# Table of Contents

1. Issue Personal ID certificates (Admin) ................................................................. 3
2. Reissue Personal ID certificates (Admin) ............................................................... 11
3. Renew Personal ID certificates (Admin) ............................................................... 14
4. Cancel Personal ID certificate order ...................................................................... 22
5. Personal ID certificate revocation process ........................................................... 23
   5.1 Place a request to revoke a Personal ID certificate ........................................... 24
   5.2 Approve a Personal ID certificate revocation request (Admin) ......................... 25
6. Resend the Email Validation for DigiCert "Client Certificate" email ......................... 26
7. Resend the Create Your DigiCert "Client Certificate" email ................................... 27
8. Turn on Client certificate renewal notifications .................................................... 28
9. Configure the Client certificate approval process .................................................. 29
10. Generate your Personal ID certificate .................................................................... 32
11. Manage your Personal ID certificate .................................................................... 34
   11.1 (Windows) Export your Personal ID certificate ................................................ 34
       11.1.1 Internet Explorer: How to export your Personal ID certificate ...................... 34
       11.1.2 Google Chrome: How to export your Personal ID certificate .................... 38
       11.1.3 Firefox: How to export your Personal ID certificate .................................. 42
   11.2 (Windows) Import your Personal ID certificate ................................................ 44
       11.2.1 Internet Explorer: How to import your Personal ID certificate .................. 45
       11.2.2 Google Chrome: How to import your Personal ID certificate .................... 49
       11.2.3 Mozilla Firefox: How to import your Personal ID certificate ..................... 54

About DigiCert ........................................................................................................... 59
1 Issue Personal ID certificates (Admin)
Use these instructions to issue theses Client certificates for yourself or a non-account:

- Digital Signature Plus
- Email Security Plus
- Authentication Plus
- Premium

The process for issuing any of the Client certificates in your CertCentral account is the same:

1. **(If Required)** Create the Certificate Signing Request (CSR).
2. Fill out the Client certificate request form.
3. Wait for approval.

**How to request a Premium Client Certificate**

Because the form for requesting any of the Client certificates is similar, we will provide instructions for requesting a Premium Certificate and note any differences between the Premium Certificate request form and the other types of Client certificate request forms.

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 CertCentral account, use one of these options to access the certificate’s order page:
   
   a. **Option 1: Not sure which client certificate you want**
      
      i. In the sidebar menu, hover over Request a Certificate and then under All Products, click Product Summary.
ii. On the Request a Certificate page, on the Client Certificates tab, select Premium and then, click Order Now.

![Request a Certificate](image)

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

   In the sidebar menu, hover over Request a Certificate and then under Client Certificates, select client certificate you want to order.

3. On the Request a Client Certificate page, under Certificate Settings, provide the certificate details:

a. **Organization**

   In the drop-down list, select the organization you are requesting the Client certificate for.

   **Note:** The organization name appears on your Client certificate.

b. **Organization Unit**

   Adding an organization unit is not required; you can leave this box blank.

   If you want to designate the organization unit for which the certificate will be used, then in the box, enter the organization unit name.

c. **Signature Hash**

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

d. **Validity Period**

   Select a validity period for the certificate: 1 Year, 2 Years, 3 Years, Custom expiration date, or Custom length.
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 **Recipient Details**:
   
a. **Recipient Name (Common Name)**
   
Enter the recipient's name as you want it to appear on the Client certificate.

   **CSR Note:** If you are using a CSR to create your certificate, enter the fully qualified domain name (for example, `www.example.com`).

b. **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 also 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 email addresses appear on the Client certificate.
When entering multiple email addresses, make sure to use commas to separate them (for example, 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, use one of these options to add your CSR:

   **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.

   a. **Upload your CSR**

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

   b. **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 into the **Add Your CSR** box.

7. To add additional Client certificate recipients, click the **Add Another Certificate** link and enter the recipient’s **Recipient Details**.
8. **Additional Information**

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

![Additional Information](image)

9. Under **Payment Information**, one of the following:

   a. **Pay with Contract Terms**

      If you have a contract and want to use it to pay for the certificate request, continue to step 8.

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

      ![Payment Information](image)

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

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

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

      ii. Select **Bill to account balance** and continue to step 8.

      **Note:** If you need to deposit funds before continuing with the certificate order, click the **Deposit** link. Be aware that when you click the link you are taken to another page inside CertCentral, and the information that you have entered about the certificate is not saved.
c. **Exclude from Contract Terms and Pay with Credit Card**
If you don't want to or can't use your contract terms to pay for the certificate, you can pay for the certificate by billing it to a credit card.

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

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

   1. **Use One of the Credit Cards Listed**
      Under **Selected Card**, select one of the available cards.

   2. **Add a Different Credit Card**
      a. Under **Selected Card**, select **Another Credit Card**.
b. Under **Credit Card Details**, type your credit card information (i.e., *card number, etc.*).

![Credit Card Details](image)

![Billing Information](image)

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

**Use account's billing contact information**

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

**Add your billing information**

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

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

**Do Not Save the Credit Card**

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

**Save the Credit Card**

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

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

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

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

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

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

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

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

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

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

13. After all email addresses are validated, the Create Your DigiCert "Client Certificate" email is sent to the first email address on the list so that the recipient can create their Client certificate.

After the recipient creates the Client certificate, on the Orders page (Certificates > Orders), the certificate should be listed with the Status of Issued.

14. CSR Note:

If you submitted a CSR, you don’t receive an email with a link to create your Client certificate. Instead, after the recipient validates their email addresses, they receive an email with the Client certificate attached.

For instructions on how to install the Client certificate, see (Windows) Importing Your Personal ID Certificate.

2 Reissue Personal ID certificates (Admin)

Use these instructions to reissue these Client certificates for yourself or a non-account user:

- Digital Signature Plus
- Email Security Plus
- Authentication Plus
- Premium

The process for reissuing any of the Client certificates in your CertCentral account is the same:

1. (If Required) Create the Certificate Signing Request (CSR).
2. Fill out the Client certificate request form.
3. Wait for approval.

How to reissue a Premium Client Certificate

Because the form for reissuing any of the Client certificates is similar, we will provide instructions for reissuing a Premium Certificate and note any differences between the Premium Certificate reissue form and the other types of Client certificate reissue forms.

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 CertCentral account, in the sidebar menu, click Certificates > Orders.
3. On the **Orders** page, use the drop-down lists, search box, advanced search features (**Show Advanced Search**), and column headers to locate the **Premium** client certificate you need to reissue.

4. In the **Order#** column, click the **Quick View** link of the certificate that needs to be reissued.

5. In the **Order details panel** (on the right), click the **Reissue Certificate** link.

6. On the **Reissue Certificate for Order** page, under **Recipient Details**, verify the prepopulated information is correct.

   **Note:** Because you are reissuing your certificate, the **Recipient Name (Common Name)** and **Recipient Email** boxes should be prepopulated with the correct information from the original certificate request.

   a. **Recipient Name (Common Name)**
      
      Recipient's name as you want it to appear on the certificate

      **CSR Note:** If you are using a CSR, the fully qualified domain name (for example, *www.example.com*)

   b. **Recipient Email**
      
      The recipient’s email address (for example,. *jaden.doe@example.com*) that you want to appear on the certificate.

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

c. Recipient CSR (optional) If you need to use a CSR to reissue your certificate, in the Recipient box, use one of these options to add your CSR:

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

- **Paste your CSR in the box**
  
  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.

7. In the **Signature Hash** drop-down list, select a signature hash (for example, SHA-256).

8. In the **Reason for Reissue** box, specify a reason for the certificate reissue.

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

10. 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 Reissue Pending.

11. 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.

   After the recipient creates the Client certificate, on the Orders page (Certificates > Orders), the certificate should be listed with the Status of Issued.

12. CSR Note:

   If you submitted a CSR, you don’t receive an email with a link to create your Client certificate. Instead, after the recipient validates their email addresses, they receive an email with the Client certificate attached.

13. For instructions on how to install the Client certificate, see (Windows) Importing Your Personal ID Certificate.

3 Renew Personal ID certificates (Admin)

Use these instructions to renew these Client certificates for yourself or a non-account user.

- Digital Signature Plus
- Email Security Plus
- Authentication Plus
- Premium

The process for issuing any of the Client certificates in your CertCentral account is the same:

1. (If Required) Create the Certificate Signing Request (CSR).
2. Fill out the Client certificate request form.
3. Wait for approval.

How to reissue a Premium Client Certificate

Because the form for renewing any of the Client certificates is similar, we will provide instructions for renewing a Premium Certificate and note any differences between the Premium Certificate renewal form and the other types of Client certificate renewal forms.

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 CertCentral account, in the sidebar menu, click Certificates > Orders.
3. On the Orders page, use the drop-down lists, search box, advanced search features (Show Advanced Search), and column headers to locate the Premium client certificate you need to reissue.

4. In the Order# column, click the Quick View link of the certificate that needs to be renewed.

5. In the Order details panel (on the right), click the Renew Certificate link.

6. On the Request a Client Certificate page, under Certificate Settings, provide the certificate details:
   a. Organization
      In the drop-down list, select the organization you are requesting the Client certificate for.
      
      Note: The organization name appears on your Client certificate.
   b. Organization Unit
      Adding an organization unit is not required; you can leave this box blank.
If you want to designate the organization unit for which the certificate will be used, then in the box, enter the organization unit name.

c. **Signature Hash**

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

d. **Validity Period**

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

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

8. **Under Certificate(s) to Request**, enter the **Recipient Details**:
   a. **Recipient Name (Common Name)**

   Enter the recipient’s name as you want it to appear on the Client certificate.
**CSR Note:** If you are using a CSR to create your certificate, enter the fully qualified domain name (for example, www.example.com).

b. **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 also 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 email addresses appear on the Client certificate.

When entering multiple email addresses, make sure to use commas to separate them (for example, 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.

9. **(Optional)** If you need to use a CSR to create your certificate, in the **Recipient CSR (optional)** box, use one of these options to add your CSR:

**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.

a. **Upload your CSR**

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

b. **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 into the Add Your CSR box.

10. To add additional Client certificate recipients, click the Add Another Certificate link and enter the recipient's Recipient Details.

11. Additional Information

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

12. Under Payment Information, one of the following:
   a. Pay with Contract Terms
      
      If you have a contract and want to use it to pay for the certificate request, continue to step 8.

      **Note:** If you have a contract, it is the default payment method.
b. **Exclude from Contract Terms and Pay with Account Balance**

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

   iii. Check **Exclude from contract terms**.
   iv. Select **Bill to account balance** and continue to step 8.

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

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

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

   i. Check **Exclude from contract terms**.
   ii. Select **Bill to credit card** and then do one of the following options:

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

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

   2. **Add a Different Credit Card**

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

![Credit Card Details](image)

```
Credit Card Details

Credit card number

Expiration date

CVV
```

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

**Use account’s billing contact information**

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

**Add your billing information**

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

![Billing Information](image)

```
Billing Information

Same as the billing contact for this account

Name on card

Country

USA

Address 1

City

Alabama

Address 2

State

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

**Do Not Save the Credit Card**

Uncheck **Save this credit card**.

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

**Save the Credit Card**

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

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

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

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

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

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

13. Under **Certificate Services Agreement**, read through the agreement, making sure you understand it and then, check **I agree to the Certificate Services Agreement above**.
14. When you are finished, click Submit Request.

15. 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.

16. 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.

After the recipient creates the Client certificate, on the Orders page (Certificates > Orders), the certificate should be listed with the Status of Issued.

17. CSR Note:

If you submitted a CSR, you don’t receive an email with a link to create your Client certificate. Instead, after the recipient validates their email addresses, they receive an email with the Client certificate attached.

For instructions on how to install the Client certificate, see (Windows) Importing Your Personal ID Certificate.

4 Cancel Personal ID certificate order
You may need to cancel a Client certificate order before the recipient. For example, you included the wrong email address in the certificate order.

Items to note about Client certificate cancelation

- You can only cancel pending Client certificate orders before the recipient generates the certificate. Once the certificate is generated, you will need to revoke the certificate.
- If you added the approval step to your Client certificate issuance process, you don’t need to cancel the order, the approver can just reject the request.

How to cancel a Client certificate order

1. In your CertCentral account, in the sidebar menu, click Certificates > Orders.
2. On the Orders page, use the filters and the advanced search features to locate the pending Client certificate order.

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

4. On the Order details page, in the Certificate Details section, in the Certificate Actions drop-down list, select Cancel Order.

5. In the Cancel Order window, click Cancel Order.

   Note: Canceling an order successfully removes it from our system and can't be undone. However, if the Client certificate ends up being needed, simply place the order again. The canceled order is logged in the Audit Logs (Account > Audit Logs).

6. Congratulations! You have successfully canceled the Client certificate order.

5 Personal ID certificate revocation process

You may need to revoke a Client certificate. For example, if an employee leaves the company, you may want to revoke the no longer needed Client certificate.

The certificate revocation process consists of three steps:
1. Place a request to have a certificate revoked.
2. Administrator approves the certificate revocation request.
3. DigiCert revokes the certificate.

This process is the same for all certificate types (TLS, code signing, and so on) and doesn't change even if administrator approvals are not required for certificate issuance.

5.1 Place a request to revoke a Personal ID certificate
Use this instruction to place a request to have a Client certificate revoked.

How to place a Client certificate revocation request

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

2. On the Orders page, use the drop-down lists, search box, advanced search features (Show Advanced Search), and column headers to locate the client certificate order for which you need to resend the Email Validation for DigiCert "Client Certificate" email.

3. In the Order# column, click the Quick View link for that certificate.

4. In the Order details panel (on the right), click the Revoke Certificate link.

5. On the Request to Revoke Certificate for Order # page, in the Reason for Revocation box, provide information for why you want this certificate revoked.
6. If you are sure that this certificate needs to be revoke, click **Request Revocation** to place this certificate revocation request.

An administrator must now approve the request before it can be submitted to DigiCert.

### 5.2 Approve a Personal ID certificate revocation request (Admin)

Use this instruction to approve a certificate revocation request.

**How to approve a request to revoke a Client certificate**

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

2. On the **Requests** page, in the **Status** drop-down list, select **Pending**, in the **Type** drop-down list, select **Revoke**, and then click **Go** to see only the certificates that need revocation approval.

3. In the “**Order #**” column, click the order number link for the certificate revocation request you need to approve.

4. In the **Order #** details panel (on the right), click **Approve** to continue with the certificate revocation.
5. In the Approve Request window, enter an Approval Comment.

**CAUTION:** In the Approve Request window, do not click Approve, unless you are sure that you want to revoke the certificate. The revocation can’t be reversed.

6. If you are sure you really need to revoke this Client certificate, click Approve.

Congratulations! You’ve submitted your certificate revocation request to DigiCert.

6 **Resend the Email Validation for DigiCert "Client Certificate" email**

Use these instructions to resend the 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.

**How to resend the email validation email**

1. In your CertCentral account, in the sidebar menu, click Certificates > Orders.
2. On the **Orders** page, use the drop-down lists, search box, advanced search features (**Show Advanced Search**), and column headers to locate the client certificate order for which you need to resend the **Email Validation for DigiCert "Client Certificate"** email.

3. In the **Order#** column, click the **Quick View** link for that certificate.

4. In the **Order** details panel (on the right), click the **Resend validation email** link.

   **Multiple Email Addresses Note:** If the Client certificate recipient has multiple email addresses listed, you can resend any or all the validation emails.

5. After you click the link, it will change to **Sent**. The **Email Validation for DigiCert "Client Certificate"** email is resent to the specified address with a new link to validate that email address.

7 **Resend the Create Your DigiCert "Client Certificate" email**

   Use these instructions 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 CertCentral account, in the sidebar menu, click **Certificates > Orders**.
2. On the Orders page, use the drop-down lists, search box, advanced search features (Show Advanced Search), and column headers to locate the client certificate order for which you need to resend the Create Your DigiCert "Client Certificate" email.

3. In the Order# column, click the Quick View link for that certificate.

4. In the Order details panel (on the right), 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.

5. The link will change to Sent. The Create Your DigiCert "Client Certificate" email is resent with a new link to create their Client certificate.

   **Note:** As soon as you resend the email, the old link expires and can't be used to create the Client certificate. If the expired link is used, this message is displayed: “The emailed link is invalid or has expired. Try resetting your password or try logging in to resolve the issue.”

### 8 Turn on Client certificate renewal notifications

Use these instructions to turn on Client certificate renewal notifications.

By default, Client certificate renewal notifications are turned off for CertCentral accounts. However, if you prefer, you can activate renewal notifications for your Client certificate orders.

**Note:** Renewal notifications are not sent for Client certificate orders that are set to automatically renew.

Once activated, these renewal notifications are configured as part of your TLS, Code Signing, and Document Sign renewal notifications. For example, if choose to include a default renewal message, this message will be included in the Client certificate renewal notifications as well.
How to turn on Client certificate renewal notifications

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

2. On the **Division Preferences** page, in the **Certificate Renewal Settings** section, under **Client Certificate Renewal Notifications**, check **Turn on client certificate renewal notifications**.

3. Then, click **Save Settings**.

4. Congratulations! You have turned on renewal notifications for you client certificates.

9 Configure the Client certificate approval process

Use these instructions to configure the approval step for your Client certificate issuance process.

By default, the Client certificate issuance process doesn't require an Administrator approval. However, if you want more control over the Client certificate process, you can configure this process to include an approval step. Once this step is activated, an administrator must approve
Client certificate orders before the Email Validation for DigiCert "Client Certificate" email is sent (*step 3 in the process below).

**Client certificate issuance process with approval step added**

1. User (admin, manager, and so on) orders a Client certificate.

2. The requestor provides an email address and possibly a CSR and then submits the order.

3. *An administrator reviews and approves the Client certificate order.

   The step is not part of the default Client certificate issuance process.

4. DigiCert sends the Email Validation for DigiCert "Client Certificate" email to each email address listed in the order enabling the recipient to prove they have control of the email address.

   **Note:** This step is the same for orders where a CSR is submitted.

5. Email recipient validates their emails addresses.

6. DigiCert sends the Create Your DigiCert “Client Certificate” email. This email contains a link to a page where the email recipient can generate their Client certificate.

   **CSR Note:** When a CSR is provided, DigiCert sends the Client certificate as an attachment to an email instead.

7. Email recipient generates their Client certificate in one of the supported browsers. See [Generate your Personal ID certificate](#)

**How to configure the Client certificate approval step**

**Important SAML Note:** If you are using SAML, turning on the Client certificate Approval feature will interrupt the SAML certificate enrollment process.

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

2. On the **Division Preferences** page, scroll to the bottom of the page and expand **Advance Settings**.
3. In the **Certificate Requests** section, under **Client Certificate Approval**, check **Client certificate requests must be approved before they will be issued.**

4. Then, click **Save Settings**.

5. Congratulations! You have added the approval step to your Client certificate issuance process.

   The next time someone orders a Client certificate, the certificate request will require an administrator approval before the certificate can be issued.
10 Generate your Personal ID certificate

After your administrator issues your Personal ID, you should receive a Create Your DigiCert...Certificate email. The email contains a link that takes you to the Generate your DigiCert...Certificate page, where you will generate your Personal ID Certificate.

Browser Note: Chrome and Microsoft Edge don’t support Client certificate generation. If you want to use your Client certificate with Chrome and Microsoft Edge, we recommend generating it in Internet Explorer (Chrome and Edge) or Safari (Chrome).

Make sure to note which browser you used to generate your Personal ID Certificate, in case you need to export it. For example, if you need your Personal ID for email signing and encryption, you will need to export your certificate and install it in your email client.

- **Internet Explorer** install the Personal ID Certificates in the Windows Certificate Store. **Both Chrome, Microsoft Edge, and Internet Explorer can access it.**
- **Safari** install the Personal ID Certificates in the Mac Certificate Store. **Both and Chrome and Safari can access it.**
- **Firefox (Windows or Mac)** installs the Personal ID Certificate in its own Certificate Store and **only Firefox can access it.**
- **Chrome Note:** Chrome does not support Client certificate generation. If you want to use your Client certificate with Chrome, we recommend generating it in Internet Explorer or Safari (Mac).
- **Microsoft Edge Note:** Edge does not support Client certificate generation. If you want to use your Client certificate with Edge, we recommend generating it in Internet Explorer.

How to generate your Client certificate

1. Open the Create Your DigiCert Certificate email.

![Create Your DigiCert Certificate email]

2. Use the Create your DigiCert Personal ID Certificate now by going to link to open the Generate your DigiCert...Certificate page:
   - To open the page in your default browser, simply click the link in the email.
ii. To open the link in the browser of choice, copy and paste the link in the address field the browser.

3. On the **Generate your DigiCert…Certificate** page, do the following:
   
i. Verify that the name, email address, and organization are correct.
   
ii. Read through the **Subscriber Agreement** and then check **I agree to the terms of the subscriber agreement**.
   
iii. Finally, click **Generate Certificate**.

4. You should receive the **"Your DigiCert Personal ID should now be installed messages"**.

   Congratulations, you have successfully generated your Personal ID Certificate.
11 Manage your Personal ID certificate

11.1 (Windows) Export your Personal ID certificate

After you generate and install your Personal ID Certificate, you may need to export your certificate, to transfer it to a new computer, to use a different browser to sign in to an account, etc.

- Internet Explorer: How to export your Personal ID certificate
- Google Chrome: How to export your Personal ID certificate
- Firefox: How to export your Personal ID certificate

11.1.1 Internet Explorer: How to export your Personal ID certificate

1. In Internet Explorer, go to **Internet Options**.

2. In the **Internet Options** window, on the **Content** tab, click **Certificates**.
3. In the **Certificates** window, on the **Personal** tab, select your Personal ID Certificate and click **Export**.

4. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.

5. On the **Export Private Key** page, select **Yes, export private key** and then, click **Next**.
6. On the Export File Format page, select **Personal Information Exchange – PKCS #12 (.PFX)**, check **Include all certificates in the certification path if possible**, and then, click **Next**.

![Certificate Export Wizard](image1)

7. On the **Security** page, add a password to protect your certificate’s private key.
   
i. Check **Password**.
   
ii. In the **Password** and **Confirm password** boxes, type your password.
   
iii. Click **Next**.

![Certificate Export Wizard](image2)
8. On the **File to Export** page, click **Browse**, locate where you want to save the Personal ID Certificate (w/private key) .pfx file, provide a file name (for example, *myPersonalCert*), click **Save**, and then, click **Next**.

**Note:** Make sure to save the .pfx file in a location that you will remember.

9. On the **Completing the Certificate Export Wizard** page, review the settings and then, click **Finish**.

10. When you receive "**The export was successful**" message, click **OK**.

    Congratulations! You exported your Personal ID Certificate w/private key as a .pfx file.
11.1.2 Google Chrome: How to export your Personal ID certificate

1. In Chrome, go to Settings.

2. On the Settings page, below On startup, expand Advanced.

3. In the Manage certificates section, click then Manage HTTPS/SSL certificates and settings link.
4. In the **Certificates** window, on the **Personal** tab, select your Personal ID Certificate and click **Export**.

![Certificate Export Wizard](image)

5. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.

![Certificate Export Wizard](image)
6. On the **Export Private Key** page, select *Yes, export private key* and then, click **Next**.

7. On the **Export File Format** page, select **Personal Information Exchange – PKCS #12 (.PFX)**, check **Include all certificates in the certification path if possible**, and then, click **Next**.
8. On the Security page, do the following: check Password.
   i. Check Password.
   ii. In the Password and Confirm password boxes, type your password.
   iii. Click Next.

9. On the File to Export page, click Browse, locate where you want to save the Personal ID Certificate (w/private key) .pfx file, provide a file name (e.g., myPersonalCert), click Save, and then, click Next.

   **Note:** Make sure to save the .pfx file in a location that you will remember.
10. On the **Completing the Certificate Export Wizard** page, review the settings and then, click **Finish**.

11. When you receive "**The export was successful**" message, click **OK**.

Congratulations! You exported your Personal ID Certificate w/private key as a .pfx file.

**11.1.3 Firefox: How to export your Personal ID certificate**

1. In Firefox, go to **Options**.
2. On the Options tab, in the sidebar menu, click Privacy & Security, scroll down to the Security section, and then, click View Certificates.

3. In the Certificate Manager window, on the Your Certificates tab, select your Personal ID Certificate and click Backup.

4. In the File Name to Backup window, go to where you want to save the Personal ID Certificate (w/private key) p12 file, provide a file name (e.g., myPersonalCertificate), and then click Save.
Note: Make sure to save the p12 file in a location that you will remember. A p12 file uses the same format as a .pfx file. If you want, you can change the extension to .pfx and resave the file as a .pfx file if needed.

5. In the Choose a Certificate Backup Password window, create a Certificate backup password and then, click OK.


11.2 (Windows) Import your Personal ID certificate
If you transferred to a new computer, or you want to use a different browser to log into an account, you need to import your Personal ID Certificate into the appropriate Certificate Store.

- Internet Explorer: How to import your Personal ID certificate
- Google Chrome: How to import your Personal ID certificate
- Mozilla Firefox: How to import your Personal ID certificate

### 11.2.1 Internet Explorer: How to import your Personal ID certificate

1. In Internet Explorer, go to **Internet Options**.

2. In the **Internet Options** window, on the **Content** tab, click **Certificates**.

3. In the **Certificates** window, on the **Personal** tab, click **Import**.
4. In the **Certificate Import Wizard**, on the **Welcome** page, click **Next**.

5. On the **File to Import** page, click **Browse**.
6. In the File Explorer **Open** window, in the file type drop-down list, select **Personal Information Exchange (*.pfx;*.p12)**.

7. Locate and select your Personal ID Certificate .pfx or .p12 file, and then click **Open**.

8. On the **File to Import** page, click **Next**.
9. On the **Private key protection** page, check **Mark this key as exportable** and **Include all extended properties**.

The **Mark this key as exportable** option enables you to export your Personal ID Certificate w/private key should you need to in the future.

10. In the **Password** box, type the password that you created when you exported your Personal ID Certificate w/private key and then, click **Next**.
11. On the **Certificate Store** page, click **Place all certificates in the following store**, in the **Certificate store** box, select **Personal** for the store, and then, click **Next**.

We recommend that you use this option so that intermediate and root certificates in the .pfx or .p12 file are placed in the appropriate Certificate Store.

12. On the **Completing the Certificate Import Wizard** page, review the settings and then, click **Finish**.

13. Congratulations! You imported your Personal ID Certificate w/private key in to the Windows Certificate store, and you can use Internet Explorer, Microsoft Edge, and Chrome to sign in to your accounts.

**11.2.2 Google Chrome: How to import your Personal ID certificate**

1. In Chrome, go to **Settings**.
2. On the Settings page, below On startup, expand Advanced.

3. In the Manage certificates section, click then Manage HTTPS/SSL certificates and settings link.
4. In the Certificates window, on the Personal tab, click Import.
5. In the Certificate Import Wizard, on the Welcome page, click Next.

6. On the File to Import page, click Browse.
7. In the File Explorer **Open** window, in the file type drop-down list, select **Personal Information Exchange (*.pfx;*.p12)**.

8. Locate and select your Personal ID Certificate .pfx or .p12 file, and then click **Open**.

9. On the **File to Import** page, click **Next**.
10. On the **Private key protection** page, check **Mark this key as exportable** and **Include all extended properties**.

The **Mark this key as exportable** option enables you to export your Personal ID Certificate w/private key should you need to in the future.

11. In the **Password** box, type the password that you created when you exported your Personal ID Certificate w/private key and then, click **Next**.

12. On the **Certificate Store** page, click **Place all certificates in the following store**, in the **Certificate store** box, select **Personal** for the store, and then, click **Next**.
We recommend that you use this option so that intermediate and root certificates in the .pfx or .p12 file are placed in the appropriate Certificate Store.

13. On the **Completing the Certificate Import Wizard** page, review the settings and then, click **Finish**.

14. Congratulations! You imported your Personal ID Certificate w/private key in to the Windows Certificate store. You can use Chrome, Microsoft Edge, and Internet Explorer to log in to your accounts.

11.2.3 **Mozilla Firefox: How to import your Personal ID certificate**

1. In Firefox, go to **Options**.
2. On the Options tab, in the sidebar menu, click Privacy & Security, scroll down to the Security section, and then, click View Certificates.

3. In the Certificate Manage window, on the Your Certificates tab, click Import.
4. In the **Certificate File to Import** window, in the file type drop-down list, select **PKCS12 Files (*.pfx;*.p12)**.

5. Then, navigate to your Personal ID Certificate .pfx or .p12 file, and then click **Open**.

6. In the **Password Required** window, in the **Password** box, type the password that you created when you exported your Personal ID Certificate w/private key and then, click **OK**.

7. Congratulations! You imported your Personal ID Certificate w/private key in to the Firefox Certificate Store. You can use Firefox to log into your accounts.
12 Configure Outlook 2016/2013/2010 to use your Email Security Plus Personal ID Certificate

Use these instructions to configure Outlook to use your Email Security Plus Personal ID Certificate. After importing your Personal ID certificate, you can then configure Microsoft Outlook to use it to sign and encrypt emails.

1. In Outlook, click File.

2. On the File page, in the sidebar menu, click Options.

3. In the Outlook Options window, in the sidebar menu, click Trust Center.

4. On the Trust Center page, in the Microsoft Outlook Trust Center section, click Trust Center Settings.
5. In the **Trust Center** window, in the sidebar menu, click **E-mail Security**.

6. On the **E-mail Security** page, in the **Encrypted e-mail** section, click **Settings**.

7. In the **Change Security Settings** window, for **Signing Certificate**, click **Choose**.

8. In the **Windows Security** window, select your Client certificate (Personal ID) and click **OK**.

10. In the Windows Security window, select your Client certificate (Personal ID) and click OK.

11. In the Change Security Settings window, click OK.

You have successfully configured Outlook to use your Personal ID Certificate for signing and encrypting your emails.

About DigiCert

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

DigiCert
2801 North Thanksgiving Way Ste. 500
Lehi, Utah 84043
Phone: 801.701.9690
Email: sales@digicert.com

© 2018 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.