

DigiCert User Guide

Version 5.2

Table of Contents

1	User Management	8
1.1	Roles and Account Access	8
1.1.1	Administrator Role	8
1.1.2	User Role	8
1.1.3	EV Verified User	8
1.1.4	CS Verified User	8
1.1.5	EV CS Verified User	8
1.2	Managing Users	9
1.2.1	How to Add Users to Your Account	9
1.2.2	How to Resend the DigiCert User Account Created - Action Required Email	10
1.2.3	How to Invite New Users to Join Your Account	10
1.2.4	How to Create Your New User (Invitee) Account	11
1.2.5	How to Approve/Activate an Invitee's User Account	12
1.2.6	How to Edit User Accounts	12
1.2.7	How to Delete (Remove) User Accounts	13
1.2.8	How to Edit Your Profile	13
1.2.9	How to View Account Users	15
1.2.10	How to Unlock a "Locked" Account	15
1.2.11	How to Retrieve Your Forgotten Username	16
1.2.12	How to Reset Your Forgotten Password	16
1.3	Managing API Users	16
1.3.1	How to Issue an API Key	16
1.3.2	How to Revoke (Remove) an API Key	17
1.3.3	How to View API Keys and API Key Users	17
1.4	Managing Guest URLs	18
1.4.1	Guest URLs	18
1.4.2	How to Create a Guest URL	18
1.4.3	How to Send the Guest URL to a "Guest"	19
1.4.4	How to Edit a Guest URL	20
1.4.5	How to Delete a Guest URL	20
1.4.6	How to View Guest URLs	21

2	Division Management	22
2.1	Managing Divisions	22
2.1.1	How to Add a New Division	22
2.1.2	How to Set Division Preferences	24
2.1.3	How to Edit a Division's Details	27
2.1.4	How to Deactivate a Division	28
2.1.5	How to Activate a Division	29
2.2	Managing Division Co-Branding (Logos)	29
2.2.1	How to Add a Division Logo	29
2.2.2	How to Replace a Division Logo	30
2.2.3	How to Remove a Division Logo	30
2.3	Managing Division Ekeys	31
2.3.1	How to Create a Division Ekey	32
2.3.2	How to View a Division Ekey	33
2.3.3	How to Edit a Division Ekey	33
2.3.4	How to Delete a Division Ekey	34
3	IP Access Restrictions	35
3.1	Configuring IP Access Restrictions	35
3.1.1	How to Turn On IP Address Restrictions	35
3.1.2	How to Turn Off IP Access Restrictions	35
3.1.3	Account Wide: Configure IP Access Restriction Rules	35
3.1.4	A Specific User: Configure IP Access Restriction Rules	36
3.1.5	All Guest URLs: Configure IP Access Restriction Rules	36
3.1.6	A Specific Guest URL: Configure IP Access Restriction Rules	37
3.1.7	How to View IP Access Restriction Rules	37
3.1.8	How to Delete an IP Access Restriction Rule	38
4	Authentication Settings	39
4.1	Password Requirements	39
4.1.1	How to Configure Password Requirements	39
4.2	DigiCert Two-Factor Authentication	41
4.3	Setting Up Two-Factor Authentication	41
4.3.1	Client Certificate Requirement	41

4.3.2	One-time Password Requirement.....	42
4.4	Configuring Two-Factor Authentication Requirements	42
4.4.1	How to Turn On Two-Factor Authentication.....	42
4.4.2	How to Turn Off Two-Factor Authentication	44
4.4.3	All Account Users: Configure Two-Factor Authentication Requirements	45
4.4.4	All Users in a Division: Configure Two-Factor Authentication Requirements	47
4.4.5	A Specific User: Configure Two-Factor Authentication Requirements.....	48
4.4.6	OTP App Authenticators: How to Allow Them to Verify a Computer for 30 Days.....	50
4.4.7	How to Delete a Two-Factor Authentication Requirement	51
4.4.8	How to View Two-Factor Authentication Requirements.....	52
4.4.9	How to View OTP and Client Certificate Authenticators	53
4.5	Two-Factor Authentication: User Instructions.....	54
4.5.1	How to Initialize Your OTP App Device	54
4.5.2	How to Sign In with Your OTP App Device	55
4.5.3	User: Resetting Your OTP App Device.....	55
4.5.4	How to Generate Your Client Certificate.....	56
4.5.5	How to Sign In with Your Client Certificate	57
4.5.6	User: Resetting Your Client Certificate	58
4.6	Two-Factor Authentication: Admin Specific Instructions.....	59
4.6.1	How to Reset a User's OTP App Device	59
4.6.2	How to Reset a User's Client Certificate.....	59
4.6.3	Admin: Resetting Your OTP App Device	60
4.6.4	Admin: Resetting Your Client Certificate	61
5	Reports Management	62
5.1	Running Reports	62
5.1.1	How to Run a Report	62
6	Account Settings (GÉANT Admin).....	63
6.1	How to Set Up Your Email Notification Account(s)	63
6.2	How to Configure Certificate Renewal Settings	63
7	Audit Logs.....	64
7.1	Running Audits.....	64
7.1.1	How to Run an Audit.....	64

7.2	Setting Up Audit Log Notifications.....	65
7.2.1	How to Create an Audit Log Notification.....	65
8	Organization and Domain Management	67
8.1	Validation Process.....	67
8.1.1	Organization Validation.....	67
8.1.2	Domain Validation.....	67
8.2	Managing Organizations	68
8.2.1	How to Add an Organization	68
8.2.2	How to View Organizations and Their Details	69
8.2.3	How to Authorize Organizations for Certificates	69
8.2.4	How to View the EV, EV Code Signing (EV CS), and Code Signing (CS) Certificate Approvers for an Organization	71
8.2.5	How to Add EV/EV CS and CS Certificate Approvers for an Organization	71
8.3	(Non-ASCII Characters) How to Add and Authorize an Organization for Grid - Public Grid Host Validation	72
8.3.1	(Non-ASCII Characters) Adding an Organization	73
8.3.2	(Non-ASCII Characters) Authorizing an Organization for Grid – Public Grid Host Validation.....	74
8.4	Managing Domains	75
8.4.1	How to Add a Domain and Authorize It for Certificates	76
8.4.2	How to View Domain Details, Validation Status, and Validation Progress	76
8.4.3	How to Authorize a Domain for Additional Certificate Types.....	77
8.4.4	How to View the Domains Validations (Pending or Active).....	77
8.4.5	How to Enable DNS CNAME Domain Control Validation (DCV).....	78
8.4.6	How to Add a Domain, Authorize it for Certificates, and Select DNS CNAME as the Validation Method.....	79
9	Product Settings.....	81
9.1	Configuring Product Settings.....	81
9.1.1	How to Configure Product Settings for the Division	81
9.1.2	(Participant Admins Only) How to Configure Product Settings for a Specific Role ..	83
9.1.3	How to View Product Settings for Your Division or Specific Roles (User or Administrator).....	84
9.1.4	How to Restore Default Product Settings	84

10	Certificate Management.....	86
10.1	Requesting Certificates	86
10.1.1	How to Request an SSL Plus, EV SSL Plus, EV Multi-Domain, Multi-Domain SSL, and Wildcard Plus Certificate	86
10.1.2	How to Request a Grid Host SSL and Grid Host Multi-Domain SSL Certificate	91
10.1.3	How to Request a Client Certificate.....	95
10.1.4	How to Request Grid Robot and Grid Premium Certificates	98
10.1.5	How to Resend an Email Validation for DigiCert “Client Certificate” Email.....	101
10.1.6	How to Resend the Create Your DigiCert “Client Certificate” Email	102
10.1.7	How to Request a Code Signing Certificate.....	102
10.1.8	How to Request an EV Code Signing Certificate.....	105
10.1.9	How to Request a Document Signing Certificate	108
10.1.10	How to Add Multiple Wildcard Domains to a Certificate.....	110
10.2	Managing Certificate Request Approvals and Rejections	111
10.2.1	How to View Certificate Requests	111
10.2.2	How to Edit a Certificate Request	111
10.2.3	How to Approve a Certificate Request.....	111
10.2.4	How to View Who Requested a Certificate (Approved Requests).....	112
10.2.5	How to View Who Approved a Certificate Request (Approved Requests).....	112
10.2.6	How to View EV Certificate Request Approvers.....	113
10.2.7	How to View CS Approvers	113
10.2.8	How to View EV CS Approvers	113
10.2.9	How to Reject a Certificate Request.....	114
10.3	Managing Certificates.....	114
10.3.1	How to View Certificates	114
10.3.2	How to Download a Certificate.....	115
10.3.3	How to Adjust Certificate Renewal Notifications.....	116
10.3.4	How to Change the Default Renewal Message for All Certificates	116
10.3.5	How to Add/Change a Renewal Message for a Specific Certificate.....	117
10.3.6	How to Disable Renewal Notices for a Specific Certificate	117
10.3.7	How to Re-enable Renewal Notices for a Specific Certificate.....	117

10.3.8	How to Add Additional Email Addresses to Receive Certificate Renewal Notifications.....	118
10.3.9	How to Activate Your EV Code Signing Hardware.....	118
10.3.10	How to Install Your EV Code Signing Certificate on Your Own Secure Token.....	120
10.3.11	How to Activate Your Document Signing Hardware.....	124
10.3.12	How to Install Your Document Signing Certificate on Your Own Secure Token.....	126
10.3.13	How to Place a Request to Revoke a Certificate.....	131
10.3.14	How to Approve a Certificate Revoke Request.....	131
10.3.15	How to Reject a Certificate Revoke Request.....	131
10.3.16	How to Request a Duplicate Certificate.....	132
10.3.17	How to Reissue a SSL Certificate.....	135
10.3.18	How to Renew a SSL Plus, EV SSL Plus, EV Multi-Domain, Multi-Domain SSL, and a Wildcard Plus Certificate.....	140
10.3.19	How to Renew a Grid Host SSL and Grid Host Multi-Domain SSL Certificates...	144
10.3.20	How to Reissue a Code Signing Certificate.....	147
10.3.21	How to Renew a Code Signing Certificate.....	148
10.3.22	How to Reissue an EV Code Signing Certificate.....	151
10.3.23	How to Renew an EV Code Signing Certificate.....	153
10.4	Intermediate Certificates.....	155
	About DigiCert.....	156

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.

1.1.1 Administrator Role

The primary function of the Administrator role is 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 your 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.

1.1.3 EV Verified User

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

1.1.4 CS Verified User

CS Verified Users can approve certificate requests for Code Signing Certificates. For a user to be a CS 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 requests 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

Use this instruction to create new user accounts yourself. After creating the account, the user is sent an email with a link that allows them to set a password and to log into their account.

1. In your account, in the sidebar menu, click **Account > Users**.
2. On the **Users** page, click **Add User**.
3. On the **Add User** page, in the **User Details** section, provide the following details for the 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.
The user will be sent an email with instructions for creating a password to log into their account.

Phone: Type a phone number at which the user can be reached.
A phone number is only required if the user will be an **EV Verified User**, an **EV CS Verified User**, and/or a **CS Verified User**.

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

4. In the **User Access** section, provide the following access information for user:

Username: The username will auto-populate.
Although you can create a unique username for each user, we recommend using their email address (e.g., *john@example.com*).

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

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

5. When you are finished, click **Add 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 > Users**.
2. On the **Users** page, click the **"User Name"** link for the person to whom you need to resend the **DigiCert User Account Created - Action Required** email.
3. On the **"User's Name"** 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 Invite New Users to Join Your Account

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

1. In your account, in the sidebar menu, click **Account > User Invitations**.
2. On the **User Invitations** page, click **Invite New User**.
3. In the **Invite New Users** window, do the following:

Email Addresses In the box, type the email addresses (comma separated) of the new users who you want to invite to join your account.

Send custom message

1. Check the box.
2. In the field that appears, type the message that you want to include in the new account invitee email.

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

You should receive the ***"Invitations successfully sent"*** message.

1.2.4 How to Create Your New User (Invitee) Account

1. In your email account inbox, locate the ***Please create your user login for DigiCert CertCentral*** email, and click the link provided for creating your account user profile.
2. On the **Create CertCentral User** page, under **Personal Information**, provide the following information:

- **Email Address**
- **First Name**
- **Last Name**
- **Phone Number**
- **Job Title**

3. Under **Account information**, do the following:

Username Create a username per your company's policy (for example they may want you to use your email address as your username).

Password/Confirm Password Create and confirm the password you want to use to log into your account.

Security Question/Security Answer Select a security question and then answer it.

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

- You should receive a ***Your request has been received*** email, which let you know that your account request has been sent to the account administrator for approval
- You cannot log into your account until your account request has been approved by your administrator, and you are notified via email (**User account for “User Name” has been approved**) that your request has been approved.

1.2.5 How to Approve/Activate an Invitee's User Account

1. In your account, in the sidebar menu, click **Account > User Invitations**.
2. On the **User Invitations** page, use the filters and column headers to locate the new user account you want to approve/activate.
3. To the right of the user account to want to activate, click the **Details** link.
4. On the **User Invitation to “Username”** page, click **Approve**.
5. In the **Approve User Invitation** window, provide the following information:

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

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

Approval Message to Invitee Enter a message to be included in the approval email.

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

The new user is added to your account (**Account > Users**). The new user is sent an email (**User account for “User Name” has been approved**) with a link that takes them to the account login page.

1.2.6 How to Edit User Accounts

If you need to edit your own user details, see [How to Edit Your Profile](#).

1. In your account, in the sidebar menu, click **Account > Users**.
2. On the **Users** page, click the **“User Name”** link for the person whose details you need to modify.
3. On the **“User’s Name”** page, update the user’s details and access as needed. (Refer to [How to Add Users to Your Account](#) for detailed descriptions.)

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

1.2.7 How to Delete (Remove) User Accounts

1. In your account, in the sidebar menu, click **Account > Users**.
2. On the **Users** page, click the **"User Name"** link for the user account that you need to delete.
3. On the **"User's Name"** page, click **Delete User**.

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

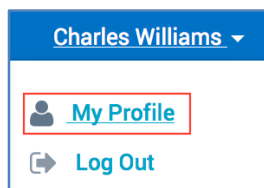
4. In the **Delete User** window, when you receive the **"Are you sure you want to delete 'User Name' user account?"** message, click **Delete User**.

The user should be removed from the account.

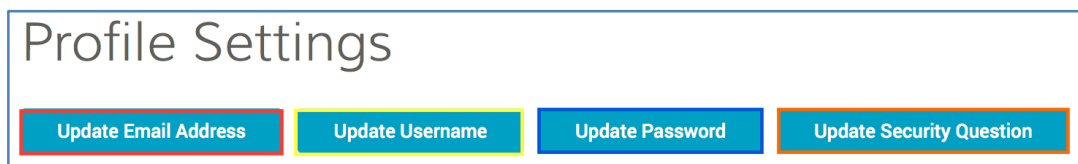
1.2.8 How to Edit Your Profile

When you are logged into your account, use this instruction to edit your user information: name, phone number, job title, email address, username, password, or security question.

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



2. On the **Profile Settings** page, update your details, such as phone number, as needed. (Refer to [How to Add Users to Your Account](#) for detail descriptions.)



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. Click **Update Email Address**.

- ii. On the **Update Email Address** page, in the **New Email** box, type your new email address.
- iii. In the **Password** box, type your password
- iv. Then click **Save Changes**.

You should receive 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. Click **Update Username**.
- ii. On the **Update Username** page, in the **New Username** box, type your new username.
- iii. In the **Password** box, type your password
- iv. Then click **Save Changes**.

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

5. **To Change Your Password:**

- i. Click **Update Password**.
- ii. On the **Update Password** page, in the **Current Password** box, type your password.
- iii. In the **New Password** and **Re-enter New Password** boxes, create and confirm your new password.
- iv. Then click **Save Changes**.

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. Click **Update Security Question**.

- ii. On the **Update Security Question** page, in the **Select a security question** drop-down list, select a new security question.
 - iii. In the **Answer your question** box, type the answer to your new security question.
 - iv. In the **Current Password** box, type your password.

If you changed your password during this session in your account, make sure to use your new password.
 - v. Then click **Save Changes**.
7. When you are finished, on the **Profile Settings** page, got to the bottom of the page and click **Save Changes**.

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

1.2.9 How to View Account Users

1. In your account, in the sidebar menu, click **Account > Users**.
2. On the **Users** page, use the available filters, such as **Division**, or the **Search** bar to locate a specific user.
3. To see the user's profile details, click the **"User Name"** link.

1.2.10 How to Unlock a "Locked" Account

This instruction covers 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

1.2.11 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.

1.2.12 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 > Account Access**.
2. On the **Account Access** page, under **API Keys**, click **Add API Key**.
3. Next, open a text editor (such as Notepad).
4. In the **Add API Key** window, do the following:

Description	Type a description/name for the API key.
--------------------	--

User In the drop-down list, select the user to whom you want to assign the API key.

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

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

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

1.3.2 How to Revoke (Remove) an API Key

1. In your account, in the sidebar menu, click **Account > Account Access**.
2. On the **Account Access** page, under **API Keys**, to the right of the API key that you need to revoke, click **Revoke**.
 - i. If you do not see the key listed on this page, in the bottom right corner below the list of keys, click **View All "# API Keys**.

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

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

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

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

1.3.3 How to View API Keys and API Key Users

1. In your account, in the sidebar menu, click **Account > Account Access**.
2. On the **Account Access** page, under **API keys**, you can view all or some of the API keys that you have issued.

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

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

4. On the **API Keys** page, all keys are listed.
5. Use the dropdown list, search box, and column headers to locate specific keys.

1.4 Managing Guest URLs

Typically, Administrators manage the administrators and user accounts in their Division(s). Managing users may include creating and editing Guest URLs so that user can order certificates but

1.4.1 Guest URLs

A Guest URL is a link to a specific certificate’s request page. You can create Guest URLs for the following certificates:

SSL

- SSL Plus
- Multi-Domain SSL
- Wildcard Plus
- EV SSL Plus
- EV Multi-Domain

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 Multi-Domain SSL

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 > Account Access**.
2. On the **Account Access** page, under **Guest URLs**, click **+ Add Guest URL**.
3. In the **Add Guest URL** window, do the following:

Description

Type a brief description for the URL that makes it easily identifiable in the list of Guest URLs.

Allowed Certificate Types

Click in the drop-down list select the certificate(s) that the Guest URL allows the guest user to request. You can select a single or multiple certificates.

Certificate Validity Periods

Click in the drop-down list select the validity period(s) for the certificate(s) that you selected. You can select a single or multiple periods.

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.

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

You can now send the Guest URL to a “guest” and let them order a specific certificate(s).

1.4.3 How to Send the Guest URL to a “Guest”

1. In your account in the sidebar menu, click **Account > Account Access**.
2. On the **Account Access** page, under **Guest URLs**, you can view all or some of the guest URLs that you have created.
 - a. To see all your guest URLs, in the bottom right corner, below the list of URLs, click **View All “#” Guest URLs**.

Note: The **View All “#” Guest URLs** link only appears if you have created more than 10 guest URLs.

- b. On the **Guest URLs** page, all guest URLs are listed.
3. To the right of the Guest URL that you want to share, click the **Share this URL** button (that is next to the **Information** button).



4. In the **Share URL** window, in the **Send the Guest URL to the following email address** box, type the email addresses (comma separated) of the guest to whom you want to send the guest URL.
5. When you are finished, click **Email this URL**.

1.4.4 How to Edit a Guest URL

1. In your account, in the sidebar menu, click **Account > Account Access**.
2. On the **Account Access**, under **Guest URLs** page, click the **"Description"** link for the Guest URL that you need to edit.
 - i. If you do not see the guest URL listed on this page, in the bottom right corner below the list of URLs, click **View All "#" Guest URLs**.

Note: The **View All "#" Guest URLs** link only appears if you have created more than 10 guest URLs.

- ii. On the **Guest URLs** page, click the **"Description"** link for the Guest URL that you need to edit.
3. In the **Edit Guest URL** window, edit the description, make certificate changes, and update the validity periods. (See [How to Create a Guest URL](#).)

Notes: You can select a single or multiple certificates. 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**.

You can now send the updated Guest URL to a "guest" and let them order a specific certificate(s).

1.4.5 How to Delete a Guest URL

1. In your account, in the sidebar menu, click **Account > Account Access**.
2. On the **Account Access** page, under **Guest URLs**, to the right of the URL that you need to delete, click **Delete**.
 - i. If you do not see the URL listed on this page, in the bottom right corner below the list of URLs, click **View All "#" Guest URLs**.

Note: The **View All "#" Guest URLs** link only appears if you have created more than 10 guest URLs.

- ii. On the **Guest URLs** page, to the right of the URL that you need to delete, click **Delete**.

CAUTION: In the **Delete Guest URL** window, do not click **Delete** unless you are sure that you want to delete the Guest URL. Deleting a Guest URL disables anyone who is using it to request a certificate.

3. In the **Delete Guest URL** window, under the ***"Are you sure you want to delete the Guest URL 'Description'? It will stop working immediately, and cannot be undone."*** message, click **Delete**.

All copies of the Guest URL link should no longer work.

1.4.6 How to View Guest URLs

1. In your account, in the sidebar menu, click **Account > Account Access**.
2. On the **Account Access** page, under **Guest URLs**, you can view all or some of the guest URLs that you have created.
3. To see all your guest URLs, in the bottom right corner, below the list of URLs, click **View All "#" Guest URLs**.

Note: The **View All "#" Guest URLs** link only appears if you have created more than 10 guest URLs.

4. On the **Guest URLs** page, all guest URLs are listed.
5. Use the search box and column headers to locate guest URLs.

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 > Divisions**.
2. On the **Divisions** page, click **New Division**.
3. On the **New Division** page, enter the following information to about the Division:

After creating the division, you can go back any time and modify these details.

*Name:	Type the name of the Division.
Description:	Type a brief description that provides basic information about the Division.
Send request renewal notifications to	Enter the email(s) for the person(s) who you want to receive request renewal notifications (comma separated).
*Certificates can be ordered for:	(NREN Administrators only)
<ul style="list-style-type: none">• All organizations• Specific organizations	Select the organizations (All or Specific) for which the division can order certificates. In the drop-down list, select the specific organization(s).

Certificates can be ordered for:

- **All domains**
- **Specific domains**

(NREN Administrators only)

Select the domains (All or Specific) for which the division can order certificates.

List the specific domains (comma separated)

4. Under **Division 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 (e.g., *john.doe@example.com*).

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

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 Division**, 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 administrator creates their password, they should log into their account and update their user details; add a phone number and job title (see [How to Edit Your Profile](#)).

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 (see [Roles and Account Access](#)).

2.1.2 How to Set Division Preferences

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

2. On the **Divisions** page, click **My Division**.
3. On the “**Division Name**” page, click **Edit Preferences**.

Subdivision Admins Note:

If your division admin allows you to configure your own division preferences, on the **Division Preferences** page, under **Use default settings**, click **Use My Own Settings**.

4. **Set Permissions**

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

On the **Division Preferences** page, set permissions:

Use these settings for my division

Select this option if you want your settings to apply only to your division.

Use these settings for my division and any subdivisions

Select this option if you want your settings to apply to your division and all subdivisions.

Allow subdivisions to override these settings

Check this box if you want the subdivisions to be able to set up their own division preferences.

5. **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)

6. **Create a Custom Request 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

7. **Configure Client Certificate Settings**

When issuing client certificates, end users (e.g., employees) may have problems that need taken care of or questions that need answered. Use the **Client Certificate Settings** to provide end users with a message and contact information about getting support/help with their client certificates.

Note: The contact information that you enter below is sent in the **Create Your “Client Certificate” DigiCert** email.

- i. In the **Contact Email** box, enter the email address for your client certificate support contact.
- ii. In the **Contact Phone Number** box, enter the phone number for your client certificate support contact.
- iii. In the **Support Message** box, type a message to your end users letting them know details about how they should contact for help with their client certificate.

8. **Configure Certificate Renewal Settings**

- i. In the **Send request renewal notifications to** box, enter the email addresses for the people you want to receive the renewal notifications (comma separated).
- ii. Under **When certificates are scheduled to expire in**, check the boxes for when you want renewal notices sent.
- iii. In the **Default Renewal Message** box, type a renewal message to be included in your renewal notification emails.

9. **Configure Advanced Settings**

i. **Configure Use Plus Feature for Subdomains**

DigiCert SSL Certificates come with a “Plus” feature which lets you automatically secure both *yoursite.com* and *www.yoursite.com*. You can use the **Use Plus Feature for Subdomains** to extend this behavior to your subdomains and secure both *subdomain.yoursite.com* and *www.subdomain.yoursite.com*.

- a) Click **+ Advanced Settings**.

- b) Under **Plus Feature**, check **Use Plus Feature for Subdomains**.

- ii. **Configure Certificate Format**

By default, your certificates are sent via email as an attachment. The **Certificate Format** feature lets you choose whether to receive your certificates as attachments or in plain text in the body of the email.

- a) Click **+ Advanced Settings**.
- b) Under **Certificate Format**, do one of the following:

Attachment.	To receive your certificates as attachments, select this option.
--------------------	--

Plain Text.	To receive your certificates as plain text in the body of the email, select this option.
--------------------	--

- iii. **Configure Domain Control Validation (DCV)**

- a) **DCV Methods**

By default, when you add domains to your account for prevalidation, a DCV email is sent to the validation contact for the organization associated with the domain.

If you prefer, you can configure your account to use a DNS-based domain validation method for your organization or the organization's that you service.

Note: When a certificate request is approved for a domain that has not been prevalidated for (added to) your account, that domain is automatically submitted for validation using the email DCV method.

- 1) Click **+Advanced Settings**.
 - 2) Under **DCV Methods**, check **Show DNS CNAME as an alternative DCV method when managing / adding domains**.

b) **For automatically submitted domains, send the DCV emails to**

By default, when you add a domain to your account for prevalidation, a DCV email (validation email) is sent to the organization's validation contact.

For a certificate request that must be approved for a domain, which has not been prevalidated for your account, you can opt to have additional DCV emails (validation emails) sent to individuals other than the organization validation contact.

- 1) Click **+Advanced Settings**
- 2) Under **For automatically submitted domains, send the DCV emails to**, check the emails addresses to which you want additional DVC emails sent.

iv. **(Admins only) Configure Request Auto Approval**

You must be an administrator to configure this setting. This setting only works for the certificates that you have permissions to approve.

For example, you must be an EV verified approver, to have your EV Certificate requests automatically approved.

- a) Click **+ Advanced Settings**.
- b) Under **Request Auto Approval**, check **Automatically approve certificate requests**.

10. When you are finished, click **Save Settings**.

2.1.3 How to Edit a Division's Details

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

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

- ii. On the **Divisions** page click **My Division**.
- iii. On the **"Division Name"** page, click **Edit Division**.

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

- i. In your account, in the sidebar menu, click **Account > Divisions**.
 - ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose details you need to edit.
3. On the **"Division's Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, modify the division's information as needed:

*Name:	Edit/change the name of the Division.
Description:	Edit/change the brief description that provides basic information about the Division.
Send request renewal notifications to	Add/remove emails for the personnel who you want to receive request renewal notifications (comma separated).
eKey (for co-branded login URLs):	Edit/change the name that you want to use for your ekey (e.g., <i>YourDivisionEkey</i>). See How to Edit a Division Ekey .
Auto Renewal User:	In the drop-down list, select a user to receive auto renewal email notifications.
Certificates can be ordered for: <ul style="list-style-type: none">• All domains• Specific domains	Select the domains (All or Specific) for which the division can order certificates. List the specific domains (comma separated)

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 out 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 > Divisions**.

2. On the **Divisions** page, click the **"Division Name"** link for the Division that you need to deactivate.
3. On the **"Division Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, click **Deactivate**.
5. In the **Deactivate Division** window, under the **"Are you sure you want to deactivate 'Division Name'?"** message, click **Deactivate**.

The division and any of its subdivisions are removed from the **Divisions** page (**Account > 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 > 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. In the **Activate Division** window, under the **"Are you sure you want to activate 'Division Name'?"** message, click **Activate**.

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:**

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

- ii. On the **Divisions** page, click **My Division**.
2. **If you are adding a logo for another Division:**
 - i. In your account, in the sidebar menu, click **Account > Divisions**.
 - ii. On the **Divisions** page, click the **"Division Name"** link for the Division to which you want to add a logo.
3. On the **"Division Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, under **Division Logo**, click **Upload Logo** to browse for, select, and open the logo *.jpeg*, *.png*, or *.gif* file.

2.2.2 How to Replace a Division Logo

1. **If you are replacing the log for your Division:**
 - i. In your account, in the sidebar menu, click **Account > Divisions**.

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.
 - ii. On the **Divisions** page, click **My Division**.
2. **If you are replacing the logo for another Division:**
 - i. In your account, in the sidebar menu, click **Account > Divisions**.
 - ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose logo you want to replace.
3. On the **"Division Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, under **Division Logo**, click **Change** to browse for, select, and open the new logo *.jpeg*, *.png*, or *.gif* file.

2.2.3 How to Remove a Division Logo

1. **If you are removing the log for your Division:**
 - i. In your account, in the sidebar menu, click **Account > Divisions**.

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.
 - ii. On the **Divisions** page, click **My Division**.
2. **If you are removing the logo for another Division:**

- i. In your account, in the sidebar menu, click **Account > Divisions**.
 - ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose logo you want to remove.
3. On the **"Division Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, under **Division Logo**, click **Remove** to remove the logo .jpeg, .png, or .gif file.

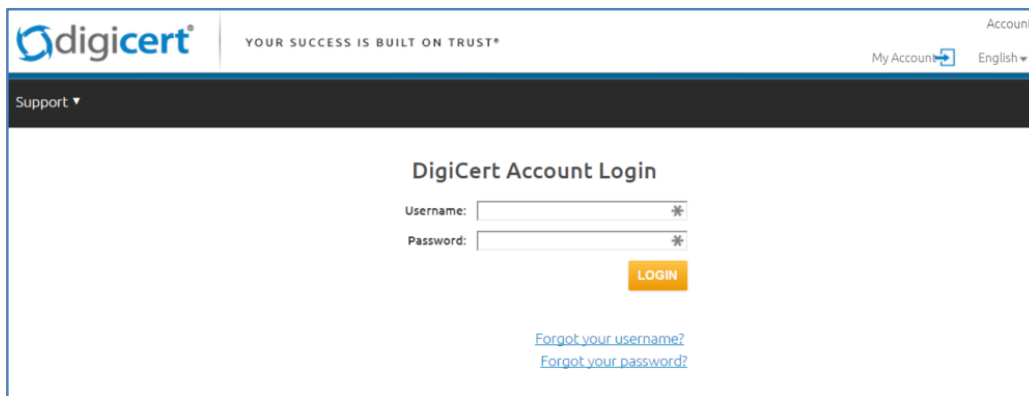
2.3 Managing Division Ekeys

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.

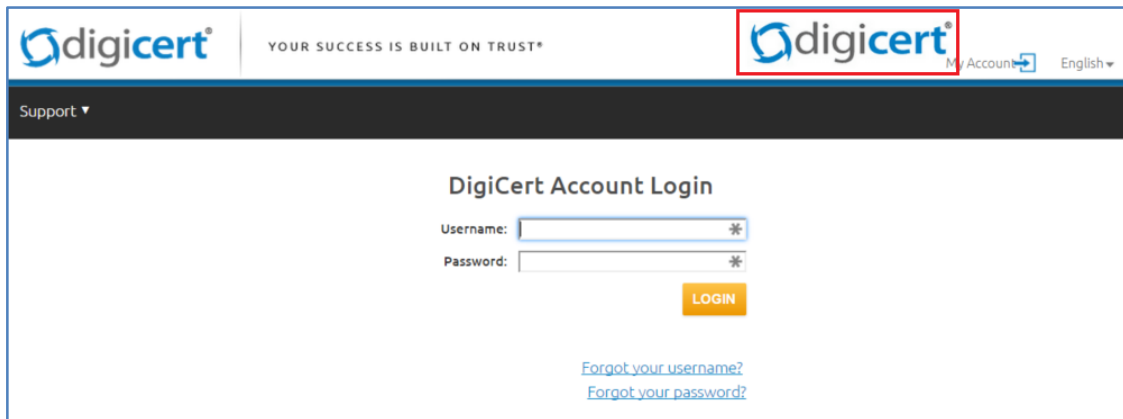
Note: If your Division was created before 2015, February 12, an ekey was not automatically generated for your Division. If you want to use an ekey to access your Division account login page, you can create your own Division ekey. See [How to Create a Division Ekey](#).

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 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:**

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

- ii. On the **Divisions** page, click **My Division**.

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

- i. In your account, in the sidebar menu, click **Account > Divisions**.
- ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose ekey you want to create.

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

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

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

On the **"Division Name"** page, next to **Branded Login URL**, you should now see the ekey (branded login URL).

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.

2.3.2 How to View a Division Ekey

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

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

- ii. On the **Divisions** page, click **My Division**.

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

- i. In your account, in the sidebar menu, click **Account > Divisions**.
- ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose ekey you want to see.

3. On the **"Division Name"** 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.

2.3.3 How to Edit a Division Ekey

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

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

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

- ii. On the **Divisions** page, click **My Division**.

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

- i. In your account, in the sidebar menu, click **Account > Divisions**.
- ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose ekey you want to edit.

3. On the **"Division Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, in the **eKey (for co-branded login URLs)** box, type the new name that you want to use for you ekey (e.g., *MyDivisionEkey*).
5. When you are finished, click **Save Division**.

On the **"Division Name"** page, next to **Branded Login URL**, you should now see the new ekey (branded login URL)).

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 their account login page. However, those users will no longer see the Division logo on their account login page.

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

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

- ii. On the **Divisions** page, click **My Division**.

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

- i. In your account, in the sidebar menu, click **Account > Divisions**.
- ii. On the **Divisions** page, click the **"Division Name"** link for the Division whose ekey you want to delete.

3. On the **"Division Name"** page, click **Edit Division**.
4. On the **Edit "Division Name"** page, in the **eKey (for co-branded login URLs)** box, delete the name of the ekey.
5. When you are finished, click **Save Division**.

On the **"Division Name"** page, next to **Branded Login URL**, you should no longer see the ekey (branded login URL).

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 their division users and specific users with in their division.

3.1.1 How to Turn On IP Address Restrictions

1. In your account, in the sidebar menu, click **Settings > IP Restrictions**.
2. On the **IP Restrictions** page, under **IP Address Restrictions**, click **On**.
3. Click **Save**.

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

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

3.1.3 Account Wide: Configure IP Access Restriction Rules

1. In your account, in the sidebar menu, click **Settings > IP Restrictions**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.
3. On the **New IP Restriction** page, do the following:

*Restriction Type	In the drop-down list, select Account Wide .
*IP Range Start and IP Range End	Enter the parameters for the IP access restrictions. In other words, enter the IP addresses from which account users can access their account.
Description	Enter a description of the IP addresses from which account users can access their account.

4. When you are finished, click **Add Rule**.

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

3.1.4 A Specific User: Configure IP Access Restriction Rules

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.
3. On the **New IP Restriction** page, do the following:

*Restriction Type	In the drop-down list, select User .
*User	In the drop-down list, select the user to which you want to apply the rule.
*IP Range Start and IP Range End	Enter the parameters for your IP access restrictions. In other words, enter the IP addresses from which account users can access their account.
Description	Enter a description of the IP addresses from which the account user can access the account.

4. When you are finished, click **Add Rule**.

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

3.1.5 All Guest URLs: Configure IP Access Restriction Rules

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.

3. On the **New IP Restriction** page, do the following:

*Restriction Type	In the drop-down list, select All Guest URLs .
*IP Range Start and IP Range End	Enter the parameters for your IP access restrictions. In other words, enter the IP addresses from which guest users can order their certificate(s).
Description	Enter a description of the IP addresses from which guest certificates can be ordered.

4. When you are finished, click **Add Rule**.

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

3.1.6 A Specific Guest URL: Configure IP Access Restriction Rules

1. In your account, in the sidebar menu, click **Settings > IP Access Restrictions**.
2. On the **IP Restrictions** page, under **IP Restriction Rules**, click **Add New Rule**.
3. On the **New IP Restriction** page, do the following:

*Restriction Type	In the drop-down list, select Guest URL .
*Guest Key	In the drop-down list, select the guest URL (listed by the description name) to which you want to apply the rule.
*IP Range Start and IP Range End	Enter the parameters for your IP access restrictions. In other words, enter the IP addresses from which guest users can order their certificate(s).
Description	Enter a description of the IP addresses from which guest certificates can be ordered.

4. When you are finished, click **Add Rule**.

Your rule is now listed on the **IP Restrictions** page (**Settings > IP Restrictions**) under **IP Restrictions Rules** with a **Rule Scope – Guest URL: “Description”**.

3.1.7 How to View IP Access Restriction Rules

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

3.1.8 How to Delete an IP Access Restriction Rule

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

4 Authentication Settings

By default, your DigiCert account requires one form of authentication—a password. For those who want to add an extra layer of security to their accounts, we also support two-factor authentication, which we recommend setting up for your DigiCert account.

4.1 Password Requirements

The strength of a password is determined by password length (minimum number of characters), number of categories required (numbers, symbols, etc.) in the password, and how often it must be renewed (time that passes before a new one must be created).

Before adding users to your DigiCert account, we recommend configure your password requirements (length, categories, and expiration) to meet your organization's security standards.

4.1.1 How to Configure Password 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 authentication settings, on the **Authentication Settings** page, under **Use default settings**, click **Use My Own Settings**.

2. **Set Permissions:**

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

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

Use these settings for my division Select this option if you want the password requirements that you configure to apply to your division only.

When your subdivision admins navigate to the **Authentication Settings** page (**Settings > Authentication Settings**), they control their password requirements.

Use these settings for my division and subdivisions

Select this option if you want the password requirements that you configure 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 authentication settings."*** message.

Allow subdivisions to override these settings

Check this box if you want your subdivisions to be able to set their own password 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, they defer to the password requirements that you configured for them.

- **Use My Own Settings**

If the admin clicks this option, they control their password requirements. They are required to create their own password requirements for their division.

3. On the **Authentication Settings** page, in the **Minimum Password Requirements** section, do the following:

Minimum Length:

In the drop-down list, select the minimum character count for your DigiCert account passwords.

Minimum Categories:

In the drop-down list, select the minimum number of categories that must be used in creating your DigiCert account passwords.

- Upper: upper case letters

- Lower: lower case letters
- Numbers: 1 thru 9 and 0
- Symbols: Unicode characters count as symbols

Expires After: In the drop-down list, select how long you want a password to be good for before users must to create a new one.

4. When you are finished, click **Save Settings** (in the **Two Factor Authentication** section).

You have successfully configured your password requirements.

4.2 DigiCert Two-Factor Authentication

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

4.3 Setting Up Two-Factor Authentication

Before you can 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.

4.3.1 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. Microsoft Edge, 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).

4.3.2 One-time Password Requirement

An OTP App installed on a mobile device allows users to log in from any computer/device form which they can access their DigiCert account. 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

4.4 Configuring Two-Factor Authentication Requirements

These instructions are for administrators only and explain how to configure 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.

4.4.1 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, in the **Two-Factor Authentication** section, under **Two-Factor Auth Status**, click **On**.

3. **Set Permissions:**

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

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

Use these settings for my division

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

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

Use these settings for my division and 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 authentication settings."*** message.

Allow subdivisions to override these 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. When you are finished, click **Save Settings**.

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

4.4.2 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, in the **Two-Factor Authentication** section, under **Two-Factor Auth Status**, click **Off**.

3. **Set Permissions:**

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

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

Use these settings 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.

Use these settings for my division and 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 authentication settings."*** message, and two factor authentication is disabled for their division.

Allow subdivisions to override these 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. When you are finished, click **Save Settings**.

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

4.4.3 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, in the **Two-Factor Authentication** section, 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.

Add Two Factor Requirement

Create a Two-Factor Authentication Requirement

OTP authentication requires the use of any mobile app that supports the Time-Based One-Time Password (TOTP) protocol.

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

Applying this rule will allow users to configure OTP during their next login.

Authentication Type:

- ☒ One-Time Password (OTP)
- ☐ Client Certificate

Apply Rule To:

- ☒ All account users
- ☐ All users in division:
- ☐ Specific user:

Charles

Create Requirement

Cancel

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

Division Admin Note:

If you are a Division Admin and have selected **Use these settings for my division and 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**.

You have now successfully configured a two-factor authentication requirement for all account users.

4.4.4 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.

Create a Two-Factor Authentication Requirement

A client certificate is an authentication certificate that is generated and stored on a specific browser,
Applying this rule will allow users to generate a browser client certificate during their next login.

Authentication Type:

☐ One-Time Password (OTP)

☒ Client Certificate

Apply Rule To:

☐ All account users

☒ All users in division:

Charles Division

☐ Specific user:

Charles

Create Requirement **Cancel**

- Under **Apply Rule To**, select **All users in division**.
- 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 **Use these settings for my division and subdivisions** so that the rule is actually applied to that division.

- Click **Create Requirement**.

You have now successfully configured a two-factor authentication requirement for all users in the specified Division.

4.4.5 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.

- 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.

Create a Two-Factor Authentication Requirement

A client certificate is an authentication certificate that is generated and stored on a specific browser,
Applying this rule will allow users to generate a browser client certificate during their next login.

Authentication Type:

☐ One-Time Password (OTP)

☒ Client Certificate

Apply Rule To:

☐ All account users

☐ All users in division:

Charles Division

☒ Specific user:

Charles

Create Requirement **Cancel**

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**.

You have now successfully configured a two-factor authentication requirement for the specified user.

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

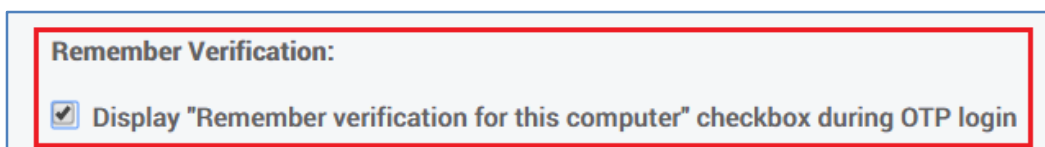
Providing OTP authenticators with this option allows them to verify the computer from which they are logging in. For the next thirty days, they can bypass entering the verification code each time they log in from that computer. At the end of the thirty days, OTP authenticators are required to enter their 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, in the **Two-Factor** Authentication section, 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. Click **Save Settings**.

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.

4.4.7 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, in the **Two-Factor Authentication** section, under **Two-Factor Authentication Requirements**, to the right of the requirement that you want to remove, click **Delete**.

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

Two-Factor Authentication Requirements			
Add New Requirement			
Authentication Type	Applies To	Date Added	
One-Time Password (OTP)	2-Factor Authentications	2016-01-13 19:32	✖ Delete
Client Certificate	Two-Factor Authentication	2016-01-13 19:24	✖ Delete


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**, to the right of the certificate that you want to nullify, click **Reset**. The certificate should no longer be listed.

Issued Client Certificates		
User	Date Added	
Two-Factor Authentication	2016-01-13 19:25	 Reset


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.

One-Time Password (OTP) Devices		
User	Date Added	
2-Factor Authentications	2016-01-13 19:34	 Reset

4.4.8 How to View Two-Factor Authentication Requirements

1. In your account, in the sidebar menu, click **Setting > 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 **Two-Factor Authentication Requirements**.

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

Two-Factor Authentication Requirements		
Add New Requirement		
Authentication Type	Applies To	Date Added
One-Time Password (OTP)	2-Factor Authentications	2016-01-13 19:32
Client Certificate	Two-Factor Authentication	2016-01-13 19:24

4.4.9 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, in the **Two-Factor Authentication** section, under **Issued Client Certificates**, the Client Certificate authenticators are listed and under **One-Time Password (OTP) Devices**, the OTP authenticators are listed.

Issued Client Certificates	
User	Date Added
Two-Factor Authentication	2016-01-13 19:25
One-Time Password (OTP) Devices	
User	Date Added
2-Factor Authentications	2016-01-13 19:34

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.

4.5 Two-Factor Authentication: User Instructions

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

4.5.1 How to Initialize Your OTP App Device

In addition to your password, a One Time Password (OTP) is required for your DigiCert account. The next time you log into your DigiCert account, you will be asked to initialize your OTP App Device.

The following list contains the OTP Applications that we that will work with your account:

- **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**.

One-Time Password (OTP) Device Initialization


Step 1 - Scan QR Code with OTP Device

In order to increase login security, two-factor authentication has been enabled on your account. Please follow the steps below to set up two-factor authentication.

If you have not already done so, install an application that supports the Time-Based One-Time Password (TOTP) protocol on your mobile device. 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



Key: MK7Y3OJQ4VNBPRIM

Step 2 - Verify Device

In order to verify that the device was properly configured, please enter the code displayed on the device.

Submit

4. You should now be logged in to your account.

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

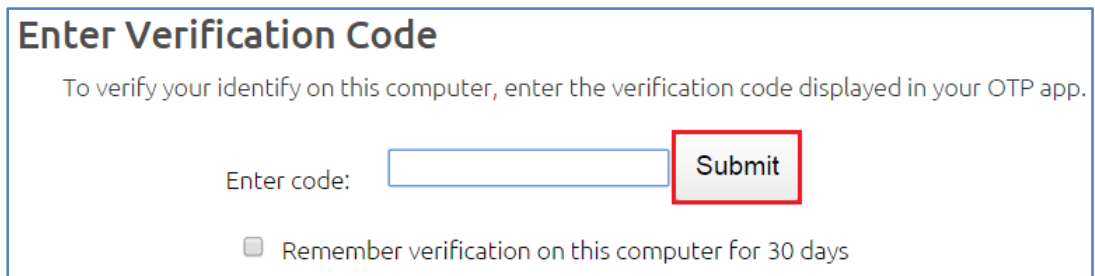
4.5.2 How to Sign In with Your OTP App Device

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.



Enter Verification Code

To verify your identify on this computer, enter the verification code displayed in your OTP app.

Enter code: **Submit**

☐ Remember verification on this computer for 30 days

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.

4.5.3 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 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](#) .

4.5.4 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, Microsoft Edge, 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**.

Two-Factor Authentication Client Certificate Initialization

Using a 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 the Console.

- **Windows** installs the Client Certificate in its own Certificate Store and can be accessed by **Chrome and Internet Explorer**.
- **Macintosh** installs the Client Certificate in its own Certificate Store and can be accessed by the keychain for **Safari and Chrome**.
- **Firefox** installs the Client Certificate in its own Certificate Store and can only be accessed by **Firefox (Windows or Mac)**.

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.

4.5.5 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, Microsoft Edge, 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

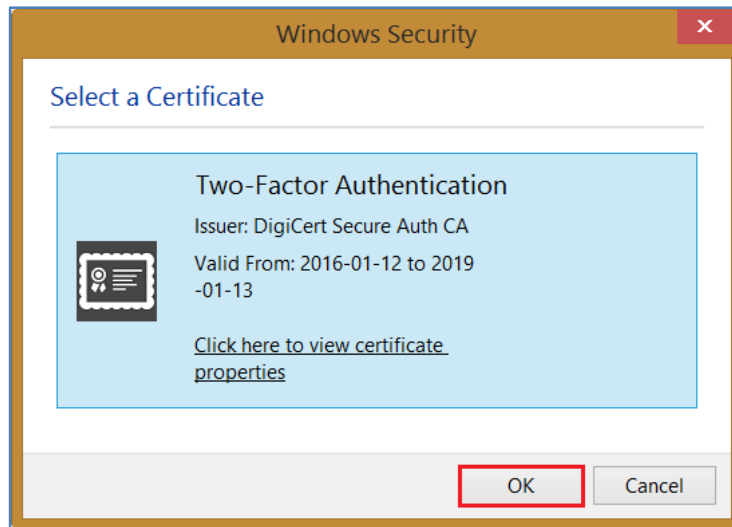
1. Log into your DigiCert account.

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.

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



4.5.6 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](#).

4.6 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.

4.6.1 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, in the **Two-Factor Authentication** section, under **One-Time Password (OTP) Devices**, locate the device that you need to reset and click **Reset**.

One-Time Password (OTP) Devices		
User	Date Added	
2-Factor Authentications	2016-01-13 19:34	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.

4.6.2 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**.

Issued Client Certificates		
User	Date Added	
Two-Factor Authentication	2016-01-13 19:25	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.

4.6.3 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](#) .

4.6.4 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 Report** (GÉANT admins) or click **Certificates > Orders Report** (NREN and Participant admins).
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 your report, click **Update Report**.

Your orders report should be displayed on the page.

6 Account Settings (GÉANT Admin)

Before emails are sent out from the account, you may want to assign an email account to receive a copy of all emails sent out from the account (e.g., approval notifications). You may also want to configure when you receive renewal notifications and add a default renewal message.

6.1 How to Set Up Your Email Notification Account(s)

1. In your account, in the sidebar menu, click **Settings > Notifications**.
2. On the **Notifications** page, in the **Send all account notifications to** box, add the email address(es) that you want copied on all emails sent from your account.

Note: If you are setting up multiple notification accounts, use commas to separate the email addresses.

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

You have successfully set up your account email notification account.

6.2 How to Configure Certificate Renewal Settings

1. In your account, in the sidebar menu, click **Settings > Notifications**.
2. On the **Notifications** page, under **Renewal Settings for GEANT Association**, in the **Send renewal notification to** box, enter the email addresses for the people you want to receive the renewal notifications (comma separated).
3. Under **Send notifications to the addresses above when certificates are scheduled to expire in**, check the boxes for when you want renewal notices to be sent.
4. In the **Default Renewal Message** box, type a renewal message to be included in your renewal notification emails.
5. When you are finished, click **Save**.

7 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.

7.1 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.

7.1.1 How to Run an Audit

1. In your account, in the sidebar menu, click **Account > Audit Logs**.
2. On the **Audit Logs** page, do any of the following to filter the results of your activity report:

Note: To filter the results of the audit, choose a filter (for example **User**). Then, in the filter's drop-down list make a selection (for example select a user). Finally, wait for the filter to modify the audit log before using another filter.

Date Range In this box, set the date parameters for your activity report.
From: and **To:**

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**.

Action: In the drop-down list, select the action that you want to monitor (e.g., **Edit user**, **Add user**, **Login**, **Change password**, etc.).

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

Division: In the drop-down list, select the division whose account activity you want to monitor.

To see the activity of all Divisions, select **All**.

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**.

7.2 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.

7.2.1 How to Create an Audit Log Notification

1. In your account, in the sidebar menu, click **Account > Audit Logs**.
2. On the **Audit Logs** page, click **Audit Log Notifications**.
3. On the **Audit Log Notifications** 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.

Division: In the drop-down list, select the Division(s) whose account activity you want you want to monitor.

Notify me about: Check any of the following options:

- **Order Changes**

Check this box to be alerted of any certificate order changes.

- **User Changes**

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

- **User Logins**

Check this box to be alerted of all account logins.

- **Logins from invalid IP Addresses**

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

- **Certificate Revocations**

Check this box to be alerted of any certificate revocations (e.g., SSL, Code Signing, etc.).

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

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

8 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.

8.1 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 include 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.

8.1.1 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.

8.1.2 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.

8.2 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.

8.2.1 How to Add an Organization

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

***Legal Name:** Enter the organization's legally registered name (e.g., *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.

***Organizational Phone Number:** Enter the phone number at which the organization can be contacted.

***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**.

8.2.2 How to View Organizations and Their Details

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, use the dropdown lists, search box, and column headers to locate specific organizations.
3. Click the **"Organization Name"** link to view basic details about the organization, any pending certificate validations, and any active certificate validations.

8.2.3 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 **Certificates > Organizations**.
2. On the **Organizations** page, click the **"Organization Name"** link of the organization that you want to authorize for certificates.
3. On the **"Organization Name"** page, in the **Submit for Organization Validation** section, select the validation types for which the organization must be validated.
 - **OV - Normal Organization Validation**
 - **EV - Extended Organization Validation (EV)***
 - **Grid - Public Grid Host Validation**
 - **CS - Code Signing Organization Validation***
 - **EV CS - Code Organization Extended Validation (EV CS)***
 - **DS - Document Signing Validation**
4. If you selected **EV - Extended Organization Validation (EV)**, **CS - Code Signing Organization Validation**, and/or **EV CS - Code Organization Extended Validation (EV CS)**, you must select an organization contact(s) to be designated as an EV Certificate/EV Code Signing Certificate request approver and/or a Code Signing Certificate request approver.

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

Submit for Organization Validation

☐ OV - Normal Organization Validation

☒ EV - Extended Organization Validation (EV)

☐ Grid - Public Grid Host Validation

☒ CS - Code Signing Organization Validation

☒ EV CS - Code Signing Organization Extended Validation (EV CS)

☐ DS - Document Signing Validation

Organization Contacts

Add contacts to this organization

To submit this organization for EV, CS, or EV CS validation, at least one of your contacts needs to be verified.

[➕ Add from Existing Contacts](#)

Contact	Validate for	EV / EV CS	CS
<div>Submit for Validation</div>			

You must add a contact to submit for validation.

5. Under **Organization Contacts**, click **+Add from Existing Contacts**.
6. In the **Add Existing Contact** window, in the **Existing Users/Contacts** drop-down list, select your **EV/EV CS** and/or **CS** approver(s).

Note: For a user to appear in the drop-down list, they must have a job title and valid telephone number.
7. Click **Add Contact(s)**.
8. Once an approver is added, under **Contact**, you can add (check) or subtract (uncheck) what types of certificates they can approve (**EV/EV CS** or **CS**).

Note: Once you submit a contact to be verified for both types of certificates, **EV/EV CS** or **CS**, you cannot remove a certificate type.
9. Click **Submit for Validation**.

We will now validate the organization for the validation types that you selected and if necessary, the EV/EV CS and CS approvers that you selected.

8.2.4 How to View the EV, EV Code Signing (EV CS), and Code Signing (CS) Certificate Approvers for an Organization

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, click the **"Organization Name"** link of the organization for which you want to view the **EV/EV CS Verified User** and **CS Verified User**.
3. On the **"Organization Name"** page, under **Organization Contacts**, the **EV/EV CS** and **CS** approvers are listed.
 - If you see the clocks to the right of the approvers name, under **Validate for EV/EV CS CS**, the approver is pending verification (they cannot approve certificate requests yet).
 - If you see checkmarks to the right of the approvers name, under **Validate for EV/EV CS CS**, the approver can approve requests for the types of certificates that are checked.

8.2.5 How to Add EV/EV CS and CS Certificate Approvers for an Organization

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, click the **"Division Name"** link of the division for which you want to add **EV/EV CS** and **CS** Certificate request approvers.

3. On the **"Organization Name"** page, under **Organization Contacts**, do any of the following:
 - a. **To Add Additional EV/EV CS and CS Approvers:**
 - i. Click **+Add from Existing Contacts**.
 - ii. In the **Add Existing Contact** window, in the **Existing Users/Contacts** drop-down list, select additional **EV/EV CS** and/or **CS** approver(s).
 - iii. Once an approver is added, under **Contact**, you can add (check) or subtract (uncheck) what types of certificates they can approve (**EV/EV CS** or **CS**).

Note: Once you submit a contact to be verified for both types of certificates, **EV/EV CS** or **CS**, you cannot remove a certificate type.
 - b. **To Verify Existing Approvers for Additional Certificate Types:**
 - i. Under **Contact**, locate the user for which you need verified for another certificate type.
 - ii. Under Validate for EV/EV CS CS, check the certificate type that the approver needs added.

Note: Once you submit a contact to be verified for both types of certificates, **EV/EV CS** or **CS**, you cannot remove a certificate type.
4. When you are finished, click **Submit for Validation**.

8.3 (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.

Non-ASCII Characters:

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

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

8.3.1 (Non-ASCII Characters) Adding an Organization

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, click **New Organization**.
3. On the **Add 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 (e.g., ¥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.

***Organizational Phone Number:** Enter the phone number at which the organization can be contacted.

***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**.

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

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, click the **"Organization Name (non-ASCII characters)"** link of the organization (non-ASCII characters) for which you want to authorize Grid – Public Grid Host Certificate types.

3. On the **“Organization Name”** page, in the **Submit Organization for Validation** section, select **Grid - Public Grid Host Validation**.

Submit for Organization Validation

☐ **OV - Normal Organization Validation**

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

☒ **Grid - Public Grid Host Validation**

☐ **CS - Code Signing Organization Validation**

☐ **EV CS - Code Signing Organization Extended Validation (EV CS)**

☐ **DS - Document Signing Validation**

*** Simplified Organization Name:**

AAeCEiOeth

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.

Submit for Validation

4. In the ***Simplified Organization Name** box, review and modify the simplified organization name as needed (e.g., *AAeCEiOeth*).
5. 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.

8.4 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.

8.4.1 How to Add a Domain and Authorize It for Certificates

1. In your account, in the sidebar menu, click **Certificates > Domains**.
2. On the **Domains** page, click **Add Domain**.
3. On the **New Domain** page, under **Domain Details**, enter the following domain information:

***Domain Name:** Enter the domain name for which certificates will be requested (e.g., *example.com*).

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

4. Under ***Validate This Domain For**, 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**.

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

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

1. In your account, in the sidebar menu, click **Certificates > Domains**.
2. On the **Domains** page, use the drop-down lists, search box, and column headers to locate specific domains.

3. Click the **"Domain Name"** link of the domain to view basic details about the domain, active validation status (pending or active), domain validation progress, and domain approval required actions.

8.4.3 How to Authorize a Domain for Additional Certificate Types

1. In your account, in the sidebar menu, click **Certificates > Domains**.
2. On the **Domains** page, click the **"Domain Name"** link of the domain for which you want to authorize additional certificate types.
3. On the **"Domain Name"** page, click **Submit for Validation**.
4. 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)***

*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)**.

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

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

8.4.4 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 **Certificates > Domains**.
2. On the **Domains** page, click the **"Domain Name"** link of the domain for which you need to see the types of certificates you can order.

3. On the “**Domain Name**” page, under **Pending Validation/Active Validation**, 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 Multi-Domain SSL 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.

8.4.5 How to Enable DNS CNAME Domain Control Validation (DCV)

By default, when domains are added to your account for prevalidation, a DCV email is sent to the validation contact for the organization associated with the domain.

Use this instruction to enable DNS-based domain validation for your organization or the organization's that you service.

Note: When a certificate request is approved for a domain that has not been added to your account, that domain is automatically submitted for validation using the DCV email method.

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

If you only have one division or are not allowed to see other divisions, you may need to click **Account > My Division**.

2. On the **Divisions** page, click **My Division**.
3. On the “**Division Name**” page, click **Edit Preferences**.
4. On the **Division Preferences** page, at the bottom of the page, click **+ Advanced Settings**.

5. Under **DCV Methods**, check **Show DNS CNAME as an alternative DCV method when managing / adding domains**.
6. At the bottom of the page, click **Save Settings**.

The next time you add domains for prevalidation, you should have the option to use DNS CNAME as an alternate DCV method.

8.4.6 How to Add a Domain, Authorize it for Certificates, and Select DNS CNAME as the Validation Method

1. In your account, in the sidebar menu, click **Certificates > Domains**.
2. On the **Domains** page, click **Add Domain**.
3. On the **New Domain** page, under **Domain Details**, enter the following domain information:

***Domain Name:** Enter the domain name for which certificates will be requested (e.g., *example.com*).

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

4. Under ***Validate This Domain For**, 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)***

*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)**.

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

Note: The default DCV method is by verification email.

6. Click **Save Domain**.

Note that you still have two steps left: 1- (DNS Provider) Add your token to a new DNS CNAME record and 2- (DigiCert Account) Verify the CNAME.

7. **Add Token to DNS CNAME Record**

- a. Under **User Actions**, in the **Your unique verification token** box, copy your verification token.
- b. Go to your DNS provider's site and create a new CNAME record.
- c. Paste your verification code into a new CNAME record.
- d. In the hostname field (or equivalent), paste the verification token that you copied from your DigiCert account.
- e. In the record type field (or equivalent), select **CNAME**.
- f. In the target host field (or equivalent) enter **dcv.digicert.com** (i.e., point the CNAME record to dcv.digicert.com).
- g. Save the record.

8. In your DigiCert account, click **check CNAME**.

You have successfully verified the CNAME.

9 Product Settings

You can use the **Product Settings** feature to regulate the certificates for your entire Division or for specific user roles (users and admins). You can use **Product Settings** to do the following:

- Determine the types of certificates that can be ordered by your entire Division or by specific Roles (*i.e., configure product settings so that your division can only order SSL, Code Signing and Client Certificates*).
- Determine the validity periods for the certificates being ordered by your entire Division or by specific Roles (*i.e., configure product settings so that the user role can only order 1-year Code Signing Certificates*).
- Determine which signature hash(es) can be used to generate the certificate ordered by your entire Division or by specific Roles (*i.e., configure product settings so that your division can only use the SHA-256 hash to generate their Wildcard Plus Certificates*).

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.

9.1 Configuring Product Settings

These instructions are for administrators only and explain how to configure your Product Settings for your Division (DigiCert account). You can configure the Product Settings for your Division (account) or for specific Roles in your Division.

Permissions Note:

Only administrators can view the **Product Settings** page and can configure product settings for their division or for specific roles (users and admins) within their division.

9.1.1 How to Configure Product Settings for the Division

When configuring Product Settings for your Division, you can determine which products can be ordered. You can determine the validity period for the certificates that can be ordered. And, you can determine which signature hash(es) can be used to generate the certificate.

For example, you can prevent everyone in your Division from ordering Grid Certificates, allow everyone in your Division to only order three-year Code Signing and SSL Plus Certificates, and allow your Division to only use the SHA256 and SHA384 signature hashes to generate their SSL types of certificates.

1. In your account, in the sidebar menu, click **Settings > Product Settings**.
2. (**Participant Admins Only**) On the **Product Settings** page, uncheck **Configure products by role**.

3. On the **Product Settings** page, under **Product** select the certificate (e.g. *SSL Plus*) that you want to modify how it can be used.
4. Under **Product Settings**, do any or all of the following to determine how the selected certificate can be used:

Note: Repeat this process as needed, until you are done modifying the needed certificates for your Division (account).

Enable this product

To prevent this certificate from being ordered, uncheck this box.

By default, this box is checked for each certificate listed under **Products**.

Note: If you uncheck this box, the validity periods and signature hashes options disappear.

Allowed Validity Periods

In the drop-down list, select the validity period(s) for the selected certificate (e.g., *2 Year*).

Some certificates have 1, 2, and 3 year options, while some have only 1 and 2 year options, and others have only 1 Year options.

Note: If you do not select a validity period, the default setting is used. For example, for an *SSL Plus Certificate* the default setting allows 1, 2, and 3 year certificates to be ordered.

Allowed Signature Hashes

In the drop-down list, select which signature hash(es) can be used to generate the selected certificate.

Note: If you do not select a validity period, the default setting is used. The *SHA-256*, *SHA-384*, and *SHA-512* signature hashes can be used to generate the certificate.

Restore Product Settings

To restore the product's default settings, click **Restore Product Settings**.

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

9.1.2 (Participant Admins Only) How to Configure Product Settings for a Specific Role

When configuring Product Settings for a specific role, you can determine the products each role can order. You can also determine the validity period for the certificates they can order.

For example, you can prevent the User role from ordering Grid Certificates, allow the User role to only order three-year Code Signing and SSL Plus Certificates, and allow the User role to only use the SHA256 and SHA384 signature hashes to generate their SSL types of certificates.

1. In your account, in the sidebar menu, click **Settings > Product Settings**.
2. On the **Product Settings** page, check **Configure products by role**.
3. Under **Role** select the role for which you are configuring the Product Settings (*Administrator or User*).
4. Under **Product** select the certificate (e.g. *SSL Plus*) you want to modify how it can be used.
5. Under **Product Settings**, do any or all of the following to determine how the selected certificate can be used:

Note: Repeat this process as needed, until you are done modifying the needed certificates for the role.

Enable this product

To prevent this certificate from being ordered, uncheck this box.

By default, this box is checked for each certificate listed under **Products**.

Note: If you uncheck this box, the validity periods and signature hashes options disappear.

Allowed Validity Periods

In the drop-down list, select the validity period(s) for the selected certificate (e.g., *2 Year*).

Some certificates have 1, 2, and 3 year options, while some have only 1 and 2 year options, and others have only 1 Year options.

Note: If you do not select a validity period, the default setting is used. For example, for an SSL Plus Certificate the default setting allows 1, 2, and 3 year certificates to be ordered.

Allowed Signature Hashes In the drop-down list, select which signature hash(es) can be used to generate the selected certificate.

Note: If you do not select a validity period, the default setting is used. The SHA-256, SHA-384, and SHA-512 signature hashes can be used to generate the certificate.

Restore Product Settings To restore the product's default settings, click **Restore Product Settings**.

6. When you are finished, scroll to the bottom of the **Product Settings** page and click **Save Settings**.

9.1.3 How to View Product Settings for Your Division or Specific Roles (User or Administrator)

1. In your account, in the sidebar menu, click **Settings > Product Settings**.
2. **To view the Product Settings for your Division:**
 - a. Uncheck **Configure products for role**.
 - b. To see all product settings for your Division: under **Product**, select **Summary**.
 - c. To see a specific certificate's product settings: under **Product**, select a certificate (e.g., *SSL Plus*).
3. **To view the Product Settings for a specific role.**
 - a. Check **Configure products for role**.
 - b. Under Role, select a role (e.g., *Administrator*).
 - c. To see all product settings for the selected role: under **Product**, select **Summary**.
 - d. To see a specific certificate's product settings: under **Product**, select a certificate (e.g., *SSL Plus*).

9.1.4 How to Restore Default Product Settings

When restoring your default product settings, you have two options: restore your entire account's default product settings or restore a individual role's product settings.

9.1.4.1 How to Restore the Default Product Settings for Your Entire Account

Regardless of how you've configured your product settings (Division wide or role based), you can use this option to restore the default product settings for your entire account.

1. In your account, in the sidebar menu, click **Settings > Product Settings**.
2. On the **Product Settings** page, in the top right-hand corner, click **Restore Default Settings**.

9.1.4.2 (Participant Admins Only) How to Restore the Default Product Settings for a Role

If you need to restore the default product settings for a role (e.g., *User*) without affecting the product settings you've configured for the other role (e.g., *Administrator*), you must do it manually, one product at a time.

1. In your account, in the sidebar menu, click **Settings > Product Settings**.
2. On the **Product Settings** page, check **Configure products by role**.
3. Under **Role** select the role for which you want to restore the default Product Settings (*Administrator* or *User*).
4. Under **Product** select the certificate (e.g. *SSL Plus*) for which you need to restore the default settings.
5. Under **Product Settings**, click **Restore Product Settings** to restore the product's default settings.
6. Repeat steps 4 and 5 as needed, until you have restored all certificates to their default product settings.
7. When you are finished, scroll to the bottom of the **Product Settings** page and click **Save Settings**.

10 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.

10.1 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**
SSL Plus, Multi-Domain SSL, Wildcard Plus, EV SSL Plus, and EV Multi-Domain
- **Grid Certificates**
Grid Premium, Grid Robot Email, Grid Robot FQDN, Grid Robot Name, Grid Host SSL, and Grid Host Multi-Domain SSL
- **Client Certificates**
Digital Signature Plus, Email Security Plus, and Premium
- **Code Signing Certificates**
Code Signing and EV Code Signing
- **Document Signing Certificates**
Document Signing - Organization (2000) and Document Signing - Organization (5000)

10.1.1 How to Request an SSL Plus, EV SSL Plus, EV Multi-Domain, Multi-Domain SSL, and 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:

- SSL Plus
- Multi-Domain SSL
- Wildcard Plus
- EV SSL Plus
- EV Multi-Domain

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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **SSL Certificate**.
3. On the **SSL Certificates** tab, select one of the available certificates and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **SSL Certificates**, select one of the available certificates.

3. **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
MA8GA1UEBxMlMw91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKEzF2b3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIchYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrB5/vhYfGECJLJbc3l
RdEbdXyHdThk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHRjB
/qdTyr+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEB08GA0Fc4rw
ix7vb15vSXe3shGijRGIZzHVGRoR3r7xQtIuMaDAr3x1V8jHbcvZTcpx0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NFiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RyFwG3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

4. 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:

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

Expand **Show Available Domains** and select one of the pre-validated domains or subdomains (e.g., *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.

b. **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 Multi-Domain SSL 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*.

For an EV Multi-Domain Certificate:

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

5. **Organization**

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

6. **Other Hostnames (SANs)**

For Multi-Doman SSL and EV Multi-Domain Certificates

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

(Optional) For Wildcard Plus Certificates

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

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

To secure subdomains on different levels (e.g., *test.secure.example.com* and *six.test.secure.example.com*) request a duplicate certificate. Since these subdomains are not on the same level as the wildcard (*) character, you must manually add them as SANs to the certificate. Getting duplicate certificates is free

and requesting multiple duplicate certificates does not invalidate the first ones while allowing you to secure additional subdomains.

7. 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 (e.g., *SHA-256*).

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

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

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.

Order Specific Renewal Message: To create a renewal message for this certificate right now, type the renewal message making sure to include information that might be relevant to the certificate's renewal.

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

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

Auto-renew**Auto-renew order
30 days before
expiration.**

If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration.**

Important Note:

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

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

An email should be sent notifying the administrator(s) and/or EV Certificate approver(s) that there is a certificate request that needs their approval.

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

10.1.2 How to Request a Grid Host SSL and Grid Host Multi-Domain SSL Certificate

The process for requesting Grid Host SSL and Grid Host Multi-Domain SSL 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 and Grid Host Multi-Domain SSL Certificates 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 Multi-Domain SSL Certificate request forms.

You can use this instruction for the following certificates:

- Grid Host SSL
- Grid Host Multi-Domain SSL

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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **Grid Certificates**.
3. On the **Grid Certificates** tab, select **Grid Host SSL** and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **Grid Certificates**, select **Grid Host SSL**.

3. 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-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCV1vdXJlTG02TER
MA8GA1UEBxMIW91ckNpdHkxZCZAJBgNVBAwTAk1UMRowGAYDVQQKEwFZb3VyQ29t
cG8ueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpFKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHdtHk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxcG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtASMIz/ZjaXfS1LjXurLU0nCOQQIDAQBoAAwDQYJ
KoZIHvCNAQEFBQADggEBAK159goyAYOpenrQ2EvCG1izrK1kS3D8JjnAiP1NHrjB
/qdTyr+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEb08GA0Fc4rw
ix7vb15vSxe3shG1jRGIZzHVGRoR3r7xQtIuMaDAr3x1V8jHbcvZTepX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziunm1Df24NBt5tpCNzfGviKT6/RyFWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

4. 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:

a. **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.

b. **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 Multi-Domain SSL Certificate:

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

5. **Organization**

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

6. **Other Hostnames (SANs)**

For a Grid Host Multi-Domain SSL 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 Multi-Domain SSL Certificate to secure.

7. 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 (e.g., *SHA-256*).

8. 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.

Additional Renewal Message: To create a renewal message for this certificate right now, type the renewal message making sure to include information that might be relevant to the certificate's renewal.

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

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

Auto-renew
Auto-renew order 30 days before expiration. If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration**.

Important Note:

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

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

10.1.3 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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **Client Certificates**.
3. On the **Client Certificates** tab, select **Premium** and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **Client Certificates**, select **Premium**.

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

***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 (e.g., *SHA-256*).

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

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

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

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

Recipient Email Enter the recipient's email address (e.g., *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 (e.g., *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.

6. **(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 used 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-----
MIICvDCAAsQCAQAwdzELMAkGA1UEBhMCVVMxSjAQBgNVBAgTCV1vdXJtdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxCSA1UEBmNVBAAsTAK1UMRowGAYDVQQKEwFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAwdMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA379BFFxfACdXsUk2wrka/nAlKbo+I9DAN32
+/SRxj/KtXVddsckW1obHGpMKPw4meJqOpQwJkICHyjSUQSpPKedGpccDMf/eoF0
J7EaQ2zzLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHdHk1RAoIVQCfjTw8WGNAD33vmHW7QOR6FYUoa4fcJh7Rv6jH5ywwx
7pVfaDbZPuTgUhw7wksKNFxcG0xcTmz/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIHvcNAQEFBQADggEBAK159goyAYOpnrxQ2EvCGLizK1kS3D8JjnA1P1NHxjB
/qdTYR+/8Dr/hMcwvU5ThGAVf68eMkk6tUNWAdpZ9C904Js2z+ENEb08GA0Fc4rw
ix7vb15vSXe3shGijRGIZzHVGRoR3z7xQtIuMaDAR3x1V8jHbcvZTcpx0Kbq6H1G
NLA4CXsOI4KGvu4FXfS2JEGb3gEJD8HaMP8V8ez5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGBnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziunM1Df24NBt5tpCNzfGviKT6/Ryfwg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

- To add additional Client Certificate recipients, click the **Add Another Certificate** link and enter the recipient's **Recipient Details**.
- When you are finished, click **Submit Request**.
- 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 (**Certificates > Orders**), the certificate should be listed with the **Status** of **Pending**.

- 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 (**Certificates > 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 (**Certificates > Orders**), the certificate should be listed with the **Status** of **Issued**.

10.1.4 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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **Grid Certificates**.
3. On the **Grid Certificates** tab, select **Grid Premium** and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **Grid Certificates**, select **Grid Premium**.

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

***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 (e.g., *SHA-256*).

***Validity Period:** Select **1 Year**.

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

4. 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:

FQDN 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.

5. **(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 used 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-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCV1vdXJtdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxZzA1BzBhNVBAAsTAK1UMRowGAYDVQQKEZFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHdTHk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtASMIz/ZjaXfS1LjXurLU0nCOQQIDAQABAAAwDQYJ
KoZIHvcNAQEFBQADggEBAK159goyAYOpennrQ2EvCG1izrK1kS3D8JjnAiP1NhrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGiZzHVGRoR3r7xQtIuMaDAR3x1V8jHbcvZTcpx0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RyFwg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

6. To add additional Client Certificate recipients, click **Add Another Certificate** and enter the recipient's **Recipient Details**.
7. When you are finished, click **Submit Request**.
8. 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 (**Certificates > Orders**), the certificate should be listed with the **Status** of **Pending**.

9. 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 (**Certificates > Orders**), the certificate should be listed with the **Status** of **Issued**.

10.1.5 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 **Certificates > Orders**.
2. On the **Orders** page, locate the certificate and click on the **"Client Certificate Name"** link for which you need to resend the **Email Validation for DigiCert "Client Certificate"** email.
3. 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.

4. 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.

10.1.6 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 **Certificates > Orders**.
2. On the **Orders** page, locate the certificate and click on the **“Client Certificate Name”** link for which you need to resend the **Create Your DigiCert “Client Certificate”** email.
3. On the **Manage Order #** page, on the **Email Addresses** line, below or to the right of the recipient’s email address, click the **Resend Issuance Email** 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.

4. 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.”

10.1.7 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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **Code Signing Certificates**.
3. On the **Code Signing Certificates** tab, select **Code Signing** and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **Code Signing Certificates**, select **Code Signing**.

3. On the **Request a 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 (e.g., *SHA-256*).

Subject Email:

- i. Click **Show Available Domains** to see the validated domains.

The email address that you provide must have a validated domain.

- ii. 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.

4. In the **Order Options** section, do the following:

Server Platform: Select the *platform for which the Code Signing Certificate is to be used.

***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-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCV1vdXJkdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTmr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIHvcNAQEFBQADggEBAK159goyAYOpenrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTyr+/8Dr/hMcwU5ThGAVf68eMkk6tUNWAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSxe3shGijRGIZzHVGRoR3r7xQtIuMaDAR3x1V8jHbcvZTcpx0Kbq6H1G
NLA4CXoOI4KGwu4FXfSzJEGb3gZJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEwXRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/Ryfwg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

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.

Additional Renewal Message:

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

Additional Emails:

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

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

Auto-renew**Auto-renew order 30 days before expiration.**

If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration**.

Important Note:

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

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

10.1.8 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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **Code Signing Certificates**.

3. On the **Code Signing Certificates** tab, select **EV Code Signing** and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **Code Signing Certificates**, select **EV Code Signing**.

2. 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**.

Additional Renewal Message: To create a renewal message for this certificate right now, type the renewal message making sure to include information that might be relevant to the certificate's renewal.

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

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

Auto-renew
Auto-renew order 30 days If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration**.

Important Note:

**before
expiration.**

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

3. 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 download 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-----
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBGNVBAgTCV1vdXJIdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKEXFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKWlobHGpMKPw4meJqOpQwJkIChYjSUQSpKzdGpccDMf/ef0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHk1RAoIVQCfjTwBWNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFfccG0xcTMr/+GrciHEuZ0chg86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIz/ZjaXfS1LjXurLUOnCOQQIDAQABoAAwDQYJ
KoZInvcNAQEFBQADggEBAK159goyAYOpnrcrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEb08GA0Fc4rw
ix7vb15vSXe3sshGijRGIZzHVGRoR3r7xQtIuMaDAR3x1V8jHbcvZTepX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGBnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/Ryfwg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

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

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

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

10.1.9 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, do one of the following:

Option 1:

Unfamiliar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.
2. On the **Request a Certificate** page, select **Document Signing Certificates**.
3. On the **Document Signing Certificates** tab, select **Document Signing – Organization (2000)** and then, click **Order Now**.

Option 2:

Familiar with certificate choices and the requesting process

1. In your account, in the sidebar menu, click **Request a Certificate** and then under **Document Signing Certificates**, select **Document Signing – Org (2000)**.

2. On the **Request Document Signing 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 (e.g., *SHA-256*).

Validity Period:

Select a validity period for the certificate: (**3 Years**, **2 Years**, or **1 Year**).

3. 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.

4. 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.

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

10.1.10 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.

10.2 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.

10.2.1 How to View Certificate Requests

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, use the drop-down lists, search box, and column headers to locate specific requests.
3. To view the details of a certificate requests, click on the **"Order #"** link.
4. In the **Order #** details pane (on the right), you can review the requests details.

10.2.2 How to Edit a Certificate Request

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, use the drop-down lists, search box, and column headers to locate the request.
3. Click the **"Order #"** link of the request that you want to edit
4. In the **Order #** details pane (on the right), click **Edit**.
5. On the **Edit Certificate Request** page, edit, add, or remove information as required.
6. When you are finished, click **Update Certificate Request**.

10.2.3 How to Approve a Certificate Request

Only an **EV Verified User** can approve EV SSL Plus, EV Multi-Domain Certificate requests. Only an **EV CS Verified User** can approve EV Code Signing Certificate requests. Only a **CS Verified User** can approve Code Signing Certificate requests.

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, use the drop-down lists, search box, and column headers to locate the request.
3. Click on the **"Order #"** link of the request that you want to approve.

4. In the **Order #** details pane (on the right), 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.

5. In the **Approve Request** window, type an **Approval Comment** and then, click **Approve**.

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

If all validation is completed and no further validation is required, the certificate should be issued to your account within minutes.

10.2.4 How to View Who Requested a Certificate (Approved Requests)

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, in the **Status** drop-down list, select **Approved** and then click **Go** to see all approved certificate requests.
3. In the **Type** drop-down list, select a certificate type (**New, Reissue, Revoke, or Duplicate**), and then click **Go** to filter the list of approved requests.
4. In the **Division** drop-down list, select a division, and then click **Go** to further filter the list of approved certificate requests.
5. Click the **"Order #"** link of the request for which you want to view the requestor.
6. In the **Order #** details pane (on the right), in the **Request Details** section, under **Request**, you should be able to see who requested the certificate.

10.2.5 How to View Who Approved a Certificate Request (Approved Requests)

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, in the **Status** drop-down list, select **Approved** and then click **Go** to see all approved certificate requests.
3. In the **Type** drop-down list, select a certificate type (**New, Reissue, Revoke, or Duplicate**) and then click **Go** to filter the list of approved requests.
4. In the **Division** drop-down list, select a division and then click **Go** to further filter the list of approved certificate requests.

5. Click the **"Order #"** link of the request for which you want to view the approver.
6. In the **Order #** details pane (on the right), in the **Request Details** section, under **Approval**, you should be able to see who approved the certificate.

10.2.6 How to View EV Certificate Request Approvers

Only **EV/EV CS Verified Users** can approve requests for EV SSL Plus and EV Multi-Domain Certificates.

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, use the drop-down lists, search box, and column headers to filter the list of organizations.
3. Click the **"Organization Name"** link of the organization whose EV/EV CS approvers you want to view.
4. On the **"Organization Name"** page, under **Organization Contacts**, all approvers are listed.
5. Contacts who can approve EV Certificate requests, have a check mark under **EV / EV CS**.

10.2.7 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 **Certificates > Organizations**.
2. On the **Organizations** page, use the drop-down lists, search box, and column headers to filter the list of organizations.
3. Click the **"Organization Name"** link of the organization whose CS approver you want to view.
4. On the **"Organization Name"** page, under **Organization Contacts**, all approvers are listed.
5. Contacts who can approve CS Certificate requests, have a check mark under **CS**.

10.2.8 How to View EV CS Approvers

Only **EV/EV CS Verified Users** can approve requests for EV Code Signing Certificates.

1. In your account, in the sidebar menu, click **Certificates > Organizations**.
2. On the **Organizations** page, use the drop-down lists, search box, and column headers to filter the list of organizations.

3. Click the **"Organization Name"** link of the organization whose **CS Approver** you want to view.
4. On the **"Organization Name"** page, under **Organization Contacts**, all approvers are listed.
5. Contacts who can approve EV CS Certificate requests, have a check mark under **EV / EV CS**

10.2.9 How to Reject a Certificate Request

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, use the drop-down lists, search box, and column headers to filter the list of requests.
3. Click the **"Order #"** link of the certificate that you want to reject.
4. In the **Order #** details pane (on the right), 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.

5. In the **Reject Request** window, enter a **Rejection Comment** to be included in the rejection email and then, click **Reject**.

The requestor is sent an email informing them that their certificate request has been rejected. Your rejection comment is included in the email.

10.3 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.

10.3.1 How to View Certificates

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. To view the details of a certificate, click the **"Order #"** link of a certificate.
4. In the **Order #** details pane (on the right), you can review the certificate details.

10.3.2 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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the certificate that you need to download.
5. In the **Order #** details pane (on the right), click **Download Certificates**.
6. 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 this option to select the best format for a specific platform.

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 this option to select a 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)

7. Next, click **Download Certificates** to save the certificate file.
8. Save the certificate file to your server or workstation, making sure to note the location.

10.3.3 How to Adjust Certificate Renewal Notifications

After requesting your certificate, you may want to adjust your certificate 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 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 Certificate Renewal Reminders

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of the certificate whose renewal reminders you want to adjust.
4. In the **Order #** details pane (on the right), in the **Manage Order** section, under **Account-Wide Renewal Message**, click the **Edit your Account Settings** link.
5. On the **Notifications** page, under **Send notifications to the addresses above when certificates are scheduled to expire**, uncheck or check notifications as desired.
6. When you are finished, click **Save**.

Renewal certificate renewal reminders for your certificates has been updated.

10.3.4 How to Change the Default Renewal Message for All Certificates

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, click the **"Order #"** for any certificate.
3. In the **Order #** details pane (on the right), in the **Manage Order** section, under **Account-Wide Renewal Message**, click the **Edit your Account Settings** link.
4. On the **Notifications** page, in the **Default Renewal Message** box, type the message that you want to be included all certificate renewal notification emails.
5. When you are finished, click **Save**.

10.3.5 How to Add/Change a Renewal Message for a Specific Certificate

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificate orders.
3. Click the **"Order #"** link of the order whose renewal message you want to change.
4. In the **Order #** details pane (on the right), in the **Manage Order** section, under **Renewal Messages for this Order #**, click the **Add** or **Edit Message** link.
5. In the box, type the renewal message that you want to include in this certificate's renewal notification emails.
6. When you are finished, click **Save**.

10.3.6 How to Disable Renewal Notices for a Specific Certificate

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificate orders.
3. Click the **"Order #"** link of the order whose renewal notices you want to disable.
4. In the **Order #** details pane (on the right), in the **Manage Order** section, under **Renewal Notices**, click the **Disable** link.

You're done. You have disabled renewal notices for that certificate. As it approaches its expiration date, you *will not* receive emails notifying you that it will soon expire.

10.3.7 How to Re-enable Renewal Notices for a Specific Certificate

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificate orders.
3. Click the **"Order #"** link of the order whose renewal notices you need to re-enable.
4. In the **Order #** details pane (on the right), in the **Manage Order** section, under **Renewal Notices**, click the **Enable** link.

You're done. You have enabled renewal notices for that certificate. As it approaches its expiration date, you *will* receive emails notifying you that it will soon expire.

10.3.8 How to Add Additional Email Addresses to Receive Certificate Renewal Notifications

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificate orders.
3. Click the **"Order #"** link of the order to which you need to add additional email accounts for receiving renewal notifications.
4. In the **Order #** details pane (on the right), in the **Manage Order** section, under **Additional Emails**, click the **Add Email** link.
5. In the box, enter the email addresses for the people you want to receive the renewal notifications (comma separated).
6. When you are finished, click **Save**.

10.3.9 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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the EV Code Signing Certificate you need to activate.
5. In the **Order #** details pane (on the right), 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.

6. On the **EV Code Signing Hardware Token Order #** page, check **I have received the hardware token** and then, click **Submit**.

7. 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.

8. 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.

9. Run the SafeNet Authentication Client.

Double-click **SafeNetAuthenticationClient-32x-64x.exe**.

10. 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**.

11. 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**.
12. On the **EV Code Signing Hardware Token Order #** page, click the **Click here when you have changed the password on the hardware token** link.
13. 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](#).

10.3.10 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 **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of the EV Code Signing Certificate that you need to install on your token.
4. In the **Order #** details pane (on the right), click **Install Certificate**.
5. Next, **record** your EV Code Signing Certificate's **initialization code** (e.g., *aaaaa11111aaaaa1111*).

Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

6. After you have recorded your certificate's initialization code, click the **<https://www.digicert.com/StaticFiles/DigiCertHardwareCertificateInstaller.zip>** link in your account, and download and run the **DigiCert Hardware Certificate Installer.exe**.
7. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.
8. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.
9. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.
10. 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 ask you to remove your token, install the drivers, and then, re-install your token.

11. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.

12. On the **Token Detection** page, click **Next**.

13. 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.

14. 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.

15. 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 **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of the EV Code Signing Certificate that you need to install on your token.
4. In the **Order #** details pane (on the right), click **Install Certificate**.
5. Next, **record** your EV Code Signing Certificate's **initialization code** (e.g., `aaaaa11111aaaaa1111`).

Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

6. After you have recorded your certificate's initialization code, click the **<https://www.digicert.com/StaticFiles/DigiCertHardwareCertificateInstaller.zip>** link in your account, and download and run the **DigiCert Hardware Certificate Installer.exe**.
7. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.

8. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.
9. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.
10. 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 ask you to remove your token, install the drivers, and then, re-install your token.

11. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.
12. 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.

13. 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.

14. (Optional) If you want to set up an 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 setting up 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.

15. 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.

16. 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.

17. 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](#).

10.3.11 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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the Document Signing Certificate that you need to activate.
5. In the **Order #** details pane (on the right), 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.

6. On the **Document Signing Hardware Token Order #** page, check **I have received the hardware token** and then, click **Submit**.
7. 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.

8. 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.

9. Run the SafeNet Authentication Client.

Double-click **SafeNetAuthenticationClient-32x-64x.exe**.

10. 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**.

11. 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**.

12. On the **Document Signing Hardware Token Order #** page, click the **Click here when you have changed the password on the hardware token** link.

13. 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](#).

10.3.12 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 **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of the Document Signing Certificate that you need to install on your token.
4. In the **Order #** details pane (on the right), click **Install Certificate**.
5. Next, **record** your Document Signing Certificate's **initialization code** (e.g., *aaaaa11111aaaaa1111*).

Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

6. 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**.
7. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.
8. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.

9. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.

10. 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 ask you to remove your token, install the drivers, and then, re-install your token.

11. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.

12. On the **Token Detection** page, click **Next**.

13. 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.

14. 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.

15. 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 **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of the Document Signing Certificate that you need to install on your token.
4. In the **Order #** details pane (on the right), click **Install Certificate**.

5. Next, **record** your Document Signing Certificate's **initialization code** (e.g., *aaaaa11111aaaaa1111*).

Later, when prompted by the **DigiCert Hardware Certificate Installer** wizard, you must enter this code

6. 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**.
7. In the **DigiCert Hardware Certificate Installer** wizard, on the **Welcome** page, click **Next**.
8. On the **License Agreement** page, read the **User License Agreement**, check **I accept and agree to the license agreement**, and then, click **Next**.
9. On the **Initialization Code** page, in the **Initialization Code** box, enter your initialization code that you previously recorded and then, click **Next**.
10. 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 ask you to remove your token, install the drivers, and then, re-install your token.

11. Next, the **DigiCert Hardware Certificate Installer** wizard analyzes your secure token device.
12. 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.

13. 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.

14. (Optional) IF you want to set up an 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 setting up 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.

15. 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.

16. 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.

17. 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](#).

10.3.13 How to Place a Request to Revoke a Certificate

1. In your account, in the sidebar menu, click **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of certificate you need to revoke.
4. In the **Order #** details pane (on the right), click **Revoke Certificate**.
5. On the **Request to Revoke Certificate for Order #** page, in the **Reason for Revocation** box, type your reason for revoking the certificate.
6. Making sure that you really need to revoke the certificate, click **Request Revocation** to request the certificate revocation.

10.3.14 How to Approve a Certificate Revoke Request

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, in the **Status** drop-down list, select **Pending** and then click **Go** to see only the certificates that need administrator approval.
3. In the **Type** drop-down list, select **Revoke** and then click **Go** to see only the certificates that need revocation approval.
4. Click the **"Order #"** link of the certificate whose revocation you need to approve.

The **Type** for the certificate should be **REVOKE**.

5. In the **Order #** details pane (on the right), 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 **Approve**, unless you are sure that you want to revoke the certificate. The revocation cannot be reversed. If you are revoking an SSL Certificate, any site using this certificate will show trust warnings when users try to access the site.

6. In the **Approve Request** window, enter an **Approval Comment** and then, click **Approve**.

10.3.15 How to Reject a Certificate Revoke Request

1. In your account, in the sidebar menu, click **Certificates > Requests**.
2. On the **Requests** page, in the **Status** drop-down list, select **Pending** and then click **Go** to see only the certificates that need administrator approval.

3. In the **Type** drop-down list, select **Revoke** and then click **Go** to see only the certificates that need revocation approval.
4. Click the **"Order #"** link of the certificate whose revocation request you need to reject.

The **Type** for the certificate should be **REVOKE**.

5. In the **Order #** details pane (on the right), click **Reject** to reject the certificate revoke request.
6. In the **Rejection Request** window, provide a **Rejection Comment**, which appears in the rejection email that is sent to the requestor, and then click **Reject**.

The requestor is sent an email informing them that their certificate request has been rejected.

10.3.16 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, Multi-Domain SSL, Wildcard Plus, and Grid Host Multi-Domain SSL Certificates is similar. For this reason, we will provide instructions for ordering a Multi-Domain SSL Certificate and note any differences between the Multi-Domain SSL Certificate request form and the EV Multi-Domain, Wildcard plus, and Grid Host Multi-Domain SSL Certificate request forms.

You can use this instruction for the following certificates:

- Multi-Domain SSL
- Wildcard Plus
- EV Multi-Domain
- Grid Host Multi-Domain SSL

How to Request a Duplicate Multi-Domain SSL 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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the Multi-Domain SSL for which you need a duplicate certificate.
5. In the **Order #** details pane (on the right), click **Request Duplicate**.
6. 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
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJgOpQwJkIChYjSUQSpPKzdGpccDMF/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrBS/vhYfGECLJbc3l
RdEbdXyHdTHk1RAoIVQCfjTwBWNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwx
7pVfaDbZPuTgUhw7wksKNFcccG0xcTMr/+GrciHEuZ0chg86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIHvCNAQEFAAQAdggEBAK159goyAYOpnrrQ2EvCGlizrK1kS3D8JjnAiP1NhrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEb08GA0Fc4rw
ix7vb15vSXe3shGijRGIZzHVGRoR3r7xQtIuMaDar3x1V8jHbcvZTepX0Kbq6H1G
NLA4CXsOI4KGwu4FXfS2JEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGBnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziunm1Df24Nbt5tpCNzfGvIKT6/RyFwG3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

7. **Multi-Domain SSL 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 (e.g., *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.

8. Grid Host Multi-Domain SSL

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.

9. Wildcard Plus Certificate

To add additional Subject Alternate Names (SANs) to the duplicate certificate, in the **Other Hostnames (SANs)** box, enter the subdomain that you want your Wildcard Certificate to secure. Note that the SANs names must be a subdomain of the specified common name. For example, if **example.com* is the common name, you can use *www.example.com*, *www.app.example.com*, and *mail.example.com* as SANs.

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

To secure subdomains on different levels (e.g., *test.secure.example.com* and *six.test.secure.example.com*) request a duplicate certificate. Since these subdomains are not on the same level as the wildcard (*) character, you must manually add them as SANs to the certificate. Getting duplicate certificates is free and requesting multiple duplicate certificates does not invalidate the first ones while allowing you to secure additional subdomains.

For EV Multi-Domain, Multi-Domain SSL, and Grid Host Multi-Domain SSL Certificates:

You cannot add additional SANs.

10. Next, enter the following information:

- | | |
|------------------------------|---|
| *Signature Hash: | In the drop-down list, select a signature hash (e.g., <i>SHA-254</i>). |
| *Server Platform: | Select the server on which the CSR was generated. |
| Reason for Duplicate: | In the box, specify the reason for the certificate duplication. |

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

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

10.3.17 How to Reissue a 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 (for example, from *www.yourname.com* to *secure.yourname.com*).
- You want to add, remove, or change some of the SANs that are listed in your Multi-Domain SSL 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:

- SSL Plus
- Multi-Domain SSL
- Wildcard Plus
- EV SSL Plus
- EV Multi-Domain
- Grid Host SSL
- Grid Host Multi-Domain 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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the certificate that needs to be reissued.
5. In the **Order #** details pane (on the right), click **Reissue Certificate**.
6. 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-----
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxExJQBgNVBAgTCVlvdXJtdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxXzA5BGNVBAwTAK1UMRowGAYDVQQKEZFb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddsckW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrB5/vhYfGECLJbc3L
RdEbdXyHdHk1RAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwqx
7pVfaDb2PuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtASMIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZInvcNAQEFBQADggEBAK159goyAYOpenrQ2EvCG1izrK1kS3D8JjnAiP1NHrjB
/qdTyr+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGiJRGIzzHVGRoR3r7xQtIuMaDAr3x1V8jHbcvZTcPX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEwXRWk1ERgg9/YcWI
obf5ziUmlDf24NBt5tpCNzfGviKT6/RyFWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----

```

7. 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](#).

8. 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 (e.g., *example.com* or *mail.example.com*). For Wildcard Plus Certificates, the name format is **.domain.com* (e.g., **.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.

Multi-Domain SSL 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 (e.g., *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 Multi-Domain SSL 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.

9. **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 (e.g., *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 Multi-Domain 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 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 (e.g., *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.

10. Other Hostnames (SANs)

Multi-Domain SSL, EV Multi-Domain, and Grid Host Multi-Domain SSL 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.

11. Next, enter the following information:

***Signature Hash:** In the drop-down list, select a signature hash (e.g., *SHA-256*).

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

Reason for Reissue: In the box, specify the reason for the certificate reissue.

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

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

10.3.18 How to Renew a SSL Plus, EV SSL Plus, EV Multi-Domain, Multi-Domain SSL, 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:

- SSL Plus
- Multi-Domain SSL
- Wildcard Plus
- EV SSL Plus
- EV Multi-Domain

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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the certificate that needs to be renewed.
5. In the **Order #** details pane (on the right), click **Renew Certificate**.
6. On the **Renew "Certificate Type" 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-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxZjAQBgNVBAgTCVlvdXJkdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxZzAxBgNVBAStAk1UMRowGAYDVQQKEzFzYyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIchYjSUQ8pPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrBS/vhYfGECLJbc31
RdEbdKyHdtHk1RAoIVQCfjTwBwGNAD337vmHW7QOR6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxcG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MI s/ ZjaXfS1LjXurLU0nCOQQIDAQABAAwDQYJ
KoZIHvcNAQEFBQADggEBAK159goyAYOpnrrQ2EvCG1izrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shG1jRGIZzHVGRoR3r7xQtIuMaDAR3x1V8jHbcvZTcpx0Kbq6H1G
NLA4CXsOI4KGwu4FXfSszJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RyFwG3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

7. 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.

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 have not uploaded your CSR yet and you want to change the common name, under **Common Name**, do one of the following:

a. If securing a pre-validated domain

Expand **Show Available Domains** and select one of the pre-validated domains or subdomains (e.g., *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.

b. 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 Multi-Domain SSL 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*.

8. **Other Hostnames (SANs)**

For EV Multi-Domain and Multi-Domain SSL 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 (e.g., *example2.com*, *example3.net*, *mail.example.net*) that you want your EV Multi-Domain or Multi-Domain SSL 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 SANs were used.

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

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

To secure subdomains on different levels (e.g., *test.secure.example.com* and *six.test.secure.example.com*) request a duplicate certificate. Since these

subdomains are not on the same level as the wildcard (*) character, you must manually add them as SANs to the certificate. Getting duplicate certificates is free and requesting multiple duplicate certificates does not invalidate the first ones while allowing you to secure additional subdomains.

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 (e.g., *SHA-256*).

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.

Additional Renewal Message: To create a renewal message for this certificate right now, type the renewal message making sure to include information that might be relevant to the certificate's renewal.

Auto-renew order 30 days before expiration. If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration**.
Important Note:
When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

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

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

10.3.19 How to Renew a Grid Host SSL and Grid Host Multi-Domain SSL Certificates

The process for renewing Grid Host SSL and Grid Host Multi-Domain SSL 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 Multi-Domain SSL 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 Multi-Domain SSL Certificate renewal forms.

This instruction can be used for the following certificates:

- Grid Host SSL
- Grid Host Multi-Domain SSL

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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the Grid Host SSL Certificate that needs to be renewed.
5. In the **Order #** details pane (on the right), click **Renew Certificate**.
6. On the **Renew "Certificate Type" 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-----
MIICvDCCAsQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHDtHklRAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwqx
7pVfaDbZPuTgUhw7wksKNFxcG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLUOnCOQQIDAQABoAAwDQYJ
KoZInvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNWAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIZzHVGRoR3r7xQtIuMaDar3x1V8jHbcv2TcPK0Kbq6H1G
NLA4CKsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0oww/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEwxRWk1ERgg9/YcWI
obf5ziunm1Df24NBt5tpCNzfGviKT6/RyfwG3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

7. Service / 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, 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.

Different Service:

If you are using a different service, under **Service / Common Name** section, In the **Service** box, enter the service that you want to use to connect to the grid server.

Common Name:

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

i. 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.

ii. **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 Multi-Domain SSL Certificate:

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

8. **Other Hostnames (SANs)**

For a Grid Host Multi-Domain 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 (e.g., *www.example2.com*, *www.example3.net*, *mail.example.net*) that you want your Grid Host Multi-Domain SSL Certificate to secure. You can also remove hostnames.

9. Next, enter the following information:

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

***Signature Hash:** In the drop-down list, select a signature hash (e.g., *SHA-256*).

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.

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

Additional Renewal Message: To create a renewal message for this certificate right now, type the renewal message making sure to include information that might be relevant to the certificate's renewal.

Auto-renew If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration.**

Important Note:

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

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

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

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

- On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
- Click the **"Order #"** link of the certificate that needs to be reissued.
- In the **Order #** details pane (on the right), click **Reissue Certificate**.
- On the **Reissue Certificate for Order #** page, in the **Reason for Reissue** box, specify the reason for the certificate reissue.

***Signature Hash:** In the drop-down list, select a signature hash (e.g., *SHA-256*).

***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.

- (**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-----
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdKJTGf0ZTER
MA8GA1UEBxMIW91ckNpdHkxMzA1UEBhMAk1UMRowGAYDVQQKEwFZb3V5Y29t
cGUESwgSW5jLjEYMBYGA1UEAwdPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFfXfACdXsUk2vrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddsckW1obHGpMKPw4meJqOpQwJkIChVjSUQSpPKzdGpccDMf/eoFO
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHdtk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywwx
7pVfaDb2PuTgUhw7wksKNFxcG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o6Sj7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABAAwDQYJ
KoZIHvcNAQEFBQADggEBBAK159goyAYOpncrQ2EvCGLizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSKe3shGiJRGIzHVGRoR3r7xQtIuMaDAr3x1V8jHbcvZTcpxK0Kbq6H1G
NLA4CXsOI4KGwu4FXfSszJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NP1EdzFnaYtUy2BDcXj3ZQEwXrWk1ERgg9/YcWI
obf5ziunm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

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

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

10.3.21 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 **Certificates > Orders**.
3. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
4. Click the **"Order #"** link of the Code Signing Certificate that needs to be renewed.
5. In the **Order #** details pane (on the right), click **Renew Certificate**.
6. 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 (e.g., *SHA-256*).

Subject Email:

- i. Click **Show Available Domains** to see the validated domains.

The email address that you provide must have a validated domain.

- ii. 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.

7. In the **Order Options** section, do the following:

Server Platform: Select the *platform for which the Code Signing Certificate is to be used.

***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 including the -----BEGIN NEW CERTIFICATE REQUEST - and -----END NEW CERTIFICATE REQUEST----- tag; paste it in to the request form in the area provided.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxZjAQBgNVBAgTCVlvdXJldGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxZzA5BQNVBAAsTAK1UMRowGAYDVQQKEwFZb3VyY29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nA1Kbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOK4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHdtHk1RAoIVQCfjTwBGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIHvNAQEFBQADggEBAK159goyAYOpncrQ2EvCGlizrK1ks3D8JjnAiP1NHrjB
/qdTYR+/8Dz/hMcwwU5ThGAVf68eMkk6tUNWAdpZ9C904Js2z+ENEB08GA0Fc4rw
ix7vb15vSXe3shGiJRGIzzHVGRoR3r7xQtIuMaDAr3x1V8jHbcvZTcPK0Kbq6H1G
NLA4CKsOI4KGwu4FXfS2JEGb3gEJD8HaMP8V8er5G0oww/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPIEdzFnaYtUy2BDcXj3ZQEwXRWk1ERgg9/YcWI
obf5ziunm1Df24NBt5tpCNzfGviKT6/RyFwg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

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.

Additional Renewal Message:

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

Auto-renew

Auto-renew order 30 days before expiration.

If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration**.

Important Note:

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

8. 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 **Certificate Request** page (**Certificates > Requests**), your certificate should be listed with the **Status** of **Pending**.

10.3.22 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:

- **For HSM Device Only:** Create your Certificate Signing Request (CSR).
- 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 **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.

- Click the **"Order #"** link of the EV Code Signing Certificate that needs to be reissued.
- In the **Order #** details pane (on the right), click **Reissue Certificate**.
- (HSM device only)** On the **Reissue Certificate for Order #** page, do the following:

- Create your CSR.

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

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

- 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-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxZjAQBgNVBAgTCVlvdXJtdGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxZzA1UEBhNVBAAsTAK1UMRowGAYDVQQKEwF2b3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKFw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/ef0
J7EaQ2szLv9AqdrQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHDtHk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywgwx
7pVfaDbZPuTgUhw7wksKNFxcG0xcTmr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZInvcNAQEFBQADggEBAK159goyAYOpnrxQ2EvCGlizrK1ks3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMk6tUNWAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGiJRGIzzHVGRoR3r7xQtIuMaDar3x1V8jHbcvZTepX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEwXRWk1ERgg9/YcWI
obf5ziunm1Df24NBt5tpCNzfGviKT6/RyFWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

- Next, on the **Reissue Certificate for Order #** page, do the following:

Server Platform:

In the list of server platforms, select the platform that your EV Code Signing Certificate is to be installed on.

Reason for Reissue:

In the box, specify the reason for the certificate reissue.

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

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

10.3.23 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 **Certificates > Orders**.
2. On the **Orders** page, use the drop-down lists, search box, advance search features (**Show Advanced Search** link), and column headers to filter the list of certificates.
3. Click the **"Order #"** link of the EV Code Signing Certificate that needs to be renewed.
4. In the **Order #** details pane (on the right), click **Renew Certificate**.
5. 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**.

Additional Renewal Message: To create a renewal message for this certificate right now, type the renewal message making sure to include information that might be relevant to the certificate's renewal.

Auto-renew
Auto-renew order 30 days If you want the certificate to be automatically renewed 30 days before it expires, check **Auto-renew order 30 days before expiration**.

**before
expiration.**

Important Note:

When you renew early, DigiCert adds the remaining time from your current certificate to your new certificate (up to 39 months).

6. 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 download 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-----
MIICvDCCAAQCAwdsEIMAKGA1UEBhMCVWVMeEjAQBGNVBAgTCV1vdXJtdGF0ZTER
MA8GA1UEBhMIW91ckNpdHkxGzAUBGNVBAgTAk1UMRowGAYDVQQKEwFZb3VyQ29t
cGFueSw5LjJlYm9yYGA1UEAxMPd3d3LmV4YV1vbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCqKCAQEA379BFFxZACdKsUk2vrQka/nAlKbo+I9DAN32
+/SRxj/KtXVddscKw1obHGPMPv4meJqOpQwJkIchYjSUQ8pPKzdGpccDMf/eoFO
J7EaQ2szLv9AqdrQw2AaeK8SmocVmd3LkEOX4VvALBOMLHVrB5/vhYfGECLEJbcS1
RdEbdKyHdtHk1RAoIVQCFjTwBWNAD387vmHW7QOR6FYUoa4fcJh7Rv6jHSyqwx
7pVfaDb2PuTgUhw7wksKNFxcG0xcTMr/+GrciHEu20chq86CBP9RiYlpp2+RMSf
m6rMEYm9o65j7vEYAEJU0JtASMIa/ZjaXfS1LjXurLU0nCCQqIDAGABoAAWdQYJ
KoZIHvchNAQEFBQADggEBAK159goyAYOpnrcQ2EvCG1azK1kS3D83jnAiF1NHxjB
/gdTYR+/8Dr/hbcwvUSThSRVf68ebK6cUhwAdp29C94Jz2+ENEbO8G80Fc-rv
ix7vb15vSka3ahG1jRG1zzHVGRoR3r7wQcTuMaDAr3alV8jHbcv2TcPK0Kbq6H1G
NLA4CKsOI4KQvu4FXfSsJEGb3gEJD8HaMP8U8er5G0ovv/g/9Z/1/b0g97kKcUvk
M2eDsvPhMx/pENGBnLPe4XMy7NP1EdsFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziunM1dE24NBt5tpCNafCviKT6/RVfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

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

10.4 Intermediate Certificates

The **Intermediate Certificates** page (**Account > Intermediates**) contains all the intermediate certificates from which your certificates are generated.

- Click the Intermediate Certificate (e.g., *TERENA SSL CA 3*) to see additional information about it
- Click **Download** if you need to install the certificate where needed in your environment (e.g., firewall, browser, server, etc.).

Note: If you are looking for your certificate's matching intermediate root, please download it from the **Manage Order#** page (**Certificates > Orders** and then click the **Order #**).

About DigiCert

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

DIGICERT

2600 WEST EXECUTIVE PKWY STE. 500

LEHI, UTAH 84043

PHONE: 801.701.9690

EMAIL: SALES@DIGICERT.COM



© 2015 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.