DigiCert User Guide

Version 4.2

Contents

1 User Management

Before you start to use your DigiCert Account, work with your DigiCert account representative to set up your account structure (Divisions and Subdivisions) and permissions. Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or in your account altogether.

For example, in the **How to View Account Users** instruction, you may not be able to use the **Division** drop-down list to view users in other Divisions.

1.1 Roles and Account Access

Account administrators do not assign permissions to individual users. Instead, they assign each user a role (Administrator or User). The role assigned to the user determines which Division account features they can access.

During account set up with your DigiCert representative, you create your account structure and define what permissions the Administrator and Users roles can access at each Divisional level.

1.1.1 Administrator Role

The primary function of the Administrator role is to allow an administrator to manage their Division and/or Subdivision(s) by having full access to the features needed to fulfill their managerial tasks. An Administrator's tasks may include managing users, two-factor authentication, reports, Divisions, Subdivisions, domains, etc. What an Administrator can and cannot do is determined during account setup with you DigiCert representative.

1.1.2 User Role

The primary function of the User role is to allow a user to fulfill specific duties inside their Division or Subdivision by providing them with just enough access to the features needed to accomplish their tasks. A User's tasks may include running reports or ordering certificates. What a User can and cannot do is determined during account setup with your DigiCert representative.

1.1.3 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 have a phone number and job title.

1.1.4 EV Verified User

EV Verified Users can approve certificate request for EV SSL Plus, EV Multi-Domain and EV Code Signing certificates. For a user to be an EV Verified User, they must have a phone number and job title.

1.1.5 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 have a phone number and job title.

1.2 Managing Users

Typically, Administrators manage the administrators and users of their Division(s). Managing users may include adding account users, deleting account users, editing user account details and roles, managing API user's keys, and managing guest keys.

1.2.1 How to Add Users to Your Account

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

2. On the **Manage Users** page, click **+ New User**.

3. On the **New Users** page, provide the following details for the new user:

   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.

   Phone: Type a phone number at which the user can be reached.

   A phone number is required if the user will be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests), an **EV CS Verified User** (able to approve EV Code Signing certificate requests), and/or a **CS Verified User** (able to approve Code Signing certificate requests).

   Job Title: Type the user's job title.

   A job title is required if the user will be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests), an **EV CS Verified User** (able to approve EV Code Signing certificate requests), and/or a **CS Verified User** (able to approve Code Signing certificate requests).

   Username: Type the username for the user.

   Although you can create a unique username for each user, we recommend using their email address (i.e. *john.doe@example.com*).

   Division: In the drop-down list, select the Division or Subdivision to which you want to assign the user.

   Role: Select a role(s) for the new user: **Administrator** or **User**.

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

The newly added user will be sent an email that contains a link, which lets them create a password to log into the account.

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

If a newly added user deletes or loses the **DigiCert User Account Created - Action Required** email before they create their password, 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 account, in the sidebar menu, click **Account > Manage Users**.
2. On the **Manage Users** page, in the **Division** drop-down list, select the Division or Subdivision to which you assigned the new user.
3. To the right of the new user to whom you need to resend the **DigiCert User Account Created - Action Required** email, click **View**.
4. On the **"User"** page, click **Resend Create User Email**.

   The newly added user will be resent the **Create User Email** with a new link, which lets them create a password to log into the account.

1.2.3 How to Edit User Accounts

1. In your account, in the sidebar menu, click **Account > Manage Users**.
2. On the **Manage Users** page, in the **Division** drop-down list, select the Division or Subdivision to which the user belongs.
3. To the right of the user account whose details you need to modify, click **View**.
4. On the ***"User's"*** page, click **Edit User**.
5. On the **Edit User** page, change any of the following details:

First Name:	Edit the user's first name.
Last Name:	Edit the user's last name.
Email:	Edit the email address at which the user can be contacted.

Phone: Add, edit, or remove the phone number at which the user can be reached.

You must provide the user's phone number if you want them to be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests), an **EV CS Verified User** (able to approve EV Code Signing certificate requests), and/or a **CS Verified User** (able to approve Code Signing certificate requests).

Job Title: Add, edit, or delete the user's job title.

You must provide the user's job title if the user will be an **EV Verified User** (able to approve EV Multi-Domain, EV SSL Plus, and EV Code Signing certificate requests), an **EV CS Verified User** (able to approve EV Code Signing certificate requests), and/or a **CS Verified User** (able to approve Code Signing certificate requests).

Username: Edit the username for the user.

Although you can create a unique username for each user, we recommend using their email address.

Role: Select a different role(s) for the user: **Administrator** or **User**.

6. When you are finished, click **Save User**.

1.2.4 How to Delete (Remove) User Accounts

1. In your account, in the sidebar menu, click **Account > Manage Users**.
2. On the **Manage Users** page, in the **Division** drop-down list, select the Division or Subdivision to which the user belongs.
3. To the right of the user account that you need to remove, click **View**.
4. On the ***"User's"*** page, click **Edit User**.
5. On the **Edit User** page, click **Delete User**.

   CAUTION: Do not click **OK**, unless you are sure that you want to remove the user from your account. In the confirmation window, when you click **OK**, that user is automatically removed from your account.

6. When you receive the **"This action cannot be undone. Are you sure you want to delete this user?"** message click **OK**.

   The user should be removed from the account.

1.2.5 How to Edit Your Profile

1. In your account, in top right corner, in the **Hello, “User”** drop-down list, select **My Profile**.
2. On the **Profile Settings** page, change any of the following details:

   First Name: Edit your first name.

   Last Name: Edit your last name.

   Language: To change the language for your account, in the drop-down list, select one of the available languages.

   Opt-In to DigiCert Newsletter: Select **Yes** if you want to receive the DigiCert Newsletter.

3. **To Change Your E-Mail Address:**

   If you are using your email address as your username, we recommend changing your username to match your new email address.

   i. To the right of your **E-Mail Address**, click the **edit** symbol (yellow pencil).

   ii. In the **Change Email** window, in the **New Email** box, enter your new email address.

   iii. In the **Password** box, enter your password

   iv. Then click **Save**.

   You should an email notifying you of the change.

4. **To Change Your Username:**

   Although you can create a unique username, we recommend using your email address for your username.

   If you changed your email address and you are using your email address as your username, we recommend changing your username to match your new email address.

   i. To the right of your **Username**, click the **edit** symbol (yellow pencil).

   ii. In the **Change Username** window, in the **New Username** box, enter your new username.

   iii. In the **Password** box, enter your password

   iv. Then click **Save**.

The next time you log into your account, you will need to use your new username to login.

5. **To Change Your Password:**

   i. To the right of **Password**, click the **Click here to change your password** link**.**

   ii. In the **Change Password** window, in the **Current Password** box, enter your password.

   iii. In the **New Password** and **Re-enter New Password** boxes, create and confirm your new password.

   iv. Then click **Save**.

   The next time you log into your account, you will need to use your new password to login.

6. **To Change Your Security Question:**

   i. To the right of **Security Question**, click the **Click here to change your security question** link**.**

   ii. In the **Change Security Question** window, in the drop-down list, select a new security question.

   iii. In the **Your Answer** box, enter the answer to your new security question.

   iv. In the **Password** box, enter your password.

   If you changed your password during this session in your account, make sure to use your new password.

   v. Then click **Save**.

7. When you are finished, click **Save**.

   If you changed your email address and/or username, you should see the changes now.

1.2.6 How to View Account Users

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

2. **Filter users by Division or Subdivision.**

   On the **Manage Users** page, in the **Division** drop-down list, select a Division or Subdivision.

3. **Rearrange users by name, username, email address, role, or Division or Subdivision.**

   On the **Manage Users** page, click one of the column headers (**Name**, **Username**, **Email**, **Role** or **Division**) to rearrange the order in which the users are listed.

4. To the right of a user, click **View** to see the user's profile.

1.2.7 How to Unlock a "Locked" Account

This instruction cover what to do if your account gets locked due to excessive login failures or for other security reasons.

If just can't access your account because you forgot your username or password, see How to Retrieve Your Forgotten Username or How to Reset Your Forgotten Password.

Users:

If you get locked out of your DigiCert account, please contact your Administrator so that they can work with us to unlock your account.

Admins:

If you or one of your users gets locked out of your DigiCert account, contact us so that we can unlock the account for you.

Contact the DigiCert Team

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

1.2.8 How to Retrieve Your Forgotten Username

This instruction explains what to do if you forgot your username. If you have already been locked out of your account, see How to Unlock a "Locked" Account.

1. Go to the DigiCert Account Login page.

2. On the login page, click **Forgot your username**.

3. In the **Forgot Your Username** wizard, type your email address and then click **Proceed**.

4. An email with your username is sent to the email address that you provided.

1.2.9 How to Reset Your Forgotten Password

This instruction explains what to do if you forgot your password. If you have already been locked out of your account, see How to Unlock a "Locked" Account.

1. Go to the DigiCert Account Login page.

2. On the login page, click **Forgot your password**.

3. In the **Forgot Your Password** wizard, type your email address and then click **Proceed**.

4. An email with instructions for resetting your password is sent to the email address that you provided.

1.3 Managing API Users

Typically, Administrators manage the administrators and user accounts of their Division(s). Managing users may include issuing and revoking API keys.

1.3.1 How to Issue an API Key

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

2. On the **Manage Users** page, in the **Division** drop-down list, select the Division or Subdivision to which the user belongs.

3. To the right of the user to whom you are issuing the API key, click **View**.

4. On the ***"User's"*** page, click **Manage API Keys**.

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

6. On the **API Keys for "user"** page, under **Issue New API Key**, in the **Key Name** box, type the name for the API key and then, click **Issue Key**.

7. In the **API Key** window, under ***"This is your new API key. Don't lose it! We cannot display it again."*** copy your API key and paste it in to your text editor.

   CAUTION: Do not close the 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 **API Key** window, once you have saved a copy of your API key, click **Close**.

10. On the **API Keys for "user"** page, under **Current API Keys**, the new API key should now be listed.

1.3.2 How to Revoke (Remove) an API Key

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

2. On the **Mange Users** page, in the **Division** drop-down list, select the Division or Subdivision to which the user belongs.

3. To the right of the user whose API key you need to revoke, click **View**.

4. On the ***"User's"*** page, click **Manage API Keys**.

5. On the **API Keys for "user"** page, under **Current API Keys**, to the right of the API key that you need to revoke, click **Revoke Key**.

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

6. On the **Revoke API Key "name"** page, under the ***"Are you sure you want to revoke this API key?"*** message, click **Revoke API Key**.

   On the **API Keys** page (**Account > API Access**) the API key's **Status** should be **Revoked**.

1.3.3 How to View API Keys and API Key Users

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

2. **Filter API Keys by Status.**

   On the **API Keys** page, in the **Status** drop-down list, select **Active, Revoked**, or **ALL** to filter the keys in the list by API key status.

3. **Rearrange users by API key name, API user's name, API key created date,** or **API key status.**

   Click one of the column headers (**Key Name**, **User**, **Created**, or **Status)** to rearrange the order in which the users are listed.

4. **Revoke a user's API key.**

   i. To the right of the API key you need to revoke, click **Revoke**.

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

   ii. On the **Revoke API Key "name"** page, under the ***"Are you sure you want to revoke this API key?"*** message, click **Revoke API Key**.

      On the **API Keys** page (**Account > API Access**) the API key's **Status** should be **Revoked**.

1.4 Managing Guest URLs

Typically, Administrators manage the administrators and user accounts of their Division(s). Managing users may include creating and editing Guest URLs.

1.4.1 Guest URLs

A Guest URL is a link to a specific certificate's request page. The following are the types of certificates for which you can create Guest URLs:

Client

- Digital Signature Plus
- Email Security Plus
- Premium

Grid

- Grid Premium
- Grid Robot Email
- Grid Robot FQDN
- Grid Robot Name
- Grid Host SSL
- Grid Host SSL UC

SSL

- EV Multi-Domain
- EV SSL Plus
- Unified Communications
- SSL Plus
- Wildcard Plus

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 a specific certificate request page within the account. The user cannot access anything else within the account.

1.4.2 How to Create a Guest URL

1. In your account, in the sidebar menu, click **Account > Guest Requests**.

2. On the **Guest URLs** page, click **+ New Guest URL**.

3. On the **New Guest URL** page, in the **Description** box, type a brief description for the URL that makes it easily identifiable in the list of URLs on the **Guest URLs** page (**Account > Guest Requests**).

4. Under **Certificate Types**, select the certificate(s) that the Guest URL allows the guest user to request.

   You can select a single certificate type or multiple types. For example, next to **Client**, click **All** to let the guest user request all types of Client Certificates.

5. Under **Certificate Validity Periods**, select the validity period(s) for the certificate(s).

   You can select a single period or multiple periods. For example, next to **Certificate Validity Periods**, click **All** to let the guest user request a 1 year, 2 year, 3 year, or Custom validity period for their certificate.

   Note:

   Some certificate types may have a maximum validity period that is less than the validity period you selected.

   For example, you select EV SSL Plus and SSL Plus, and then you select 3 years. When the guest user orders an EV SSL Plus Certificate, the validity period will be for only 2 years. If the guest user orders an SSL Plus Certificate, the validity period will be for 3 years.

6. When you are finished, click **Save Guest URL**.

   The Guest URL should now be listed on the **Guest URLs** page (**Account > Guest Requests**). You can now send the Guest URL to a “guest” and let them order a specific certificate(s).

1.4.3 How to Edit a Guest URL

1. In your account, in the sidebar menu, click **Account > Guest Requests**.

2. On the **Guest URLs** page, to the right of the Guest URL that you need to edit, click **Edit**.

3. On the **Edit "Guest URL name"** page, do the following:

Description	Edit the brief description for the URL that makes it easily identifiable in the list of Guest URLs on the **Guest URLs** page (**Account > Guest URLs**).
Certificate Types	Select a different certificate(s) or add a certificate(s) that the URL allows the guest user to request. You can select a single certificate type or multiple types. For example, next to **Client**, click **All** to let the guest user request all types of Client Certificates.
Certificate Validity Periods	Select the validity period(s) for the certificate(s). Some certificate types may have a maximum validity period that is less than the validity period you selected.

4. When you are finished, click **Save Guest URL**.

   The updated Guest URL should be listed on the **Guest URLs** page (**Account > Guest Requests**). You can now send the updated Guest URL to a "guest" and let them order a specific certificate(s).

1.4.4 How to Delete a Guest URL

1. In your account, in the sidebar menu, click **Account > Guest Requests**.

2. On the **Guest URLs** page, to the right of the Guest URL that you need to delete, click **Edit**.

3. On the **Edit "Guest URL name"** page, click **Delete Guest URL**.

   CAUTION: Do not click **Delete Guest URL**, 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.

4. On the **Delete "Guest URL name"** page, under the ***"Are you sure you want to delete this Guest URL?"*** message, click **Delete Guest URL**.

   The Guest URL should no longer be listed on the **Guest URLs** page (**Account > Guest URLs**). Any copies of the Guest URL link should no longer work.

1.4.5 How to view Guest URLs

1. In your account, in the sidebar menu, click **Account > Guest Requests**.

2. **Rearrange Guest URLs by the description.**

   On the **Guest URLs** page, click one of the **Description** column header to rearrange the order in which the Guest URLs are listed.

2 Division Management

Before you start to use your DigiCert account, work with your DigiCert account representative to set up your account structure (Divisions and Subdivisions) and permissions. Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or in your account altogether.

For example, in the **Managing Co-Branding (Logos)** section, you may not be able to add, replace, or remove logos.

2.1 Managing Divisions

Managing Divisions typically involves adding new Divisions along with the Division's first administrator. Once you've added a Division, managing a Division may include editing basic Division details, deactivating/reactivating a Division, managing co-branding, and ekeys, and configuring Division two-factor authentication requirements.

During account setup with your DigiCert representative, you create Division types and define the types of Divisions that an Administrator can manage.

2.1.1 How to Add a New Division

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

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

3. On the **New Division** page, enter the following information to about the Division:

   You can go back and modify these details after you've add the Division, if necessary.

   Name: Type the name of the Division.

   Description: Type a brief description that provides basic information about the Division.

   Type: In the drop-down list, select the Division type.

4. Under **Administrator**, enter the following information about the Division Administrator:

First Name: Type the administrator’s first name.

Last Name: Type the administrator’s last name.

Email: Type an email address at which the administrator can be contacted, sent password setting email.

Username: Type the username for the administrator.

Although you can create a unique username for the administrator, we recommend using their email address (i.e. *john.doe@example.com*).

Role: In the drop-down list, select **Administrator**.

Note: Do not click **Save Division** until you are sure the **Administrator** details are filled out correctly, especially the administrator’s email address. Once you click **Save**, you can no longer modify the information for the Division administrator you created. You can only edit the **Division Details**.

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

   The Division Administrator should receive an email that contains a link, which lets them create their password to log into their account.

6. After the Division Administrator creates their password, they should log into their account and update their user details (**Account > Manage Users**); add a phone number and job title.

   Note: To be an **EV Verified User**, and **EV CS Verified User** or a **CS Verified User**, the administrator must have a phone number and job title.

2.1.2 How to Set Division Preferences

1. In your account, in the sidebar menu, click **Account > My Division**.

2. On the **“Division”** page, click **Edit Preferences**.

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own Division Preferences, on the **Division Preferences** page, under **Use default settings**, click **Use My Own Settings**.

3. Set Permissions

   On the **Division Preferences** page, do any of the following things:

Use these settings for my division

Select this option if you want the time display preference and/or certificate quest note to apply to your division only.

Use these settings for my division and any subdivisions

Select this option if you want the time display preference and/or certificate quest note to apply to your division and any subdivisions.

Allow subdivisions to override these settings

Check this box if you want the subdivisions to be able to set their own time display preference and/or certificate request note.

4. Set the Time Display Preference

   Under Time Display, in the Time Display Format drop-down list, select one of the following preferences:

   - 12 Hour (yyyy-mm-dd hh:mm am/pm)
   - 24 Hour (yyyy-mm-dd hh:mm)

5. Create a Custom Note for All the Certificate Request Pages

   Under **Request Note**, in the **Custom Note for Request Pages** box, type the note that you want to add to the top of all certificate request pages.

   Note: This message appears on all SSL Certificate, Client, Grid, Code Signing, and Document Signing requests pages

6. When you are finished, you can leave the page.

2.1.3 How to Edit a Division's Details

1. **If you are editing your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are editing another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose details need changing, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, change any of the following information:

Name:	Edit the name of the Division.
Description:	Edit the description that provides basic information about the Division.

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

2.1.4 How to Deactivate a Division

Deactivating a Division deactivates the parent Division and any of its Subdivisions. Members of the deactivated Division and/or Subdivisions are locked of their account. Deactivating a Division does not revoke any of the certificates tied to that Division or its Subdivisions. If certificates need to be revoked, you must do that separately.

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

2. On the **Divisions** page, to the right of the Division you need to deactivate, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, click **Deactivate**.

5. When you receive the ***"This will deactivate this division and any sub-divisions it contains. Continue?"*** message, click **OK**.

   The Division and any of it Subdivision are removed from the **Divisions** page (**Account > All Divisions**). To see the deactivated Divisions, on the **Divisions** page, click **Inactive Divisions**.

2.1.5 How to Activate a Division

Reactivating a Division activates the parent Division and any of its Subdivisions. Members of the activated Division and/or Subdivisions may once again access their account.

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

2. On the **Divisions** page, click **Inactive Divisions**.

3. On the **Inactive Divisions** page to the right of the Division that you need to reactivate, click **Activate**.

4. When you receive the ***"This will activate this division and any subdivisions it contains. Continue?"*** message, click **OK**.

   The Division and any of it Subdivision are removed from the **Inactive Divisions** page and moved to the **Divisions** page (**Account > All Divisions**).

2.2 Managing Division Co-Branding (Logos)

Managing Divisions may also involve managing account co-branding, which may include adding a logo, changing a logo, or removing a logo. During account setup with your DigiCert representative, you can decide how your co-branding system will work.

Depending on how your account was set up with your DigiCert representative, you may be managing co-branding for your Division and all its Subdivisions, for your Division, or for your Subdivision. Typically, only Administrators can add logos, replace logos, or remove (delete) logos.

2.2.1 How to Add a Division Logo

1. **If you are adding a log for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are adding a logo for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account to which you want to add a logo, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, under **Division Logo**, click **Upload Logo** to browse for, select, and open the logo *.jpeg*, *.png*, or *.gif* file.

   The logo should be added and now appear in your account.

2.2.2 How to Replace a Division Logo

1. **If you are replacing the log for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are replacing the logo for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose logo you want to replace, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, under **Division Logo**, click **Change** to browse for, select, and open the new logo *.jpeg*, *.png*, or *.gif* file.

   The new logo should be added and now appear in your account.

2.2.3 How to Remove a Division Logo

1. **If you are removing the log for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are removing the logo for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose logo you want to remove, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, under **Division Logo**, click **Remove** to remove the logo *.jpeg*, *.png*, or *.gif* file.

   The logo should no longer appear in your account.

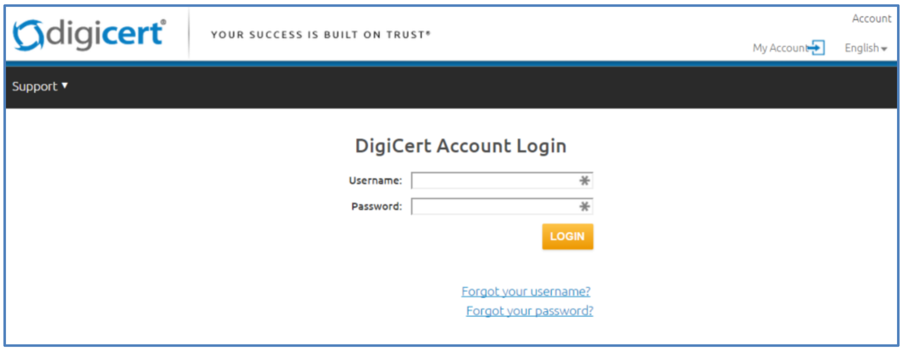
2.3 Managing Division Ekeys

When a Division is created, an ekey is automatically generated for that Division. An ekey is a branded login URL. When this URL is used to access a Division account, the Division logo is displayed on its account login page.

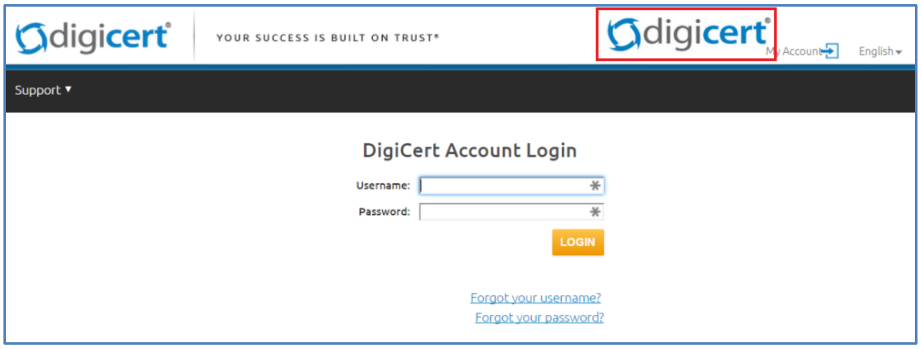
Note: If your Division was created before 2015, February 12, an ekey was not automatically generated for your Division. If you want to use an ekey to access your Division account login page, you can create your own Division ekey. See How to Create a Division Ekey.

For Example:

Normally, your Division account login URL is *https://www.digicert.com/account/login.php* and your Division login page looks like this:



When you have a Division logo, and you use the ekey branded login URL, your Division account login URL is something like this *https://www.digicert.com/account/login.php?ekey=random-hex-number* and your login page looks something like this:



2.3.1 How to View a Division Ekey

1. **If you are viewing the ekey for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are viewing the ekey for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose ekey you want to see, click **View**.

3. On the **"Division"** page, next to **Branded Login URL**, you should see the ekey for that Division.

   If you see ***"No ekey associated with this division"***, the ekey for that Division was not automatically generated when the Division was created. See How to Create a Division Ekey.

4. You can send the ekey to your Division account users so that they can access the branded Division account login page.

2.3.2 How to Create a Division Ekey

For the ekey to have any benefit for the Division, you must add a Division logo. See Managing Division Co-Branding (Logos).

1. **If you are creating the ekey for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are creating the ekey for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose ekey you want to create, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, in the **ekey (for co-branded login URLs)** box, type the name that you want to use for you ekey (i.e. *YourDivisionEkey*).

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

   You should now see the ekey (branded login URL) on the **Division's** page (**Account > All Divisions > View**, or **Account > My Division**).

6. You can now send the ekey (*https://www.digicert.com/account/login.php?ekey=YourDivisionEkey*) to your Division account users so that they can access the branded Division account login page.

2.3.3 How to Edit a Division Ekey

When editing the ekey, any users who are using the current ekey can still us that ekey to access the Division account login page. However, those users will no longer see the Division logo on the Division account login page.

1. **If you are editing the ekey for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are editing the ekey for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose ekey you want to edit, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, in the **ekey (for co-branded login URLs)** box, type the new name that you want to use for you ekey (i.e. *MyDivisionEkey*).

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

   You should now see the new ekey (branded login URL) on the **Division's** page (**Account > All Divisions > View**, or **Account > My Division**).

6. You can now send the new ekey (*https://www.digicert.com/account/login.php?ekey=MyDivisionEkey*) to your Division account users so that they can access the branded Division account login page.

2.3.4 How to Delete a Division Ekey

If you delete the ekey, any users who are using the current ekey can still us that ekey to access the Division account login page. However, those users will no longer see the Division logo on the Division account login page.

1. **If you are deleting the ekey for your Division:**

   In your account, in the sidebar menu, click **Account > My Division**.

2. **If you are deleting the ekey for another Division:**

   i. In your account, in the sidebar menu, click **Account > All Divisions**.

   ii. On the **Divisions** page, to the right of the Division account whose ekey you want to delete, click **View**.

3. On the **"Division"** page, click **Edit Division**.

4. On the **Edit "Division"** page, in the **ekey (for co-branded login URLs)** box, delete name of the ekey.

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

   You should no longer see the ekey (branded login URL) on the **Division's** page (**Account > All Divisions > View**, or **Account > My Division**).

3 IP Access Restrictions

IP access restrictions can be used to add an extra layer of security to your DigiCert account. You can set up IP access restrictions for the entire account, for your division, or for specific users.

Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or in your account altogether. For example, if you do not want divisions to set up their own IP access restrictions, you may not see some of the inheritability selections in your account.

3.1 Configuring IP Access Restrictions

These instructions are for administrators only and explain how to configure your IP access restriction rules for your DigiCert account.

Permissions Note:

Only administrators can view the **IP Restrictions** page and can configure IP access restrictions for account users, division users, and specific users.

3.1.1 How to Turn On IP Address Restrictions

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.

   Subdivision Admins Note:

If your Division Admin already set up default rules for your subdivision and granted you permission to create your own IP access restriction rules, on the **IP Restrictions** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **IP Restrictions** page, under **IP Address Restrictions**, click **On**.

3. **Set Permissions:**

Note: If you don’t have subdivisions, then you don’t see the **“Use this setting for”** settings.

On the **IP Restrictions** page, do any of the following things:

Use this setting for my division	Select this option if you want the IP restriction rules that you create to apply to your division only. When your subdivision admins navigate to the **IP Restrictions** page (**Settings > IP Access Restrictions**), they control whether IP access restrictions are enabled.
Use this setting for my division and any subdivisions	Select this option if you want the IP access restriction rules that you create to apply to your division and all subdivisions. When your subdivision admins navigate to the **IP Restrictions** page (**Settings > IP Access Restrictions**), they receive the ***“You cannot modify your IP restriction settings because they have been set by your account administrator. Please contact your account administrator for more information.”*** message.
Allow subdivisions to override this setting	Check this box if you want your subdivisions to be able to configure their own IP access restriction rules.

When your subdivision admins navigate to the **IP Restrictions** page (**Settings > IP Access Restrictions**), they are presented with the following options:

- **Use Default Settings**

  If the admin clicks this option, IP access restrictions are enabled for their division, and they defer to the IP access restriction rules that you create for them.

- **Use My Own Settings**

  If the admin clicks this option, they control whether IP access restrictions are enabled. They are required to create their own IP access restriction rules for their division.

4. You have successfully turned on the IP access restrictions for your DigiCert account, and you are ready to configure your IP access restriction rules.

3.1.2 How to Turn Off IP Access Restrictions

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.

   Subdivision Admins Note:

   If your Division Admin already set up default rules for your subdivision and granted you permission to create your own IP access restriction rules, on the **IP Restrictions** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **IP Restrictions** page, under **IP Address Restrictions**, click **Off**.

3. **Set Permissions:**

   Note: If you don't have subdivisions, then you don't see the **"Use this setting for"** settings.

   On the **IP Restrictions** page, do any of the following things:

Use this setting for my division	Select this option if you want to disable IP access restrictions for your division only.

When your subdivision admins navigate to the **IP Restrictions** page (**Settings > IP Access Restrictions**), they control whether IP access restrictions are disabled.

Use this setting for my division and any subdivisions

Select this option if you want to disable IP access restriction for your division and all subdivisions.

When your subdivision admins navigate to the **IP Restrictions** page (**Settings > IP Access Restrictions**), they receive the ***"You cannot modify your IP restriction settings because they have been set by your account administrator. Please contact your account administrator for more information."*** message.

Allow subdivisions to override this setting

Check this box if you want your subdivisions to be able to disable IP access restrictions for themselves.

When your subdivision admins navigate to the **IP Restrictions** page (**Settings > IP Access Restrictions**), they are presented with the following options:

- **Use Default Settings**

  If the admin clicks this option, IP access restrictions are disabled for their division, and they defer to your for IP access restriction rules.

- **Use My Own Settings**

  If the admin clicks this option, they control whether IP access restrictions are enabled. They are required to create their own IP access restriction rules for their division.

4. You successfully turned off the IP access restrictions for your DigiCert account.

3.1.3 Account Wide: Configure IP Access Restriction Rules

The parameters of an account wide rule are dependent on the permissions that you set for your account (Divisions and Subdivisions).

Permission Parameters:

To enforce an account wide rule:

Select **Use this setting for my division and any subdivisions** and do not check **Allow subdivision to override this setting**.

Your account wide IP access restriction rule is enforced for the entire account.

To enforce a division rule:

Select **Use this setting for my division**.

Your account wide IP access restriction rule is enforced for your division only.

To set up default settings for the entire account:

Select **Use this setting for my division and any subdivisions** and check **Allow subdivision to override this setting**.

Your account wide IP access restriction rule is the default setting for the entire account but allows other divisions/subdivisions to enforce their own rules for their account if needed.

How to Configure an Account Wide Rule

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.

   Subdivision Admins Note:

   If your Division Admin already set up default rules for your subdivision and granted you permission to create your own IP access restriction rules, on the **IP Restrictions** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.

3. On the **New IP Restriction** page, in the **Restriction Type** drop-down list, select **Account Wide**.

4. In the **IP Range Start** and **IP Range End** boxes, enter the parameters for your IP access restrictions.

5. In the **Description** box, enter a description of the restriction.

6. Click **Add Rule**.

   Your rule is now listed on the **IP Restrictions** page (**Settings > IP Access Restrictions**) under **IP Restrictions Rules** with a **Rule Scope – All Account Users**.

3.1.4 Division: Configure IP Access Restriction Rules

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.

Subdivision Admins Note:

If your Division Admin already set up default rules for your subdivision and granted you permission to create your own IP access restriction rules, on the **IP Restrictions** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.
3. On the **New IP Restriction** page, in the **Restriction Type** drop-down list, select **Division**.
4. In the **Division** drop-down list, select the division/subdivision to which you want to apply the rule.
5. In the **IP Range Start** and **IP Range End** boxes, enter the parameters for your IP access restrictions.
6. In the **Description** box, enter a description of the restriction.
7. Click **Add Rule**.

   Your rule is now listed on the **IP Restrictions** page (**Settings > IP Access Restrictions**) under **IP Restrictions Rules** with a **Rule Scope – Division: "Division Name"**.

3.1.5 A Specific User: Configure IP Access Restriction Rules

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.

   Subdivision Admins Note:

   If your Division Admin already set up default rules for your subdivision and granted you permission to create your own IP access restriction rules, on the **IP Restrictions** page, under **Use default settings**, click **Use My Own Settings**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.
3. On the **New IP Restriction** page, in the **Restriction Type** drop-down list, select **User**.
4. In the **User** drop-down list, select the user to which you want to apply the rule.
5. In the **IP Range Start** and **IP Range End** boxes, enter the parameters for your IP access restrictions.
6. In the **Description** box, enter a description of the restriction.
7. Click **Add Rule**.

   Your rule is now listed on the **IP Restrictions** page (**Settings > IP Access Restrictions**) under **IP Restrictions Rules** with a **Rule Scope – User: "User Name"**.

3.1.6 How to View IP Access Restriction Rules

You can only see the rules that you created for your Division/Subdivision. You cannot see the rules for another Division.

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, the rules are listed according to **Rule Scope** (**All Account Users**, **Division: "Division Name"**, and **User: "User Name"**.)

3.1.7 How to Delete an IP Access Restriction Rule

You can only delete the rules that you created for your Division/Subdivision. You cannot see or delete the rules created for another Division.

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, to the right of the rule that you want to delete, click **Delete**.

   Your rule is removed from the list of rules on the **IP Restrictions** page (**Settings > IP Access Restrictions**) under **IP Restrictions Rules**.

4 DigiCert Two-Factor Authentication

Two-factor authentication increases the security of your DigiCert account by allowing you to require two methods of identity verification before someone can log in and access their account. You can require two-factor authentication for all account users, all users in a Division, and for specific individual users (i.e. *Jane Doe in Accounting*).

Depending on your organization's security requirements, some of the two-factor authentication rules for your account and its setup may be different.

4.1 Setting Up Two-Factor Authentication

Before you begin creating the rules for implementing two-factor authentication, you need to decide which two-factor authentication option will work best for your DigiCert account.

4.1.1 Client Certificate Requirement

A Client Certificate allows users to log in only from the computer/device on which their certificate is installed. Client Certificates may also be limited to a specific browser(s).

Windows: Installs the Client Certificate in its own Certificate Store. Internet Explorer and Chrome can access the certificate.

Mac: Installs the Client Certificate in its own Certificate Store. The keychain for Safari and Chrome can access the certificate.

Firefox: Installs the Client Certificate in its own Certificate Store. Only Firefox can access the certificate (Windows or Mac).

4.1.2 One-time Password Requirement

An OTP App installed on a mobile device allows users to log in from any computer/device. Because our Two-Factor Authentication process implements the Time-based One-Time Password (TOTP) protocol, you must use a Mobile Application that supports the TOTP protocol.

The TOTP protocol supports a time-based variation of the One-time password (OTP) algorithm. Each time an OTP is generated, it can only be used for a short period and once expired, cannot be reused. OTPs with short life spans help enhance security.

Most OTP Applications (compatible with the TOTP protocol) will work with our process. The following list contains the OTP Applications that we have tested:

Google Authenticator: Android, iPhone, Blackberry

Authy: Android, iPhone

Authenticator: Windows Phone

Duo Mobile: iPhone

4.2 Configuring Two-Factor Authentication Requirements

These instructions are for administrators only and explain how to configure your two-factor authentication rules/requirements for your DigiCert account.

Permissions Note:

Only administrators can view the **Authentication Settings** page and can configure two-factor authentication requirements for account users, division users, and specific users.

4.2.1 How to Turn On Two-Factor Authentication

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, under **Two-Factor Auth Status**, click **On**.

3. Set Permissions:

   If you do not have any subdivisions, you do not see the **“Enable”** settings.

   On the **Authentication Settings** page, do any of the following things:

Enable two factor authentication for my division

Select this option if you want the two-factor authentication requirements that you create to apply to your division only.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they control whether two-factor authentication is enabled.

Enable two factor authentication for my division and any subdivisions

Select this option if you want the two-factor authentication requirements that you create to apply to your division and all subdivisions.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they receive the ***"You cannot modify your two factor auth settings"*** message.

Allow subdivisions to override two factor authentication settings

Check this box if you want your subdivisions to be able to set their own two-factor authentication requirements.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they are presented with the following options:

- **Use Default Settings**

  If the admin clicks this option, two-factor authentication is enabled for their division, and they defer to the two-factor authentication requirements that you create for them.

- **Use My Own Settings**

  If the admin clicks this option, they control whether two-factor authentication is enabled. They are required to create their own two-factor authentication requirements for their division.

4. You have turned on two-factor authentication for your DigiCert account and are ready to configure your two-factor authentication requirements.

4.2.2 How to Turn Off Two-Factor Authentication

Turning off two-factor authentication does not delete your requirements or any of the Client Certificates or OTP App Devices configured for your account. When you turn Two-Factor authentication back on, your certificates and devices should still be configured, and the rules should still be there, ready to be used, modified, or deleted.

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, under **Two-Factor Auth Status**, click **Off**.

3. Set Permissions:

If you do not have any subdivisions, you do not see the **“Disable”** settings.

On the **Authentication Settings** page, do any of the following things:

Disable two factor authentication for my division

Select this option if you want to disable two-factor authentication for your division only.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they control whether two-factor authentication is disabled.

Disable two factor authentication for my division and any subdivisions

Select this option if you want to disable two-factor authentication for your division and all subdivisions.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they receive the ***“You cannot modify your two factor auth settings”*** message, and two factor authentication is disabled for their division.

Allow subdivisions to override two factor authentication settings

Check this box if you want your subdivisions to be able to disable two-factor authentication themselves.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they are presented with the following options:

- **Use Default Settings**

  If the admin clicks this option, they defer to your settings and two-factor authentication is disabled for their division.

- **Use My Own Settings**

  If the admin clicks this option, they control whether two-factor authentication is disabled. They are required to create their own two-factor authentication requirements for their division.

4. You have turned off two-factor authentication for your DigiCert account.

4.2.3 All Account Users: Configure Two-Factor Authentication Requirements

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, under **Two-Factor Authentication Requirements**, click **Add New Requirement**.

3. On the **Add Two Factor Requirement** page, under **Authentication Type**, select one of the following options:

   - **One-Time Password (OTP)**

     Select this option if you want all account users to use an OTP App on their mobile device to complete the authentication process. Users can log into their DigiCert account from any computer/device.

- **Client Certificate**

  Select this option if you want all account users to use a Client Certificate to complete the authentication process. Users can only log into their DigiCert account from a computer/device on which the certificate is installed.

4. Under **Apply Rule To**, select **All account users**.

   Division Admin Note:

   If you are a Division Admin and have selected **Enable two factor authentication for my division and any subdivisions**, when you apply the rule to **All account users**, you are creating a rule for every user in your division and for every user in all your subdivisions.

5. Click **Create Requirement**.

   The rule is automatically created and it appears in the list of requirements on the **Authentication Settings** page, under **Two-Factor Authentication Requirements**. You have now successfully configured a two-factor authentication requirement for all account users.

4.2.4 All Users in a Division: Configure Two-Factor Authentication Requirements

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, click **Add New Requirement**.

3. On the **Add Two Factor Requirement** page, under **Authentication Type**, select one of the following options:

   - **One-Time Password (OTP)**

     Select this option if you want all users of the Division to use an OTP App on their mobile device to complete the authentication process. Users can log into their DigiCert account from any computer/device.

   - **Client Certificate**

     Select this option if you want all users of the Division to use a Client Certificate to complete the authentication process. Users can only log into their DigiCert account from a computer/device on which the certificate is installed.

4. Under **Apply Rule To**, select **All users in division**.

5. In the **All users in division** drop-down list, select the Division to which you want the two-factor authentication requirement to apply.

   Division Admin Note:

   If you are creating a rule for a Subdivision, make sure that you selected **Enable two factor authentication for my division and any subdivisions** so that the rule is actually applied to that division.

6. Click **Create Requirement**.

   The rule is automatically created and it appears in the list of requirements on the **Authentication Settings** page, under **Two-Factor Authentication Requirements**. You have now successfully configured a two-factor authentication requirement for all users in the specified Division.

4.2.5 A Specific User: Configure Two-Factor Authentication Requirements

You can only create two-factor authentication requirements for users in your own Division. To create two-factor authentication requirements for users in a subdivision, you will need to check **Allow subdivisions to override two factor authentication settings** to let the subdivision admin create those rules.

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, click **Add New Requirement**.

3. On the **Add Two Factor Requirement** page, under **Authentication Type**, select one of the following options:

   - **One-Time Password (OTP)**

     Select this option if you want the specified user to use an OTP App on their mobile device to complete the authentication process. The user can log into their DigiCert account from any computer/device.

   - **Client Certificate**

     Select this option if you want the specified user to use a Client Certificate to complete the authentication process. The user can only log into their DigiCert account from a computer/device on which the certificate is installed.

4. Under **Apply Rule To**, select **Specific user**.

5. In the **Specific user** drop-down list, select the user to which you want the two-factor authentication requirement to apply.

   Note: You can only select a user from your own Division. If you need to create a rule for a user in one of your subdivisions, you must allow the subdivision admin to create their own division rules.

6. Click **Create Requirement**.

   The rule is automatically created and it appears in the list of requirements on the **Authentication Settings** page, under **Two-Factor Authentication Requirements**. You have now successfully configured a two-factor authentication requirement for the specified user.

4.2.6 OTP App Authenticators: How to Allow Them to Verify a Computer for 30 Days

Providing OTP authenticators with this option allows them to verify the computer from which they are logging in. For the next thirty days, they can bypass entering the verification code each time they log in from that computer. At the end of the thirty days, OTP authenticators are required to enter their verification code and decide if they want to remember the verification on that computer for the next thirty days.

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, under **Remember Verification**, check **Display "Remember verification for this computer" checkbox during OTP login**.

   Division Admin Note:

   If you are a Division Admin and have selected **Enable two factor authentication for my division and any subdivisions**, when you permit OTP authenticators to verify a computer for 30 days, you are allowing every OTP authenticator in your division and for every OTP authenticator in all your subdivisions this privilege.

3. You have now successfully configured the option to allow OTP App authenticators to verify a computer for 30 days when logging into their DigiCert account.

4.2.7 How to Delete a Two-Factor Authentication Requirement

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

Subdivision Admins Note:

If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Authentication Settings** page, under **Two-Factor Authentication Requirements**, locate the requirement that you want to remove and click **Delete**.

   The requirement is automatically removed. You have successfully deleted a two-factor authentication requirement.

3. ### To Nullify the Client Certificate

   If you delete a Client Certificate two-factor authentication requirement, the client certificates for the users who were part of that requirement are still listed under **Issued Client Certificates**.

   In the future, if you decide to recreate a Client Certificate two-factor authentication requirement for any of those users, they can reuse that certificate as their second factor.

   If you prefer, you can nullify the Client Certificates and force the user to generate a new certificate the next time you create a Client Certificate two-factor authentication requirement for them.

   Under **Issued Client Certificates**, locate the certificate that you want to nullify and click **Reset**. The certificate should no longer be listed.

4. ### To Nullify the OTP Device

   If you delete a One-Time Password (OTP) two-factor authentication requirement, the OTP App devices for the users who were part of that requirement are still listed under **One-Time Password (OTP) Devices**.

   In the future, if you decide to recreate a One-Time Password (OTP) two-factor authentication requirement for any of those users, they can use their initialized OTP App device as their second factor.

   If you prefer, you can nullify the OTP App device and force the user to reinitialize their device the next time you create a One-Time Password (OTP) two-factor authentication requirement for them.

   Under **One-Time Password (OTP) Devices**, locate the user whose device you want to nullify and click **Reset**. The OTP App device should no longer be listed.

4.2.8 How to View Two Factor Authentication Requirements

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

2. On the **Authentication Settings** page, under **Two-Factor Authentication Requirements**, each requirement is listed with authentication type, who the rule applies to, and date created information.

4.2.9 How to View OTP and Client Certificate Authenticators

Users do not appear in the list until they have initialized their OTP device or generated their Client Certificate.

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

   If your Division Admin didn't grant you permissions to control your own two-factor authentication requirements, then you cannot view **OTP and Client Certificate Authenticators**.

2. On the **Authentication Settings** page, under **Issued Client Certificates**, the Client Certificate authenticators are listed and under **One-Time Password (OTP) Devices**, the OTP authenticators are listed.

3. **Subdivision Admins Note:**

   When you have finished, on the **Authentication Settings** page, click **Use Default Settings** if you want to continue using your Parent Division's two-factor authentication settings. If you don't click **Use Default Settings**, then the two-factor authentication requirement(s) of the Parent Division is not enforced.

4.3 Two-Factor Authentication: User Instructions

The instructions in this section explain how to use two-factor authentication (OTP or Client Certificate).

4.3.1 How to Initialize Your OTP App Device

After your administrator has turned on and configured two-factor authentication, you must initialize the second factor of your two-factor authentication: your OTP App Device. The next time you log into your DigiCert account, you will be asked to initialize your OTP App Device.

Because our Two-Factor Authentication process implements the Time-based One-Time Password (TOTP) protocol, you must use a Mobile Application that supports the TOTP protocol.

Most OTP Applications (compatible with the TOTP protocol) will work with our process. The following list contains the OTP Applications that we have tested:

- **Google Authenticator:** Android, iPhone, Blackberry
- **Authy:** Android, iPhone
- **Authenticator:** Windows Phone
- **Duo Mobile:** iPhone

1. Install an OTP App that is compatible with the TOTP protocol on your mobile device.
2. Log into your DigiCert account.
3. On the **One-Time Password (OTP APP) Device Initialization** page, do the following:
   i. On your mobile device, open your OTP App.
   ii. Use your OTP App to scan the QR code.
   iii. In the **Enter code** box, type the code that is displayed on your device.
   iv. Click **Submit**.
4. You should now be logged in to your account.

   You should receive an email confirming that you initialized your OTP device.

4.3.2 How to Sign In with Your OTP App Device

After you have initialized your OTP App device, you will need to supply your account credentials and use the code generated in your OTP App to log into your DigiCert account.

1. Log into your DigiCert account.

   On the **DigiCert Account Login** page, in the **Username** and **Password** boxes, type your username and password and then, click **LOGIN**.
2. On your mobile device, open your OTP App.
3. On the **Enter Verification Code** page, in the **Enter code** box, type the code displayed in your OTP App.
4. (Optional) If you want to verify this computer for thirty days, check **Remember verification on this computer for 30 days**.

   Depending on how your OTP authentication requirement was configured, you may be able to opt to remember the verification on this computer. With this option checked, when you log into your DigiCert account from this computer, you are only required to enter your credential for the next thirty days. At the end of thirty days, you are required to enter your verification code again and choose whether to verify this computer for another thirty days.

5. Click **Submit**.

   This completes the authentication process and logs you into your account.

4.3.3 User: Resetting Your OTP App Device

If you lose your OTP App Device (phone, tablet, iPad, etc.), you should immediately contact your administrator to get your OTP App Device reset. Do not be tempted to wait until you get your new device because you have a trusted computer from which you can log into your DigiCert account. It is important to have your administrator reset your OTP App Device immediately to prevent unauthorized access to your DigiCert account.

Lost My OTP App Device

1. Contact your administrator.

2. After your administrator resets your device, you will need to login to your DigiCert account and reinitialize your OTP App device.

   See How to Initialize Your OTP App Device .

4.3.4 How to Generate Your Client Certificate

After your administrator has turned on and configured two-factor authentication, you must initialize the second factor of your two-factor authentication: your Client Certificate. The next time that you log into your DigiCert account, you will be asked to generate your Client Certificate.

Depending on which Web browser you use to initialize/generate your Client Certificate, you may need to use that browser to log into your DigiCert account.

- **Windows** installs the Client Certificate in its own Certificate Store. It **can be shared with Chrome and Internet Explorer**.

- **Mac:** Installs the Client Certificate in its own Certificate Store. It **can be shared with the keychain for Safari and Chrome**.

- **Firefox:** Installs the Client Certificate in its own Certificate Store. It **can only be accessed with Firefox (Windows or Mac OS)**.

For more information about taking care of your Client Certificate, see Managing Your Client Certificate.

Generating Your Client Certificate

1. Log into your DigiCert account.

2. On the **Two-Factor Authentication Client Certificate Initialization** page, click **Generate Certificate**.

3. When the browser presents your certificates, select your newly generated Client Certificate and click **OK**.

4. You should now be logged into your account.

   Your certificate should now be installed in the Certificate Store related to the browser that you are currently using. You should receive an email confirming that you successfully created a two-factor authentication Client Certificate.

4.3.5 How to Sign In with Your Client Certificate

After you have generated your Client Certificate, you will need to supply your credentials and select that certificate to log into the DigiCert account. You can only log into your DigiCert account from a computer on which this certificate is installed.

Depending on which Web browser you used to initialize/generate your Client Certificate, you may need to use that browser to log into the Console.

- **Windows** installs the Client Certificate in its own Certificate Store. It **can be shared with Chrome and Internet Explorer**.

- **Mac:** Installs the Client Certificate in its own Certificate Store. It **can be shared with the keychain for Safari and Chrome**.

- **Firefox:** Installs the Client Certificate in its own Certificate Store. It **can only be accessed with Firefox (Windows or Mac OS)**.

For more information about taking care of your Client Certificate, see Managing Your Client Certificate.

Signing In with Your Client Certificate

1. Log into your DigiCert account.

   On the **DigiCert Account Login** page, in the **Username** and **Password** boxes, type your username and password and then, click **LOGIN**.

   Note: Make sure to log in with a browser that can access your Client Certificate. You should be safe using the browser that you used to initialize/generate the Client Certificate.

2. When your browser presents your certificates, select the Client Certificate that you generated for logging into your DigiCert account during the Client Certificate initialization. See How to Generate Your Client Certificate.

This completes the authentication process and logs you into your account.

4.3.6 User: Resetting Your Client Certificate

If you lose your Client Certificate (lose computer, computer breaks down, or certificate is deleted from your computer or the Certificate Store), you should immediately contact your administrator to get your certificate reset.

Lost My Client Certificate

1. Contact your administrator.
2. After your administrator resets your Client Certificate, you will need to login to your DigiCert account and generate a new Client Certificate.

   See How to Generate Your Client Certificate.

4.4 Two-Factor Authentication: Admin Specific Instructions

The instructions in this section explain how to reset a user's (admin or user) two-factor authentication client certificate or OTP App device for their DigiCert account.

4.4.1 How to Reset a User's OTP App Device

If one of your users or admins loses their OTP App Device (phone, tablet, iPad, etc.), you can reset their OTP App Device in your DigiCert account.

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

   If your Parent Division Admin didn't grant you permissions to control your own two-factor authentication requirements, then you cannot reset a User's **OTP App device**.

2. On the **Authentication Settings** page, under **One-Time Password (OTP) Devices**, locate the device that you need to reset and click **Reset**.

   Subdivision Admins Note:

   When you are finished, on the **Authentication Settings** page, click **Use Default Settings** if you want to continue using your Parent Division's two-factor authentication settings. If you don't click **Use Default Settings**, then the two-factor authentication requirement(s) of the Parent Division is not enforced.

3. The next time that user tries to log into your DigiCert account, they will need to initialize their OTP App Device.

4.4.2 How to Reset a User's Client Certificate

If one of your users or admin loses their Client Certificate (loses computer, computer breaks down, or certificate is deleted from their computer or the Certificate Store), you can reset their Client Certificate in your DigiCert account.

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

   Subdivision Admins Note:

   If you are the admin of a Subdivision and your Division Admin granted you permission to control your own two-factor authentication requirements, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

   If your Division Admin didn't grant you permissions to control your own two-factor authentication requirements, then you cannot reset a User's Client Certificate.

2. On the **Authentication Settings** page, under **Issued Client Certificates**, locate the certificate that you need to reset and click **Reset**.

   Subdivision Admins Note:

   When you are finished, on the **Authentication Settings** page, click **Use Default Settings** if you want to continue using your Parent Division's two-factor authentication settings. If you don't click **Use Default Settings**, then the two-factor authentication requirement(s) of the Parent Division is not enforced.

3. The next time that user tries to log into your DigiCert account, they will need to generate a new Client Certificate.

4.4.3 Admin: Resetting Your OTP App Device

If you lose your OTP App Device (phone, tablet, iPad, etc.), and you do not have another admin who can reset your OTP App Device for you, contact us immediately to get your OTP App Device reset.

1. Contact DigiCert.

   Contact our Support Team:
   support@digicert.com
   Direct Phone: 1-801-701-9600.

2. After the request is confirmed and your OTP App Device is reset, you will need to login to your DigiCert account and reinitialize your OTP App device.

See How to Initialize Your OTP App Device .

4.4.4 Admin: Resetting Your Client Certificate

If you lose your Client Certificate or the computer on which it is installed, and you do not have another admin who can reset your Client Certificate for you, contact us immediately to get your certificate reset.

1. Contact DigiCert.

   Contact our Support Team:
   support@digicert.com
   Direct Phone: 1-801-701-9600.

2. After the request is confirmed and your Client Certificate is reset, you will need to login to your DigiCert account and generate a new Client Certificate.

   See How to Generate Your Client Certificate.

5 Reports Management

Before you start to use your DigiCert account, work with your account representative to set up your account structure (Divisions and Subdivisions) and permissions. Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or your account altogether.

5.1 Running Reports

Once you have added your users, Divisions, domains, and organizations, you will want to run reports to see what certificates have been issued for each Division, what certificates have been revoked for each Division, etc.

5.1.1 How to Run a Report

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

2. On the **Orders Report** page, use the drop-down lists to filter the results of your orders report.

   For example, to see a report for February 2015, in the first drop-down list, select **February**. In the second drop-down list, select **2015**.

3. When you are finished setting the parameters for you report, click **Update Report**.

4. Your orders report should be displayed on the page.

6 Audit Logs

Before you start to use your DigiCert account, work with your account representative to set up your account structure (Divisions and Subdivisions) and permissions. Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or your account altogether.

6.1 Running Audits

Once you've added your users, Divisions, domains, and organizations, you may need to run account audits to highlight areas where training is required, to reconstruct events, detect intrusions, and discover problem areas.

6.1.1 How to Run an Audit

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

2. On the **Audit Logs** page, do any of the following to filter the results of your activity report:

   From: and **To:** In these boxes, set the date parameters for your activity report.

   User: In the drop-down list, select a specific user whose account activity you want to monitor.

   To see the activity of all account users, select **All users**.

   Action: In the drop-down list, select the action that you want to monitor (i.e. **Edit profile**, **Add user**, **Login with invalid ip address**, etc.).

   To see all account activity, select **All actions**.

   Result: In the drop-down list, select **Successful** or **Failed** to drill down into the action that you selected.

   To see all results for the selected action, select **All result**.

3. When you are finished, click **Filter**.

   The results of your audit should be displayed on the page.

6.2 Setting Up Audit Log Notifications

To be of help to your organization log data must be reviewed. You can use the audit log notifications feature to keep you aware of certain activities as well as make your log review more meaningful.

6.2.1 How to Create an Audit Log Notification

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

2. On the **Audit Log Settings** page, under **Create a New Notification**, do the following:

Email Address: Enter the email address of the person to whom the audit log notifications are to be sent.

Notify me about: Check any of the following options:

- **User Changes**

  Check this box to be alerted of any edits made to any of your user accounts.

- **All Logins**

  Check this box to be alerted of all account logins.

- **Logins from invalid IP Addresses**

  Check this box to be alerted of all account logins from invalid IP Addresses

3. When you are finished, click **Save**.

   The designated individual should start receiving the selected audit log notifications.

7 Organization and Domain Management

Before you start to use your DigiCert account, work with your account representative to set up your account structure (Divisions and Subdivisions) and permissions. Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or your account altogether.

7.1 Validation Process

Before an SSL, Grid, Client, Code Signing, Document Signing certificate can be issued, it must first go through a validation process. Regardless of the type of certificate that you request, the certificate’s validation process always includes organization validation. Because SSL and Grid SSL certificates are issued to a domain, their validation processes also includes domain validation. Code Signing, Document Signing, Client, and Grid Premium and Robot certificates validation processes only include organization validation.

Once your domains and organizations have been pre-validated, future certificate issuance and renewals for that domain and organization can be done quickly for the associated validation types.

7.1.1 Organization Validation

To validate an organization, we first verify 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 is especially true with Extended Validation SSL and Extended Validation Code Signing Certificates, which require a series of extensive identity verifications.

7.1.2 Domain Validation

The aim of our 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 contact 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.

In cases where a domain is controlled by a third party (party other than the party requesting a certificate), simple methods are in place to quickly complete the process of getting approval to issue a certificate from the actual domain owner.

7.2 Managing Organizations

In your account, you cannot add domains for validation until you have added your organizations to which the domains are assigned and we have validated those organizations.

Managing organizations typically involves adding an organization and a validation contact. The validation contact is the individual we contact should we have any questions or problems validating the organization. Once an organization has been validated, organization management may involve authorizing the organization for specific certificates.

7.2.1 How to Add an Organization

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

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

3. On the **New Organization** page, in the **Organization Details** section, enter the following information about the organization:

Legal Name: Enter the organization’s legally registered name (i.e. *YourOrganization, Inc.*).

Assumed Name: If the organization has a DBA name (doing business as name), and they want it to appear on their certificates, enter the assumed name.

If the organization does not have a DBA or they do not want the assumed name to appear on their certificates, leave this box blank.

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.

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

State / Province / Region / County: Enter the state, province, region, or county where the organization is legally located.

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

4. In the **Validation Contact** section, enter the following information about the contact:

   We will contact this individual should we have any questions or problems validating the organization.

   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.

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

   The organization should be listed on the **Organizations** page (**Account > Organizations Validation**).

7.2.2 How to View Organizations and Their Details

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. Filter organizations by status.

   On the **Organizations** page, in the **Status** drop-down list, select **All**, **Active**, **Pending**, or **Inactive** to filter the organizations.

3. Filter organizations by Division.

   In the **Division** drop-down list, select the Division or Subdivision to filter the organizations.

4. Rearrange organizations by organization name or status.

   Click one of the column headers (**Name** or **Status**) to rearrange the order in which the organizations are listed.

5. To View Organization Details, Pending Validations, and Active Validations

   To the right of an organization, click **Manage** to view basic details about the organization, any pending certificate validations, and any active certificate validations.

7.2.3 How to Authorize Organizations for Certificates

After you add your organizations, you can 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 account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select **All**, **Active**, **Pending**, or **Inactive** to filter the organizations.

3. In the **Division** drop-down list, select the Division or Subdivision to filter the organizations.

4. To the right of an organization for which you want to authorize certificates, click **Manage**.

5. On the **"Organization's"** page, click **Submit for Validation**.

6. In the **Submit Organization for Validation** window, select the validation types for which the organization must be validated.

   - **OV - Normal Organization Validation**

- Grid - Public Grid Host Validation
- EV CS - Code Organization Extended Validation (EV CS)*
- EV - Extended Organization Validation (EV)**
- DS - Document Signing Validation
- CS - Code Signing Organization Validation***

7. *In the **EV CS Verified User** drop-down list, select an account user that you want to designate as an EV Code Signing Certificate request approver.

   Only an **EV CS Verified User** can approve EV Code Signing Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

   Note: The **EV CS Verified User** drop-down list box only appears if you checked **EV CS - Code Organization Extended Validation (EV CS)**.

8. **In the **EV Verified User** drop-down list, select an account user that you want to designate as an EV Certificate request approver.

   Only an **EV Verified User** can approve Extended Validation (EV) Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

   Note: The **EV Verified User** drop-down list box only appears if you checked **EV - Extended Organization Validation (EV)**.

9. ***In the **CS Verified User** drop-down list, select an account user that you want to designate as a Code Signing Certificate request approver.

   Only a **CS Verified User** can approve Code Signing Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

   Note: The **CS Verified User** drop-down list box only appears if you checked **CS - Code Signing Organization Validation**.

10. Click **Submit for Validation**.

    We will now validate the organization for the validation types that you selected.

7.2.4 (Non-ASCII Characters) How to Add and Authorize an Organization for Grid - Public Grid Host Validation

“Organization names on grid certificates can only contain ASCII type characters. This means that no accents, diacritical marks, non-English letters, or non-English punctuation are allowed. We have provided a conversion of your organization name that complies with this requirement for you to review and modify if needed.”

ASCII Character Note: You can use the following ASCII characters: United States ASCII letters (a thru z), all numbers, spaces, and the following special characters: **, . - _ @** (comma, period, dash, underscore, and at sign).

If you submit an Organization that contains non-ASCII characters in its name for **Grid – Public Grid Host Validation**, you will be asked to use a simplified version of the Organization name. This simplified version of the organization name appears in the details of the Grid Client and Grid Host SSL certificate types.

These instructions cover adding an organization (non-ASCII characters) and submitting the organization for Grid Public Host Validation.

Note:

You can use non-ASCII characters in the organization names when authorizing organizations for the following certificate types:

- OV - Normal Organization Validation
- EV - Extended Organization Validation (EV)
- DS - Document Signing Validation
- CS - Code Signing Organization Validation
- EV CS - Codes Signing Organization Extended Validation (EV CS)

The non-ASCII organization name appears in the details of the SSL, EV SSL, Document Signing, and Code Signing certificate types.

7.2.4.1 (Non-ASCII Characters) Adding an Organization

1. In your account, in the sidebar menu, click **Account > Organization Validation**.
2. On the **Organizations** page, click **+ New Organization**.
3. On the **New Organization** page, in the **Organization Details** section, enter the following information about the organization:

Legal Name: Enter the organization’s legally registered name, noting that it is okay to use non-ASCII characters (i.e. *¥ÃÆÇÊµìØþ*).

Assumed Name: If the organization has a DBA name (doing business as name), and they want it to appear on their certificates, enter the assumed name.

If the organization does not have a DBA or they do not want the assumed name to appear on their certificates, leave this box blank.

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.

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

State / Province / Region / County: Enter the state, province, region, or county where the organization is legally located.

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

4. In the **Validation Contact** section, enter the following information about the contact:

   We will contact this individual should we have any questions or problems validating the organization.

   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.

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

   The organization should be listed on the **Organizations** page (**Account > Organizations Validation**).

7.2.4.2 (Non-ASCII Characters) Authorizing an Organization for Grid – Public Grid Host Validation

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select **All**, **Active**, **Pending**, or **Inactive** to filter the organizations.

3. In the **Division** drop-down list, select the Division or Subdivision to filter the organizations.

4. To the right of an organization (non-ASCII characters) for which you want to authorize Grid – Public Grid Host certificate types, click **Manage**.

5. On the **"Organization's"** page, click **Submit for Validation**.

6. In the **Submit Organization for Validation** window, select **Grid - Public Grid Host Validation**.

7. In the ***Simplified Organization Name** box, review and modify the simplified organization name as needed (i.e. *AAeCEiOeth*).

8. Click **Submit for Validation**.

We will now validate the organization for the Grid - Public Grid Host validation type.

When ordering any type of Grid certificate (Client or SSL), the simplified organization name appears in the details of the certificate.

7.2.5 How to View the EV, EV Code Signing, and Code Signing Certificate Approvers for an Organization

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select **All**, **Active**, **Pending**, or **Inactive** to filter the organizations.

3. In the **Division** drop-down list, select the Division or Subdivision to filter the organizations.

4. To the right of an organization for which you want to view the **EV Verified**, **EV CS Verified Users**, and **CS Verified Users**, click **Manage**.

5. **EV Verified Users:**

   On the **"Organization's"** page, under **Pending Validation** or **Active Validation** (depending on whether the organization is validated yet), under **EV - Extended Organization Validation (EV)**, the **EV Verified Users** are listed.

6. **EV CS Verified Users:**

   On the **"Organization's"** page, under **Pending Validation** or **Active Validation** (depending on whether the organization is validated yet), under **EV CS - Code Signing Organization Validation**, the **EV CS Verified Users** are listed.

7. **CS Verified Users:**

On the **"Organization's"** page, under **Pending Validation** or **Active Validation** (depending on whether the organization is validated yet), under **CS - Code Signing Organization Validation**, the **CS Verified Users** are listed.

7.2.6 How to Add EV Certificate, EV Code Signing Certificate, and Code Signing Certificate Approvers for an Organization

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select **All**, **Active**, **Pending**, or **Inactive** to filter the organizations.

3. In the **Division** drop-down list, select the Division or Subdivision to filter the organizations.

4. To the right of an organization for which you want to add the **EV Verified** and **CS Verified Users**, click **Manage**.

5. On the **"Organization's"** page, click **Submit for Validation**.

6. **To Add an EV Verified User:**

   In the **Submit Organization for Validation** window, check **EV - Extended Organization Validation (EV)***.

7. **To Add an EV CS Verified User:**

   In the **Submit Organization for Validation** window, check **EV CS - Code Signing Organization Validation****.

8. **To Add a CS Verified User:**

   In the **Submit Organization for Validation** window, check **CS - Code Signing Organization Validation*****.

9. *****In the **EV Verified User** drop-down list, select an account user that you want to designate as an EV Certificate request approver.

   Only an **EV Verified User** can approve Extended Validation (EV) Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

   Note: The **EV Verified User** drop-down list box only appears if you checked **EV - Extended Organization Validation (EV)**.

10. ******In the **EV CS Verified User** drop-down list, select an account user that you want to designate as an EV Code Signing Certificate request approver.

    Only an **EV CS Verified User** can approve EV Code Signing Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

Note: The **EV CS Verified User** drop-down list box only appears if you checked **EV CS - Code Signing Organization Validation**.

11. *****In the **CS Verified User** drop-down list, select an account user that you want to designate as a Code Signing Certificate request approver.

    Only a **CS Verified User** can approve Code Signing Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

    Note: The **CS Verified User** drop-down list box only appears if you checked **CS - Code Signing Organization Validation**.

12. Click **Submit for Validation**.

    The EV Verified and CS Verified Users should be added to that **"Organization's"** page (**Account > Organization Validation**).

7.3 Managing Domains

Once an organization has been added, you can assign domains to an organization for validation. You can also select the type of authorization for which the domain should be validated.

Managing domains typically involves adding domains along with authorizing validation for the domains. Once a domain has been validated, domain management may involve authorizing additional validation types for which the domain must be validated.

7.3.1 How to Add a Domain and Authorize It for Certificates

1. In your account, in the sidebar menu, click **Account > Domain Validation**.

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

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

Organization:	In the drop-down list, select the organization to which the domain is assigned.
Domain Name:	Enter the domain name for which certificates will be requested (i.e. *example.domain.com*).

4. Under **Authorization**, check the validation types for which the domain must be validated.

   - **OV - Normal Organization Validation**
   - **Grid - Public Grid Host Validation**
   - **EV - Extended Organization Validation (EV)***

5. ***In the EV Verified User** drop-down list, select an account user that you want to designate as an EV Certificate requests approver.

   Only an **EV Verified User** can approve Extended Validation (EV) Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

   Note: The **EV Verified User** drop-down list box only appears if you checked **EV - Extended Organization Validation (EV),** and the organization that you selected earlier (step 3) has not been pre-authorized for **EV-Extended Organization Validation (EV)**.

6. When you are finished, click **Save Domain**.

   The domain should be listed on the **Domains** page (**Account > Domain Validation**). We will now validate the domain for the validation types that you selected.

7.3.2 How to View Domain Details, Validation Status, and Validation Progress

1. In your account, in the sidebar menu, click **Account > Domain Validation**.

2. In the **Division** drop-down list, select the Division or Subdivision to filter the domains.

3. Rearrange domains by organization name, domain name, date the domain was added, validations, or pending validations.

   On the **Domains** page, click one of the column headers (**Organization**, **Domain Name**, **Date Added**, **Validated For**, or **Pending Validation For**) to rearrange the order in which the organizations are listed.

4. To View Domain Details, Validation Status, and Validation Progress

   To the right of a domain, click **View** to view basic details about the domain, active validation status (pending or active), domain validation progress, and domain approval required actions.

7.3.3 How to Authorize a Domain for Additional Certificate Types

1. In your account, in the sidebar menu, click **Account > Domain Validation**.

2. On the **Domains** page, in the **Division** drop-down list, select the Division or Subdivision to filter the domains.

3. To the right of the domain for which you want to authorize additional certificate types, click **View**.

4. On the **"Domain's"** page, click **Submit for Validation**.

5. In the **Submit Domain for Validation** window, check the validation types for which the domain must be validated.

- **OV - Normal Organization Validation**
- **Grid - Public Grid Host Validation**
- **EV - Extended Organization Validation (EV)***

6. ***In the EV Verified User** drop-down list, select an account user that you want to designate as an EV Certificate requests approver.

   Only an **EV Verified User** can approve an Extended Validation (EV) Certificate request. Note that only users with a job title and valid telephone number appear in the drop-down list.

   Note: The **EV Verified User** drop-down list box only appears if you checked **EV-Extended Organization Validation (EV),** and the organization listed under **Details** has not been pre-authorized for **EV-Extended Organization Validation (EV)**.

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

   We will now validate the domain for the additional validation types that you selected.

7.3.4 How to View the Domains Validations (Pending or Active)

Use this instruction if you need to see what types of certificates you can order for a domain,

1. In your account, in the sidebar menu, click **Account > Domain Validation**.
2. On the **Domains** page, in the **Division** drop-down list, select the Division or Subdivision to filter the domains.
3. To the right of a domain that you need to see the types of certificates you can order, click **View**.
4. On the **"Domain's"** page, under **Pending Validation** or **Active Validation** (depending on whether the domain is validated yet), the types of validation are listed.

   - **OV - Normal Organization Validation**

     For this validation type, you can order SSL Plus, Unified Communications, and Wildcard Plus Certificates.

   - **Grid - Public Grid Host Validation**

     For this validation type, you can order Grid Host SSL and Grid Host SSL UC Certificates.

   - **EV - Extended Organization Validation (EV)**

     For this validation type, you can order EV SSL Plus and EV Multi-Domain Certificates

Note: Although it may appear that the EV Verified Users are for the domain, they are not. The EV Verified Users that are listed are for the organization and can approve EV Certificates for any of the applicable domains assigned to their organization.

7.3.5 Domain Name System (DNS) Validation

If you'd like to enable DNS-based domain validation for your organization or the organization's you service, please contact support@digicert.com so that we can enable it for you.

8 Limit Products

You can use the Limit Products feature to regulate the products that a specific role (in your DigiCert account) can order. In addition, you can also regulate the validity period of the certificates the role can order.

Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or in your account altogether. For example, if you do not want divisions to set up their own product limitations, you may not see some of the inheritability selections in your account.

8.1 Configuring Product Limitations

These instructions are for administrators only and explain how to configure your product limitations for your DigiCert account.

Permissions Note:

Only administrators can view the **Limit Products** page and can configure product limitations for their division, subdivision, account users, and account admins.

8.1.1 How to Turn On Limit Products

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

   Subdivision Admins Note:

   If your Division Admin already set up product limitations for your subdivision but granted you permission to set up your own product limitations, on the **Limit Products** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Limit Products** page, under **Limit Products**, check **Restrict the products that users with different roles can order**.

3. **Set Permissions:**

   Note: If you don't have subdivisions, then you don't see the **"Use this setting for"** settings.

   On the **Limit Products** page, do any of the following things:

Use this setting for my division

Select this option if you want the product limitations that you place on users and/or admins to apply to your division only.

When your subdivision admins navigate to the **Limit Product** page (**Settings > Limit Products**), they control whether product limitations are enabled.

Use this setting for my division and any subdivisions

Select this option if you want the product limitations that you place on users and/or admins to apply to your division and all subdivisions.

When your subdivision admins navigate to the **Limit Products** page (**Settings > Limit Products**), they receive the ***"These settings have been set by another division. To update these settings, please contact your account administrator."*** message.

Allow subdivisions to override this setting

Check this box if you want your subdivisions to be able to configure their own product limitations.

When your subdivision admins navigate to the **Limit Products** page (**Settings > Limit Products**), they are presented with the following options:

- **Use Default Settings**

  If the admin clicks this option, product limitations are enabled for their division, and they defer to the limitations that you placed on users and/or admins for them.

- **Use My Own Settings**

  If the admin clicks this option, they control whether product limitations are enabled. They are required to place their own product limitations on the users and admins for their division.

4. You have successfully turned on **Limit Products** for your DigiCert account, and you are ready to configure your product limitations.

8.1.2 How to Turn Off Limit Products

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

   Subdivision Admins Note:

   If your Division Admin already set up product limitations for your subdivision but granted you permission to set up your own product limitations, on the **Limit Products** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Limit Products** page, under **Limit Products**, uncheck **Restrict the products that users with different roles can order**.

3. **Set Permissions:**

   Note: If you don't have subdivisions, then you don't see the **"Use this setting for"** settings.

   On the **Limit Products** page, do any of the following things:

Use this setting for my division	Select this option if you want to disable **Limit Products** for your division only. When your subdivision admins navigate to the **Limit Products** page (**Settings > Limit Products**), they control whether **Limit Products** is disabled.

Use this setting for my division and any subdivisions

Select this option if you want to disable **Limit Products** for your division and all subdivisions.

When your subdivision admins navigate to the **Limit Products** page (**Settings > Limit Products**), they receive the ***"These settings have been set by another division. To update these settings, please contact your account administrator."*** message.

Allow subdivisions to override this setting

Check this box if you want your subdivisions to be able to disable **Limit Products** for themselves.

When your subdivision admins navigate to the **Limit Products** page (**Settings > Limit Products**), they are presented with the following options:

- **Use Default Settings**

  If the admin clicks this option, **Limit Products** is disabled for their division, and they defer to the limitations that you placed on users and/or admins for them.

- **Use My Own Settings**

  If the admin clicks this option, they control whether **Limit Products** are enabled. They are required to place their own product limitations on the users and admins for their division.

4. You successfully turned off the Limit Products for your DigiCert account.

8.1.3 How Set Up Product Limitations for the User and Administrator Roles

When setting up product limitations for the User and Admin Roles, you can limit the products these roles can order, and you can limit the validity period for the certificates they can order.

For example, you can prevent the User role from ordering Grid Certificates and prevent them from ordering one and two year Code Signing, EV Code Signing, and Document Signing Certificates.

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

Subdivision Admins Note:

If your Division Admin already set up product limitations for your subdivision but granted you permission to set up your own product limitations, on the **Limit Products** page, under **Use default settings**, click **Use My Own Settings**.

2. On the **Limit Products** page, under **Choose Products**, click **Administrator** or **User** to regulate the certificates and/or validity periods of the certificates for which that the role can order.

3. How to Prevent Specific Certificates from Being Ordered

   a. Under the **Administrator** or **User** role, locate the product and uncheck all validity periods for the certificate (**One Year**, **Two Year**, and **Three Year**).

   b. Example 1: If you want to prevent the User role from ordering Grid Certificates, uncheck **One Year** for **Grid Host SSL**, **Grid Host SSL UC**, **Grid Premium**, **Grid Robot Email**, **Grid Robot FQDN**, and **Grid Robot Name**.

   c. Example 2: If you want to prevent the Administrator role from ordering Code Signing and EV Code Signing Certificates, uncheck **One Year**, **Two Year**, and **Three Year** for **Code Signing** and **EV Code Signing**.

   d. Example 3: If wanted to prevent the User role from ordering any certificates, uncheck the **One Year**, **Two Year**, and **Three Year** column headings. This unchecks the one-year, two-year, and three-year options for all certificates.

4. How to Regulate Validity Periods

   a. Under the **Administrator** or **User** role, locate the product and uncheck the validity periods that you want to prevent them from ordering (**One Year**, **Two Year**, or **Three Year**).

   b. Example 1: If you want to prevent the Administrator role from ordering one year **SSL Plus**, **Unified Communications**, and **Wildcard Plus** Certificates, uncheck **One Year** for those certificates.

   c. Example 2: If you want to prevent the Administrator role from ordering any three-year certificates, uncheck the **Three Year** column heading. This unchecks the three-year option for all certificates.

5. When you are finished, scroll to the bottom of the **Limit Products** page and click **Save Settings**.

   You have successfully set up limitations for certificates and validity periods.

8.1.4 How to View Certificate and Validity Restrictions for the User and Administrator Role

You can only see the product limitations that you set up for your Division/Subdivision. You cannot see the product limitations for another Division.

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

2. On the **Limit Products** page, under **Choose Products**, click **Administrator** or **User** to see the certificates and/or validity periods restrictions setup for the role.

9 Certificate Management

Before you start to use your DigiCert account, work with your account representative to set up your account structure (Divisions and Subdivisions) and permissions. Depending on how your account is structured, some of the features discussed in this section may not be included in your Division, Subdivision, or your account altogether.

After we vet your organizations and pre-validate their domains and subdomains for the types of certificates authorized, you can start requesting, approving, receiving, and installing/configuring your certificates.

9.1 Requesting Certificates

The certificate lifecycle begins when administrators and users log into their account and request certificates for their assigned domains and subdomains, for signing code, and for authentication. Account users can only request the types of certificates that have been authorized for their organization and the domains and/or subdomains assigned to their Division or Subdivision.

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

- **SSL Certificates**
  EV Multi-Domain, EV SSL Plus, Unified Communications, SSL Plus, and Wildcard Plus

- **Grid Certificates**
  Grid Premium, Grid Robot Email, Grid Robot FQDN, Grid Robot Name, Grid Host SSL, and Grid Host SSL UC

- **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)

9.1.1 How to Request an SSL Plus, EV SSL Plus, EV Multi-Domain, Unified Communications and a Wildcard Plus Certificate

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

- Create your Certificate Signing Request (CSR).
- Fill out the request form.

- Wait for approval.

The form for requesting each type of SSL Certificate is similar. For this reason, we will provide instructions for ordering an SSL Certificate and note any differences between the different types of SSL Certificate request forms.

You can use this instruction for the following certificates:

- EV Multi-Domain
- EV SSL Plus
- SSL Plus
- Unified Communications
- Wildcard Plus

How to Request an SSL Certificate

1. Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Request a Certificate** page, select **SSL Certificates**.

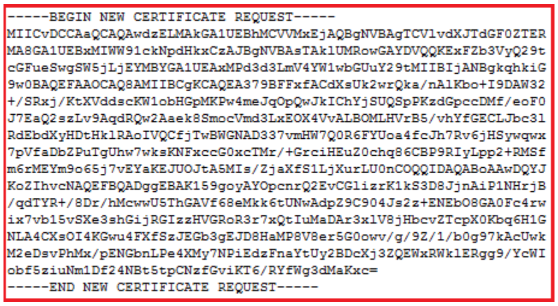
4. On the **SSL Certificates** tab, select one of the available certificates and then, click **Order Now**.

5. **Paste your CSR**

   On the **Request "certificate name"** page, under **Certificate Settings**, in the **Paste your CSR** box, do one of the following:

   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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

6. Common Name

   After uploading your CSR, the **Common Name** box should be prepopulated with the common name from the CSR and the organization to which the domain is assigned populates the **Organization** field.

   If you have not uploaded your CSR yet, under **Common Name**, do one of the following:

   - **If securing a pre-validated domain**

     Expand **Show Available Domains** and select one of the pre-validated domains or subdomains (i.e. *example.com (Organization Name)* or *mail.example.com (Organization Name)*).

     The selected domain name is entered in the **Common Name** box, and the organization to which the domain is assigned populates the **Organization** field.

   - **If securing a non-validated domain**

     In the box, enter the domain that you want to secure. Note that because you are using a non-validated domain, certificate issuance may take a bit longer while we validate the domain.

     Note that because you are using a non-validated domain, the **Organization** field will not auto populate.

   ### For an EV Multi-Domain Certificate:

   The common name is listed as the first SAN (subject alternative name) name in the certificate.

   ### For a Unified Communications Certificate:

   The common name is listed as the first SAN (subject alternative name) name in the certificate.

   ### For a Wildcard Plus Certificate:

The common name would be **.example.com*.

7. **Organization**

   In the **Organization** drop-down list, select the Organization to which the domain is assigned.

8. **Other Hostnames (SANs)**

   For EV Multi-Domain, and Unified Communications Certificates

   In the **Other Hostnames (SANs)** box, enter additional hostnames (i.e. *example2.com*, *example3.net*, *mail.example.net*) that you want your EV Multi-Domain or Unified Communications Certificate to secure.

   (Optional) For Wildcard Plus Certificates

   In the **Other Hostnames (SANs)** box, enter additional hostnames (i.e. *example2.com*, *example3.net*, *mail.example.net*) that you want your Wildcard Certificate to secure.

   Wildcard Plus Certificates only secure the first level of subdomains. To really secure your entire domain, specify SANs as many level deep as you need.

   Some mobile clients, including Windows Mobile 5, do not support wildcards, but they do support Subject Alternative Names. If you want to be Windows Mobile 5 compliant, add SANs to your Wildcard Certificate.

9. Next, enter the following information:

   Organization Unit: Enter the name of your department, group, etc.

   Validity Period: Select a validity period for the certificate: **1 Year**, **2 Years**, **3 Years**, or **Custom Expiration Date**).

   For EV SSL Plus and EV Multi-Domain Certificates:

   The maximum validity period is **2 Years**.

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

10. In the **Order Information** section, do the following:

    Server Platform: Select the server on which the CSR was generated.

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

These comments are not meant to be included in the certificate.

11. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

    An email should be sent notifying the admins or EV Certificate approvers that there is a certificate request that needs their approval.

    On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.1.2 How to Request a Grid Host SSL and Grid Host SSL UC Certificate

The process for requesting Grid Host SSL and Grid Host SSL UC Certificates is the same:

- Create your Certificate Signing Request (CSR).
- Fill out the request form.
- Wait for approval.

The form for requesting the Grid Host SSL Certificate and Grid SSL UC Certificate is similar. For this reason, we will provide instructions for requesting a Grid Host SSL Certificate and note any differences between the Grid Host SSL Certificate and the Grid Host SSL UC Certificate request forms.

You can use this instruction for the following certificates:

- Grid Host SSL
- Grid Host SSL UC

How to Request a Grid Host SSL Certificate

1. Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

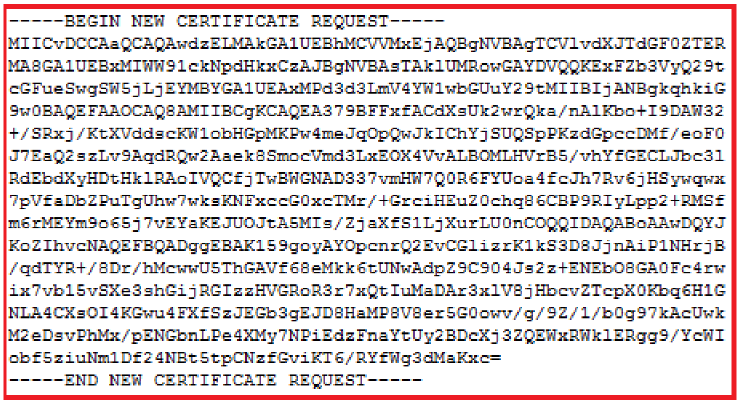
3. On the **Request a Certificate** page, select **Grid Certificates**.

4. On the **Grid Certificates** tab, select **Grid Host SSL** and then, click **Order Now**.

5. **Paste your CSR**

On the **Request Grid Host SSL Certificate** page, under **Certificate Settings**, in the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

6. **Service / Common Name**

Under **Service / Common Name** section do the following:

i. In the **Service** box, enter the service that you want to use to connect to the grid server.

ii. After uploading your CSR, the **Common Name** box should be prepopulated with the common name from the CSR and the organization to which the domain is assigned populates the **Organization** field.

If you have not uploaded your CSR yet, under **Common Name**, do one of the following:

- **If securing a pre-validated domain**

  Expand **Show Available Domains** and select one of the pre-validated domains or subdomains (i.e. *example.com (Organization Name)* or *mail.example.com (Organization Name)*).

  The selected domain name is entered in the **Common Name** box, and the organization to which the domain is assigned populates the **Organization** field.

- **If securing a non-validated domain**

  In the box, enter the domain that you want to secure. Note that because you are using a non-validated domain, certificate issuance may take a bit longer while we validate the domain.

  Note that because you are using a non-validated domain, the **Organization** field will not auto populate.

For a Grid Host SSL UC Certificate:

The common name is listed as the first SAN (subject alternative name) name in the certificate.

7. **Organization**

   In the **Organization** drop-down list, select the Organization to which the domain is assigned.

8. **Other Hostnames (SANs)**

   For a Grid Host SSL UC Certificate

   In the **Other Hostnames (SANs)** box, enter additional hostnames (i.e. *www.example2.com*, *www.example3.net*, *mail.example.net*) that you want your Grid Host SSL UC Certificate to secure.

9. Next, enter the following information:

   Validity Period: Select a validity period for the certificate: **1 Year**.

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

10. Under **Order Information**, do the following:

    Server Platform: Select the server on which the CSR was generated.

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

11. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

    An email should be sent notifying the admins that there is a certificate request that needs their approval.

On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.1.3 How to Request a Client Certificate

The process for requesting any of the Client Certificates is the same:

- **(Optional)** Create your Certificate Signing Request (CSR).
- Fill out the request form.
- Wait for approval.

The form for requesting any of the Client Certificates is similar. For this reason, we will provide instructions for requesting a Premium Certificate and note any differences between the Premium Certificate request form and the other Client Certificate request forms.

You can use this instruction for the following certificates:

- Digital Signature Plus
- Email Security Plus
- Premium

How to Request a Premium Client Certificate

1. (Optional) If required, create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Request a Certificate** page, click **Client Certificates**.

4. On the **Client Certificates** tab, select **Premium** and then click **Order Now**.

5. On the **Request a Client Certificate** page, under **Certificate Settings**, enter the following settings information:

Validity Period:	In the drop-down list, select a validity period for the certificate: (**3 Years**, **2 Years**, or **1 Year**).
Organization:	In the drop-down list, select the organization for which you are requesting the Client Certificate. The organization's name appears on your Client Certificate.

Organization Unit: Enter the name of your department, group, etc.

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

6. Under **Order Options**, in the **Automatic Renewal** drop-down list, select how often you want the certificate to be automatically renewed.

7. Under **Certificate(s) to Request** , enter the following **Recipient Details**:

Recipient Name Enter the recipient's name (i.e. *John Doe*) as you want it to appear on the Client Certificate.

Recipient Email Enter the recipient's email address (i.e. *john.doe@example.com*) that you want to appear on the Client Certificate.

This email address is used to send the recipient an email so that they can generate their Client Certificate.

Multiple Email Addresses Note:

You can enter multiple email addresses if needed; note that all the email addresses appear on the Client Certificate.

When entering multiple email addresses, make sure to use commas to separate them (i.e. *john.doe@example.com*, *john.doe@example2.com*, *jdoe@example3.com*).

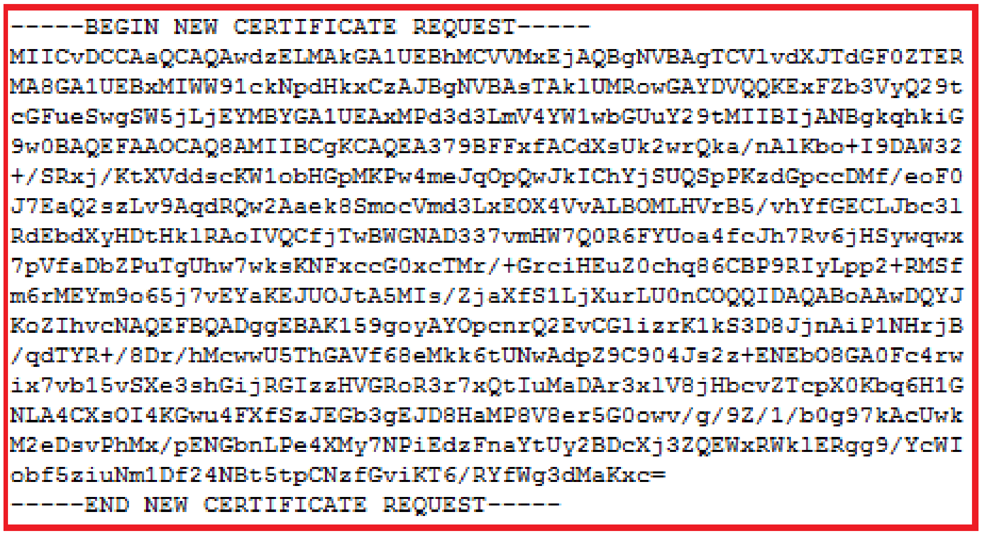
The first email address listed is used to send the recipient an email so that they can generate their Client Certificate.

8. **(Optional)** If you need to use a CSR to create your certificate, in the **Recipient CSR (optional)** box, do one of the following:

CSR Note: Only the Public Key embedded in the CSR is use to create your Client Certificate. All other fields in the CSR are ignored.

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

9. To add additional Client Certificate recipients, click **Add Another Certificate** and enter the recipient's **Recipient Details**.

10. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

11. When you are finished, click **Submit Request**.

12. You should be taken to the certificate's **Manage Order #** page where you can see the status of the email address verifications. Each of the email addresses listed in the certificate request is sent an email that contains a link so that the recipient can validate that they own that email address. If the certificate recipient loses a validation email, you can resend it. See How to Resend an Email Validation for DigiCert "Client Certificate" Email.

    On the **Orders** page (**Orders > Certificate Orders**), the certificate should be listed with the **Status** of **Pending**.

13. After all email addresses are validated, the **Create Your DigiCert "Client Certificate"** email is sent to the first email address on the list so that the recipient can create their Client Certificate. If the certificate recipient loses the certificate creation email, you can resend it. See How to Resend the Create Your DigiCert "Client Certificate" Email.

    After the recipient creates the Client Certificate, on the **Orders** page (**Orders > Orders**), the certificate should be listed with the **Status** of **Issued**.

    CSR Note:

    If you submitted a CSR, you do not receive an email with a link to create your Client Certificate. Instead, you need to download your Client Certificate from your account. See How to Download a Certificate.

After the recipient validates their email address(es) and their Client Certificate has been issued, on the **Orders** page (**Orders > Certificate Orders**), the certificate should be listed with the **Status** of **Issued**.

9.1.4 How to Request Grid Robot and Grid Premium Certificates

The process for requesting any of the Grid Robot Certificates and the Grid Premium Certificate is the same:

- Fill out the request form.
- Wait for approval.

The form for requesting any of the Grid Robot and Grid Premium Certificates is similar. For this reason, we will provide instructions for requesting a Grid Premium Certificate and note any differences between the Grid Premium Certificate request form and the Grid Robot Certificate request forms.

You can use this instruction for the following certificates:

- Grid Premium
- Grid Robot Email
- Grid Robot FQDN
- Grid Robot Name

How to Request a Grid Premium Client Certificate

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

2. On the **Request a Certificate** page, click **Grid Certificates**.

3. On the **Grid Certificates** tab, select **Grid Premium** and then click **Order Now**.

4. On the **Request a Client Certificate** page, under **Certificate Settings**, enter the following settings information:

   Validity Period: In the drop-down list, select **1 Year**.

   Organization: In the drop-down list, select the organization for which you are requesting the Client Certificate.

   The organization's name appears on your Client Certificate.

Organization Unit: Enter the name of your department, group, etc.

For Grid Robot Email, Robot FQDN, and Robot Name Certificates:

The Organization Unit field is not required.

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

5. Under **Order Options**, in the **Automatic Renewal** drop-down list, select how often you want the certificate to be automatically renewed.

6. Under **Certificate(s) to Request** , enter the following **Recipient Details**:

Recipient Name Enter the recipient's name (i.e. *John Doe*) as you want it to appear on the Client Certificate.

Recipient Email Enter the recipient's email address (i.e. *john.doe@example.com*) that you want to appear on the Client Certificate.

This email address is used to send the recipient an email so that they can generate their Client Certificate.

For Grid Robot Email:

Only the recipients email address is required.

Recipient Email Enter the recipient's email address (i.e. *john.doe@example.com*) that you want to appear on the Client Certificate.

This email address is used to send the recipient an email so that they can generate their Client Certificate.

For Grid Robot FQDN:

FDQN Enter the recipient's fully qualified domain name (FQDN) that you want to appear on the Client Certificate.

Recipient Email Enter the recipient's email address (i.e. *john.doe@example.com*) that you want to appear on the Client Certificate.

This email address is used to send the recipient an email so that they can generate their Client Certificate.

7. To add additional Client Certificate recipients, click **Add Another Certificate** and enter the recipient's **Recipient Details**.

8. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

9. When you are finished, click **Submit Request**.

10. You should be taken to the certificate's **Manage Order #** page where you can see the status of the email address verifications. The email address entered in the certificate request is sent an email that contains a link so that the recipient can validate that they own that email address. If the certificate recipient loses a validation email, you can resend it. See How to Resend the Email Validation for DigiCert "Client Certificate" Email.

    On the **Orders** page (**Orders > Certificate Orders**), the certificate should be listed with the **Status** of **Pending**.

11. After the email address is validated, the **Create Your DigiCert "Client Certificate"** email is sent to that email address so that the recipient can create their Client Certificate. If the certificate recipient loses the certificate creation email, you can resend it. See How to Resend the Create Your DigiCert "Client Certificate" Email.

    After the recipient creates the Client Certificate, on the **Orders** page (**Orders > Certificate Orders**), the certificate should be listed with the **Status** of **Issued**.

9.1.5 How to Resend an Email Validation for DigiCert "Client Certificate" Email

If a Client Certificate recipient deletes or loses an **Email Validation for DigiCert "Client Certificate"** email before they validate that email address, you can resend that email.

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

2. On the **Orders** page, in the **Status** drop-down list, select **Pending** to see only the certificates that have not been issued.

3. In the **Division** drop-down list, select the Division to filter the list of pending certificates.

4. To the right of the Client Certificate for which you need to resend the **Email Validation for DigiCert "Client Certificate"** email, click **View**.

5. On the **Manage Order #** page, on the **Email Addresses** line, below or to the right of the validation email that you need to resend, click the (**Resend**) link.

    Multiple Email Addresses Note:

    If the Client Certificate recipient has multiple email addresses listed in their request form, you can resend any or all of the validation emails.

6. The link should change to **(Sent)**. The **Email Validation for DigiCert "Client Certificate"** email is resent to the Client Certificate recipient to the specified address with a new link, which lets them validate that email address.

9.1.6 How to Resend the Create Your DigiCert "Client Certificate" Email

If a Client Certificate recipient deletes or loses the **Create Your DigiCert "Client Certificate"** email before they create their Client Certificate, you can resend that email.

1. In your account, in the sidebar menu, click **Orders > Certificate Orders**.
2. On the **Orders** page, in the Status drop-down list, select **Pending** to see only the certificates that have not been issued.
3. In the **Division** drop-down list, select the Division to filter the list of pending certificates.
4. To the right of the Client Certificate for which you need to resend the **Create Your DigiCert "Client Certificate"** email, click **View**.
5. On the **Manage Order #** page, on the **Email Addresses** line, below or to the right of the recipient's email address, click the (**Resend**) link.

   Multiple Email Addresses Note:

   Although the recipient can validate multiple email addresses, the **Create Your DigiCert "Client Certificate"** email can only be sent to the first email address listed.

6. The link should change to **(Sent)**. The **Create Your DigiCert "Client Certificate"** email is resent to the Client Certificate recipient with a new link, which lets them create their Client Certificate.

   Note: As soon as you resend the email, the old link expires and cannot be used to create the Client Certificate. 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."

9.1.7 How to Request a Code Signing Certificate

The process for requesting a Code Signing Certificate is as follows:

- **For Sun Java Platform Only:** Create your Certificate Signing Request (CSR).
  Sun Java is the only platform for which you are required to submit a CSR.
- Fill out the request form.
- Wait for approval.

How to Request a Code Signing Certificate

1. **For Sun Java Platform Only:** Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Request a Certificate** page, click **Code Signing**.

4. On the **Code Signing** tab, select **Code Signing** and then, click **Order Now**.

5. On the **Request Code Signing Certificate** page, under **Certificate Settings** section, enter the following settings information:

   Organization: In the drop-down list, select the organization for which you are requesting the Code Signing Certificate.

   Note: The organization's name appears on your Code Signing Certificate.

   Organization Unit: Enter the name of your department, group, etc.

   Validity Period: Select a validity period for the certificate: **1 Year**, **2 Years**, or **3 Years**.

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

   Subject Email:

   - Click **Show Available Domains** to see the validated domains.

     The email address that you provide must have a validated domain.

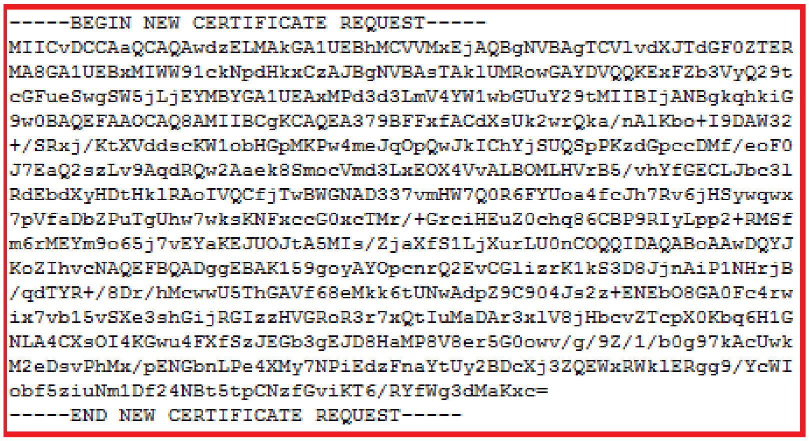
   - Then, enter the email address that you want to appear as the subject on the Code Signing Certificate.

     The email address that you provide is visible when viewing your signature on an application/code that you sign.

6. Under **Order Options**, in the **Server Platform** box, select the platform for which the Code Signing Certificate is to be used.

7. **(Sun Java Platform only)** In the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKWlobHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

8. In the **Comments to Administrator** box, enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc.

9. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

    An email should be sent notifying the CS Certificate approvers that there is a certificate request that needs their approval.

    On the **Request** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.1.8 How to Request an EV Code Signing Certificate

The process for requesting an EV Code Signing is as follows:

- Fill out the request form.
- Wait for approval.

How to Request an EV Code Signing Certificate

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

2. On the **Request a Certificate** page, click **Code Signing**.

3. On the **Code Signing** tab, select **EV Codes Signing** and then, click **Order Now**.

4. On the **Request EV Code Signing Certificate** page, enter the following settings information:

Organization: In the drop-down list, select the organization for which you are requesting the Code Signing Certificate.

Note: The organization's name appears on your Code Signing Certificate.

Organization Unit: Enter the name of your department, group, etc.

Validity Period: Select a validity period for the certificate: **1 Year**, **2 Years**, or **3 Years**.

5. Under **Provisioning Options**, select an EV Code Signing Certificate provision option and complete the necessary steps for that option:

   - **Preconfigured Hardware Token**

     Select this option if you want DigiCert to install your EV Code Signing Certificate on a secure token and then ship it to you. See Currently Supported eTokens.

     After selecting this option, enter your **Shipping Information**: your name and the address to which you want the token to be sent.

   - **Use Existing Token**

     Select this option if you already have a supported hardware token and want to install your EV Code Signing Certificate on that token yourself. See Currently Supported eTokens.

     After selecting this option, in the **Platform** drop-down list, select the hardware token on which you will be installing your EV Code Signing Certificate.

   - **Install on HSM**

     Select this option if you want to down load the EV Code Signing Certificate and install it on your HSM device yourself.

     If you select this option, you are required to provide audit documentation to DigiCert demonstrating that you are qualified. Only then can we issue your EV Code Signing Certificate.

     After selecting this option, do the following:

     i. Create your CSR.

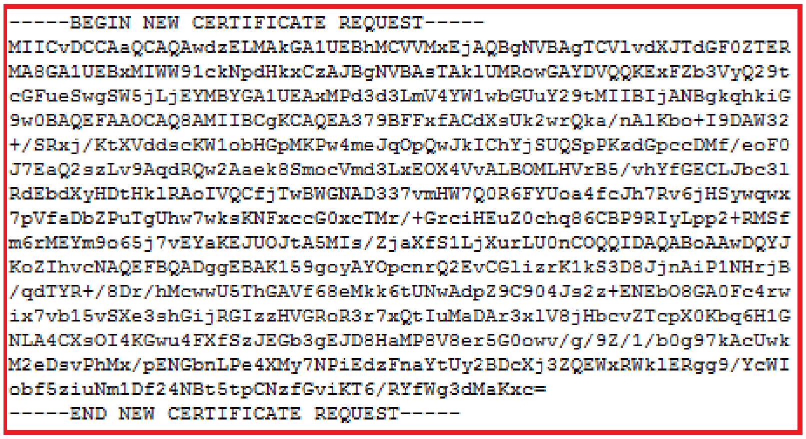
        Note: To remain secure, certificates must use 2048-bit keys.

To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

ii. In the **Select Platform** box, select the platform on which you will be installing your EV Code Signing Certificate.

iii. In the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

6. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

   An email should be sent notifying the EV Certificate approvers that there is a certificate request that needs their approval.

   On the **Request** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.1.9 How to Request a Document Signing Certificate

The process for requesting any of the Document Signing certificates is the same:

- Fill out the request form.
- Wait for approval.

Because the request form is the same for all Document Signing certificates, you can use this instruction for the following certificates:

- Document Signing - Organization (2000)
- Document Signing - Organization (5000)

How to Request Document Signing Certificate - Organization Certificate

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

2. On the **Request a Certificate** page, click **Document Signing**.

3. On the **Document Signing** tab, select a **Document Signing - Organization** certificate and then, click **Order Now**.

4. On the **Request Document Signing Certificate – Organization Certificate** page, under **Certificate Settings**, enter the following settings information:

   Organization: In the drop-down list, select the organization to which the document signing certificate requestor belongs.

   For example, if you are ordering a Document Signing certificate for Jane Doe in Legal, select the Organization to which she belongs.

   Note: The organization's name does not appear on the Document Signing certificate.

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

   Validity Period: Select a validity period for the certificate: (**3 Years**, **2 Years**, or **1 Year**).

5. Under **Provisioning Options**, select a Document Signing Certificate provision option and complete the necessary steps for that option:

   - **Preconfigured Hardware Token**

     Select this option if you want DigiCert to install your Document Signing Certificate on a secure token and then ship it to you. See Currently Supported eTokens.

     After selecting this option, enter the Document Signing certificate recipient's **Shipping Information**: the name and the address to which you want the token to be sent.

   - **Use Existing Token**

Select this option if you already have a supported hardware token and want to install your Document Signing Certificate on that token yourself. See Currently Supported eTokens.

After selecting this option, in the **Platform** drop-down list, select the hardware token on which you will be installing your Document Signing Certificate.

6. Under **Subject Information**, enter the following information for the certificate requestor:

Person's Full Name Enter the name to appear on the Document Signing certificate. For example, if you are the requestor, enter your name. If you are requesting the certificate for Jane Doe in Legal, enter her name.

Note: The person's full name appears on the Document Signing certificate.

Phone: Enter a phone number at which the individual can be reached.

Email: Enter an email address at which the individual can be reached.

Job Title: Type the user's job title.

7. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

   An email should be sent notifying the admins that there is a certificate request that needs their approval.

   On the **Request** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.1.10 How to Add Multiple Wildcard Domains to a Certificate

If you need to request a certificate with multiple Wildcard domains, please contact support@digicert.com so that we can create that certificate for you.

9.2 Managing Certificate Request Approvals and Rejections

After a user requests a certificate, an Administrator, an EV Verified User, or a 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, an EV Verified User, or a CS Verified User can also reject the certificate request, if needed. For example, if the user ordered the wrong type of certificate.

9.2.1 How to View Certificate Requests

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

2. Filter certificates by **Status**.

   On the **Requests** page, in the **Status** drop-down list, select **Pending**, **Approved**, **Rejected**, or **All** to filter the certificates.

3. Filter certificates by **Type**.

   In the **Type** drop-down list, select **All**, **New Request**, **Reissue**, **Revoke**, or **Duplicate** to filter the certificates.

4. Filter certificates by **Division**.

   In the **Division** drop-down list, select the Division or Subdivision to filter the certificates.

5. Rearrange certificates by order number, common name, certificate type, certificate status, Division or Subdivision, certificate request date, or certificate requester.

   Click one of the column headers (**Order ID**, **Common Name**, **Type**, **Status**, **Division**, **Requested**, or **Requester**) to arrange the order in which the certificate requests are listed.

6. To view the certificate request details, to the right of a certificate request click **View**.

9.2.2 How to Edit a Certificate Request

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

2. On the **Requests** page, in the **Division** drop-down list, select a division to filter the list of requests.

3. In the **Status** drop-down list, select **Pending** to see only the certificates that need approval.

4. In the **Type** drop-down list, select a type to further filter the list of requests.

5. To the right of the certificate that you want to edit, click **View**.

6. On the **"Certificate's" Request** page, click **Edit**.

7. On the **Edit Certificate Request** page, edit, add, or remove information as required.

8. In the **Comments to Administrator** box, enter a reason for the edits.

9. When you are finished, click **Update Certificate Request**.

9.2.3 How to Approve a Certificate Request

Only an **EV Verified User** can approve EV SSL Plus, EV Multi-Domain, and EV Code Signing 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.

10. In your account, in the sidebar menu, click **Orders > Certificate Requests**.

11. On the **Requests** page, in the **Division** drop-down list, select a division to filter the list of requests.

12. In the **Status** drop-down list, select **Pending** to see only the certificates that need administrator approval.

13. In the **Type** drop-down list, select a type to further filter the list of requests.

14. To the right of the certificate that you want to approve, click **View**.

15. On the **"Certificate's" Request** page, review the information (such as who requested the certificate and their division), verifying that it is correct, and then click **Approve**.

    Note: If the certificate request was submitted through a guest URL, the request info is highlighted yellow.

16. In the **Approve Request** window, enter an **Approval Comment** and then, click **Approve**.

    On the **Orders** page (**Orders > Certificate 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.

9.2.4 How to View Who Requested a Certificate (Approved Requests)

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

2. On the **Requests** page, in the **Status** drop-down list, select **Approved** to see all approved certificate requests.

3. In the **Type** drop-down list, select a certificate type (**All**, **New Request**, **Reissue**, **Revoke**, **or Duplicate**) to filter the list of approved requests.

4. In the **Division** drop-down list, select a division to further filter the list of approved certificate requests.

5. To the right of the requests for which you want to view the requestor, click **View**.

6. On the **"Certificate" Request** page, under **Request Info**, you should be able to see who the certificate was **Requested By**.

9.2.5 How to View Who Approved a Certificate Request (Approved Requests)

7. In your account, in the sidebar menu, click **Orders > Certificate Requests**.

8. On the **Requests** page, in the **Status** drop-down list, select **Approved** to see all approved certificate requests.

9. In the **Type** drop-down list, select a certificate type (**All**, **New Request**, **Reissue**, **Revoke**, **or Duplicate**) to filter the list of approved requests.

10. In the **Division** drop-down list, select a division to further filter the list of approved certificate requests.

11. To the right of the requests for which you want to view the approver, click **View**.

12. On the **"Certificate" Request** page, under **Approval**, you should be able to see who the certificate request was **Approved By**.

9.2.6 How to View EV Approvers

Only **EV Verified Users** can approve requests for EV Multi-Domain, EV SSL Plus, and EV Code Signing Certificates.

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select a status to filter the list of organizations.

3. In the **Division** drop-down list, select a division to filter the list of organizations.

4. To the right of the organization whose **EV Approver** you want to view, click **Manage**.

5. On the **"Organization's"** page, under **Pending Validation** or **Active Validation** (depending on whether the organization is validated yet), under **EV - Extended Organization Validation (EV)**, the **EV Verified Users** are listed.

9.2.7 How to View EV CS Approvers

Only **EV CS Verified Users** can approve requests for EV Code Signing Certificates.

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select a status to filter the list of organizations.

3. In the **Division** drop-down list, select a division to filter the list of organizations.

4. To the right of the organization whose **CS Approver** you want to view, click **Manage**.

5. On the **"Organization's"** page, under **Pending Validation** or **Active Validation** (depending on whether the organization is validated yet), under **EV CS - Code Signing Organization Validation**, the **EV CS Verified Users** are listed.

9.2.8 How to View CS Approvers

Only **CS Verified Users** can approve requests for Code Signing Certificates.

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Organizations** page, in the **Status** drop-down list, select a status to filter the list of organizations.

3. In the **Division** drop-down list, select a division to filter the list of organizations.

4. To the right of the organization whose **CS Approver** you want to view, click **Manage**.

5. On the **"Organization's"** page, under **Pending Validation** or **Active Validation** (depending on whether the organization is validated yet), under **CS - Code Signing Organization Validation**, the **CS Verified Users** are listed.

9.2.9 How to Reject a Certificate Request

1. In your account, in the sidebar menu, click **Account > Organization Validation**.

2. On the **Requests** page, in the **Division** drop-down list, select a division to filter the list of requests.

3. In the **Status** drop-down list, select **Pending** to see only the certificates that need administrator approval.

4. In the **Type** drop-down list, select a type to further filter the list of requests.

5. To the right of the certificate that you want to reject, click **View**.

6. On the **"Certificate's" Request** page, click **Reject**.

   CAUTION: In the **Reject Request** window, do not click **Reject**, unless you are sure that you want to reject the certificate request. The rejection cannot be reversed.

7. In the **Reject Request** window, enter a **Rejection Comment** and then, click **Reject**.

   Your rejection comment appears on the rejection email that is sent to the requestor.

8. The requestor is sent an email informing them that their certificate request has been rejected. Your rejection comment is included in the email.

9.3 Managing Certificates

After DigiCert issues your certificate, the certificate management process begins. Managing certificates includes downloading the certificates so that they can be installed, configured, and used. Certificate management also involves tracking, revoking (placing revoke requests, rejecting revoke requests, and approving revoke requests), reissuing, duplicating, and renewing certificates.

9.3.1 How to View Certificates

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

2. Filter certificates by **Status**.

   On the **Orders** page, in the **Status** drop-down list, select **Issued**, **Expired**, **Pending**, **Revoked**, **Rejected**, **Needs Approval**, or **All** to filter the certificates.

3. Filter the certificates by **Division**.

   In the **Division** drop-down list, select a Division or Subdivision to filter the certificates.

4. Rearrange certificates by order number, certificate request date, common name, certificate status, certificate validity period, certificate type, or certificate expiration date.

   Click one of the column headers (**Order #**, **Date**, **Common Name, Status, Validity, Product**, or **Expires**) to rearrange the order in which the certificates are listed.

5. To view the certificate details, to the right of a certificate, click **View**.

9.3.2 How to Download a Certificate

After your certificate is issued, you may want to download the certificate to your server or workstation so it can be installed (code signing certificates) or installed and configured (SSL and Grid SSL Certificates).

1. On the server or workstation where you need to install the certificate, log into your account.

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the certificate that you need to download, click **View**.

6. On the **Manage Order #** page, click **Download Certificates**.

7. On the **Download Certificates for Order #** page, in the **Format** section, select one of the following certificate formats:

Recommended 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.

Best format for Use the drop-down list to select server software that is different from the server software or software that was selected during the certificate request.

For example, you created the certificate on an IIS 8 server but you need to install the certificate on an Apache server.

Specific file format Use the drop-down list to select a specific file format for your certificate.

For example, the server software requires the certificate to be in a special format (such as a single .pem file that contains all the certificates: server, intermediate, and root)

8. Next, click **Download Certificates** to save the certificate file.
9. Save the certificate file to your server or workstation, making sure to note the location.

9.3.3 How to Adjust a Certificate's Renewal Notifications

After requesting your certificate, you may want to adjust the certificate's renewal notifications. By default, you receive an email notification at each of the following times as the certificate nears or passes its expiration date:

- Email 104 Days Before Expiration
- Email 90 Days Before Expiration
- Email 60 Days Before Expiration
- Email 30 Days Before Expiration
- Email 7 Days Before Expiration
- Email 3 Days Before Expiration
- Email 7 Days After Expiration

Adjusting a Certificate's Renewal Reminders

1. In your account, in the sidebar menu, click **Orders > Certificate Orders**.
2. On the **Orders** page, in the **Status** drop-down list, select **Pending** or **Issued**.
3. In the **Division** drop-down list, select the appropriate Division or Subdivision.
4. To the right of the certificate whose renewal reminders you want to adjust, click **View**.

5. On the **Manage Order #** page, next to **Renewal notices**, click the **Manage renewal notice frequency** link.

6. On the **Updated Renewal Notice Preferences** page, uncheck or check notifications as desired.

7. When you are finished, click **Save**.

9.3.4 How to Activate Your EV Code Signing Hardware

Before you can access the EV Code Signing Certificate and use it to sign code, you need to activate your token, download and install the SafeNet driver for your token, and obtain and change your token password

To access the certificate on your token, you need to get your token password from the order details inside your account. After retrieving your certificate's token password from your order, the password will disappear and it is not recoverable. We recommend that you change your token password after logging into the token for the first time.

1. On the computer from which you want to sign code (applications), log into your account.

   Note: You need to install the SafeNet drivers on any computer from which you want to use your EV Code Signing Certificate token to sign code.

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the certificate that you need to activate, click **View**.

6. On the **Manage Order #** page, click **Initialize Token**.

   If you have not received your token, do not continue. Leave the page and wait for your token to arrive before continuing.

7. On the **EV Code Signing Hardware Token Order #** page, check **I have received the hardware token** and then, click **Submit**.

8. Next, locate **"The current password that you will need to enter is:"** and record your DigiCert provided password*****.

   ***Note:** Your pre-assigned password will only be visible once. Make sure to take note of this password so you can access the certificate on your token.

9. Click the **Click here to download the SafeNet drivers for Windows** link to download the **SafeNetAuthenticationClient.exe**.

This lets you enable code signer authentication. Once enabled, SafeNet pops up before you sign a code and requires you to enter a password to verify that you are the actual signer.

Note: If you need driver software for other OS platforms, please email Support at support@digicert.com or call Support at 1-801-701-9600.

10. Run the SafeNet Authentication Client.

    Double-click **SafeNetAuthenticationClient-32x-64x.exe**.

11. In the **SafeNet Authentication Client Setup Wizard**, do the following:

    i. On the **Welcome to the SafeNet Authentication Client Installation Wizard** page, click, **Next**.

    ii. On the **Interface Language** page, in the language drop-down list, select a language to use for the SafeNet Authentication Client interface language and then click **Next**.

    iii. On the **License Agreement** page, read through the license agreement, select **I accept the license agreement** and then click **Next**.

    iv. On the **Installation Type** page, select **Standard installation**.

    If you need legacy support, select **BSec-compatible**.

    v. On the **Destination Folder** page, click **Next** to install the SafeNet drivers.

    If you do not want to use the default location, click **Browse** to select a different folder before clicking **Next**.

    vi. On the **SafeNet Authentication Client has been successfully installed** page, click **Finish**.

12. To change your token password, do the following:

    It is important to complete this step to change your password because your password disappears from your account.

    i. Plug in your DigiCert EV Code Signing Certificate token.

    ii. Open SafeNet Authentication Client Tools.

    iii. In the **SafeNet Authentication Client Tools** window, click **Change Token Password.**

    iv. On the **Change Password** page, In the **Current Token Password** box, enter the password that you retrieved from the **…Hardware Token Order #** page (see step 8).

v. In the **New Token Password** and **Confirm Password** boxes, create and confirm your new token password.

vi. Click **OK**.

13. On the **EV Code Signing Hardware Token Order #** page, click the **Click here when you have changed the password on the hardware token** link.

14. You're done! You can begin using your DigiCert EV Code Signing Certificate to sign code. For instructions on how to sign code with your EV Code Signing Certificate, see Code Signing Support & Tutorial.

9.3.5 How to Install Your EV Code Signing Certificate on Your Own Secure Token

This instruction is for installing your EV Code Signing Certificate on your own supported secure token. You must have a FIPS 140-2 Level 2 compliant device.

- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 5200
- SafeNet eToken 5205
- SafeNet eToken PRO 72K
- SafeNet eToken PRO Anywhere
- SafeNet iKey 4000

When installing an EV Code Signing Certificate on a token, there are two types of installations:

- **You are using an existing token, and you remember the password.**
  See Installing Your EV Code Signing Certificate on Your Token.

- **You are using a new token, or you are using an existing token and have forgotten your password.**
  See Installing Your EV Code Signing Certificate and Reinitializing Your Token.

Installing Your EV Code Signing Certificate on Your Token

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

2. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

3. In the **Division** drop-down list, select the appropriate Division or Subdivision.

4. To the right of the certificate that you need to install on your token, click **View**.

5. On the **Manage Order #** page, click **Install Certificate**.

6. Next, **record** your EV Code Signing Certificate's **initialization code** (i.e. *aaaaa11111aaaaa1111*).

   Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

7. After you have recorded your certificate's initialization code, click **DigiCert Hardware Certificate Installer** link in your account, and download and run the **DigiCert Hardware Certificate Installer**.

8. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.

9. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.

10. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.

11. On the **Token Detection** page, plug in your token and then, click **Next**.

    Make sure that only one token is plugged in. If more than one token is plugged in, the wizard asks you to remove the tokens that are not being used for EV Code Signing Certificate installation.

    Also, make sure that the drivers for the token are installed. If not the wizards asks you to remove your token, install the drivers, and then, re-install your token.

12. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.

13. On the **Token Detection** page, click **Next**.

14. On the **Token Password** page, in the **Token Password** box, enter your password and then, click **Finish**.

    Please do not remove your token while the installation process is being completed or you will have to start over. Using a strong network connection is also recommended because if the connection goes down, you will have to restart the process.

15. On the **Certificate Installation** page, after you receive four green checkmarks, click **Close**.

    It may take a few minutes for the wizard to install the EV Code Signing Certificate.

16. You're done! You can begin using your DigiCert EV Code Signing Certificate to sign code. For instructions on how to sign code with your EV Code Signing Certificate, see Code Signing Support & Tutorial.

Installing Your EV Code Signing Certificate and Reinitializing Your Token

1. In your account, in the sidebar menu, click **Orders > Certificate Orders**.
2. On the **Orders** page, in the **Status** drop-down list, select **Issued**.
3. In the **Division** drop-down list, select the appropriate Division or Subdivision.
4. To the right of the certificate that you need to install on your token, click **View**.
5. On the **Manage Order #** page, click **Install Certificate**.
6. Next, **record** your EV Code Signing Certificate's **initialization code** (i.e. *aaaaa11111aaaaa1111*).

   Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code
7. After you have recorded your certificate's initialization code, click **DigiCert Hardware Certificate Installer** link in your account, and download and run the **DigiCert Hardware Certificate Installer**.
8. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.
9. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.
10. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.
11. On the **Token Detection** page, plug in your token and then, click **Next**.

    Make sure that only one token is plugged in. If more than one token is plugged in, the wizard asks you to remove the tokens that are not being used for EV Code Signing Certificate installation.

    Also, make sure that the drivers for the token are installed. If not the wizards asks you to remove your token, install the drivers, and then, re-install your token.
12. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.
13. On the **Token Detection** page, check **Re-initialize my token and permanently delete any existing certificates and keys** and then, click **Next**.

    Use this option if you fall into one of the following situations:

    - You forgot your password, and you did not set up an administrator token password.
    - You want to reset your password and clear all certificates and keys from the token.

- You need to reset your password for security purposes, and you did not set up an administrator token password.

14. On the **Token Setup** page, enter the following information and then, click **Next**:

Token Name Provide a name for your token.

If you have more than one token, provide a unique name to help identify what you are storing on it (i.e. EV Code Signing Token).

Password: Under **Token Password**, enter and confirm the password for the token.

Confirm: You are required to enter this password whenever you use the EV Code Signing Certificate on the token.

Password must be 8 – 16 characters long.

Password must have at least one lower case letter, one upper case letter, one number, and one punctuation.

15. (Optional) If you want to set up and administrator password, on the **Administrator Setup** page, do the following to setup an administrator password:

    - Check **Set Administrator Password**.
    - In the **Password** and **Confirm** boxes, enter and confirm the token administrator password.

    We recommend that you setup an administrator password. If the token becomes locked, you can use this password to unlock the token. Without an administrator password, you must reinitialize the token, which permanently deletes all certificates and keys. You can also use the administrator password to reset the token password.

16. Click **Finish**.

    Please do not remove your token while certificate installation is being completed, or you will have to start over. Using a strong network connection is also recommended because if the connection goes down, you will have to restart the process.

17. On the **Certificate Installation** page, after you receive four green checkmarks, click **Close**.

    It may take a few minutes for the wizard to install the EV Code Signing Certificate.

18. You're done! You can begin using your DigiCert EV Code Signing Certificate to sign code. For instructions on how to sign code with your EV Code Signing Certificate, see Code Signing Support & Tutorial.

9.3.6 How to Activate Your Document Signing Hardware

Before you can access the Document Signing Certificate and use it to sign documents, you need to activate your token, download and install the SafeNet driver for your token, and obtain and change your token password

To access the certificate on your token, you need to get your token password from the order details inside your account. After retrieving your certificate's token password from your order, the password will disappear and it is not recoverable. We recommend that you change your token password after logging into the token for the first time.

1. On the computer from which you want to sign documents, log into your account.

   Note: You need to install the SafeNet drivers on any computer from which you want to use your Document Signing Certificate token to sign documents.

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the certificate that you need to activate, click **View**.

6. On the **Manage Order #** page, click **Initialize Token**.

   If you have not received your token, do not continue. Leave the page and wait for your token to arrive before continuing.

7. On the **Document Signing Hardware Token Order #** page, check **I have received the hardware token** and then, click **Submit**.

8. Next, locate **"The current password that you will need to enter is:"** and record your DigiCert provided password*****.

   ***Note:** Your pre-assigned password will only be visible once. Make sure to take note of this password so you can access the certificate on your token.

9. Click the **Click here to download the SafeNet drivers for Windows** link to download the **SafeNetAuthenticationClient.exe**.

   This lets you enable code signer authentication. Once enabled, SafeNet pops up before you sign a document and requires you to enter a password to verify that you are the actual signer.

   Note: If you need driver software for other OS platforms, please email Support at support@digicert.com or call Support at 1-801-701-9600.

10. Run the SafeNet Authentication Client.

    Double-click **SafeNetAuthenticationClient-32x-64x.exe**.

11. In the **SafeNet Authentication Client Setup Wizard**, do the following:

    i. On the **Welcome to the SafeNet Authentication Client Installation Wizard** page, click, **Next**.

    ii. On the **Interface Language** page, in the language drop-down list, select a language to use for the SafeNet Authentication Client interface language and then click **Next**.

    iii. On the **License Agreement** page, read through the license agreement, select **I accept the license agreement** and then click **Next**.

    iv. On the **Installation Type** page, select **Standard installation**.

        If you need legacy support, select **BSec-compatible**.

    v. On the **Destination Folder** page, click **Next** to install the SafeNet drivers.

        If you do not want to use the default location, click **Browse** to select a different folder before clicking **Next**.

    vi. On the **SafeNet Authentication Client has been successfully installed** page, click **Finish**.

12. To change your token password, do the following:

    It is important to complete this step to change your password because your password disappears from your account.

    i. Plug in your DigiCert Document Signing Certificate token.

    ii. Open SafeNet Authentication Client Tools.

    iii. In the **SafeNet Authentication Client Tools** window, click **Change Token Password.**

    iv. On the **Change Password** page, In the **Current Token Password** box, enter the password that you retrieved from the **…Hardware Token Order #** page (see step 8).

    v. In the **New Token Password** and **Confirm Password** boxes, create and confirm your new token password.

    vi. Click **OK**.

13. On the **Document Signing Hardware Token Order #** page, click the **Click here when you have changed the password on the hardware token** link.

14. You're done! You can begin using your DigiCert Document Signing Certificate to sign documents. For instructions on how to sign documents with your Document Signing Certificate, see Document Signing Support & Tutorial.

9.3.7 How to Install Your Document Signing Certificate on Your Own Secure Token

This instruction is for installing your Document Signing Certificate on your own supported secure token. You must have a FIPS 140-2 Level 2 compliant device.

- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 5200
- SafeNet eToken 5205
- SafeNet eToken PRO 72K
- SafeNet eToken PRO Anywhere
- SafeNet iKey 4000

When installing a Document Signing Certificate on a token, there are two types of installations:

- **You are using an existing token, and you remember the password.**
  See Installing Your Document Signing Certificate on Your Token.

- **You are using a new token, or you are using an existing token and have forgotten your password.**
  See Installing Your Document Signing Certificate and Reinitializing Your Token.

Installing Your Document Signing Certificate on Your Token

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

2. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

3. In the **Division** drop-down list, select the appropriate Division or Subdivision.

4. To the right of the certificate that you need to install on your token, click **View**.

5. On the **Manage Order #** page, click **Install Certificate**.

6. Next, **record** your Document Signing Certificate's **initialization code** (i.e. *aaaaa11111aaaaa1111*).

   Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

7. After you have recorded your certificate's initialization code, click DigiCert Hardware Certificate Installer link in your account, and download and run the **DigiCert Hardware Certificate Installer**.

8. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.

9. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.

10. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.

11. On the **Certificate Details** page, plug in your token and then, click **Next.**

    Make sure that only one token is plugged in. If more than one token is plugged in, the wizard asks you to remove the tokens that are not being used for Document Signing Certificate installation.

    Also, make sure that the drivers for the token are installed. If not the wizards asks you to remove your token, install the drivers, and then, re-install your token.

12. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.

13. On the **Token Detection** page, click **Next**.

14. On the **Token Password** page, in the **Token Password** box, enter your password and then, click **Finish**.

    Please do not remove your token while the installation process is being completed or you will have to start over. We also recommend using a strong network connection because if the connection goes down, you will have to restart the process.

15. On the **Certificate Installation** page, after you receive four green checkmarks, click **Close**.

    It may take a few minutes for the wizard to install the Document Signing Certificate.

16. You're done! You can begin using your DigiCert Document Signing Certificate to sign documents. For instructions on how to sign documents with your Document Signing Certificate, see Document Signing Support & Tutorial.

Installing Your Document Signing Certificate and Reinitializing Your Token

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

2. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

3. In the **Division** drop-down list, select the appropriate Division or Subdivision.

4. To the right of the certificate that you need to install on your token, click **View**.

5. On the **Manage Order #** page, click **Install Certificate**.

6. Next, **record** your Document Signing Certificate's **initialization code** (i.e. *aaaaa11111aaaaa1111*).

   Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

7. After you have recorded your certificate's initialization code, click DigiCert Hardware Certificate Installer link in your account, and download and run the **DigiCert Hardware Certificate Installer**.

8. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.

9. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.

10. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.

11. On the **Certificate Details** page, plug in your token and then, click **Next**.

    Make sure that only one token is plugged in. If more than one token is plugged in, the wizard asks you to remove the tokens that are not being used for Document Signing Certificate installation.

    Also, make sure that the drivers for the token are installed. If not the wizards asks you to remove your token, install the drivers, and then, re-install your token.

12. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.

13. On the **Token Detection** page, check **Re-initialize my token and permanently delete any existing certificates and keys** and then, click **Next**.

    Use this option if you fall into one of the following situations:

    - You forgot your password, and you did not set up an administrator token password.
    - You want to reset your password and clear all certificates and keys from the token.
    - You need to reset your password for security purposes, and you did not set up an administrator token password.

14. On the **Token Setup** page, enter the following information and then, click **Next**:

    Token Name Provide a name for your token.

    If you have more than one token, provide a unique name to help identify what you are storing on it (i.e. Document Signing Token).

Password: Under **Token Password**, enter and confirm the password for the token.

Confirm: You are required to enter this password whenever you use the EV Code Signing Certificate on the token.

Password must be 8 – 16 characters long.

Password must have at least one lower case letter, one upper case letter, one number, and one punctuation.

15. (Optional) IF you want to set up and administrator password, on the **Administrator Setup** page, do the following to setup an administrator password:

    - Check **Set Administrator Password**.
    - In the **Password** and **Confirm** boxes, enter and confirm the token administrator password.

    We recommend that you setup an administrator password. If the token becomes locked, you can use this password to unlock the token. Without an administrator password, you must reinitialize the token, which permanently deletes all certificates and keys. You can also use the administrator password to reset the token password.

16. Click **Finish**.

    Please do not remove your token while certificate installation is being completed, or you will have to start over. We also recommend using a strong network connection because if the connection goes down, you will have to restart the process.

17. On the **Certificate Installation** page, after you receive four green checkmarks, click **Close**.

    It may take a few minutes for the wizard to install the Document Signing Certificate.

18. You're done! You can begin using your DigiCert Document Signing Certificate to sign documents. For instructions on how to sign documents with your Document Signing Certificate, see Document Signing Support & Tutorial.

9.3.8 How to Place a Request to Revoke a Certificate

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

2. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

3. In the **Division** drop-down list, select the appropriate Division or Subdivision.

4. To the right of the certificate that you need to place a request to revoke, click **View**.

5. In the **Manage Order #** section, click **Revoke Certificate**.

6. On the **Revoke Certificate for Order #** page, in the **Reason for Revocation** box, type your reason for revoking the certificate.

7. Making sure that you really need to revoke the certificate, click **Request Revocation** to request the certificate revocation.

9.3.9 How to Approve a Certificate Revoke Request

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

2. On the **Requests** page, in the **Status** drop-down list, select **Pending** to see only the certificates that need administrator approval.

3. In the **Type** drop-down list, select **Revoke** to see only the certificates that need revocation approval.

4. To the right of the certificate whose revocation you need to approve, click **View**.

   The **Type** for the certificate should be **REVOKE**.

5. On the **Request to Revoke Order #** page, making sure that you really need to revoke the certificate, click **Approve** to revoke the certificate.

   CAUTION: In the **Approve Request** window, do not click **Reject**, unless you are sure that you want to reject the certificate request. The rejection cannot be reversed.

6. In the **Approve Request** window, enter an **Approval Comment** and then, click **Approve**.

9.3.10 How to Reject a Certificate Revoke Request

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

2. On the **Requests** page, in the **Status** drop-down list, select **Pending** to see only the certificates that need administrator approval.

3. In the **Type** drop-down list, select **Revoke** to see only the certificates that need revocation approval.

4. To the right of the certificate whose revocation you need to reject, click **View**.

   The **Type** for the certificate should be **REVOKE**.

5. On the **Revoke Request for Order #** page, click **Reject** to reject the certificate revoke request.

6. In the **Rejection Comment** window, provide a **Rejection Comment** and then, click **Reject**.

   Note that your rejection comment appears on the rejection email that is sent to the requestor.

7. The requestor is sent an email informing them that their certificate request has been rejected. Your rejection comment is included in the email.

9.3.11 How to Request a Duplicate Certificate

Your SSL Certificate comes with an unlimited server license. Having an unlimited server license means that you can use one certificate on as many different servers as you want.

The process for requesting a duplicate certificate is the same:

- Create your Certificate Signing Request (CSR).
- Fill out the request form.
- Wait for approval.

The form for requesting a duplicate for EV Multi-Domain, Unified Communications, Wildcard Plus, and Grid Host SSL UC certificates is similar. For this reason, we will provide instructions for ordering a Unified Communications Certificate and note any differences between the UC Certificate request form and the EV Multi-Domain, Wildcard plus, and Grid Host SSL UC request forms.

You can use this instruction for the following certificates:

- EV Multi-Domain
- Unified Communications
- Wildcard Plus
- Grid Host SSL UC

How to Request a Duplicate Unified Communication Certificate

To create a duplicate certificate, for each server, send us a new CSR so that we can create a new certificate for it. The details in the duplicate certificate will be the same as in the original certificate, and the duplicate certificate does not/cannot revoke previous copies of your certificate.

1. On the server for which you want the certificate, create a new CSR/keypair.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

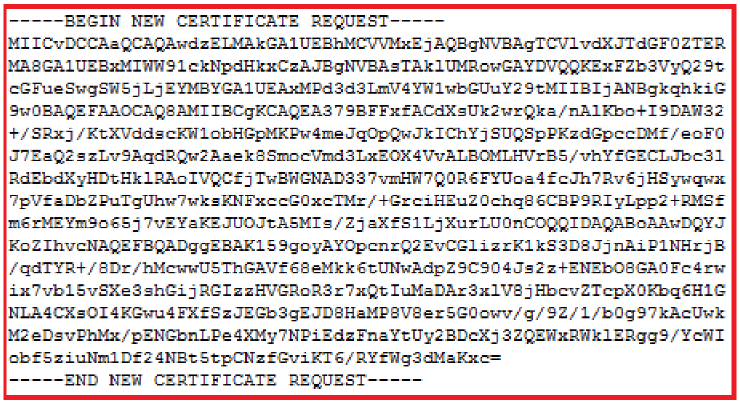
5. To the right of the Unified Communications Certificate that needs to be duplicated, click **View**.

6. On the **Manage Order #** page, click **Get Duplicate**.

7. On the **Request Duplicate Certificate for Order #** page, in the **Paste your CSR** box, do one of the following:

   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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

8. (UC and EV Multi-Domain Certificates) To select a different common name, do the following:

   i. Under **Common Name** section, click **Show Available Domains**.

   ii. Select one of the available domains or subdomains (i.e. *example.com* or *mail.example.com*).

   The common name must be from one of the available domains or a subdomain of one of the available domains.

   iii. The selected domain name is entered in the **Common Name** box.

   The common name is listed as the first SAN (subject alternative name) name in the certificate.

   For a Wildcard Plus Certificate:

   You cannot change the common name.

9. (Grid Host SSL UC) To select a different common name, do the following:

Note: When requesting a duplicate certificate do not change, add (if blank), or remove the Service; these actions will create a certificate reissue, which automatically revokes the original certificate or previous certificate reissues.

i. In the **Common Name** section, click **Show Available Domains**.

ii. Select one of the available domains or subdomains (i.e. *example.com* or *mail.example.com*).

The common name must be from one of the available domains or a subdomain of one of the available domains.

iii. The selected domain name is entered in the **Common Name** box.

The common name is listed as the first SAN (subject alternative name) name in the certificate.

10. (Wildcard Plus Certificate) To add additional Subject Alternate Names (SANs) to the duplicate certificate, in the **Other Hostnames (SANs)** box, type the SANs names that you want to add.

For example, if the common name is **.example.com*, you can add SANs such as *www.example.com* or *www.app.example.com*.

Wildcard Plus Certificates only secure the first level of subdomains. To really secure your entire domain, specify SANs as many level deep as you need.

Some mobile clients, including Windows Mobile 5, do not support wildcards, but they do support Subject Alternative Names. If you want to be Windows Mobile 5 compliant add SANs to your Wildcard Certificate.

For EV Multi-Domain, UC, and Grid Host SSL UC Certificates:

You cannot add additional SANs.

11. Next, enter the following information:

Signature Hash:	In the drop-down list, select a signature hash.
Server Platform:	Select the server on which the CSR was generated.
Reason for Duplicate:	In the box, specify the reason for the certificate duplication.

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

On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.12 How to Reissue an SSL Certificate

All DigiCert certificates come with unlimited free reissues. Some reasons you may reissue your certificate include:

- You lost your private key, or you want to re-key your certificate.
- You want to change the domain on the certificate (i.e. from *www.yourname.com* to *secure.yourname.com*).
- You want to add, remove, or change some of the SANs that are listed in your UC certificate.

The process for reissuing a certificate is the same:

- Create your Certificate Signing Request (CSR).
- Fill out the request form.
- Wait for approval.

The form for requesting a reissue for each type of SSL Certificate is similar, including Grid Host SSL certificates. For this reason, we will provide instructions for reissuing an SSL Certificate and note any differences between the different SSL Certificate request forms.

You can use this instruction for the following certificates:

- EV Multi-Domain
- EV SSL Plus
- Unified Communications
- SSL Plus
- Wildcard Plus
- Grid Host SSL UC
- Grid Host SSL

How to Reissue an SSL Certificate

1. On the server for which you want the certificate, create a new CSR/keypair.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

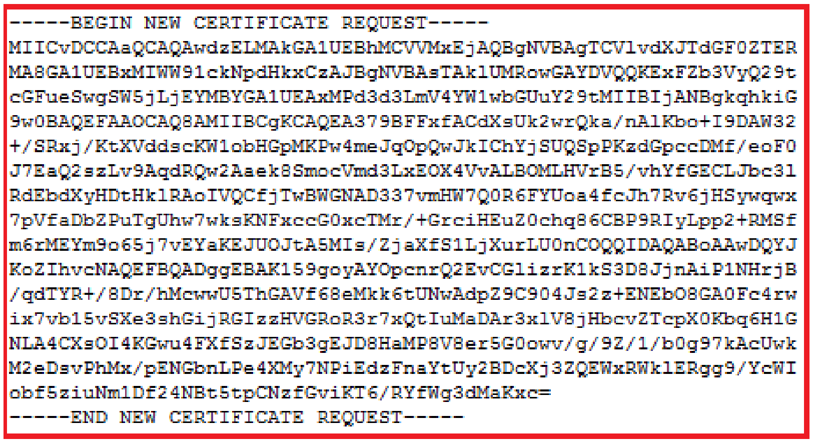
4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the certificate that needs to be reissued, click **View**.

6. On the **Manage Order #** page, click **Reissue Certificate**.

7. On the **Reissue Certificate for Order #** page, in the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKWlobHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

8. Certificate Rekey

If you just want to rekey your certificate, you don't need to change any of the certificate details. You can skip to Step 12.

9. Common Name

SSL Plus, EV SSL Plus, and Wildcard Plus Certificates:

To change the common name for the reissued certificate, in the **Common Name** section, click **Show Available Domains** and select one of the available domains or subdomains (i.e. *example.com* or *mail.example.com*). For Wildcard Plus Certificates, the name format is **.domain.com* (i.e. **.example.com*).

- The common name must be from one of the available domains or a subdomain of one of the available domains. The selected domain name is entered in the **Common Name** box.

- Changing the common name when reissuing an SSL Plus, EV SSL Plus, or Wildcard certificate will automatically revoke the original certificate and any previous reissues.

Unified Communications and EV Multi-Domain Certificates:

To change the common name for the reissued certificate, in the **Common Name** section, click **Show Available Domains** and select one of the available domains or subdomains (i.e. *example.com* or *mail.example.com*) that is not listed as one of the hostnames on the certificate (original or reissued).

- Changing the common name when reissuing a Unified Communications or EV Multi-Domain certificate automatically revokes the original certificate and any previous reissues, unless you add the old common name as a SAN on the reissued certificate.

  If you just need to select a different common name from the list of other hostnames (SANs), you should request a duplicate certificate instead of a reissuing the certificate.

- The common name is listed as the first SAN (subject alternative name) name in the certificate.

10. **Service/Common Name**

    Grid Host SSL Certificate:

    i. To change the service for the reissued certificate, in the **Service** box, enter the service that you want to use to connect to the grid server.

       Changing the service automatically revokes the original certificate and any previous reissues.

    ii. To change the common name for the reissued certificate, in the **Common Name** section, click **Show Available Domains** and select one of the available domains or subdomains (i.e. *example.com* or *mail.example.com*).

       The common name must be from one of the available domains or a subdomain of one of the available domains. The selected domain name is entered in the **Common Name** box.

       Changing the common name automatically revokes the original certificate and any previous reissues.

    Grid Host SSL UC Certificate:

    i. To change the service for the reissued certificate, in the **Service** box, enter the service that you want to use to connect to the grid server.

       Changing the service automatically revokes the original certificate or previous reissues.

ii. To change the common name for the reissued certificate, in the **Common Name** section, click **Show Available Domains** and select one of the available domains or subdomains (i.e. *example.com* or *mail.example.com*).

The common name is listed as the first SAN (subject alternative name) name in the certificate.

For a certificate reissue, you can change the common name without revoking the original certificate or previous reissues.

Note: If you just need to select a different common name from the list of other hostnames (SANs), you should request a duplicate certificate instead of a reissue.

11. **Other Hostnames (SANs)**

Unified Communications, EV Multi-Domain, and Grid Host SSL UC Certificates:

i. **Add SANs**

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

Adding SANs does not revoke the original certificate or previous reissues.

ii. **Remove SANs**

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

Removing SANs automatically revokes the original certificate or previous reissues

Wildcard Plus Certificates

If you just need to make a new copy of the certificate with a new list of SANs, you should request a duplicate certificate instead of a reissuing the certificate.

12. Next, enter the following information:

Signature Hash:	In the drop-down list, select a signature hash.
Server Platform:	Select the server on which the CSR was generated.
Reason for Reissue:	In the box, specify the reason for the certificate reissue.

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

On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.13 How to Renew an SSL Plus, EV SSL Plus, EV Multi-Domain, Unified Communications and a Wildcard Plus Certificate

The process for renewing any of the available SSL Certificates is the same:

- Create your Certificate Signing Request (CSR).
- Fill out the request form.
- Wait for approval.

The form for renewing each type of SSL Certificate is similar. For this reason, we will provide instructions for renewing an SSL Certificate and note any differences between the different types of SSL Certificate renewal forms.

This instruction can be used for the following certificates:

- EV Multi-Domain
- EV SSL Plus
- SSL Plus
- Unified Communications
- Wildcard Plus

How to Renew an SSL Certificate

1. Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued** or **Expired**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

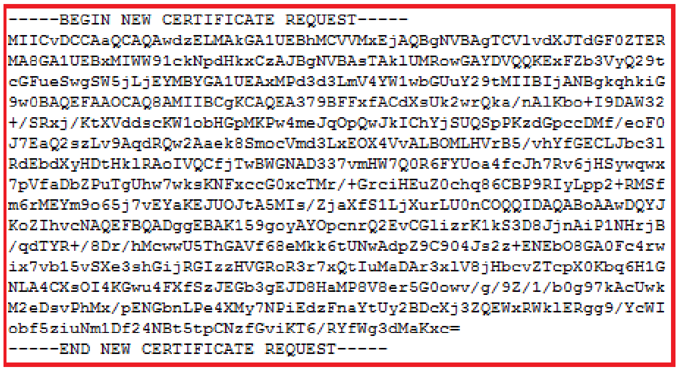
5. To the right of the certificate that needs to be renewed, click **View**.

6. On the **Manage Order #** page, click **Renew Certificate**.

7. On the **Renew Order #** page, under **Certificate Settings**, in the **Paste your CSR** box, do one of the following:

   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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

8. **Common Name**

   Because you are renewing your certificate, the **Common Name** box should be prepopulated with the common name and the organization to which the domain is assigned populates the **Organization** field.

   If you are using a different common name, under **Common Name**, click **Show Available Domains** and select one of the available domains or subdomains (i.e. *example.com (Organization Name)* or *mail.example.com (Organization Name)*).

   The selected domain name is entered in the **Common Name** box, and the organization to which the domain is assigned populates the **Organization** field.

   - For an EV Multi-Domain Certificate:

     The common name is listed as the first SAN (subject alternative name) name in the certificate.

   - For a Unified Communications Certificate:

     The common name is listed as the first SAN (subject alternative name) name in the certificate.

   - For a Wildcard Plus Certificate:

     The common name would be **.example.com*.

   Note: The common name must be from one of the available domains or a subdomain of one of the available domains.

9. **Other Hostnames (SANs)**

For EV Multi-Domain, and Unified Communications Certificates

Because you are renewing your certificate, the **Other Hostnames (SANs)** box should be prepopulated with the additional hostnames.

If you want to add hostnames, in the **Other Hostnames (SANs)** box, enter additional hostnames (i.e. *example2.com*, *example3.net*, *mail.example.net*) that you want your EV Multi-Domain or Unified Communications Certificate to secure. You can also remove hostnames.

(Optional) For Wildcard Plus Certificates

Because you are renewing your certificate, the **Other Hostnames (SANs)** box should be prepopulated with SANs, if additional hostnames were used.

If you want to add SANs, in the **Other Hostnames (SANs)** box, enter additional hostnames (i.e. *example2.com*, *example3.net*, *mail.example.net*) that you want your Wildcard Certificate to secure. You can also remove SANs.

Wildcard Plus Certificates only secure the first level of subdomains. To really secure your entire domain, specify SANs as many level deep as you need.

Some mobile clients, including Windows Mobile 5, do not support wildcards, but they do support Subject Alternative Names. If you want to be Windows Mobile 5 compliant add SANs to your Wildcard Certificate.

10. Next, enter the following information:

Organization Unit: Enter the name of your department, group, etc.

Validity Period: Select a validity period for the certificate: **1 Year**, **2 Years**, **3 Years**, or **Custom Expiration Date**).

For EV SSL Plus and EV Multi-Domain Certificates:

The maximum validity period is **2 Years**.

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

11. In the **Order Information** section, do the following:

Server Platform: Select the server on which the CSR was generated.

Comments to Administrator:	Enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc. These comments are not meant to be included in the certificate.

12. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

    On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.14 How to Renew a Grid Host SSL and Grid Host SSL UC Certificate

The process for renewing Grid Host SSL and Grid Host SSL UC Certificates is the same:

- Create your Certificate Signing Request (CSR).
- Fill out the request form.
- Wait for approval.

The form for renewing the Grid Host SSL Certificate and Grid SSL UC Certificate is similar. For this reason, we will provide instructions for requesting a Grid Host SSL Certificate and note any differences between the Grid Host SSL Certificate and the Grid Host SSL UC Certificate renewal forms.

This instruction can be used for the following certificates:

- Grid Host SSL
- Grid Host SSL UC

How to Renew a Grid Host SSL Certificate

1. Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued** or **Expired**.

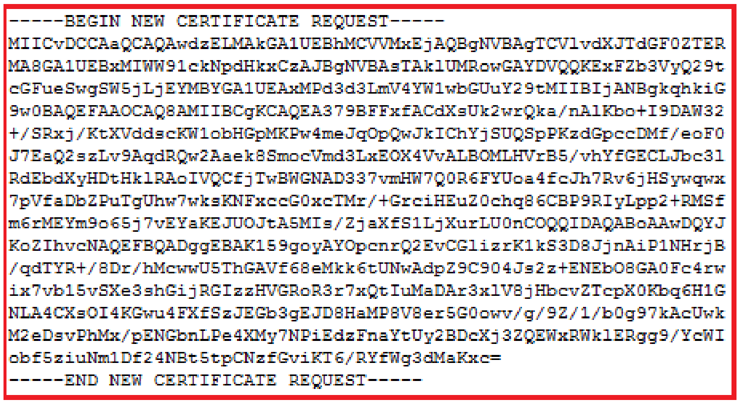
4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the certificate that needs to be renewed, click **View**.

6. On the **Manage Order #** page, click **Renew Certificate**.

7. On the **Renew Order #** page, under **Certificate Settings**, in the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

8. Service / Common Name

Because you are renewing your certificate, the **Service / Common Name** box should be prepopulated with the service and common name and the organization to which the domain is assigned populates the **Organization** field.

If you are using a different service and/or common name, under **Service / Common Name** section do the following:

i. In the **Service** box, enter the service that you want to use to connect to the grid server.

ii. Under **Common Name**, click **Show Available Domains** and select one of the available domains or subdomains (i.e. *example.com (Organization Name)* or *mail.example.com (Organization Name)*).

The selected domain name is entered in the **Common Name** box, and the organization to which the domain is assigned populates the **Organization** field.

Note that the common name must be from one of the available domains or a subdomain of one of the available domains.

For a Grid Host SSL UC Certificate:

The common name is listed as the first SAN (subject alternative name) name in the certificate.

9. **Other Hostnames (SANs)**

   For a Grid Host SSL UC Certificate

   Because you are renewing your certificate, the **Other Hostnames (SANs)** box should be prepopulated with the additional hostnames.

   If you want to add hostnames, in the **Other Hostnames (SANs)** box, enter additional hostnames (i.e. *www.example2.com*, *www.example3.net*, *mail.example.net*) that you want your Grid Host SSL UC Certificate to secure. You can also remove hostnames.

10. Next, enter the following information:

Validity Period:	Select a validity period for the certificate: **1 Year** or **Custom Expiration Date**).
Signature Hash:	In the drop-down list, select a signature hash.

11. Under **Order Information**, do the following:

Server Platform:	Select the server on which the CSR was generated.
Comments to Administrator:	Enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc.

12. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

    On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.15 How to Reissue a Code Signing Certificate

Reissuing your Code Signing Certificate does not automatically revoke the original certificate or any previous reissues. However, all new applications should be signed with your reissued Code Signing Certificate.

If you revoke a Code Signing Certificate, applications that were signed with the revoked certificate remain valid as long as they were time stamped when they were signed.

The process for reissuing a Code Signing Certificate is as follows:

- **For Sun Java Platform Only:** Create your Certificate Signing Request (CSR). Sun Java is the only platform for which you are required to submit a CSR.
- Fill out the request form.
- Wait for approval.

How to Reissue a Code Signing Certificate

1. **For Sun Java Platform Only:** Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the Code Signing Certificate that needs to be reissued, click **View**.

6. On the **Manage Order #** page, click **Reissue Certificate**.

7. On the **Reissue Certificate for Order #** page, do the following:

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

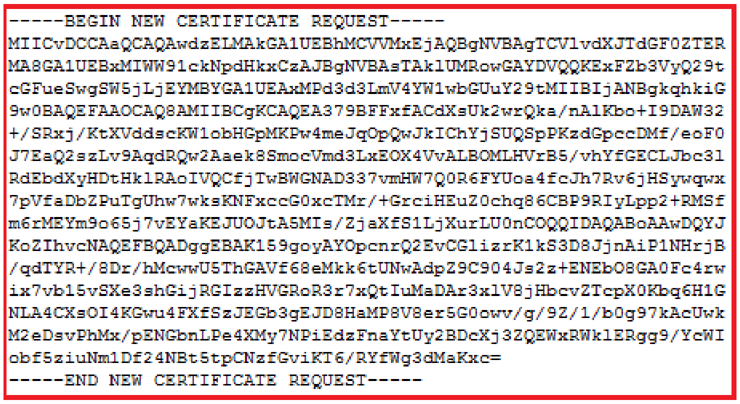
   Server Platform: In the list of server platforms, select the platform for which your Code Signing Certificate is to be used.

   Reason for Reissue: In the box, specify the reason for the certificate reissue.

8. **(Sun Java Platform only)** In the **Paste your CSR** box, do one of the following:

   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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

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

   On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.16 How to Renew a Code Signing Certificate

The process for renewing a Code Signing Certificate is as follows:

- **For Sun Java Platform Only:** Create your Certificate Signing Request (CSR). Sun Java is the only platform for which you are required to submit a CSR.
- Fill out the request form.
- Wait for approval.

How to Renew a Code Signing Certificate

1. **For Sun Java Platform Only:** Create your CSR.

   Note: To remain secure, certificates must use 2048-bit keys.

   To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

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

3. On the **Orders** page, in the **Status** drop-down list, select **Issued** or **Expired**.

4. In the **Division** drop-down list, select the appropriate Division or Subdivision.

5. To the right of the certificate that needs to be renewed, click **View**.

6. On the **Manage Order #** page, click **Renew Certificate**.

7. On the **Renew Code Signing Order#** page, under **Certificate Settings** section, enter the following settings information:

Organization: In the drop-down list, select the organization for which you are requesting the Code Signing Certificate.

Note: The organization's name appears on your Code Signing Certificate.

Organization Unit: Enter the name of your department, group, etc.

Validity Period: Select a validity period for the certificate: **1 Year**, **2 Years**, or **3 Years**.

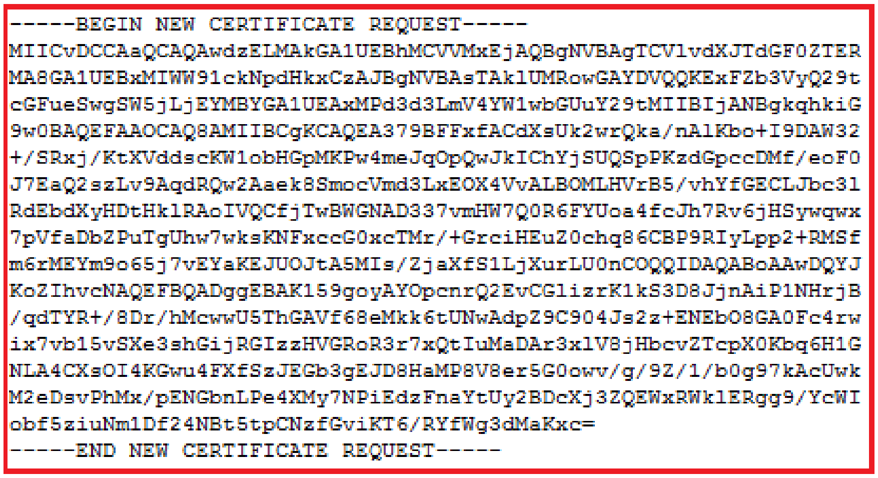
Signature Hash: In the drop-down list, select a signature hash.

8. Under **Order Options**, in the **Server Platform** box, select the platform for which the Code Signing Certificate is to be used.

9. **(Sun Java Platform only)** In the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCV1vdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHDtHk1RAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

10. In the **Comments to Administrator** box, enter any information that your administrator might need for approving your request, about the purpose of the certificate, etc.

11. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

    An email should be sent notifying the CS Certificate approvers that there is a certificate request that needs their approval.

    On the **Request** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.17 How to Reissue an EV Code Signing Certificate

Reissuing your EV Code Signing Certificate automatically revokes the original certificate and any previous reissues. You need to sign new applications using the reissued certificate.

Any application that you signed with a revoked certificate remain valid as long as they were time stamped when you signed them.

The process for reissuing an EV Code Signing is as follows:

- Fill out the request form.
- Wait for approval.

How to Reissue an EV Code Signing Certificate

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

2. On the **Orders** page, in the **Status** drop-down list, select **Issued**.

3. In the **Division** drop-down list, select the appropriate Division or Subdivision.

4. To the right of the EV Code Signing Certificate that needs to be reissued, click **View**.

5. On the **Manage Order #** page, click **Reissue Certificate**.

6. **(HSM device only)** On the **Reissue Certificate for Order #** page, do the following:

    i. Create your CSR.

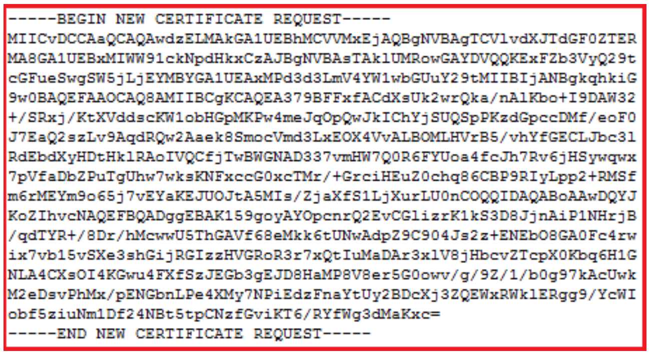
    Note: To remain secure, certificates must use 2048-bit keys.

    To learn how to create a CSR, see [Create a CSR (Certificate Signing Request)](#).

    ii. In the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

7. Next on the **Reissue Certificate for Order #** page, do the following:

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

Server Platform: In the list of server platforms, select the platform for which your EV Code Signing Certificate is to be used.

Reason for Reissue: In the box, specify the reason for the certificate reissue.

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

   On the **Requests** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.

9.3.18 How to Renew an EV Code Signing Certificate

The process for renewing an EV Code Signing is as follows:

- Fill out the request form.
- Wait for approval.

How to Renew an EV Code Signing Certificate

1. In your account, in the sidebar menu, click **Orders > Certificate Orders**.
2. On the **Orders** page, in the **Status** drop-down list, select **Issued** or **Expired**.
3. In the **Division** drop-down list, select the appropriate Division or Subdivision.
4. To the right of the certificate that needs to be renewed, click **View**.

5. On the **Manage Order #** page, click **Renew Certificate**.

6. On the **Renew EV Code Signing Order#** page, enter the following settings information:

   Organization: In the drop-down list, select the organization for which you are requesting the Code Signing Certificate.

   Note: The organization's name appears on your Code Signing Certificate.

   Organization Unit: Enter the name of your department, group, etc.

   Validity Period: Select a validity period for the certificate: **1 Year**, **2 Years**, or **3 Years**.

7. Under **Provisioning Options**, select an EV Code Signing Certificate provision option and complete the necessary steps for that option:

   - **Preconfigured Hardware Token**

     Select this option if you want DigiCert to install your EV Code Signing Certificate on a secure token and then ship it to you. See Currently Supported eTokens.

     After selecting this option, enter your **Shipping Information**: your name and the address to which you want the token to be sent.

   - **Use Existing Token**

     Select this option if you already have a supported hardware token and want to install your EV Code Signing Certificate on that token yourself. See Currently Supported eTokens.

     After selecting this option, in the **Platform** drop-down list, select the hardware token on which you will be installing your EV Code Signing Certificate.

   - **Install on HSM**

     Select this option if you want to down load the EV Code Signing Certificate and install it on your HSM device yourself.

     If you select this option, you are required to provide audit documentation to DigiCert demonstrating that you are qualified. Only then can we issue your EV Code Signing Certificate.

     After selecting this option, do the following:

     i. Create your CSR.

Note: To remain secure, certificates must use 2048-bit keys.

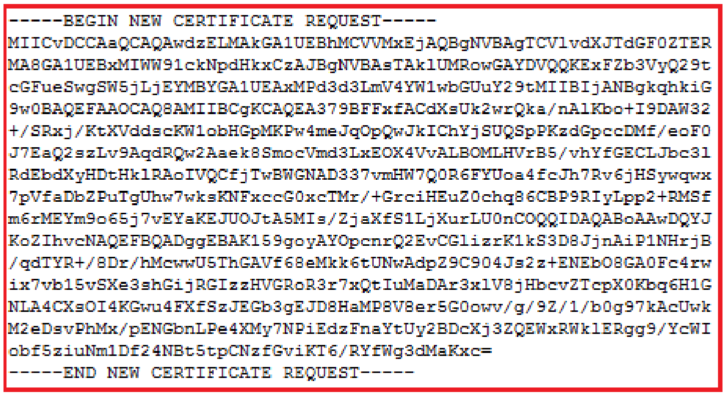
To learn how to create a CSR, see Create a CSR (Certificate Signing Request).

ii. In the **Select Platform** box, select the platform on which you will be installing your EV Code Signing Certificate.

iii. In the **Paste your CSR** box, do one of the following:

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 request form in the area provided.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHk1RAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

8. Under **Terms of Service**, read through the terms of service, making sure you understand the terms and then, check **I agree to the Terms of Service above**.

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

   An email should be sent notifying the EV Certificate approvers that there is a certificate request that needs their approval.

   On the **Request** page (**Orders > Certificate Requests**), your certificate should be listed with the **Status** of **Pending**.