does not appear when adding your first credit card. The first credit card added to your account is automatically set as the default credit card.



13. Under **Certificate Services Agreement**, read through the agreement, making sure you understand it and then, check **I agree to the Certificate Services Agreement above**.

14. When you are finished, click **Submit Certificate Request**.

    - On the **Certificate Requests** page (**Certificates > Requests**), your certificate should be listed with the *status* of **Pending**.
    - Before the certificate can be issued, an administrator may need to approve the certificate request.
    - When an approval is required, the administrator is sent an email informing them that they need to approve the certificate request.

7.4.3 How to Request a Multi-Domain SSL or EV Multi-Domain Certificate

Use these instructions to order a Secure Site Multi-Domain SSL, Secure Site EV Multi-Domain SSL, Multi-Domain SSL, and EV Multi-Domain SSL Certificates.

The major difference between the EV Multi-Domain and Multi-Domain certificate issuance process is the degree of organization verification (validation) DigiCert does for the certificate type. See SSL Certificate Validation Process from DigiCert.

Depending on your organizations policies and how your CertCentral account is set up, you may need administrator approval before your order is submitted. After approval, your order will be submitted to DigiCert, so we can complete your order and issue your certificate.

Request a Multi-Domain SSL or EV Multi-Domain SSL certificate

When ordering an EV Multi-Domain Certificate, you will need to add a verified contact. This step is not required for ordering a Multi-Domain Certificate.

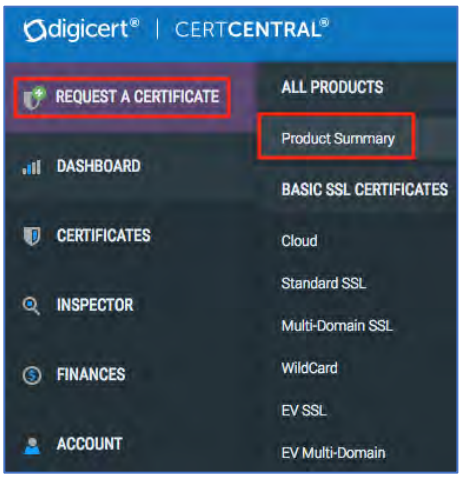
1. Create your CSR.

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

2. In your CertCentral account, do one of the following:

   a. **Option 1: Not sure which certificate you want**

      i. In the sidebar menu, hover over **Request a Certificate** and then under **All Products**, click **Product Summary**.



ii. On the **Request a Certificate** page, look over the certificate options and select the certificate you want to order.

- On the **Business SSL Certificates** tab, select **Secure Site Multi-Domain SSL** or **Secure Site EV Multi-Domain SSL** and then, click **Order Now**.
- On the **Basic SSL Certificates** tab, select **Multi-Domain SSL** or **EV Multi-Domain SSL** and then, click **Order Now**.

b. **Option 2: Know which certificate you want**

In the sidebar menu, hover over **Request a Certificate** and then select the certificate you want to order.

- Under **Business SSL Certificates**, click **Secure Site Multi-Domain SSL** or **Secure Site EV Multi-Domain SSL.**
- Under **Basic SSL Certificates**, click **Multi-Domain SSL** or **EV Multi-Domain SSL**.

3. **Add your CSR**

We use information included in your CSR to populate corresponding values in the order form: Common Name, Organization Unit, and Organization. If any of this information is not included in the CSR, the field in the form is left blank.

Note: Add your CSR before you start filling out the order form. Adding the CSR after will overwrite or delete information from the specified fields in the form (such as the **Organization Unit** field).

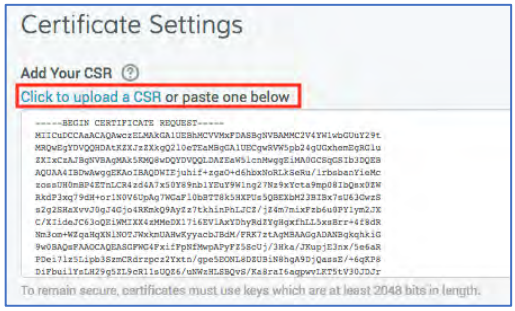
On the **Request "Certificate Name"** page, under **Certificate Settings**, in the **Add Your CSR** box, use one of these options to add your CSR:

- **Upload your CSR**

  Click the **Click to upload a CSR** link to browse for, select, and open your CSR file.

- **Paste your 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:**

After adding your CSR to the order form, we populate the **Common Name** box with the common name from the CSR.

To add the common name yourself, use one of these options:

- Add a recently created domain

  Under **Common Name**, expand **Show Recently Created Domains** and select an available (pre-validated) domain.

- Add a new domain

  When adding a new domain, you will need to complete domain validation (demonstrate control over the domain) before we can issue your certificate. See Domain Validation (Pending Order): Domain Control Validation (DCV) Methods.

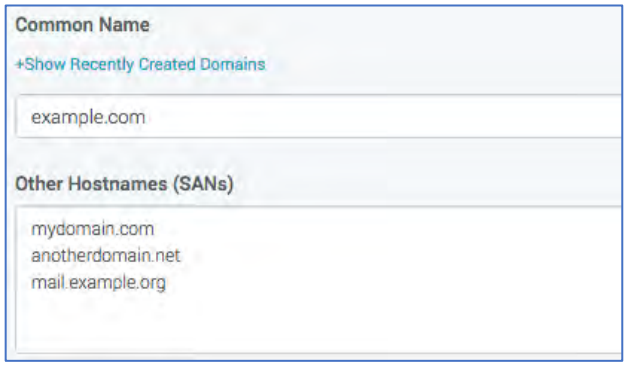
  Under **Common Name**, in the **Common Name** box, type the domain that you want to secure.

When adding a new domain, certificate issuance may take a bit longer while we validate the domain.

5. **Other Hostnames (SANs)**

   After uploading your CSR, we populate the **Other Hostnames (SANs)** box with the SANs included in the CSR. You can still remove or add additional SANs as needed.

   In the **Other Hostnames (SANs)** box, enter additional hostnames (for example, *mydomain.com*, *anotherdomain.net*, *mail.example.org*) that you want your certificate to secure.



6. **Validity Period***

   Select a validity period for the certificate: **1 year**, **2 years**, **Custom expiration date**, or **Customer length**.

   ***Custom validity periods**

   - Certificate pricing is prorated to match the custom certificate length.
   - Certificate validity can't exceed the industry allowed maximum lifecycle period for the certificate. For example, you can't set a 900-day validity period for a certificate.

7. **Additional Certificate Options**

   Expand **Additional Certificate Options**, and provide this information as needed (some information is required; other information is optional):

a. **Signature Hash**

We recommend using the default signature hash (for example, *SHA-256*).

In the drop-down list, select a signature hash.

b. **Server Platform**

In the drop-down list, select the server on which the CSR was generated.

c. **Organization Unit(s)**

You can leave this box blank. Adding an organization unit (OU) for which the certificate and domain will be used is not required. However, if you include OUs in your order, DigiCert will need to validate them before we can issue your certificate.

If your CSR includes an OU, we populate the **Organization Unit** box in the order form with that OU information. If you want to use a different OU than the one included in your CSR, click the delete icon (trash can) and add a different one.

To add the OU yourself, in **the Organization Unit** box, enter the OU.

d. **Auto-Renew**

To set up automatic renewal for this certificate, check **Auto-renew order 30 days before expiration**.

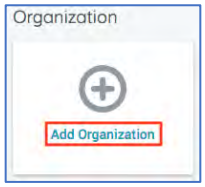
With auto renew enabled, a new certificate order will be automatically submitted when this order nears its expiration date. If your certificate still has time remaining before it expires, DigiCert adds the remaining time from your current certificate to your new certificate (up to 825 days – approximately 27 months).

Important: **Auto-Renew** can't be used with credit card payments. To automatically renew a certificate, the order must be charged to account balance. You can configure the finance settings for your account on the **Finance Settings** page (in the sidebar menu, click **Finances > Settings**).

8. **Organization**

To add an organization, click **Add Organization** and complete one of the options below.

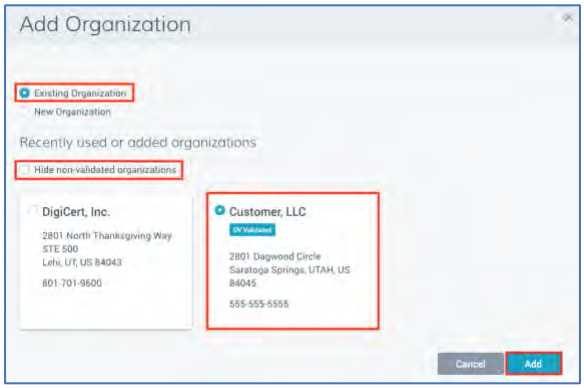
Note: Depending on how your account is configured, you may not be able to use **Option 2: Add a new organization**.



Option 1: Add an existing organization

If your CSR includes an organization currently used in your account, we populate the **Organization** card in the order form with the organization information. If you want to use a different organization than the one included in your CSR, click the delete icon (trash can) and add a different one.

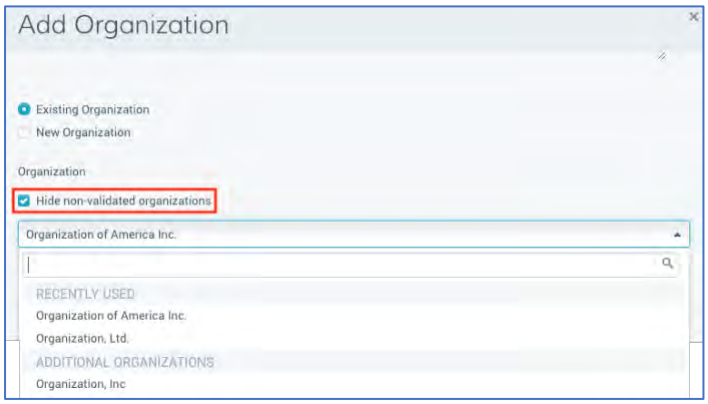
a. In the **Add Organization** window, select **Existing Organization**.



b. To see only a list of fully validated organizations, check **Hide non-validated organizations**.

c. Select one of the available organizations.

If have more than nine organizations in your account, use the **Organization** drop-down list to select an organization.

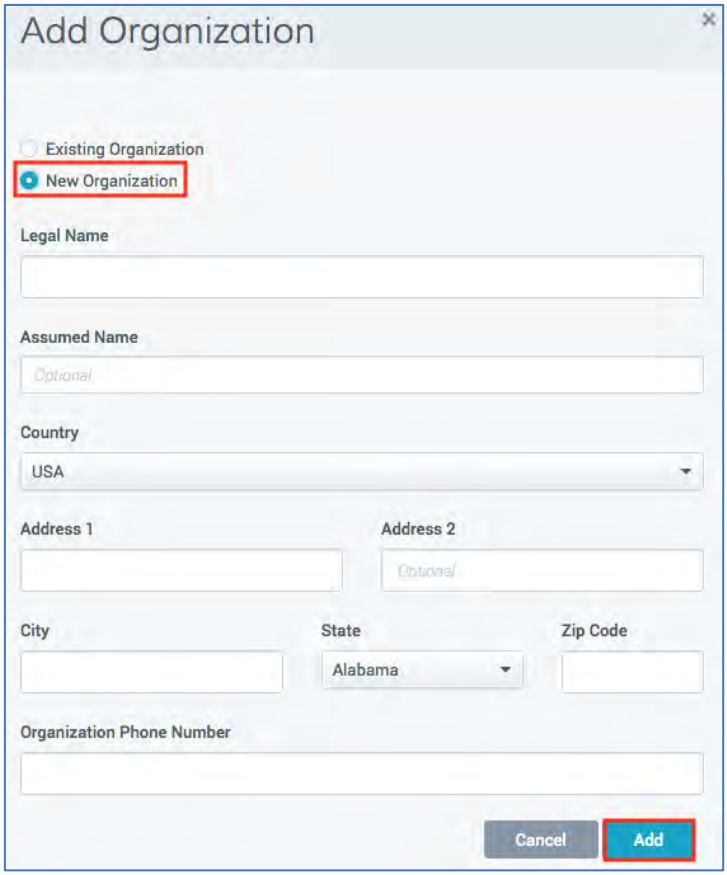


d. Click **Add**.

Option 2: Add a new organization

When adding a new organization, we will need to validate the organization before we can issue your certificate. Also, when you add a new organization, you, the requestor, becomes the organization contact for the newly added organization.

a. In the **Add Organization** window, select **New Organization**.



b. Add these organization details:

i. **Legal Name**

Enter the organization's legally registered name.

ii. **Assumed Name**

Does your organization have a DBA name (doing business as name) that you want to appear on the certificate?

Yes – Enter it here
No – Leave this box blank.

iii. **Country**

In the drop-down list, select the country where the organization is legally located.

iv. **Address 1**

Enter the address where the organization is legally located.

v. **Address 2**

Does the organization have a second address that you need to include?

Yes – Enter it here.
No – Leave this box blank.

vi. **City**

Enter the city where the organization is legally located.

vii. **State / Province / Territory/ Region / County**

Enter the state, province, territory, region, or county where the organization is legally located.

viii. **Zip / Postal Code**

Enter the zip or postal code for the organization's location.

ix. **Organization Phone Number**

Enter a phone number at which the organization can be contacted.

c. When you are finished, click **Add**.

9. **Contacts**

When ordering an EV Multi-Domain and Secure Site EV Multi-Domain SSL Certificate, you need to add a verified EV Contact.

Note: **Contacts** does not appear on the Multi-Domain and Secure Site Multi-Domain SSL certificate request form.

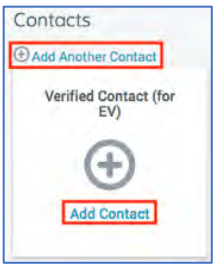
EV Verified Users can approve certificate requests for EV SSL Certificates. For a user to be an EV Verified User, they must have a phone number and job title.

Feature Note:

If you've enabled the **Allow non-DigiCert users to be used as verified contacts** feature, you will see two options: **Existing Contact** and **New Contact**. The **Existing Contact** option lets you assign a CertCentral user as the verified EV contact. The **New Contact** option lets you enter information for a non-CertCentral account user. Use option 1 or 2.

If you haven't enabled this feature, you won't see any options. You can only add account users as verified EV contacts. Use Option 1.

To add a verified EV contact, under **Contacts**, click **Add Contact** and complete one of the options below.

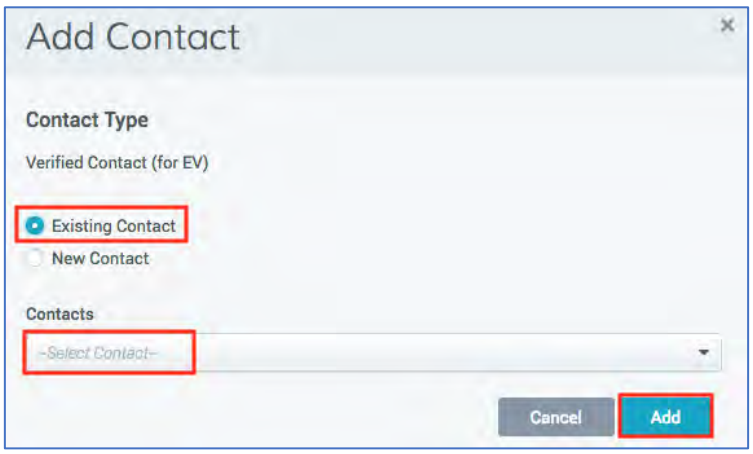


Option 1: Add an existing contact

If your CSR includes an organization currently used in your account and this same organization already has assigned EV verified contacts, the **Verified Contact (for EV)** cards are populated with their information (name, title, email, and phone number).

If you want to use a different EV verified contact, click the delete icon (trash can) and add a different one.

i. In the **Add Contact** window, select **Existing Contact**.



ii. In the **Contacts** drop-down list, select a verified contact for EV.

Is the contact you selected missing a **Job Title** or a **Phone** number? Then, you need to add the missing information. For example, if the contact has a job title but no phone number, you will only need to add the phone number.

i. In the **Job Title** box, enter the contact's job title.

ii. In the **Phone** box, enter the contact's phone number (and **Ext**).

When adding **Job Title** and/or **Phone** for an existing contact, the user profile will be updated with the new information.

iii. Click **Add**.

iv. To add another verified contact, click **Add Another Contact** and repeat the previous steps as needed.

Option 2: Add New Contact

a. In the **Add Contact** window, select **New Contact**.

b. Add the contact's **First Name**, **Last Name**, and **Job Title**.

c. Next, add an **Email** address and **Phone** number at which the contact can be contacted for verifying an EV SSL Certificate request.

d. When you are finished, click **Add**.

e. To add another verified contact, click **Add Another Contact** and repeat the previous steps as needed.

10. **Additional Order Options**

Expand **Additional Order Options** and enter the information below as needed. None of this information is required.

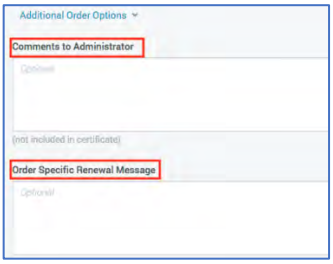
- **Comments to Administrator**

  Enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc.

  Note: These comments are not included in the certificate.

- **Order Specific Renewal Message:**

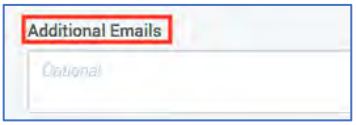
  To create a renewal message for this certificate right now, type a renewal message with information that might be relevant to the certificate's renewal.



11. **Additional Emails**

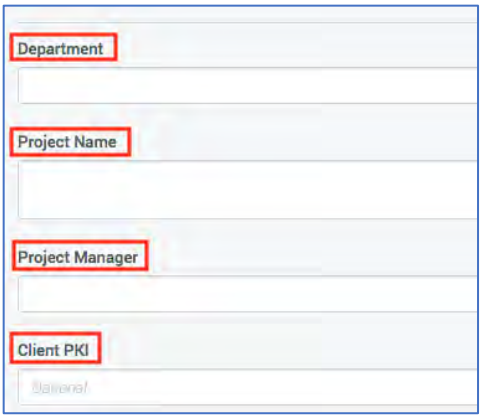
In the box, enter the email addresses (comma separated) for the people you want to receive the certificate notification emails, such as certificate issuance, duplicate certificate, certificate renewals, etc.

Note: The recipients cannot manage the order, just receive certificate related emails.



12. **Customized Fields**

    If your company/organization has added any custom fields to your certificate request form, enter the additional information, required and optional.

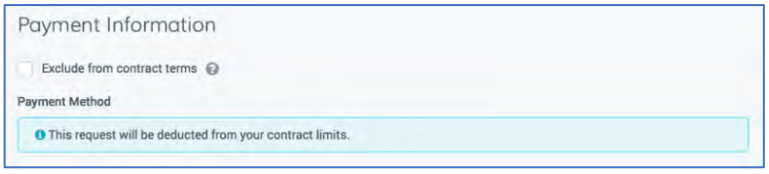


13. Under **Payment Information**, use one of the following options to pay for the certificate:

    a. **Pay with Contract Terms**

    If you have a contract and want to use it to pay for the certificate request, continue to step 14.

    Note: If you have a contract, it is the default payment method.



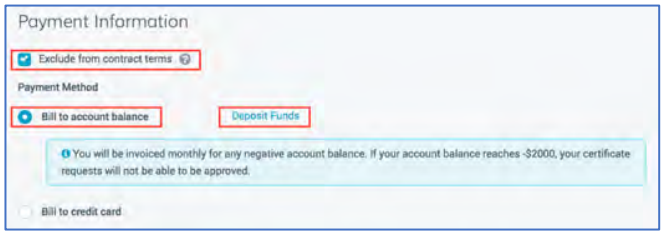
    b. **Exclude from Contract Terms and Pay with Account Balance**

    If you don't want to or can't use your contract terms to pay for the certificate, you can pay for the certificate by billing it to your account.

        i. Check **Exclude from contract terms**

        ii. Select **Bill to account balance**.

Note: If you need to deposit funds before continuing with the certificate order, click the **Deposit** link. Be aware that when you click the link you are taken to another page inside CertCentral, and the information that you have entered about the certificate is not saved.



c. **Exclude from Contract Terms and Pay with Credit Card**

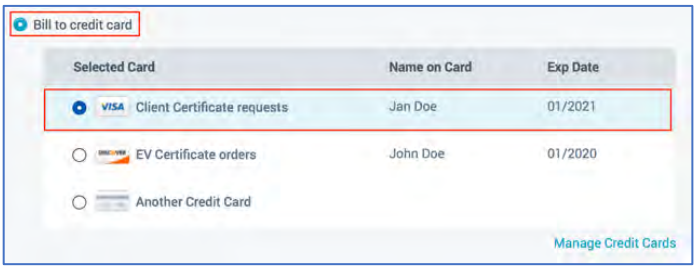
If you don't want to or can't use your contract terms to pay for the certificate, you can pay for the certificate by billing it to a credit card.

i. Check **Exclude from contract terms**.

ii. Select **Bill to credit card** and then do one of the following options:

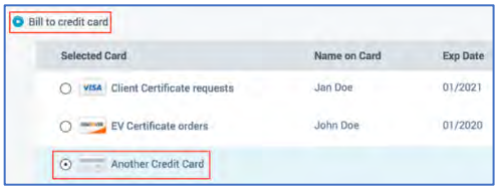
1. **Use One of the Credit Cards Listed**

Under **Selected Card**, select one of the available cards.

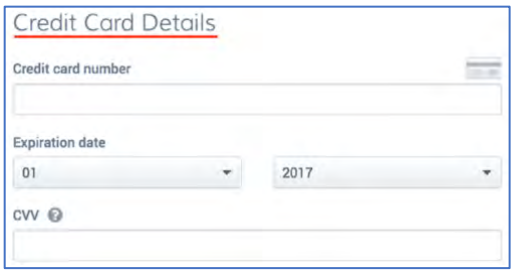


2. **Add a Different Credit Card**

a. Under **Selected Card**, select **Another Credit Card**.



b. Under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



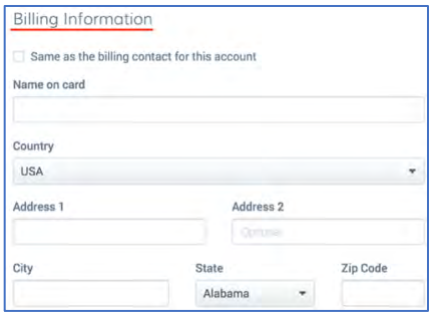
c. Then, under **Billing Information**, use one of the following options add the billing contact information:

Use account's billing contact information

To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.

Add your billing information

Type your billing information (i.e., *Name on card, Country, etc.*).



d. Under **Credit Card Options**, save or don't save your credit card information:

Do Not Save the Credit Card

Uncheck **Save this credit card**.

The credit card will not be added to your account. If you want to use the credit card again, you will need to reenter its information in your account.

Save the Credit Card

To Save the Credit Card do 1 or more of the following tasks:

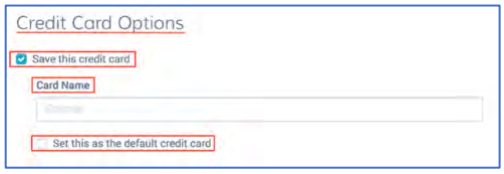
1) Check **Save this credit card**.

2) (Optional) Under **Card Name**, type a name for the credit card that will be helpful when using or identifying the card (i.e., *Pay Account Balance*).

Note: If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*).

3) (Optional) If you want to use this credit card as the default credit card for your account, check **Set this as the default credit card**.

Note: This option does not appear when adding your first credit card. The first credit card added to your account is automatically set as the default credit card.



14. Under **Certificate Services Agreement**, read through the agreement, making sure you understand it and then, check **I agree to the Certificate Services Agreement above**.

15. When you are finished, click **Submit Certificate Request**.

- On the **Certificate Requests** page (**Certificates > Requests**), your certificate should be listed with the *status* of **Pending**.
- Multi-Domain SSL – Before the certificate can be issued, an administrator may need to approve the certificate request.
- EV Multi-Domain – Before the certificate can be issued an EV Certificate approver may need to approve the certificate request.
- If approval is required, the administrator, manager, or EV Certificate approver is sent an email informing them that they need to approve the certificate request.

7.5 Managing Guest URLs

A Guest URL is a link to a specific certificate's request page. You can create Guest URLs for the following certificates:

Business SSL
- Secure Site SSL
- Secure Site Multi-Domain SSL
- Secure Site Wildcard SSL
- Secure Site EV SSL
- Secure Site EV Multi-Domain SSL

Basic SSL
- Standard SSL
- Multi-Domain SSL
- Wildcard
- EV SSL
- EV Multi-Domain

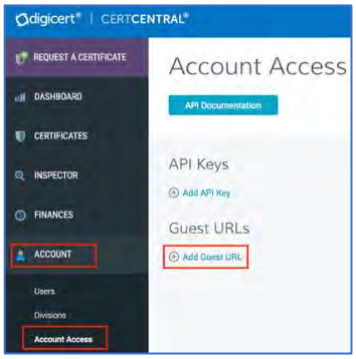
Client
- Authentication Plus
- Digital Signature Plus
- Email Security Plus
- Premium

A Guest URL lets you provide a guest user with the ability to request a certificate without adding them to your account. Guest URLs only give users access to a specific certificate request page within the account. The user cannot access anything else within the account.

7.5.1 How to Create a Guest URL

Use these instructions to create a guest URL so non-CertCentral account users can order certificates when needed. Once created, you can send the guest URL out as needed.

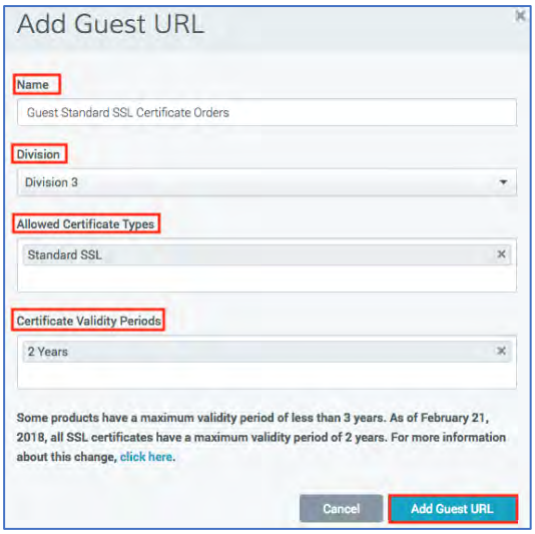
1. In your CertCentral account, in the sidebar menu, click **Account > Account Access**.



2. On the **Account Access** page, under **Guest URLs**, click **+ Add Guest URL**.
3. In the **Add Guest URL** window, complete these tasks to configure your quest URL:

Name	Type a brief name for the URL that makes it easily identifiable in the list of Guest URLs.
Division	In the drop-down list, select the division you want the guest URL certificate orders to be billed to.
Allowed Certificate Types	Click in the drop-down list to select the certificates the Guest URL will allow the guest user to request. You can select single or multiple certificates.

Certificate Validity Periods	Click in the drop-down list select the validity period(s) for the certificate(s) that you selected. You can select single or multiple periods. Some certificate types may have a maximum validity period that is less than the validity period you selected. For example, you select Code Signing and Standard SSL and then, you select 3 years. When the guest user orders a Standard SSL Certificate, the validity period will only be for 2 years. When the guest user orders a Code Signing Certificate, the validity period will be for 3 years.



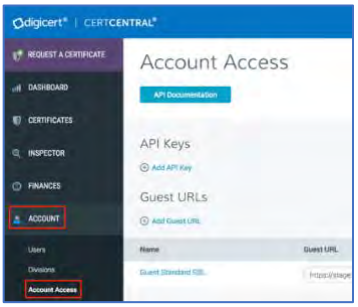
4. When you are finished, click **Add Guest URL**.

   You can now send the Guest URL to a "guest" and let them order a specific certificate(s).

7.5.2 How to Send the Guest URL to a "Guest"

Use these instructions to send the guest URL to a non-CertCentral account user so they can order a needed certificate. After the recipient orders their certificate, the request will still need your approval before it is submitted to DigiCert to process.

1. In your CertCentral account in the sidebar menu, click **Account > Account Access**.

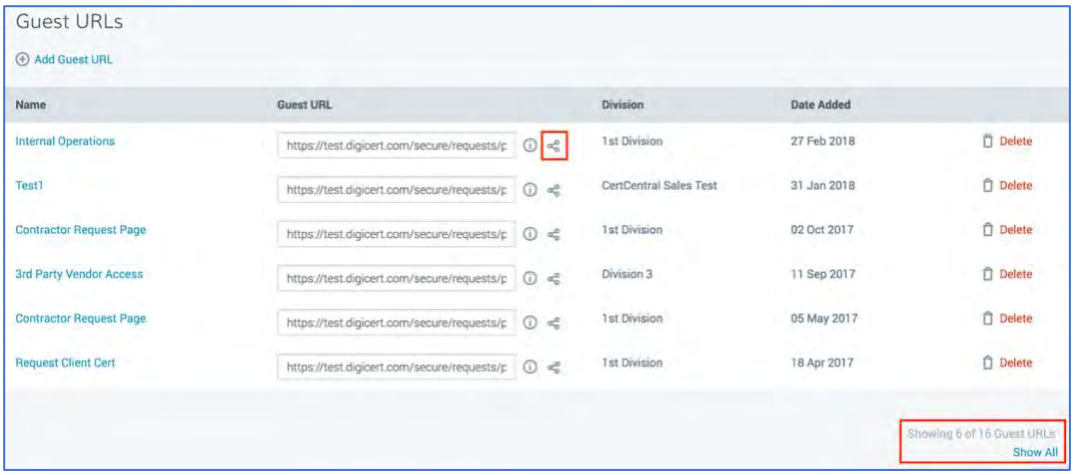


2. On the **Account Access** page, under **Guest URLs**, you can view all or some of the guest URLs that you have created.

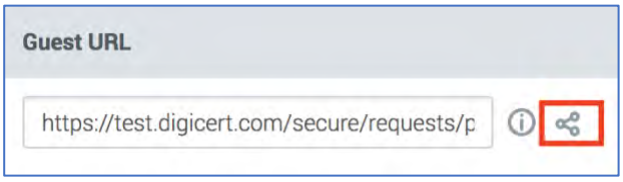
    a. To see all your guest URLs, in the bottom right corner, below the list of URLs, click **Show All**.

    Note: The **Show All** link only appears if you have created more than 10 guest URLs.

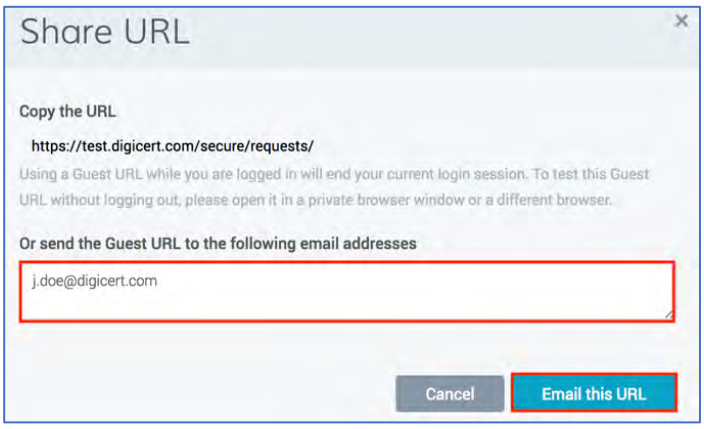
    b. On the **Guest URLs** page, all guest URLs are listed**.**



3. To the right of the Guest URL that you want to share, click the **Share this URL** button (that is next to the **Information** button).



4. In the **Share URL** window, in the **or Send the Guest URL to the following email address** box, type the email addresses (comma separated) of the guest to whom you want to send the guest URL.

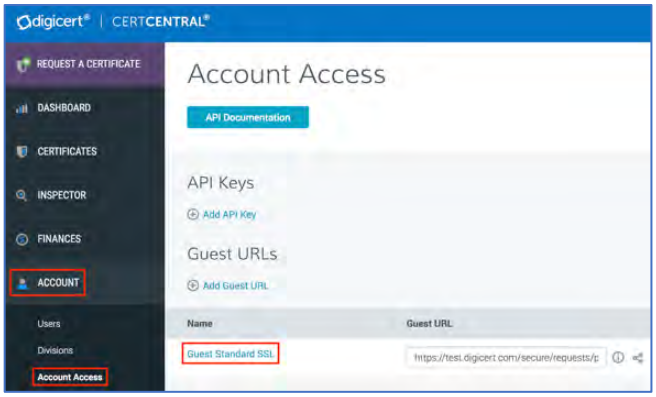


5. When you are finished, click **Email this URL**.

7.5.3 How to Edit a Guest URL

Use these instructions to make changes to a guest URL (for example, modify the name).

1. In your CertCentral account, in the sidebar menu, click **Account > Account Access**.



2. On the **Account Access**, under **Guest URLs** page, click the **"Name"** link for the Guest URL that you need to edit.

    a. If you do not see the guest URL listed on this page, in the bottom right corner below the list of URLs, click **Show All**.

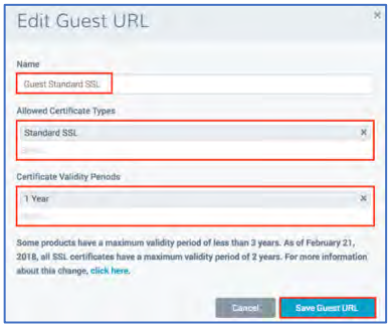
    Note: The **Show All** link only appears if you have created more than 10 guest URLs.

    b. On the **Guest URLs** page, click the **"Name"** link for the Guest URL that you need to edit.

3. In the **Edit Guest URL** window, edit the **Name**, make **Allow Certificate Types** changes, and update the Certificate Validity Periods. (See How to Create a Guest URL.)

    Notes: You can select single or multiple certificates. Some certificate types may have a maximum validity period that is less than the validity period you selected.

    For example, you select Code Signing and Standard SSL and then, you select 3 years. When the guest user orders a Standard SSL Certificate, the validity period will only be for 2 years. When the guest user orders a Code Signing Certificate, the validity period will be for 3 years.



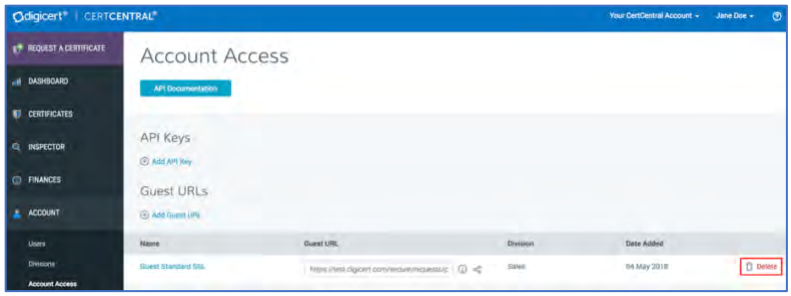
4. When you are finished, click **Save Guest URL**.

    You can now send the updated Guest URL to a "guest" and let them order specific certificates.

7.5.4 How to Delete a Guest URL

Use these instructions to delete a no longer needed guest URL. Note that deleting a guest URL disables anyone who is using it to request a certificate.

1. In your CertCentral account, in the sidebar menu, click **Account > Account Access**.



2. On the **Account Access** page, under **Guest URLs**, to the right of the URL that you need to delete, click **Delete**.

   i. If you do not see the URL listed on this page, in the bottom right corner below the list of URLs, click **Show All**.

   Note: The **Show All** link only appears if you have created more than 10 guest URLs.

   ii. On the **Guest URLs** page, to the right of the URL that you need to delete, click **Delete**.

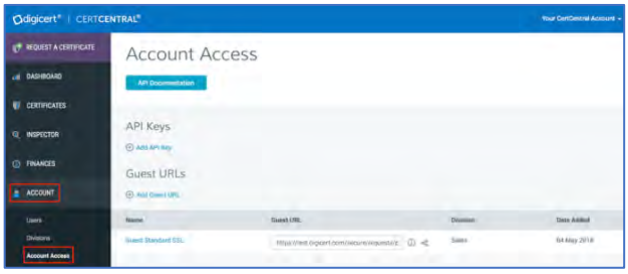
   CAUTION: In the **Delete Guest URL** window, do not click **Delete** unless you are sure that you want to delete the Guest URL. Deleting a Guest URL disables anyone who is using it to request a certificate.

3. In the **Delete Guest URL** window, under the ***"Are you sure you want to delete the Guest URL 'Description'? It will stop working immediately, and cannot be undone."*** message, click **Delete**.

4. All copies of the Guest URL link should no longer work.

7.5.5 How to View Guest URLs

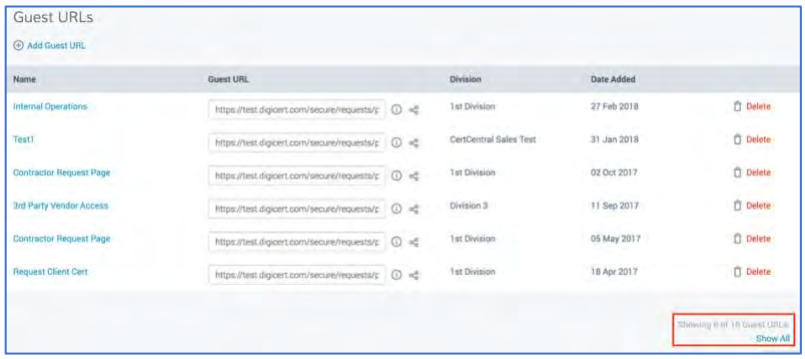
1. In your account, in the sidebar menu, click **Account > Account Access**.



2. On the **Account Access** page, under **Guest URLs**, you can view all or some of the guest URLs that you have created.

3. To see all your guest URLs, in the bottom right corner, below the list of URLs, click **Show All**.

   Note: The **Show All** link only appears if you have created more than 10 guest URLs.



4. On the **Guest URLs** page, all guest URLs are listed**.**

5. Use the search box and column headers to locate guest URLs.

7.6 Managing Certificate Request Approvals

By default, certificate requests require as approval before they are submitted to DigiCert for certificate issuance.

After a user requests a certificate, an Administrator, a manager, an EV Verified User, a CS Verified User, or an EV CS Verified User must approve the certificate request. Next, the request is sent to DigiCert to verify that all the pre-validation requirements have been met. Then, we issue the certificate.

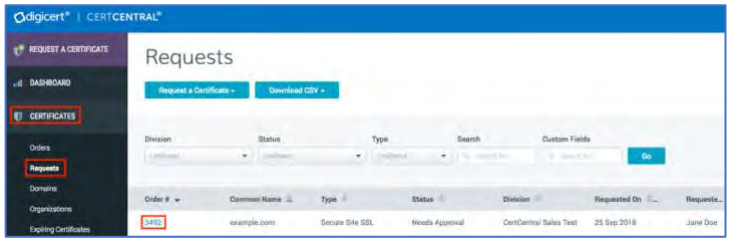
After a user requests a certificate, any Administrator, manager, EV Verified User, CS Verified User, or EV CS Verified User can also reject the certificate request, if needed. For example, if the user ordered the wrong type of certificate.

7.6.1 How to Approve a Certificate Request

Use these instructions to approve a certificate request.

Only an **EV Verified User** can approve EV SSL, EV Multi-Domain, Secure Site EV SSL, and Secure Site EV Multi-Domain SSL Certificate requests. Only an **EC CS Verified User** can approve EV Code Signing Certificate requests. Only a **CS Verified User** can approve Code Signing Certificate requests.

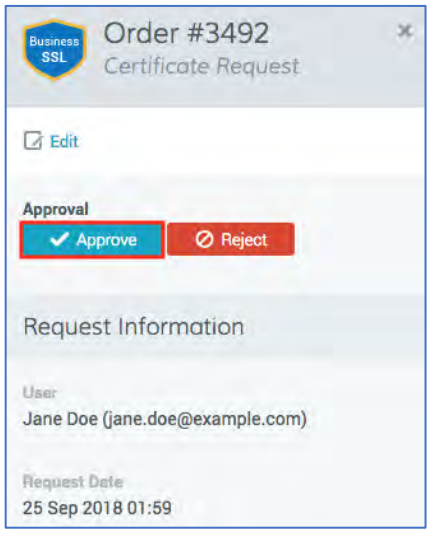
1. In your CertCentral account, in the sidebar menu, click **Certificates > Requests**.



2. On the **Requests** page, use the drop-down lists, search box, and column headers to filter the list of requests.

3. In the **Order#** column, click the **Order number** link of the certificate requests that you want to approve.

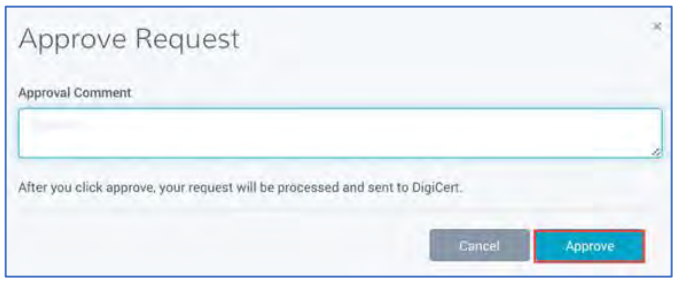
4. In the **Order#** details pane (on the right), review the request information, certificate Information, etc., verifying that all information is correct, and then click **Approve**.



5. In the **Approve Request** window, type an **Approval Comment** and then click **Approve**.

   On the **Orders** page (**Certificates > Orders**), your certificate should be listed with the ***status*** of **Pending**.

   If all validation is completed and no further validation is required, the certificate should be issued to your account within minutes.



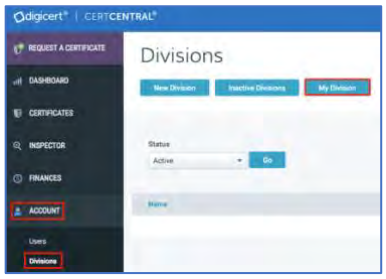
7.6.2 How to Remove the Approval Step from the Certificate Order Process

Use these instructions to remove the approval step from your certificate order process. Admin approvals are not required as orders are submitted directly to DigiCert for certificate issuance, bypassing the request process completely.

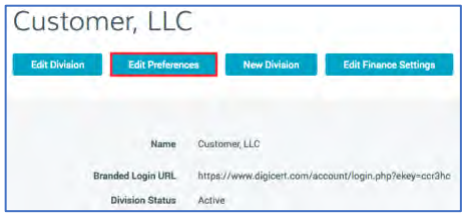
Note: Administrator approvals are still required for certificate revocations, Guest URL certificate requests, and Finance Manager, Standard User, and Limited User certificate requests.

1. In your CertCentral account, in the sidebar menu, click **Account > Divisions**.

   If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.



2. On the **Divisions** page, click **My Division**.
3. On the **"Division Name"** page, click **Edit Preferences**.



4. On the **Division Preferences** page, expand **+Advanced Settings**.
5. In the **Certificate Requests** section, under **Approval Steps**, select **Skip approval step: remove the approval step from your certificate order processes.**

6. At the bottom of the page, click **Save Settings**.

   The next time someone orders a certificate, the request will be submitted directly to DigiCert for certificate issuance.

   Note: These orders don't require an admin approval, so they won't be listed on the **Requests** page (**Certificates > Requests**). Instead, these orders will only appear on the **Orders** page (**Certificate > Orders**).

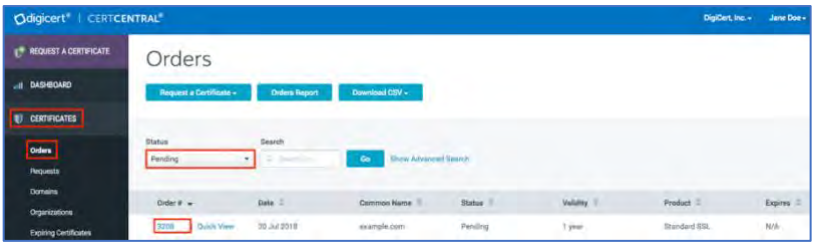
7.7 How to Cancel a Certificate Order

You may need to cancel a **pending** certificate order after it has been approved but before it has been issued.

Note: You can only cancel **pending** certificate orders. If the order is still waiting for approval, you don't need to cancel it. An approver can just reject the request.

Use these instructions to cancel a **pending** certificate order after it has been approved.

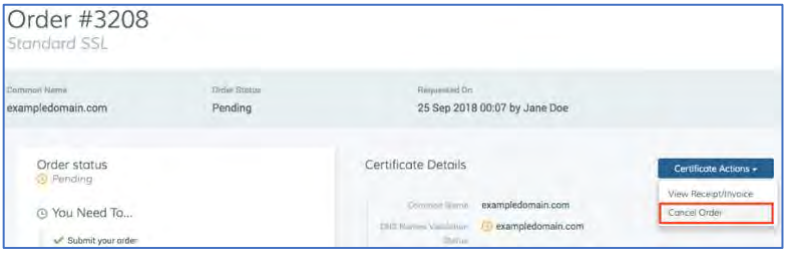
1. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.



2. On the **Orders** page, use the filters and the advanced search features to locate the **pending** 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**.

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

6. Congratulations! You have successfully canceled the order.

7.8 Accessing a Certificate

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

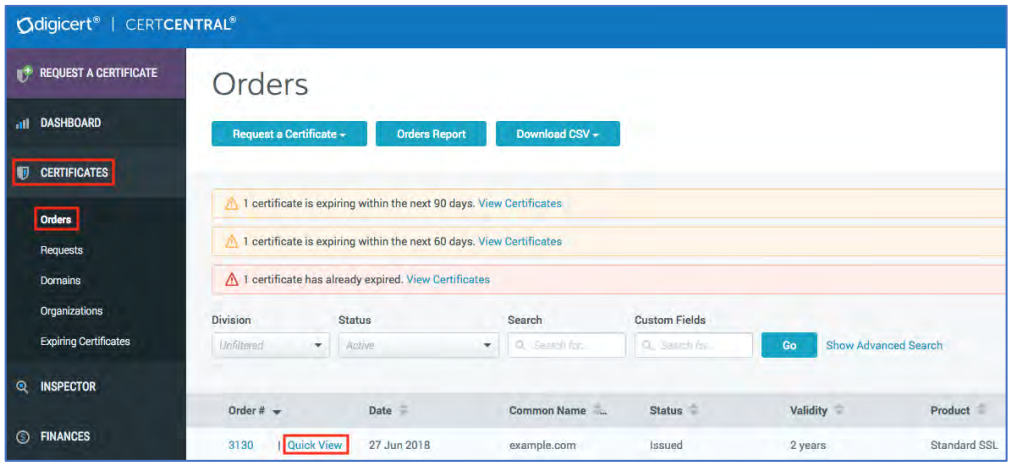
7.8.1 How to Download a Certificate from Your Account

Use these instructions to download your certificate. After your certificate is issued, you may want to download the certificate.

- How to Download a TLS/SSL Certificate (Secure Site SSL, Standard SSL, EV SSL, etc.)
- How to Download a Client Certificate (Premium, Digital Signature, etc.)
- How to Download a Code Signing Certificate

How to Download a TLS/SSL Certificate (Secure Site SSL, Standard SSL, EV SSL, etc.)

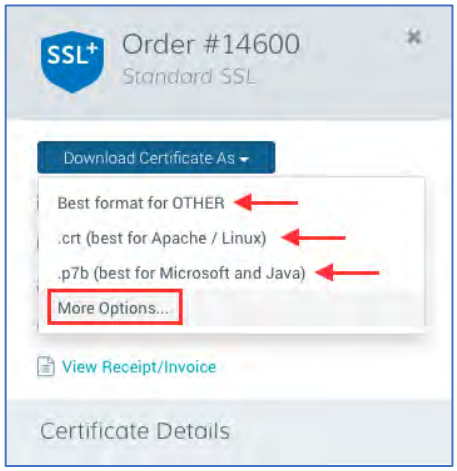
1. On the server or workstation where you need to install the certificate, log into your CertCentral account.
2. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



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 certificate that you need to download.
5. In the **Order #** details pane (on the right), in the **Download Certificate As** drop-down list, select one of the following options to download a copy of the certificate:

Best format for…	Use this option to download the certificate in the format recommended for the server platform or software that was selected when you ordered the certificate. Save the certificate file to your server or workstation, making sure to note the location.

.crt (best for Apache/Linux)	Use this option to download the certificate in a .crt format, best for Apache/Linux platforms. Save the certificate file to your server or workstation, making sure to note the location.
.p7b (best for Microsoft and Java)	Use this option to download the certificate in a .p7b format best for Microsoft and Java platforms. Save the certificate file to your server or workstation, making sure to note the location.
More Options…	See Step 6.



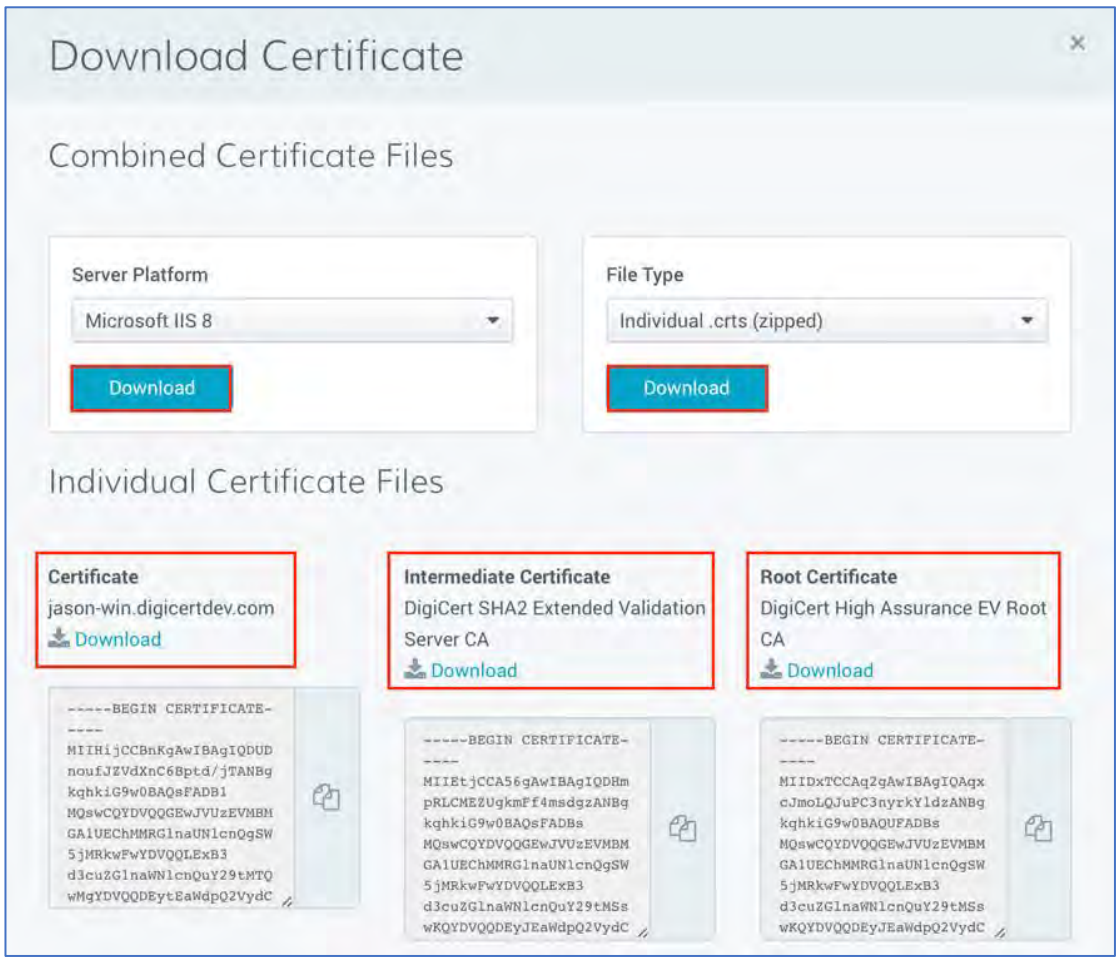
6. In the **Download Certificates As** drop-down list, click **More Options…** to see more **Server Platform** options (e.g., *Tomcat*), **File Type** options (e.g., *A single. pem file containing all the certs*), or to download only the **Certificate**, the **Intermediate Certificate**, or the **Root Certificate**.

   a. **To Download a Combined Certificate File:**

   In the **Download Certificate** window, under **Combined Certificate Files** do either of the following options:

Server Platform	1. In the drop-down list, select a server platform (e.g., *Tomcat*) and then click **Download**. 2. Save the certificate file to your server or workstation, making sure to note the location.
File Type	1. In the drop-down list, select a file type (e.g., *a single .pem file containing all the certs*) and then click **Download**.

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



b. **To Download an Individual Certificate File (Server, Intermediate, and Root):**

Under **Individual Certificate Files**, do any of the following:

Certificate

1. To download just the server certificate file, click **Download**.
2. Save the server certificate file to your server or workstation, making sure to note the location.

Intermediate Certificate

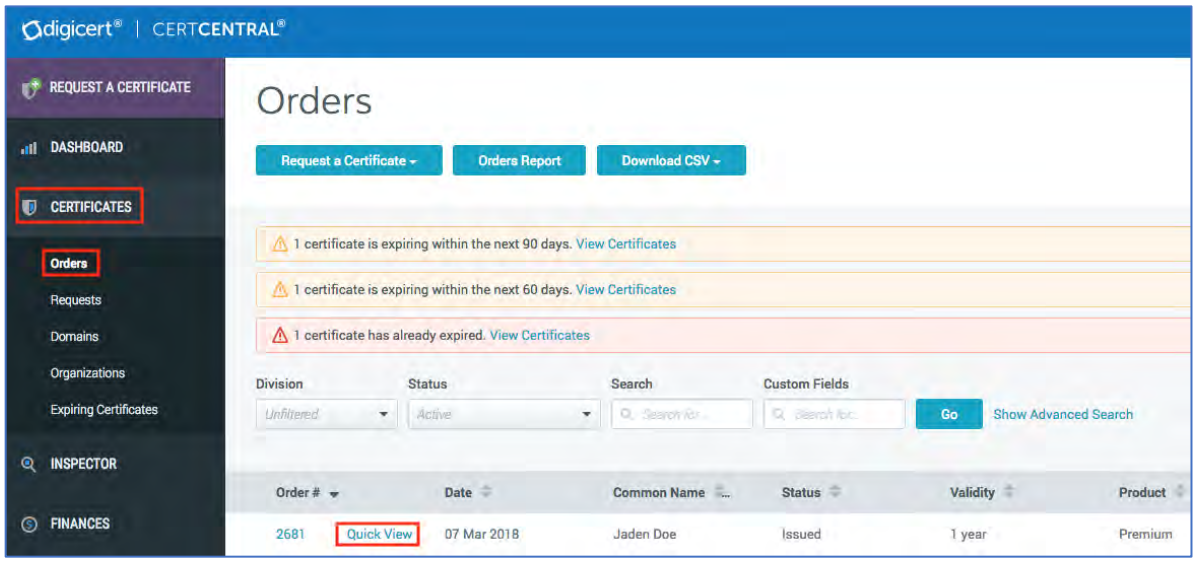
1. To download just the intermediate certificate file, click **Download**.
2. Save the intermediate certificate file to your server or workstation, making sure to note the location.

Root Certificate

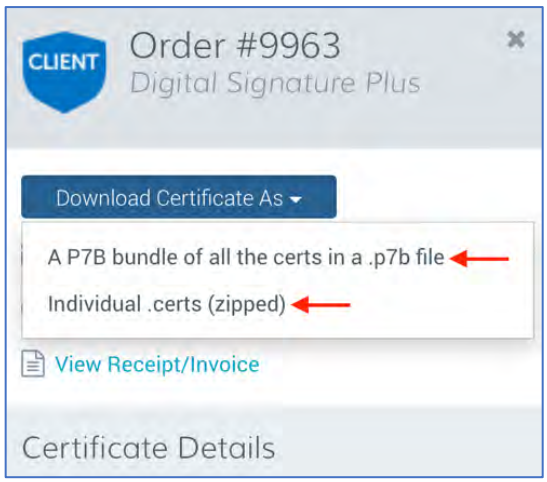
1. To download just the root certificate file, click **Download**.
2. Save the root certificate file to your server or workstation, making sure to note the location.

How to Download a Client Certificate (Premium, Digital Signature, etc.)

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



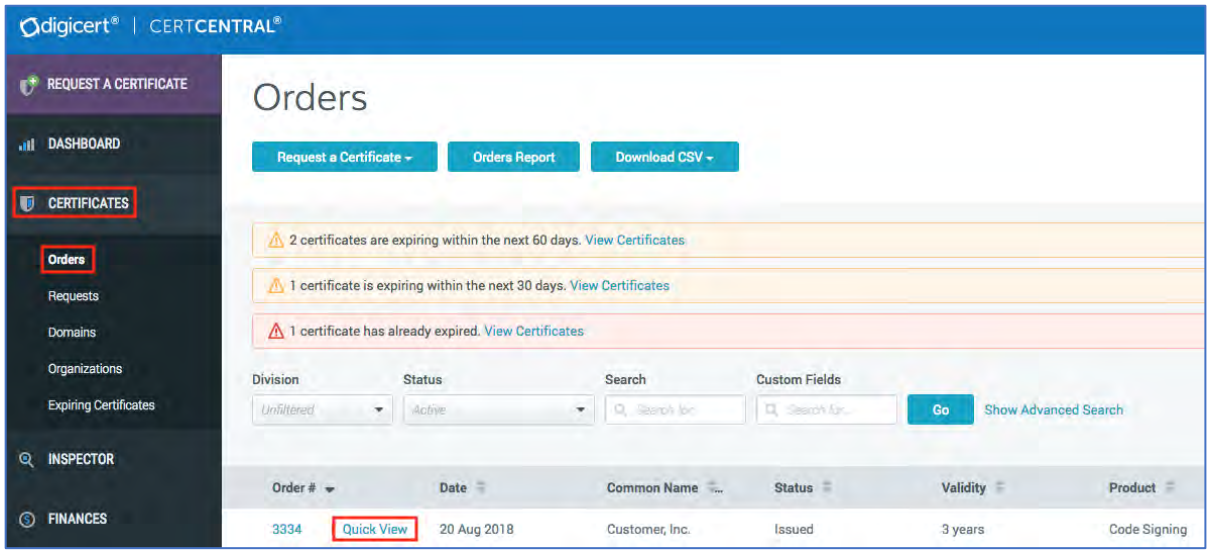
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. In the **Order #** column, click the **Quick View** link of the certificate that you need to download.
4. In the **Order #** details pane (on the right), in the **Download Certificate As** drop-down list, select one of the following options to download a copy of the certificate: **A P7B bundle of all the certs in a .p7b file** or **Individual .certs (zipped)**.



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

How to Download a Code Signing Certificate

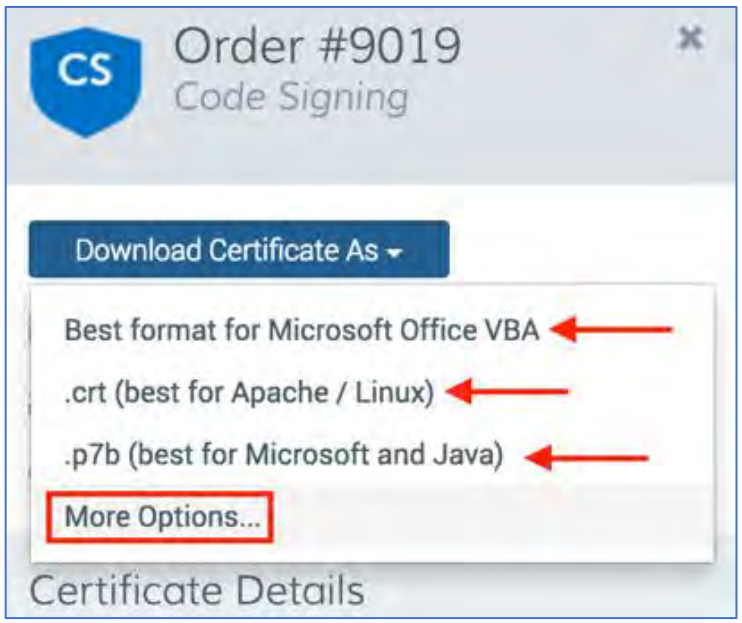
1. On the server or workstation where you need to install the certificate, log into your CertCentral account.



2. In your account, in the sidebar menu, click **Certificate > 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 of the certificate that you need to download.
5. In the **Order #** details pane (on the right), in the **Download Certificate As** drop-down list, select one of the following options to download a copy of the certificate:

Best format for…	Use this option to download the certificate in the format recommended for the server software or software that was selected during the certificate request. Save the certificate file to your server or workstation, making sure to note the location.
.crt (best for Apache/Linux)	Use this option to download the certificate in a .crt format, best for Apache/Linux platforms. Save the certificate file to your server or workstation, making sure to note the location.
.p7b (best for Microsoft and Java)	Use this option to download the certificate in .p7b format best for Microsoft and Java platforms.

	Save the certificate file to your server or workstation, making sure to note the location.
More Options…	See Step 6.

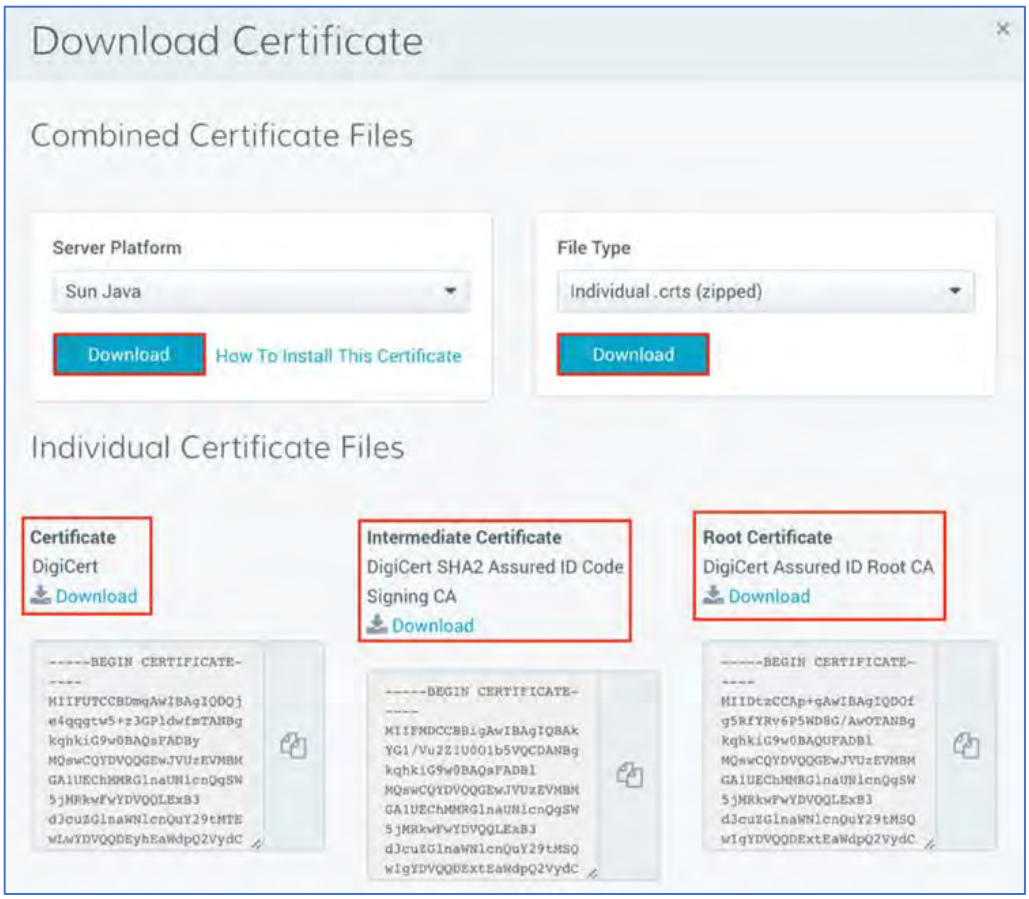


6. In the **Download Certificates As** drop-down list, click **More Options…** to see more Server Platform options (e.g. *Adobe Air*), File Type options (e.g., *A single .pem file containing all the certs*), or to download only the code signing, intermediate, or root certificate.

   a. **To Download a Combined Certificate File:**

   In the **Download Certificate** window, under **Combined Certificate Files** do either of the following options:

Server Platform	1. In the drop-down list, select a server platform (e.g. *Adobe Air*) and then click **Download**. 2. Save the certificate file to your server or workstation, making sure to note the location.
File Type	1. In the drop-down list, select a file type (e.g., *A single .pem file containing all the certs*) and then click **Download**. 2. Save the certificate file to your server or workstation, making sure to note the location.



b. **To Download an Individual Certificate File (Code Signing, Intermediate, and Root):**

Under **Individual Certificate Files**, do any of the following:

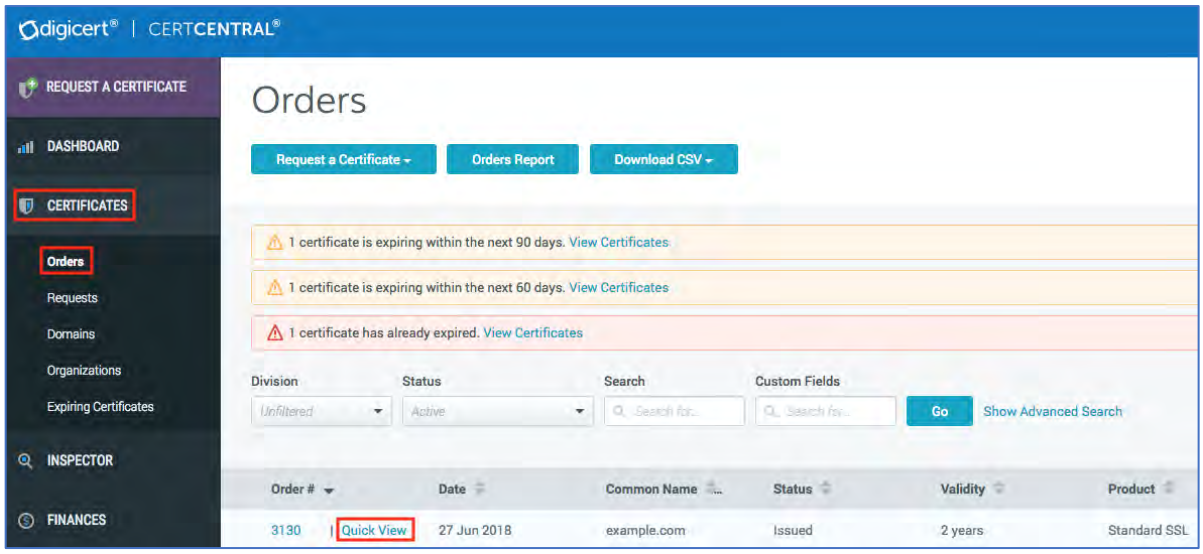
Certificate	1. To download just the code signing certificate file, click **Download**. 2. Save the server certificate file to your server or workstation, making sure to note the location.
Intermediate Certificate	1. To download just the intermediate certificate file, click **Download**. 2. Save the intermediate certificate file to your server or workstation, making sure to note the location.
Root Certificate	1. To download just the root certificate file, click **Download**. 2. Save the root certificate file to your server or workstation, making sure to note the location.

7.8.2 How to Email a Certificate from Your CertCentral Account

Use these instructions to email a copy of a certificate. After a certificate has been issued, you can email the 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.

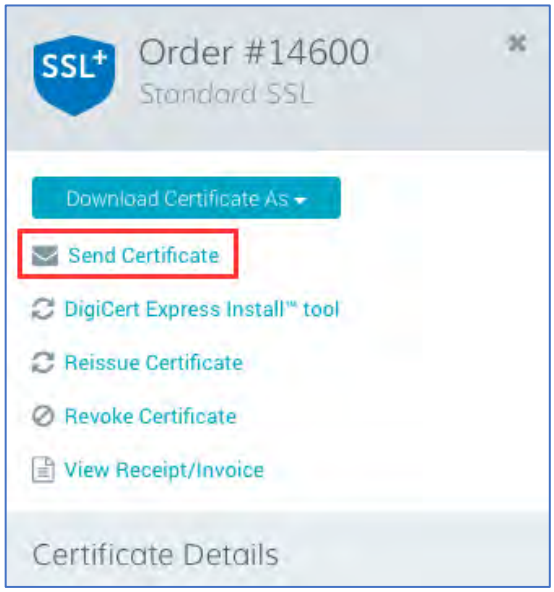
1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



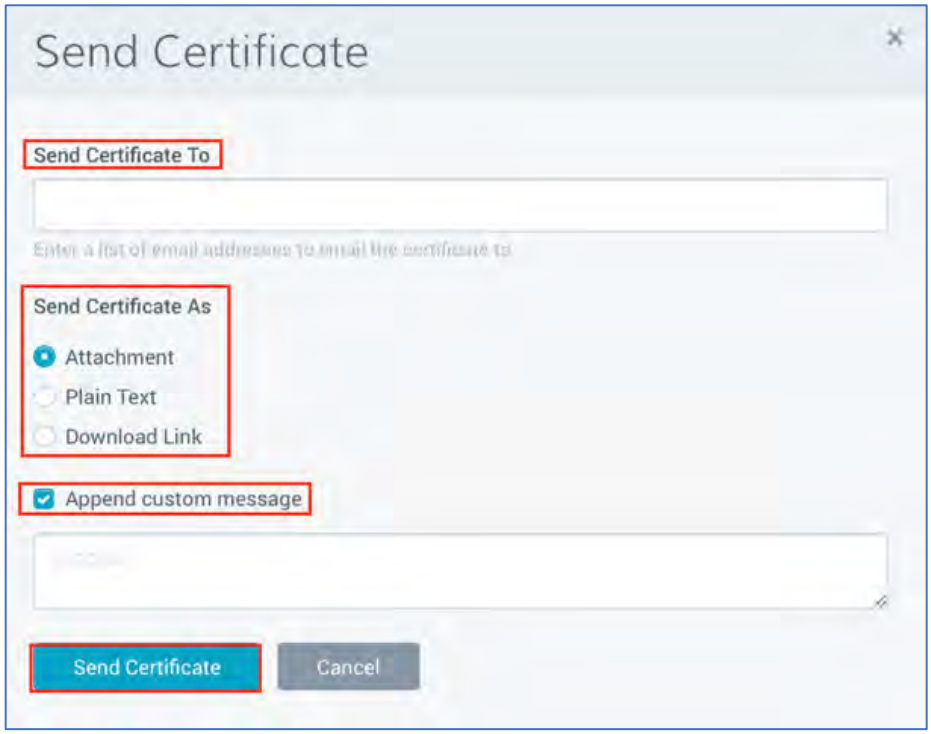
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.

3. In the **Order#** column, click the **Quick View** link of the certificate that you want to send out.

4. In the **Order#** details pane (on the right), click **Send Certificate**.



5. In the **Send Certificate** window, in the **Send Certificate To** box, enter the email addresses for the people you want to receive the certificate (comma separated).



6. Under **Send Certificate As**, do the following:

Attachment	To send the certificate as an attachment to the email, select this option.
Plain Text	To send the certificate as plain text in the body of the email, select this option.
Download Link	To send a link to a download page (from which you can download the certificate) in the body of the email, select this option. **Note:** To access the download page the receiver does not need to have a CertCentral account.
Append custom message	1. Check this box to add a custom message to the certificate email. 2. In the text box that appears, enter the message that you want sent with the email (i.e., "*Install this certificate on the server in the left corner of the server room*").

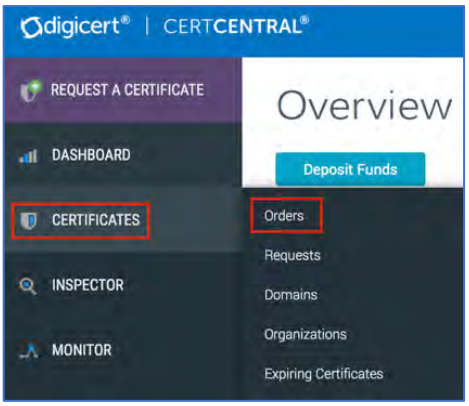
7. When you are finished, click **Send Certificate**.

7.8.3 How to Email a Duplicate Certificate from Your CertCentral Account

Use these instructions to email a duplicate certificate. After a duplicate certificate has been issued, you can email the original or the duplicate certificate to specified email addresses. You can also select the delivery format for the certificate: attachment, plaintext, or download link.

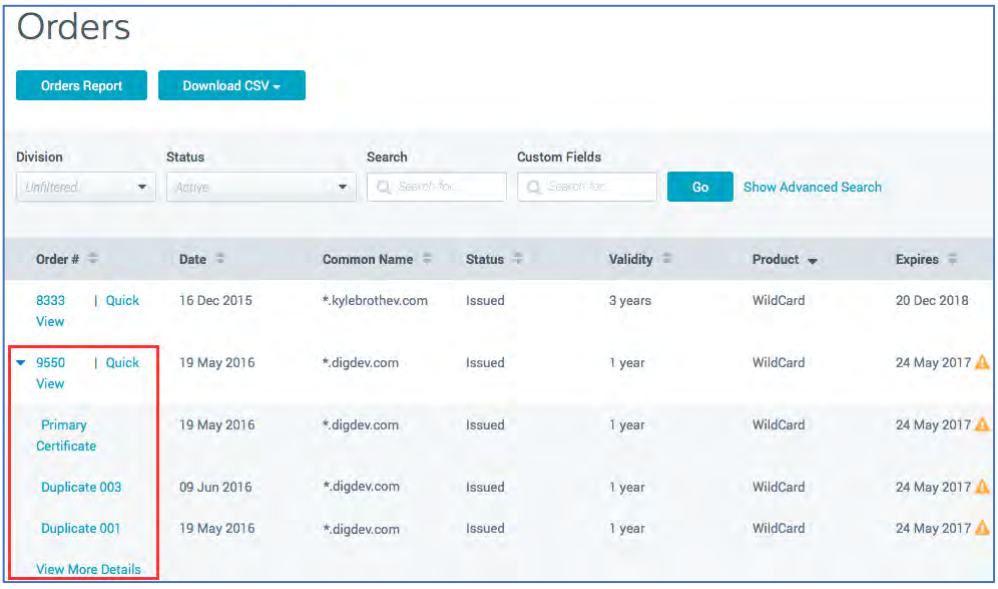
Note: When you email a certificate, it is logged as an event in the audit log.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



2. On the **Orders** page, use the drop-down list, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.

   Note: Certificates with duplicates will have a right arrow next to them. Click the side arrow to see the original certificate and 4 most recently created duplicate certificates.



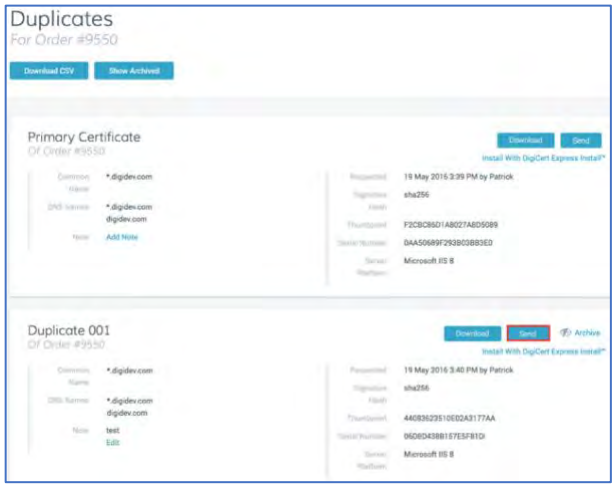
3. Click the **"Duplicate #"** link of the duplicate certificate (e.g., *Duplicate 001*) that you need to send out.

   If the certificate you want to send out is not listed, do the following:

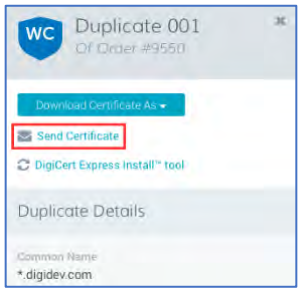
   a. Click **View More Details**.

b. On the **Duplicates** page, locate the duplicated certificate, and then click **Send**.

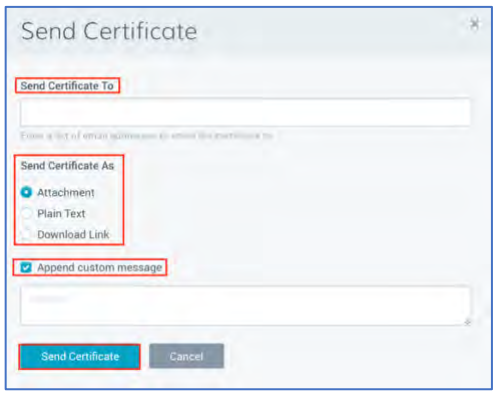
c. Go to step 5.



4. In the **Order #** detail pane (on the right), above **Duplicate Details**, click **Send Certificate**.



5. In the **Send Certificate** window, in the **Send Certificate To** box, enter the email addresses for the people you want to receive the certificate (comma separated).



6. Under **Send Certificate As**, do the following:

Attachment	To send the certificate as an attachment to the email, select this option.

Plain Text	To send the certificate as plain text in the body of the email, select this option.
Download Link	To send a link to a download page (from which you can download the certificate) in the body of the email, select this option. **Note:** To access the download page the receiver does not need to have a CertCentral account.
Append custom message	1. Check this box to add a custom message to the certificate email. 2. In the text box that appears, enter the message that you want sent with the email (i.e., "*Install this certificate on the server in the left corner of the server room*").

7. When you are finished, click **Send Certificate**.

7.9 How to Grant "Limited" Users Access to a Certificate Order

Use these instructions to grant a limited user access to a certificate order to they can manage an order that's not theirs (such as, download a certificate, renew a certificate, and other certificate related actions). Instead of changing the user's role, you can grant them access to manage that specific order.

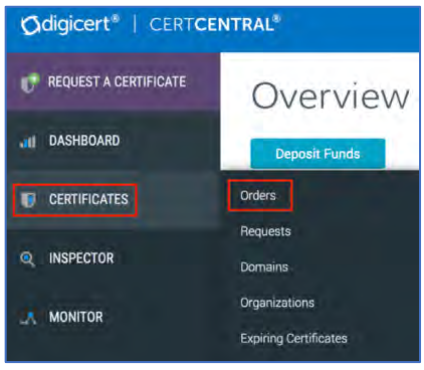
Note: The "limited" user role can only see certificates that they have ordered. To allow a "restricted" admin, manager, financial manager, or standard user to manage the order, you can add them to the division (see 1.1 Unrestricted versus Restricted).

You can grant a "limited" user access while the order is pending or after the certificate has been issued.

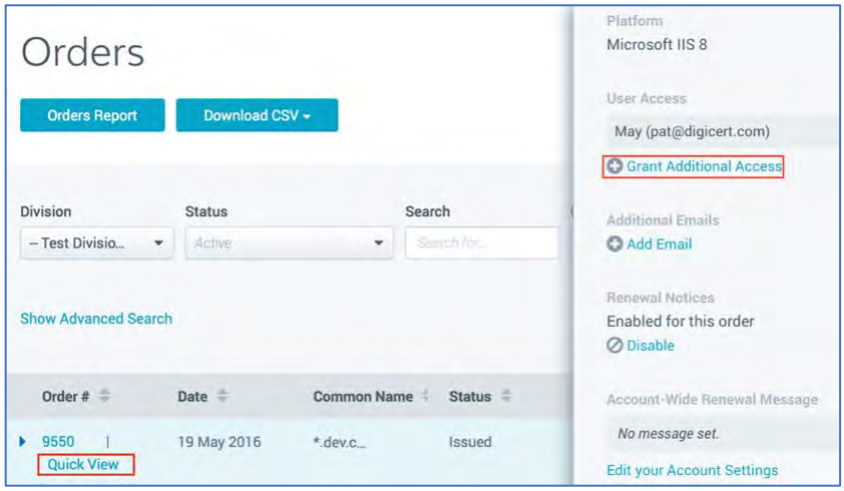
- Grant a Limited User Access to a Certificate Order
  While the certificate order is active, you can add users.
- Grant a Limited User Access to a Certificate (Pending Order)
  You can only add users while the certificate request is pending.

Grant a Limited User Access to a Certificate Order

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



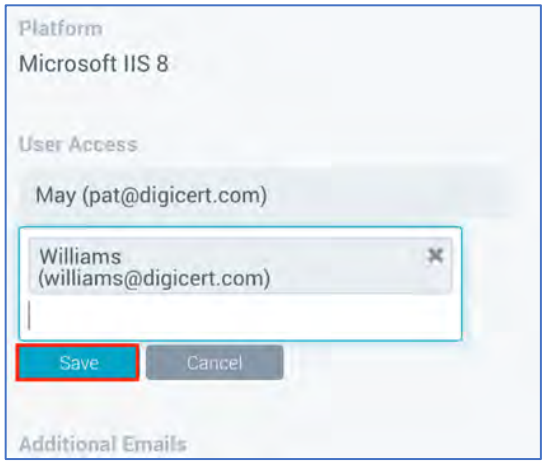
2. On the **Orders** page, use the drop-down lists, search box, and column headers and advanced search features to find the order that you need to grant the limited user access to.



3. In the **Order #** column, click the **Quick View** link of the certificate order to which you want to add additional user access.

4. In the **Order #** details pane, in the **Order Details** section under **User Access**, click the **Grant Additional Access** link.

5. In the drop-down list, select the limited users you want to be able access to the certificate order.



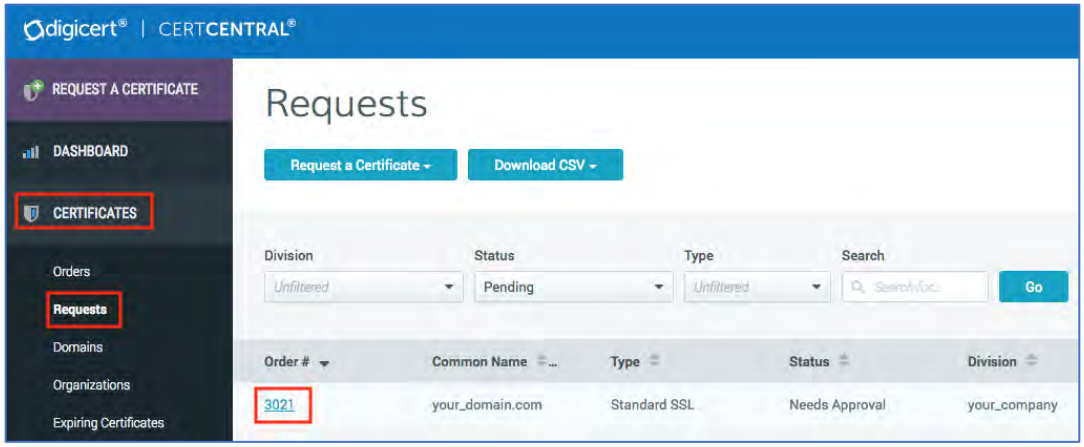
6. Click **Save**.

7. You can remove a limited user's access to a certificate order at any time by removing their name from the **User Access** box.

Grant a Limited User Access to a Certificate Request (Pending Order)

Once the order has been issued, the limited user will have permission to access the certificate order, allowing them to download the certificate, renew the certificate, and to perform other certificate related actions.

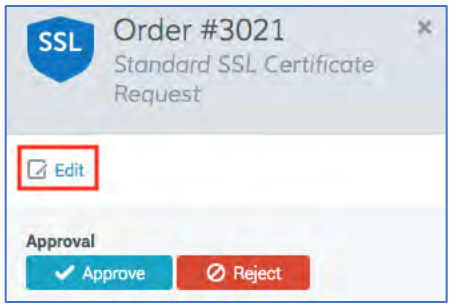
1. In your CertCentral account, in the sidebar menu, click **Certificates > Request**.



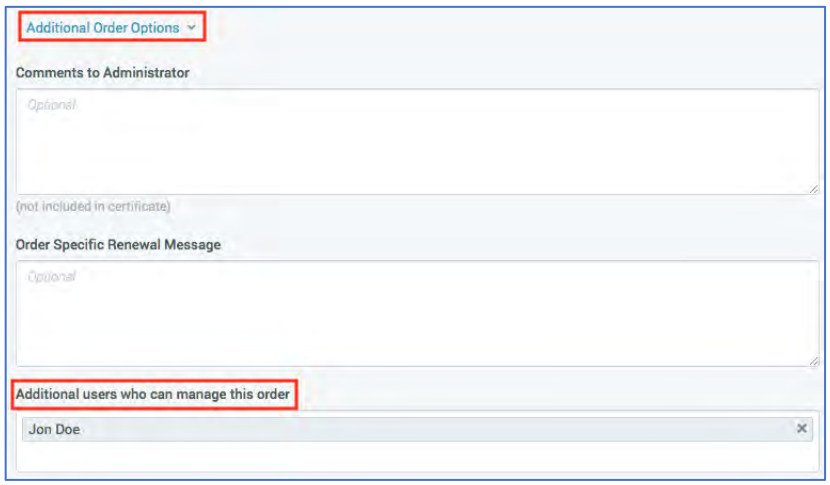
2. On the **Requests** page, use the drop-down lists, search box, and column headers and advanced search features to find the request that you need to grant the limited user access to.

3. In the **Order #** column, click the **order number** link of the certificate request you want to add additional user access to.

4. In the **Order number** details pane, click the **Edit** link.



5. On the **Edit Request** page, expand **Additional Order Options**.



6. Click in the **Additional users who can manage order** box and select the limited users that need access to manage the certificate order.
7. Under **Certificate Services Agreement**, read through the agreement and then check **I agree to the Certificate Services Agreement above**.

8. Click **Update Certificate Request**.
9. Before the certificate is issued, you can remove a limited user's access to a certificate request at any time by removing their name from the **Additional users who can manage order** box.

8 Accessing Your Secure Site Certificate Benefits

All Secure Site certificates come with these benefits:

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

How to access your priority validation, priority support, and site seals

To access your Secure Site certificate's priority validation, priority support, and site seals, you need to log in to your CertCentral account.

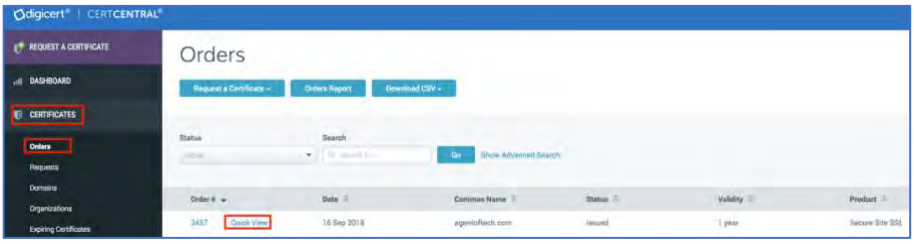
8.1 Accessing Your Secure Site Certificate's Priority Support

Use these instructions to access priority support for your Secure Site TLS/SSL certificate order.

All Secure Site Certificates include access to priority support: certificate pre-issuance support and certificate post issuance support.

Priority support is tied to your Secure Site certificate order (pending and issued). You can only access that support from your certificate's order page.

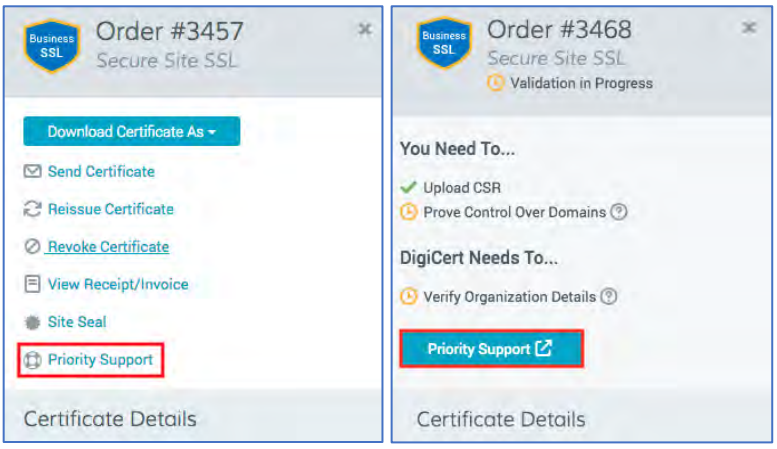
1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



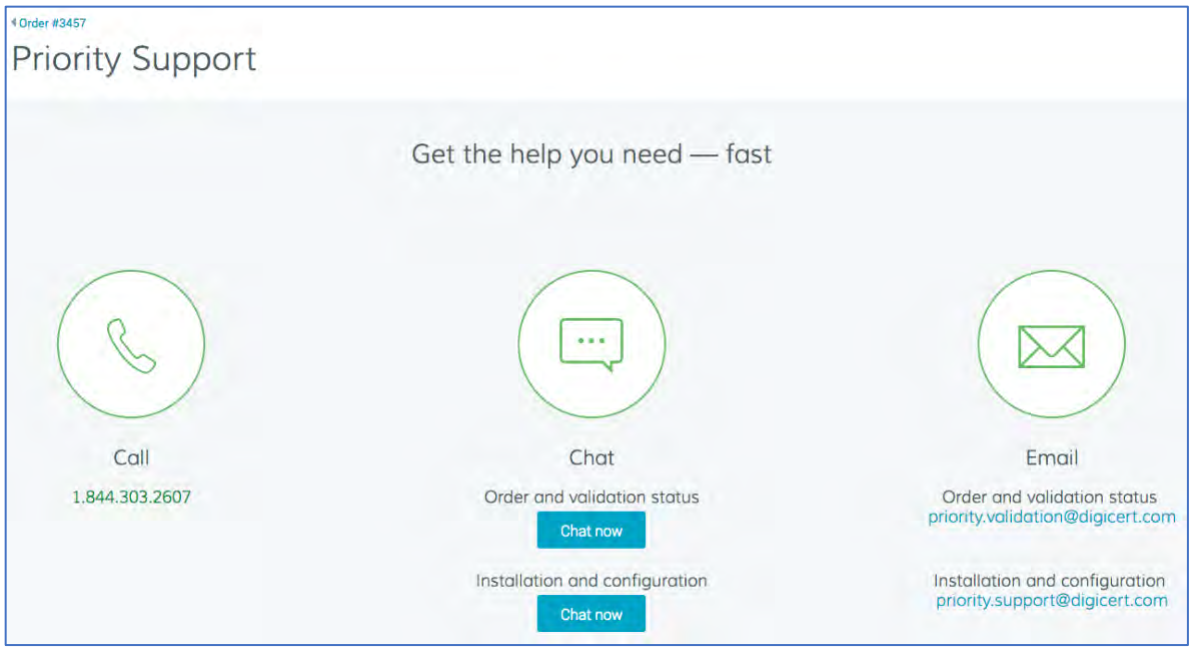
2. On the **Orders** page, use the filters and advanced search features to locate the Secure Site certificate order.

3. In the **Order #** column, click the **Quick View** link for the Secure Site certificate.

4. In the **Order** details pane (on the right), click **Priority Support**.



5. On the **Priority Support** page, use the priority support phone, email, or chat contact methods.



8.2 Accessing Your Secure Site Certificate's Site Seal

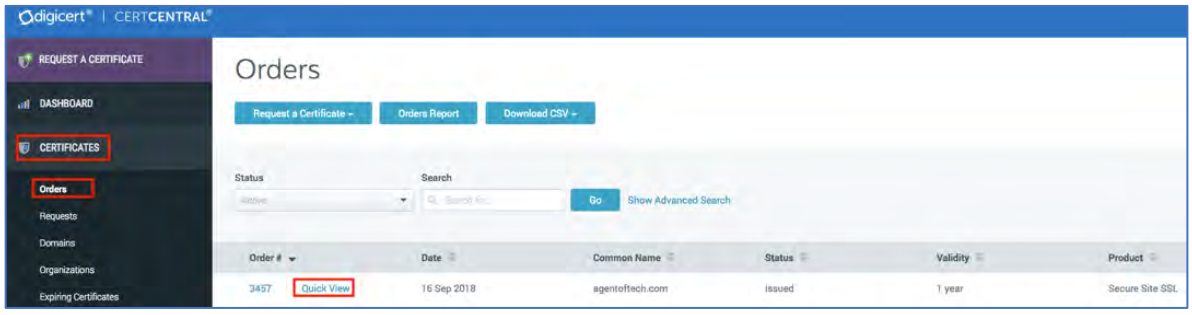
Use these instructions to access the site seal for your Secure Site TLS/SSL certificate order.

- For more answers to some of the frequently asked questions about site seals, see Site Seal FAQ.
- For site seal installation instructions, see Install Your Site Seal.

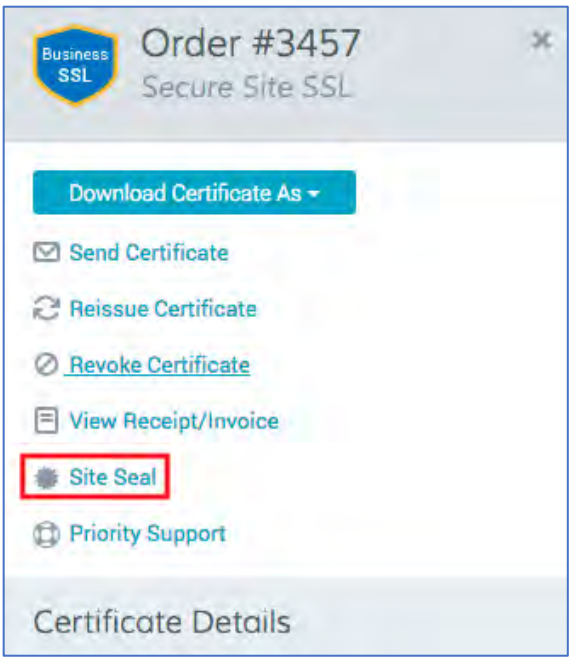
All Secure Site Certificates include access to the two most recognized trust marks on the web: DigiCert and Norton Secured. Pick the premium site seal you want to use to display proof of trust on your site.

Your site seal is tied to your issued Secure Site certificate order. You can only access the seals from your "issued" certificate's order 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 Secure Site certificate order.
3. In the **Order #** column, click the **Quick View** link for the Secure Site certificate.
4. In the **Order** details pane (on the right), click **Site Seal**.



5. On **Site Seal** page, use the various options (which seal, size, color text, and language) to get the site seal you want.

    a. Site Seals

    b. Sizes

    DigiCert:

    - small – 80 x 47 px
    - standard – 100 x 59 px
    - large – 130 x 76 px

    c. Norton:

    - small – 110 x 63 px
    - standard – 133 x 78 px
    - large – 177 x 98 px

    d. Text color

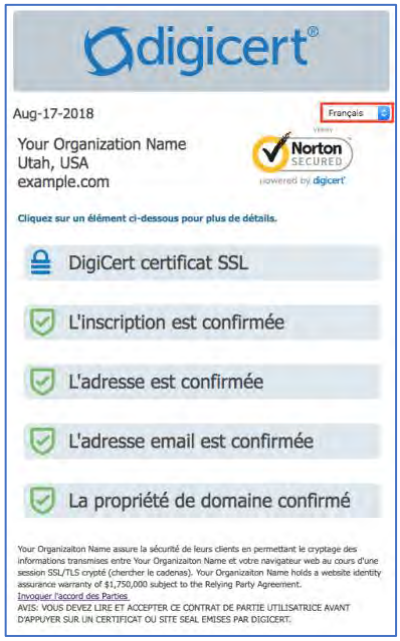
    - White – Affected text: "SSL Certificates" (below the seal image)

- Black – Affected text: "SSL Certificates" (below the seal image)

e. Languages

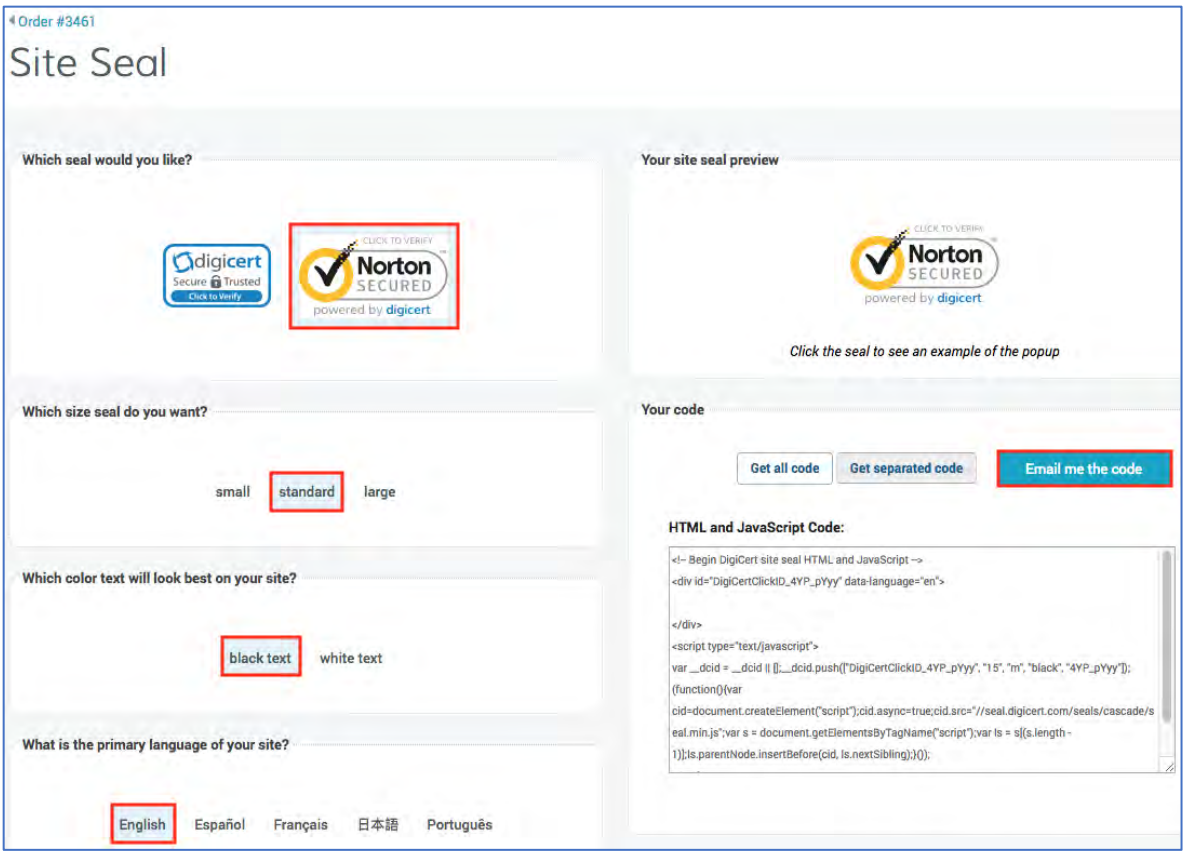
- English (default language)
- French
- Japanese
- Portuguese
- Spanish

6. To see what the site seal popup looks like, click on the site seal.



7. Then, use the **Email me the code** option to email the site seal code to those involved in putting the site seal on your website.

Note: When you email the code, all code is sent to the recipients.



9 Automatic Certificate Renewal

During the certificate order process, you have the option to automatically renew an SSL, client, grid, or standard code signing certificate 30 days before it expires. If you change your mind, after the certificate has been issued, you can open the **Order #** details pane and turn automatic renewal On or Off for a certificate.

9.1 Turning on Automatic Renewals for a Certificate

You can turn on automatic certificate renewals for these types of certificates:

- TLS/SSL (Basic and Business)
- Standard Code Signing
- Client
- Private SSL
- Grid

Once the feature has been turned on, 30 days before the certificate expires, it will be automatically renewed.

Exceptions:

EV code signing and document signing certificates do not support automatic renewals. The auto-renew feature is also disabled for certificate orders that were paid for with a credit card.

9.1.1 SSL Certificate: How to Turn on Automatic Renewals

Use these instructions to turn on automatic renewals for Business TLS/SSL, Basic TLS/SSL, Private SSL, and Grid Host SSL Certificates.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the SSL certificate that needs to be automatically renewed.
3. In the **Order #** column, click the **Quick View** link of the SSL certificate.
4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Auto-Renew**, check the box.
5. The **Auto-Renew** option should now be on.

   Each time the certificate reaches the 30 days before it expires mark, it will be automatically renewed.

9.1.2 Client Certificate: How to Turn on Automatic Renewals

Use these instructions to turn on automatic renewals for Client and Grid Host Client Certificates.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the client certificate that needs to be automatically renewed.
3. In the **Order #** order column, click the **Quick View** link of the client certificate.
4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Auto-Renew**, in the **Auto-Renew** drop-down list select how many times you want the client certificate to be automatically renewed (1 – 99).

   Each time the certificate reaches the 30 days before it expires mark, it will be automatically renewed. Depending on how often you set the certificate to renew, it could renew only once or up to 99 times.

9.1.3 Code Signing Certificate: How to Turn on Automatic Renewals

Use these instructions to turn on automatic renewals for Standard Code Signing Certificates only.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the code signing certificate that needs to be automatically renewed.
3. In the **Order #** order column, click the **Quick View** link of the code signing certificate.

4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Auto-Renew**, check the box.

5. The **Auto-Renew** option should now be on.

   Each time the certificate reaches the 30 days before it expires mark, it will be automatically renewed.

9.2 Turning Off Automatic Renewals for a Certificate

You can turn off automatic certificate renewals for the following types of certificates:

- SSL (Business and Basic)
- Standard code signing
- Client
- Private SSL
- Grid

Once the feature has been turned off, the certificate will not be automatically renewed.

9.2.1 SSL Certificate: How to Turn Off Automatic Renewals

Use these instructions to turn off automatic renewals for Business TLS/SSL, Basic TLS/SSL, Private SSL, and Grid Host SSL certificates.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.

2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the SSL certificate that needs to have automatically renewals turned off.

3. In the **Order #** order column, click the **Quick View** link of the TLS/SSL certificate.

4. In the **Order #** details pane (on the right), in the **Other Information** section, under **Auto-Renew**, uncheck the box.

5. The **Auto-Renew** option should now be off.

   The certificate will not be automatically renewed.

9.2.2 Client Certificate: How to Turn Off Automatic Renewals

Use these instructions to turn off automatic renewals for Client and Grid Host Client certificates.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.

2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the client certificate that needs to have automatically renewals turned off.

3. In the **Order #** column, click the **Quick View** link of the client certificate.

4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Auto-Renew**, in the **Auto-Renew** drop-down list select **Don't automatically renew**.

   The certificate will not be automatically renewed.

9.2.3 Code Signing Certificate: How to Turn Off Automatic Renewals

Use these instructions to turn off automatic renewals for standard code signing certificates only.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the code signing certificate that needs to have automatically renewals turned off.
3. In the **Order #** column, click the **Quick View** link of the code signing certificate.
4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Auto-Renew**, uncheck the box.
5. The **Auto-Renew** option should now be off.

   The certificate will not be automatically renewed.

10 Individual Certificate Renewal Notifications

In your CertCentral account, you can control renewal notices per certificate order. For example, if a certificate is only needed for a one time use and there are no plans to renew it, you can disable renewal notices for that certificate order. If something changes and that certificate order needs to be renewed, you can enable renewal notices so that you don't forget to renew it before it expires.

10.1 How to Turn Off Renewal Notifications for a Certificate Order

Use these instructions to turn off renewal notifications for a certificate order.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the certificate that needs to have renewal notices turned off (disabled).
3. In the **Order #** column, click the **Quick View** link for the certificate.
4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Renewal Notices**, click **Disable**.

   Caution: Once renewal notices are disabled, you will not be notified before, when, or after this certificate order expires.

5. Under **Renewal Notices**, it should now read ***Disabled for this order***.

   Renewal notices *will not be sent* for this certificate order.

10.2 How to Turn on Renewal Notifications for a Certificate Order

Use these instructions to turn on renewal notifications for a certificate order.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, and column headers to locate the certificate that needs to have renewal notices turned on (enabled).
3. In the **Order #** column, click the **Quick View** link for the certificate.
4. In the **Order #** details pane (on the right), in the **Order Details** section, under **Renewal Notices**, click **Enable**.
5. Under **Renewal Notices**, it should now read ***Enabled for this order***.

   Renewal notices *will now be sent* for this certificate order.

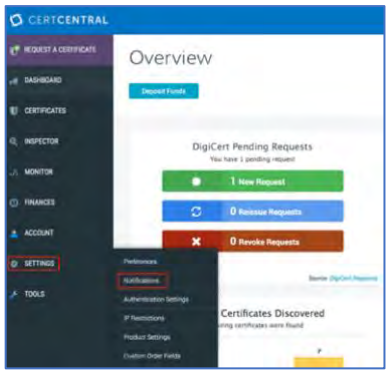
11 Account Notifications

Before emails are sent out from the account, you may want to assign an email account to receive a copy of all emails sent out from the account (e.g., approval notifications). You may also want to configure when you receive renewal notifications and add a default renewal message that can be includes on all your renewal notifications.

11.1 How to Set Up Your Email Notification Accounts

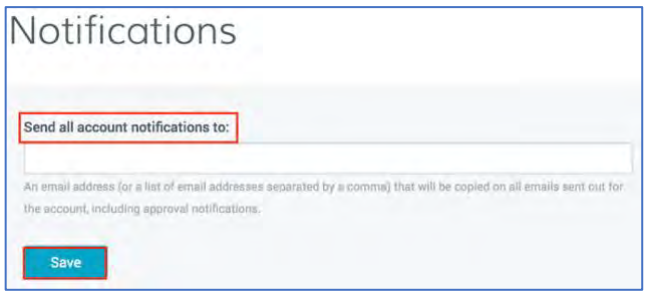
Use these instructions to set up your CertCentral account email notifications. Before emails are sent out from the account, you may want to assign an email account to receive a copy of all emails sent out from the account (e.g., approval notifications).

1. In your CertCentral account, in the sidebar menu, click **Settings > Notifications**.



2. On the **Notifications** page, in the **Send all account notifications to** box, add the email addresses that you want copied on all emails sent from your account.

   Note: If you are setting up multiple notification accounts, use commas to separate the email addresses.



3. When you are finished, click **Save**.

   You have successfully set up your account email notification account.

11.2 Certificate Renewal Notifications

After DigiCert has issued your first certificate, you need to configure your **Certificate Renewal Settings**, such as when renewal notifications are sent and to whom notifications are sent, to help prevent unexpected certificate expirations.

11.2.1 Certificate Renewal Settings

When configuring your certificate renewal settings, you have two options from which to choose:

- **Non-Escalation Certificate Renewals**

  The first option is to send all renewal notifications to the same email addresses at every stage as certificates gets closer to expiring or after they have expired.

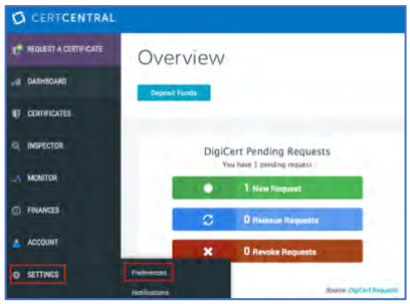
- **Escalation Certificate Renewals**

  The second option is to configure email escalation settings where you determine which email addresses will receive which renewal notifications at each stage as certificates get closer to expiring or after they have expired.

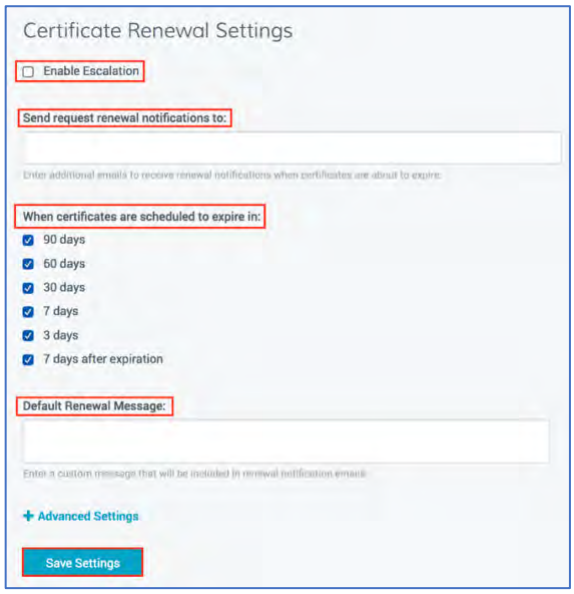
11.2.2 How to Configure Non-Escalation Renewal Notifications

Use the steps below to send all renewal notifications to the same email addresses at every stage as certificates gets closer to expiring or after they have expired.

1. In your CertCentral Account in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, scroll down the page and in the **Certificate Renewal Settings** section, uncheck **Enable Escalation**.



3. In the **Send request renewal notifications to** box, enter the email addresses for the people who you want to receive the renewal notifications (comma separated).

4. Under **When certificates are scheduled to expire in**, check the boxes for when you want renewal notices to be sent.

   These options determine when email notifications are sent. For example, if you only check **30 days**, **7 days**, and **3 days**, no email notifications will be sent **90 days** or **60 days** before certificates expire, or **7 days** after certificates have expired.

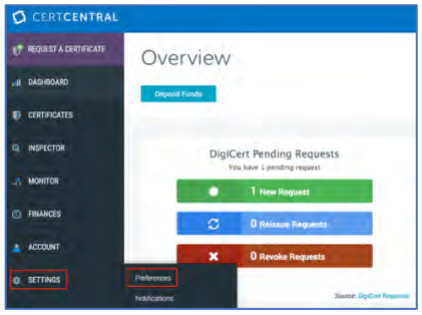
5. In the **Default Renewal Message** box, type an optional renewal message that can be included in all your renewal notification emails.

6. When you are finished, click **Save Settings**.

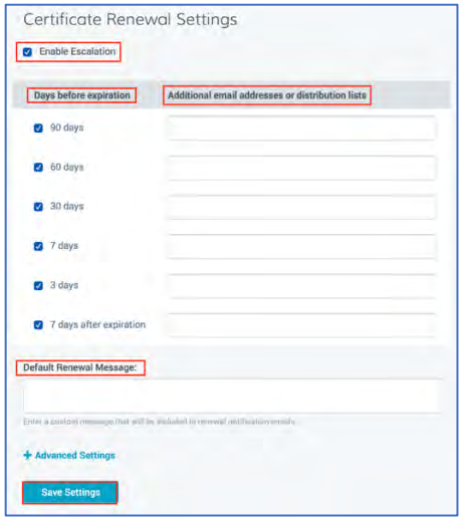
11.2.3 How to Configure Escalation Renewal Notifications

Use the steps below to configure email escalation settings where you determine which email addresses will receive which renewal notifications at each stage as certificates get closer to expiring or after they have expired.

1. In your CertCentral account, in the sidebar menu, click **Settings > Preferences**.



2. On the **Division Preferences** page, scroll down the page and in the **Certificate Renewal Settings** section, check **Enable Escalation**.



3. Under **Days before expiration**, check the boxes for when you want renewal notices to be sent.
4. Under **Additional email addresses or distribution lists**, enter the email addresses for the people you want to receive each renewal notification (comma separated).
5. In the **Default Renewal Message** box, type an optional renewal message that can be included in all your renewal notification emails.
6. When you are finished, click **Save Settings**

12 Managing Funds

To find out about available pricing options, please contact your Account Representative. Their number is listed in your CertCentral account in the **CertCentral** banner.

12.1 Managing Credit Cards

In your CertCentral account, on the **Credit Cards** page (**Finances > Credit Cards**), you can add and manage all credit cards for your account. You can also add a credit card from the **Deposit Funds** page (**Finances > Deposit Funds**) and any of the **Request Certificate** pages.

Each account User (*Administrator, Manager, Finance Manager, User*) can only see and manage the credit cards which they have added themselves on the **Credit Cards** page, the **Request Certificate** pages, and the **Deposit Funds** page (for those who have permissions to access this page).

12.1.1 Credit Management Features

Credit Card Storage

DigiCert's gateway (PCI compliant and maintains strong security standards) stores the credit card information. DigiCert only stores what is needed to reference the correct credit card with our payment gateway provider. DigiCert stores the following credit card information on our servers:

- Last 4 digits of the credit card
- Cardholder name
- Cardholder address
- Card expiration date
- Unique profile ID to assist with referencing the credit card to a specific user

Default Credit Card

When you add the first credit card to your account, it automatically becomes your default account credit card. As you add additional credit cards, you have the option to set a different card as the default account credit card at any time.

Same as Billing Contact for This Account

Users (*Administrators, Finance Managers, Managers, and Users*) have the option to use the account's billing contact information (name and address) when adding credit cards.

Card Name

When adding or editing credit card information, you can name the credit card (i.e., *IT Credit Card*, *Sales Credit Card*, *etc.*). If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*).

One Time Credit Card Use

When using a new credit card to deposit funds or request a certificate, you do not have to save the credit card information to your account. If you do not save the card, the next time you want to use that card to request a certificate or you deposit funds, you will need to reenter that card's information.

Deactivating Credit Cards

If you no longer want a credit card to be available for depositing funds or for requesting certificates, you can deactivate it. Note that you cannot delete a credit card once it has been saved to your account; you can only deactivate it.

Once a credit card is deactivated the following things happen:

- The card is tagged as **Inactive** and cannot be used for any further transactions.
- The card cannot be reactivated. To use the card again, you will need to add it as a new card.
- On the **Credit Cards** page, the card is now listed as **Inactive**.
- If you deactivate the default credit card, you must select a different card to use as your default credit card.

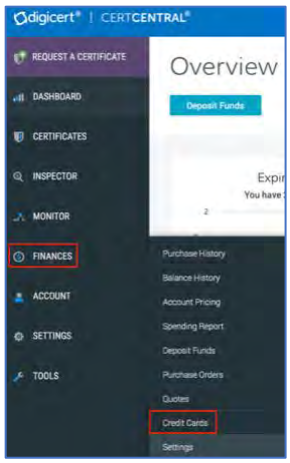
No Automatic Renewals

If you purchase a certificate with a credit card during the certificate request process, you lose the ability to automatically renew that certificate. To enable automatic renewals, you must use contract terms to pay for the certificate or you must bill it to account balance.

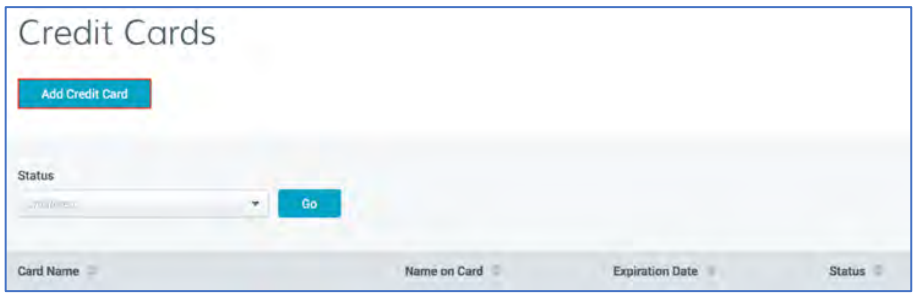
12.1.2 (Admins and Managers) How to Add a Credit Card to Your Account

If you are an Administrators, Finance Managers, and Managers, use these instructions to add a credit card to your account. These roles have permissions to access their account's **Finances** menu.

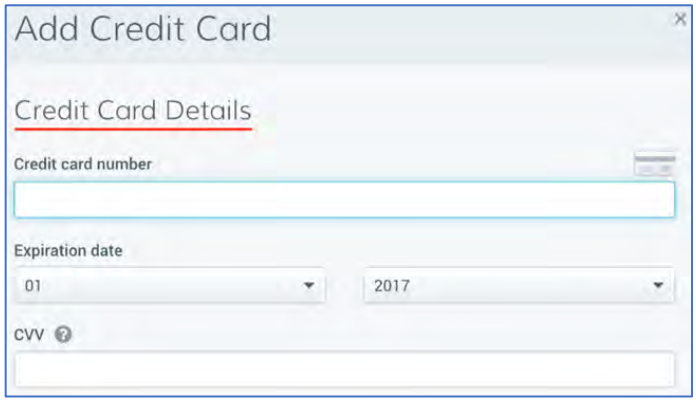
1. In your CertCentral account, in the sidebar menu, click **Finances > Credit Cards**.



2. On the **Credit Cards** page, click **Add Credit Card**.

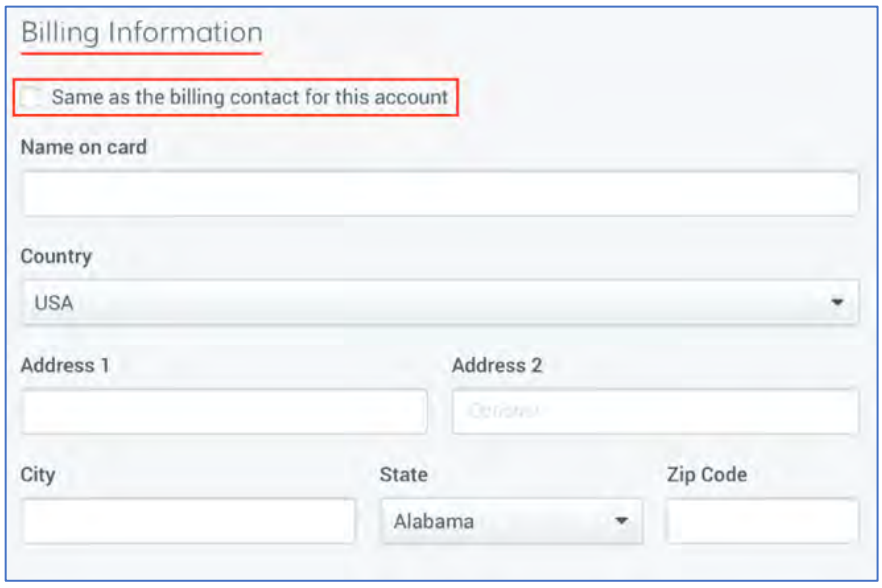


3. In the **Add Credit Card** window, under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



4. Under **Billing information**, do one of the following:

Use account's billing contact information	To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.
Add your billing information	Type your billing information (i.e., *Name on card, country, etc.*).

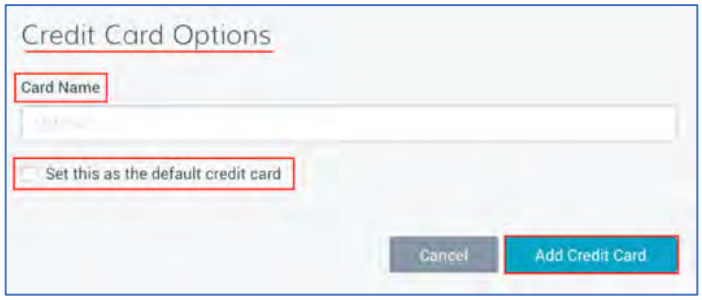


5. Under **Credit Card Options**, do any or none of the following:

Card Name	(Optional) Type a name for the credit card that will be helpful when using or identifying the card (i.e., *EV SSL Certificate orders*).

Note: If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*).

Set this as the default credit card	Check this box if you want to use this credit card as the default credit card for your count. **Note:** This option does not appear when adding your first credit card. The first credit card added to your account is automatically set as the default credit card.

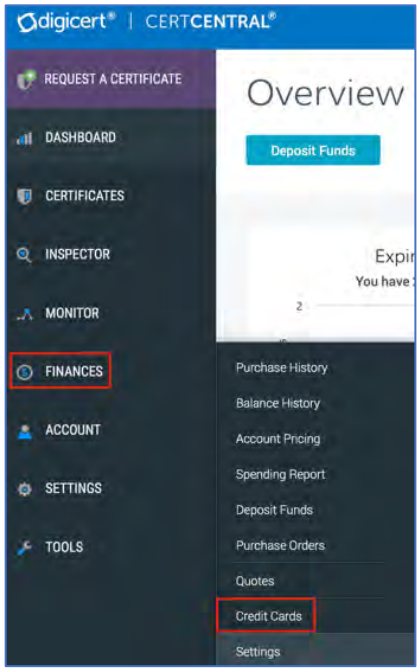


6. When you are done, click **Add Credit Card**.

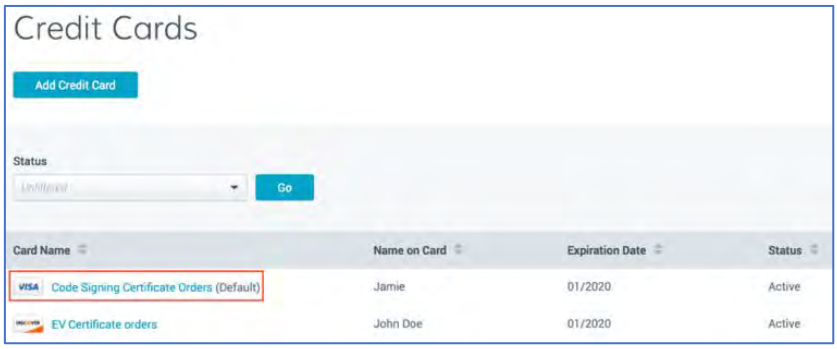
12.1.3 (Admins and Managers) How to Deactivate a Credit Card

If you are an Administrators, Finance Managers, and Managers, use these instructions to deactivate a credit card in your account. These roles have permissions to access their account's **Finances** menu.

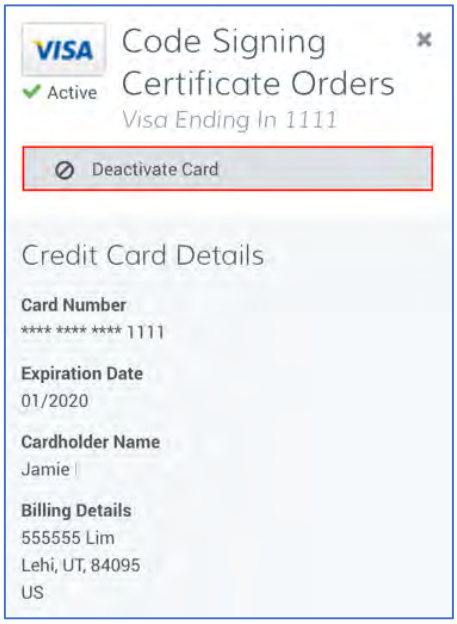
1. In your CertCentral account, in the sidebar menu, click **Finances > Credit Cards**.



2. On the **Credit Cards** page, use the **Status** filter and column headers (i.e., *Expiration Date*) to locate the credit card you want to deactivate, and then click the **Card Name** (e.g., *Code Signing Certificate Orders*).

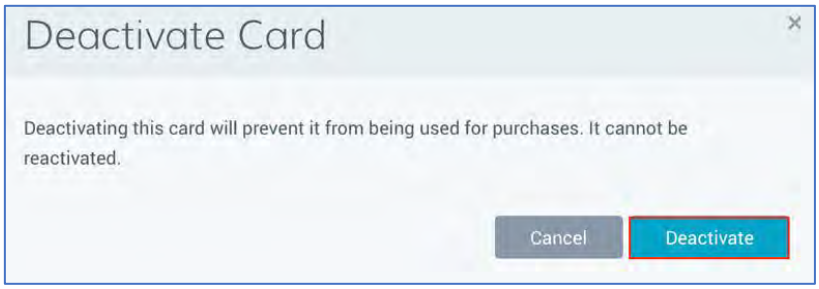


3. In the **Credit Card** details pane (on the right), click **Deactivate Card**.



4. In the **Deactivate Card** window, under ***Deactivating this card will prevent it from being used for purchases. It cannot be reactivated***, click **Deactivate**.

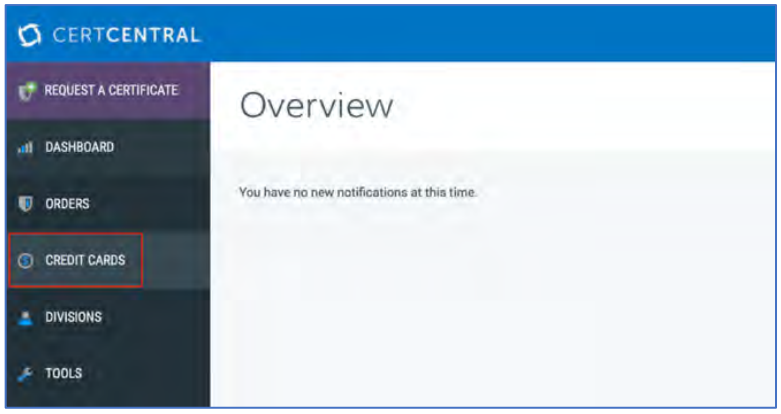
   Note: Once you deactivate a credit card, you cannot reactivate it. To use that credit card again, you must re-add it to your account.



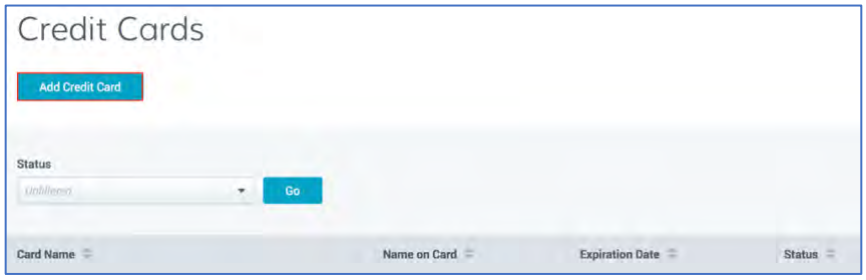
12.1.4(Users) How to Add a Credit Card to Your Account

Use these instructions to add a credit card to your account. These instructions are for the User role only. This role does not have permissions to access their account's **Finances** menu. Users can only use credit cards for purchasing certificates.

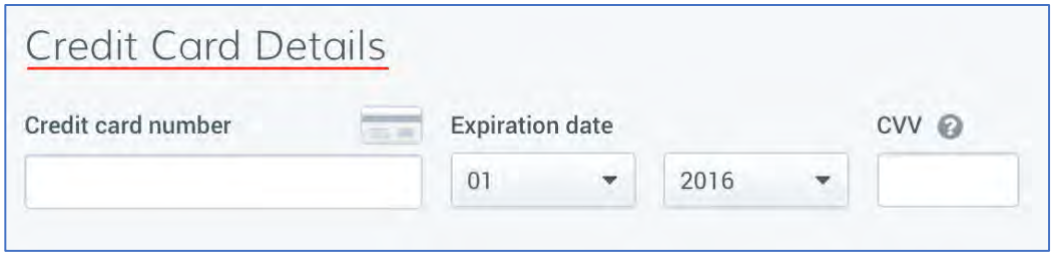
1. In your CertCentral account, in the sidebar menu, click **Credit Cards**.



2. On the **Credit Cards** page, click **Add Credit Card**.



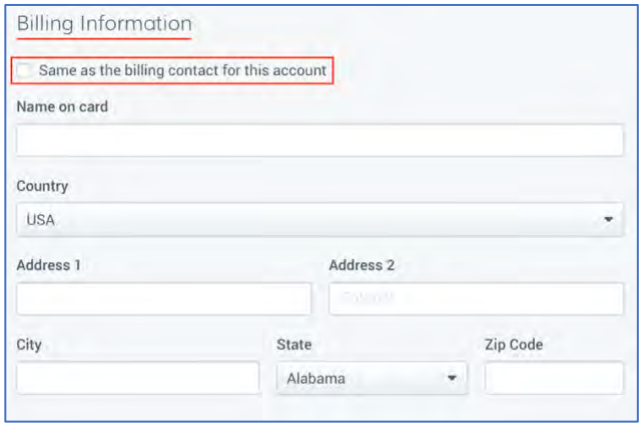
3. In the **Add Credit Card** window, under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



4. Under **Billing information**, do one of the following:

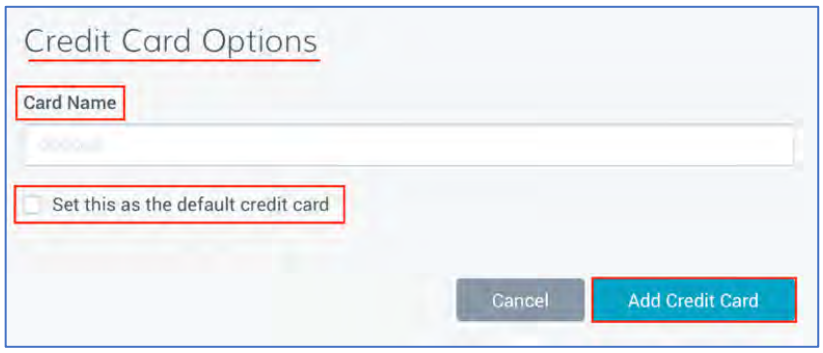
Use account's billing contact information	To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.

Add your billing information	Type your billing information (i.e., *Name on card, Country, etc.*).



5. Under **Credit Card Options**, do any or none of the following:

Card Name	(Optional) Type a name for the credit card that will be helpful when using or identifying the card (i.e., *EV SSL Certificate orders*). **Note:** If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*).
Set this as the default credit card	Check this box if you want to use this credit card as the default credit card for your count. **Note:** This option does not appear when adding your first credit card. The first credit card added to your account is automatically set as the default credit card.

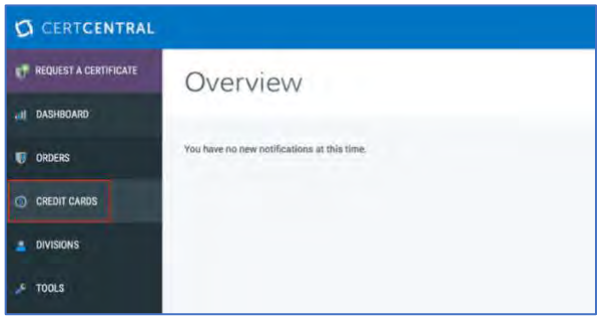


6. When you are done, click **Add Credit Card**.

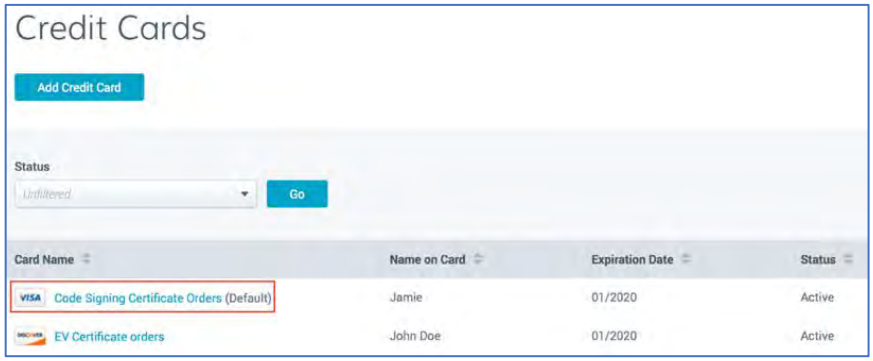
12.1.5 (Users) How to Deactivate a Credit Card

Use these instructions to deactivate a credit card in your account. These instructions are for the User role only. This role does not have permissions to access their account's **Finances** menu.

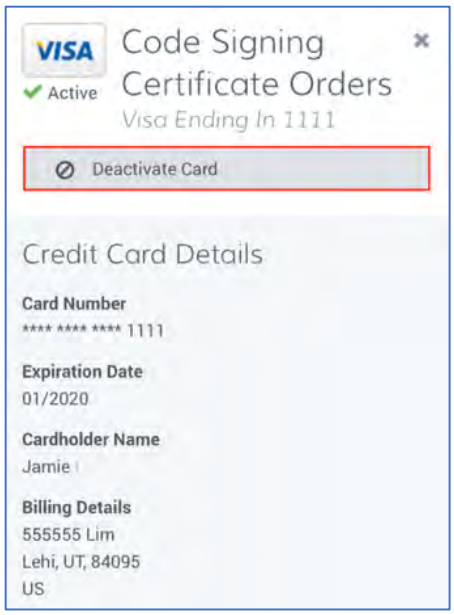
1. In your CertCentral account, in the sidebar menu, click **Credit Cards**.



2. On the **Credit Cards** page, use the **Status** filter and column headers (i.e., *Expiration Date*) to locate the credit card you want to deactivate, and then click the **Card Name** (i.e., *Code Signing Certificate Orders*).

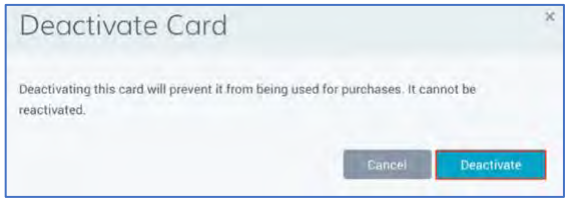


3. In the **Credit Card** details pane (on the right), click **Deactivate Card**.



4. In the Deactivate Card window, under ***Deactivating this card will prevent it from being used for purchases. It cannot be reactivated***, click **Deactivate**.

   Note: Once you deactivate a credit card, you cannot reactivate it. To use that credit card again, you must re-add it to your account.



12.2 (Admins and Managers) How to make a Credit Card Payment

To find out about available pricing options, please contact your Account Representative. Their number is listed in your CertCentral account in the **CertCentral** banner.

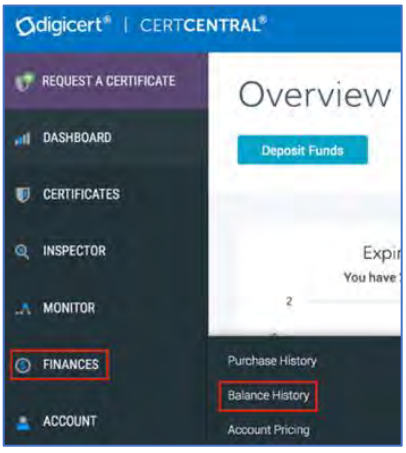
- **Pay Account Balance**: Use this instruction to pay off your account balance.
- **Make a Credit Card Deposit**: Use this instruction to submit funds to your account to cover current and future certificate purchases.

  Note: As soon as DigiCert confirms the details of the deposit, your funds are available to you.

12.2.1 (Admins and Managers) How to Use a Credit Card to Pay Your Account Balance

Use these instructions to pay your account balance with a credit card.

1. In your CertCentral account, in the sidebar menu, click **Finances > Balance History**.

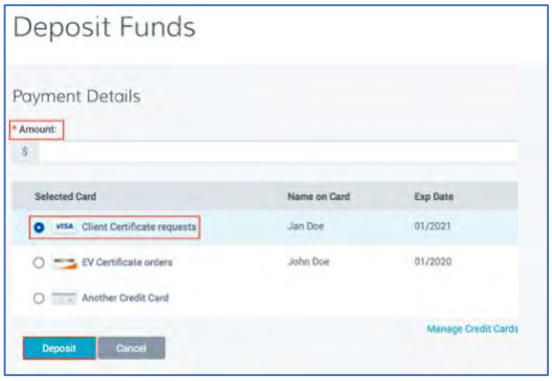


2. On the **Balance History** page, take note of the balance, and then click **Deposit Funds**.

3. On the **Deposit Funds** page, under **Payment Details**, type the **Amount** (account balance) and then do one of the following options:

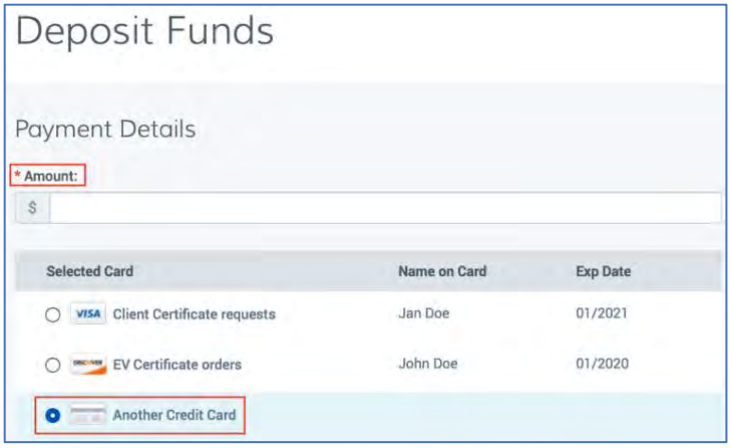
   a. **Use One of the Credit Cards Listed to Pay Account Balance**

      i. Under **Selected Card**, select one of the available credit cards.

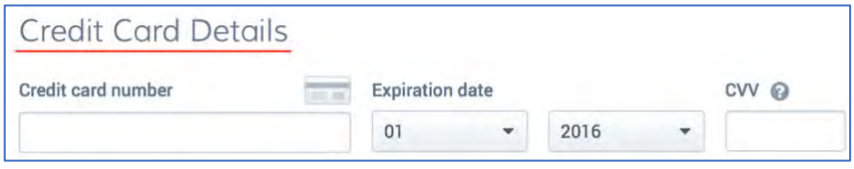


   b. **Add a Different Credit Card to Pay Account Balance**

      i. Under **Selected Card**, select **Another Credit Card**.



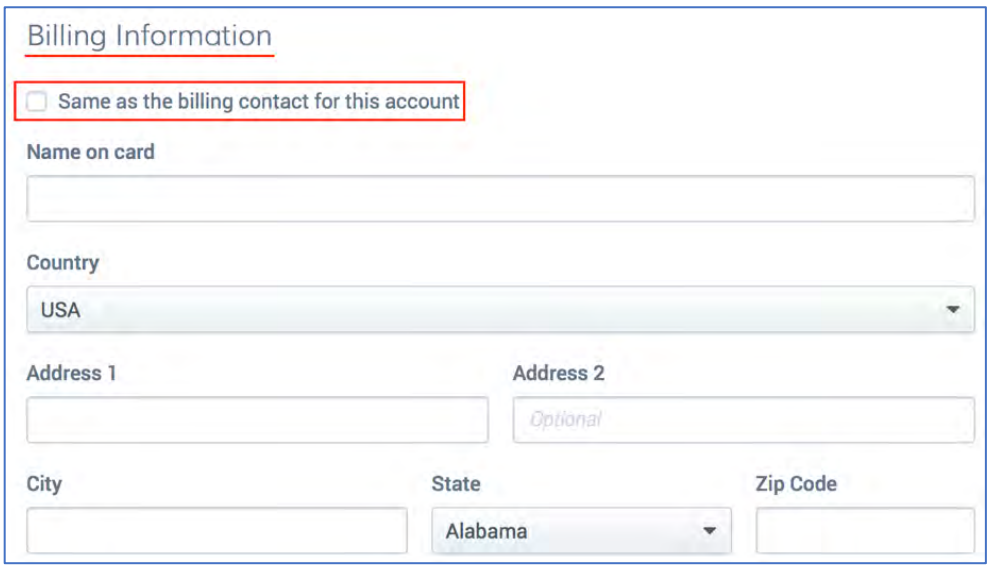
      ii. Under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



      iii. Under **Billing information**, do one of the following:

Use account's billing contact information	To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.

Add your billing information	Type your billing information (i.e., *Name on card, Country, etc.*).

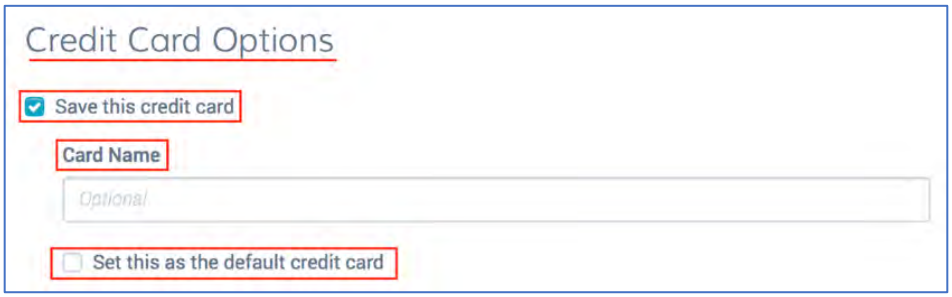


iv. Under **Credit Card Options**, do any or none of the following:

Do Not Save the Credit Card	a) Uncheck **Save this credit card**. b) The credit card will not be added to your account. If you want to use the credit card again, you will need to reenter its information in your account.
Save the Credit Card	a) To Save the Credit Card do 1 or more of the following: b) Check **Save this credit card**. c) (Optional) Under **Card Name**, type a name for the credit card that will be helpful when using or identifying the card (i.e., *Pay Account Balance*). **Note:** If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*). d) (Optional) If you want to use this credit card as the default credit card for your

account, check **Set this as the default credit card**.

Note: This option does not appear when adding your first credit card. The first credit card added to your account is automatically set as the default credit card.



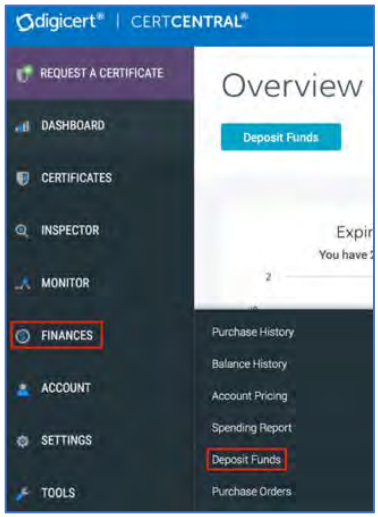
4. When you are finished, click **Deposit**.

   You have successfully submitted a payment to pay off your account balance.

12.2.2 (Admins and Managers) How to Use a Credit Card to Deposit Funds

Use these instructions to deposit funds with a credit card.

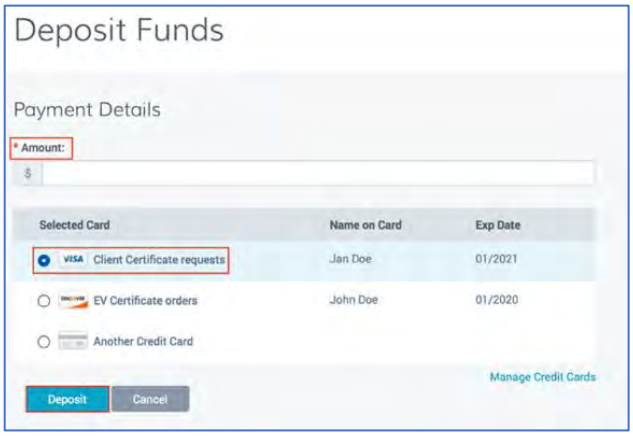
1. In your CertCentral account, in the sidebar menu, click **Finance > Deposit Funds**.



2. On the **Deposit Funds** page, under **Payment Details**, type the **Amount** you want to deposit and then do one of the following options:

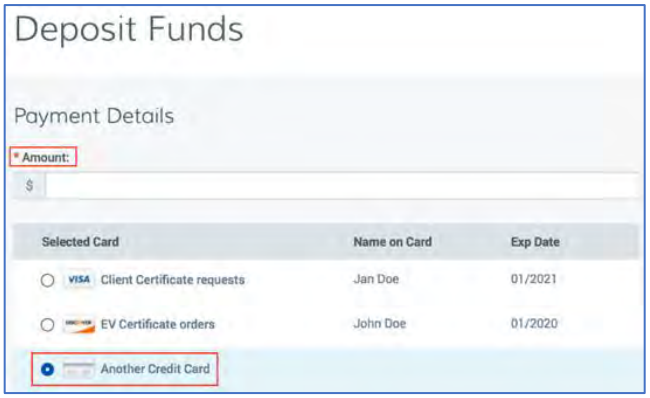
a. **Use One of the Credit Cards Listed to Deposit Funds**

i. Under **Selected Card**, select one of the available credit cards.

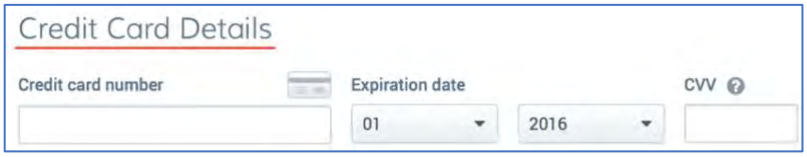


b. **Add a Different Credit Card to Deposit Funds**

i. Under **Selected Card**, select **Another Credit Card**.



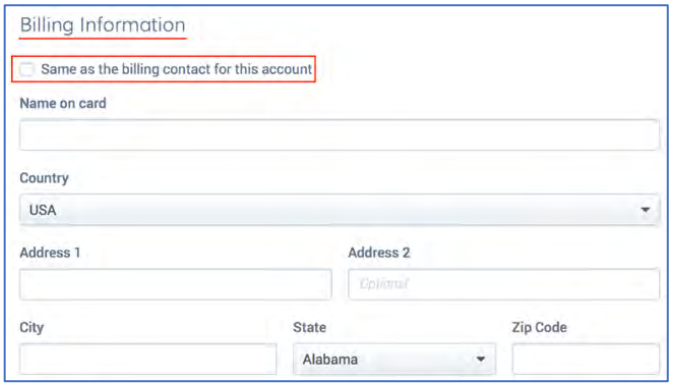
ii. Under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).



iii. Under **Billing information**, do one of the following:

Use account's billing contact information	To use your account's billing contacts information for the credit card, check the **Same as billing contact for this account** box.

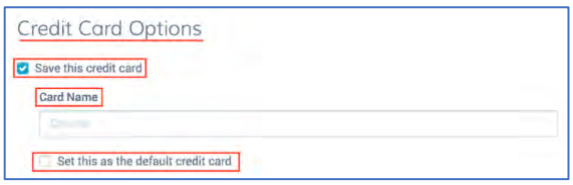
Add your billing information	Type your billing information (i.e., *Name on card, Country, etc.*).



iv. Under **Credit Card Options**, do any or none of the following:

Do Not Save the Credit Card	a) Uncheck **Save this credit card**. b) The credit card will not be added to your account. If you want to use the credit card again, you will need to reenter its information in your account.
Save the Credit Card	To Save the Credit Card do 1 or more of the following: a) Check **Save this credit card**. b) (Optional) Under **Card Name**, type a name for the credit card that will be helpful when using or identifying the card (i.e., *Pay Account Balance*). **Note:** If no name is provided, the card name defaults to the card type and last four digits of the card number (i.e., *AMEX ####*). c) (Optional) If you want to use this credit card as the default credit card for your account, check **Set this as the default credit card**. **Note:** This option does not appear when adding your first credit card. The first credit card added

to your account is automatically set as the default credit card.



3. When you are finished, click **Deposit**.

   You have successfully used your credit card to make an account deposit. As soon as we confirm the details of your deposit, your funds are available to you.

12.3 (Admins and Managers) How to Make a Purchase Order Payment

To find out about available pricing options, please contact your Account Representative. Their number is listed in your CertCentral account in the **CertCentral** banner.

- **Pay Account Balance**

  Use these instructions to pay off your account balance.

- **Make an Account Deposit**

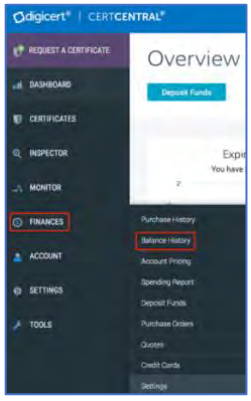
  Use these instructions to submit funds to your account to cover current and future certificate purchases.

  Note: As soon as DigiCert confirms the details of the purchase order, your funds are available to you.

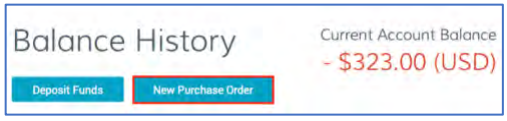
12.3.1 How to Use a Purchase Order to Pay Your Account Balance

Use these instructions to pay your account balance with a purchase order (PO).

1. In your CertCentral account, in the sidebar menu, click **Finances > Balance History**.

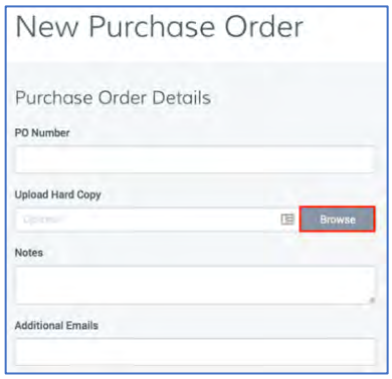


2. On the **Balance History** page, take note of the balance, and then click **New Purchase Order**.



3. On the **New Purchase Order** page, under **Purchase Order Details**, do the following:

PO Number	Type the PO number.
Upload Hard Copy	Click **Browse**, browse for, select, and upload a signed hard copy of your PO. **Note:** You can also email or fax your signed purchase order. Please email it to support@digicert.com or fax it to +1 801-705-0481
Notes	Type any notes applicable to the payment.
Additional Emails	Add the emails or distribution list that you want to be notified when the PO is approved.



4. Next enter the account billing contact information, as follows:

   a. **Use your account's billing contact information**

   To use your account's billing contacts information for the purchase order, select **Use my account billing contact**.

b. **Update your account's billing contact information**

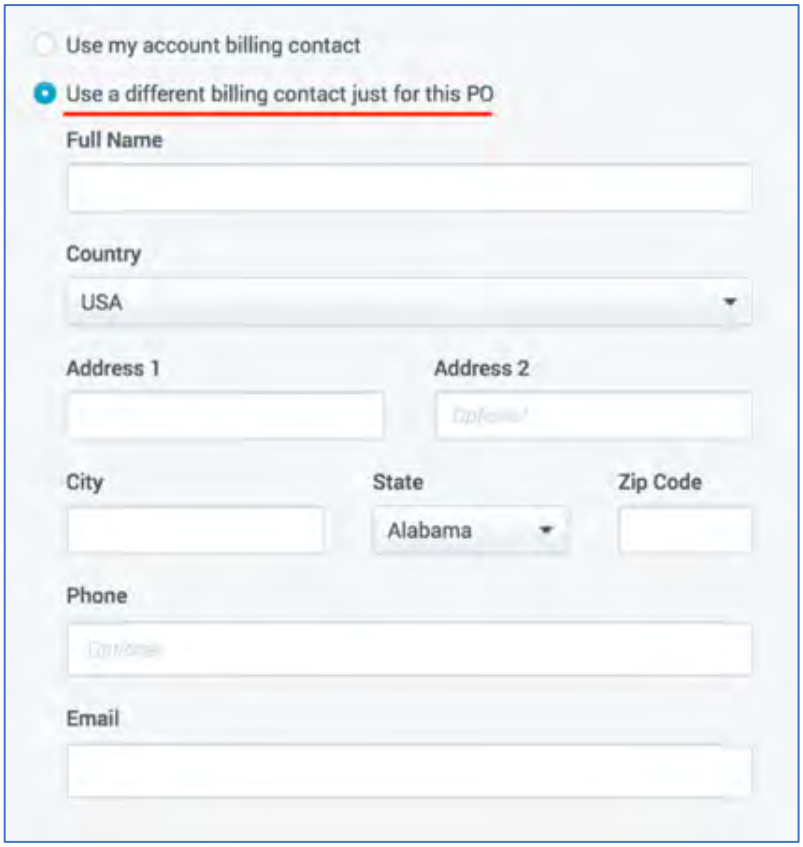
   i. To update the billing contact information, click **Edit Billing Contact**.

   ii. In the **Edit Billing Contact** window, update the contact's information as needed and then click **Update Billing Contact**.

c. **Use a different billing contact**

   i. To use a different billing contact for this PO only, select **Use a different billing contact just for this PO**.

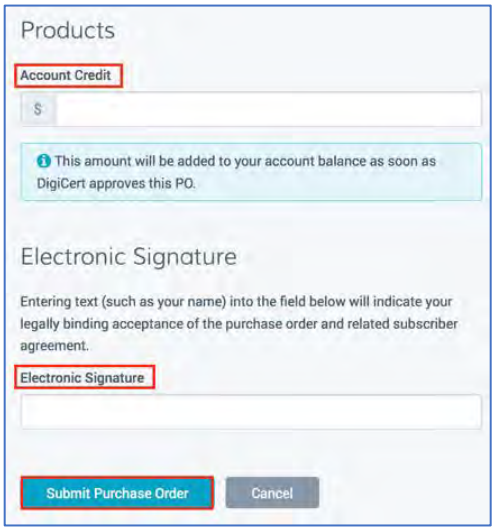
   ii. Enter the contact information for the person to whom you want the invoice sent, making sure that information matches the contact information on the hardcopy of the PO that you are submitting.



5. Under **Products**, do the following:

Account Credit:	In this box, enter the amount needed to pay off the division's account balance.
Electronic Signature:	In this box, enter your signature.

Note: Entering text (such as your name) into the box indicates your legally binding acceptance of the purchase order and related subscriber agreement.



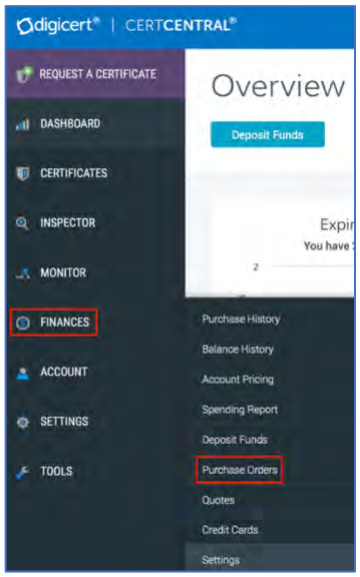
6. When you are finished, click **Submit Purchase Order**.

   You have successfully submitted a purchase order to pay off your account balance. We will send you an invoice with information about payment options.

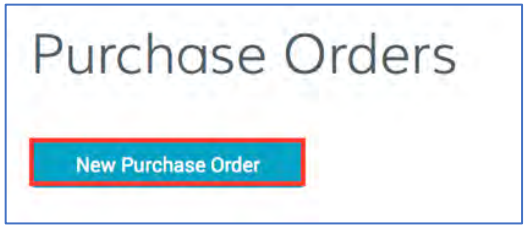
12.3.2 How to Use a Purchase Order to Deposit Funds

Use these instructions to deposit funds with purchase order.

1. In your CertCentral account, in the sidebar menu, click **Finances > Purchase Orders**.

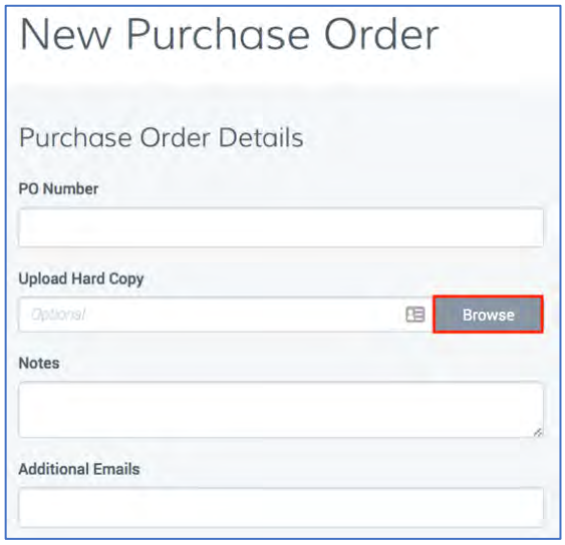


2. On the **Purchase Orders** page, click **New Purchase Order**.



3. On the **New Purchase Order** page, under **Purchase Order Details**, do the following:

PO Number	Type the PO number.
Upload Hard Copy	Click **Browse**, browse for, select, and upload a signed hard copy of your PO. **Note:** You can also email or fax your signed purchase order. Please email it to support@digicert.com or fax it to +1 801-705-0481
Notes	Type any notes applicable to the payment.
Additional Emails	Add the emails or distribution list that you want to be notified when the PO is approved.



4. Next enter the account billing contact information, as follows:

    a. **Use your account's billing contact information**

    To use your account's billing contacts information for the purchase order, select **Use my account billing contact**.

b. **Update your account's billing contact information**

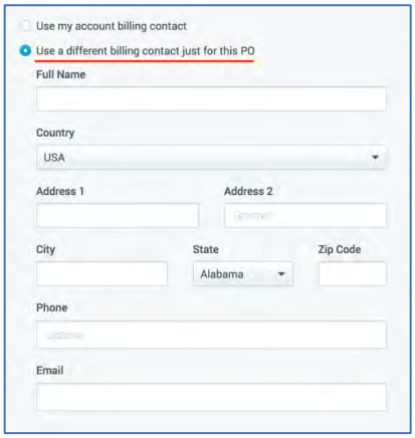
   i. To update the billing contact information, click **Edit Billing Contact**.

   ii. In the **Edit Billing Contact** window, update the contact's information as needed and then click **Update Billing Contact**.

c. **Use a different billing contact**

   i. To use a different billing contact for this PO only, select **Use a different billing contact just for this PO**.

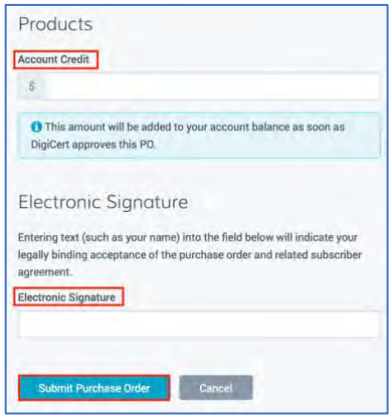
   ii. Enter the contact information for the person to whom you want the invoice sent, making sure that information matches the contact information on the hardcopy of the PO that you are submitting.



5. Under **Products**, do the following:

Account Credit:	In this box, enter the amount that you want to deposit into your division's account.
Electronic Signature:	In this box, enter your signature.

Note: Entering text (such as your name) into the box indicates your legally binding acceptance of the purchase order and related subscriber agreement.



6. When you are finished, click **Submit Purchase Order**.

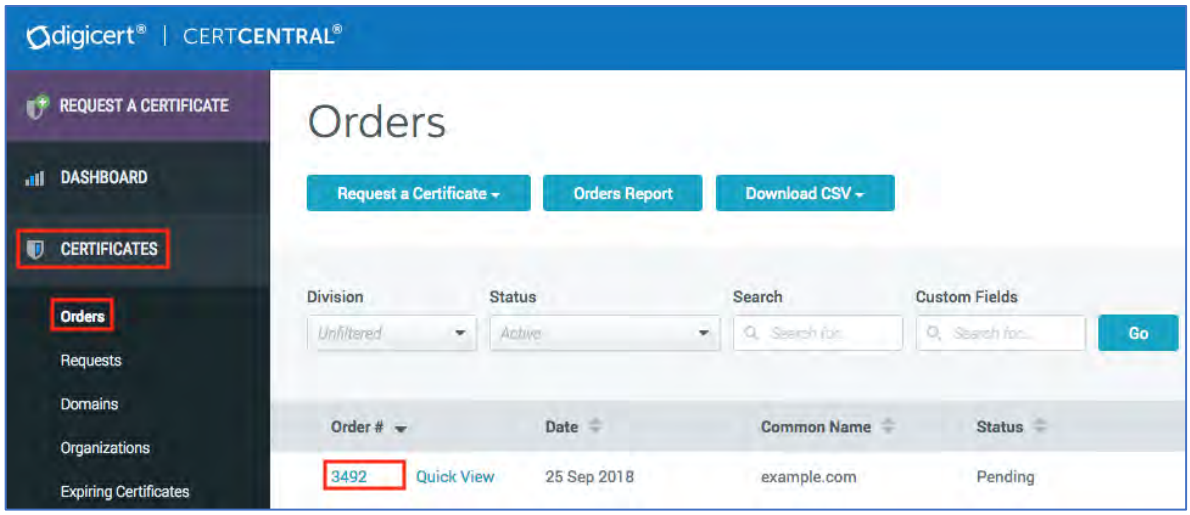
   You have successfully submitted a purchase order to make an account deposit. We will send you an invoice with information about payment options.

12.4 How to View the Receipt/Invoice for a Certificate Order

12.4.1 How to View the Receipt/Invoice for a Pending Certificate Order

Use these instructions to see the credit card receipt for a pending certificate order.

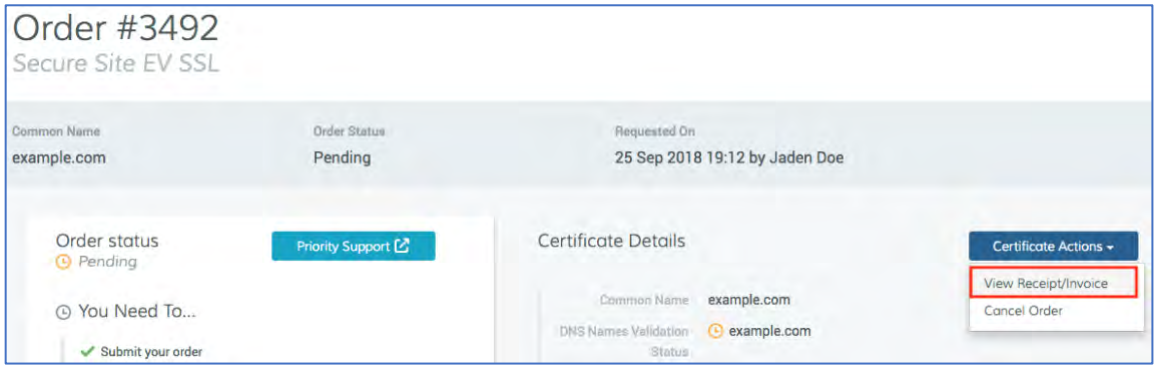
1. In your CertCentral account, in the sidebar menu, click **Certificate > Orders**.



2. On the **Orders** page, use the filters and advanced search features to locate the issued certificate order.

3. In the **Order #** column of the certificate, click the **Order number** link.

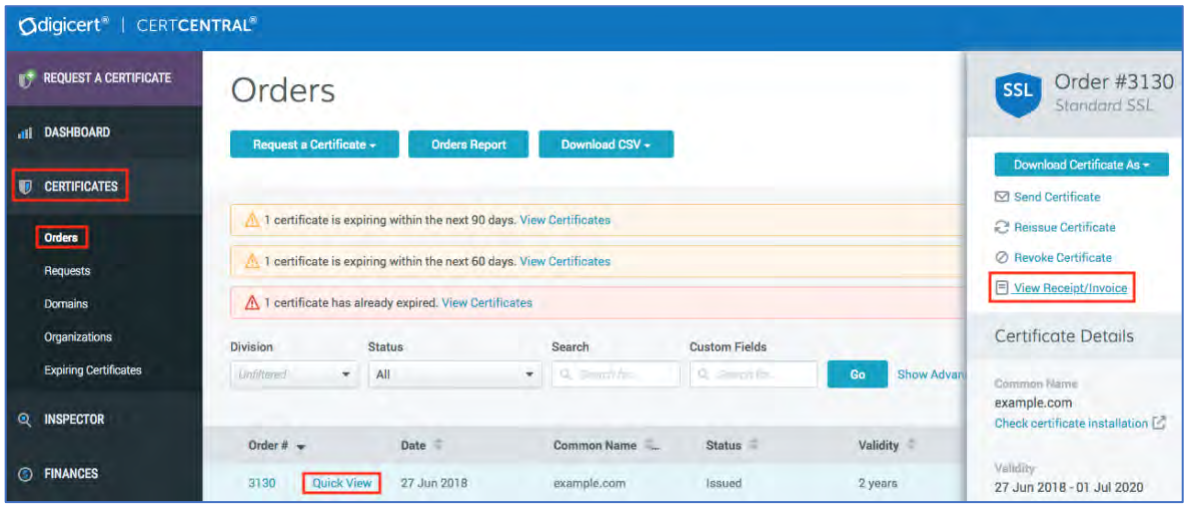
4. On the **Order #** details page, in the **Certificate Details** section, in the **Certificate Actions** drop-down list, select **View Receipt/Invoice**.



12.4.2 How to View the Receipt/Invoice for an Issued Certificate Order

Use these instructions to view the receipt of invoice for an issued certificate order.

1. In your CertCentral account, in the sidebar menu, click **Certificates > Orders**.



2. On the **Orders** page, use the filters and column headers to locate the certificate order for which you want to see the receipt/invoice.
3. In the **Order #** column, click the **Quick View** link for the issued certificate.
4. In the **Order** details pane (on the right), click the **View Receipt/Invoice** link.

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