

# DigiCert CertCentral<sup>®</sup> Client Certificates

**Version 1.5**

## Table of Contents

1	How to Issue Personal ID Certificates (Admin) .....	3
2	Generating Your Personal ID Certificate .....	13
2.1	How to Generate Your Certificate Personal ID Certificate.....	13
3	Managing Your Personal ID Certificate .....	15
3.1	(Windows) Exporting Your Personal ID Certificate .....	15
3.1.1	Internet Explorer: How to Export Your Personal ID Certificate.....	15
3.1.2	Google Chrome: How to Export Your Personal ID Certificate .....	19
3.1.3	Firefox: How to Export Your Personal ID Certificate .....	24
3.2	(Windows) Importing Your Personal ID Certificate.....	27
3.2.1	Internet Explorer: How to Import Your Personal ID Certificate .....	27
3.2.2	Google Chrome: How to Import Your Personal ID Certificate .....	32
3.2.3	Mozilla Firefox: How to Import Your Personal ID Certificate.....	37
4	Configuring Outlook 2013 to Use Your Email Security Plus Personal ID Certificate .....	39
	About DigiCert.....	42

# 1 How to Issue Personal ID Certificates (Admin)

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

- i. **(If Required)** Admin creates the Certificate Signing Request (CSR).
- ii. Admin fills out the Client Certificate request form.
- iii. User waits for approval.

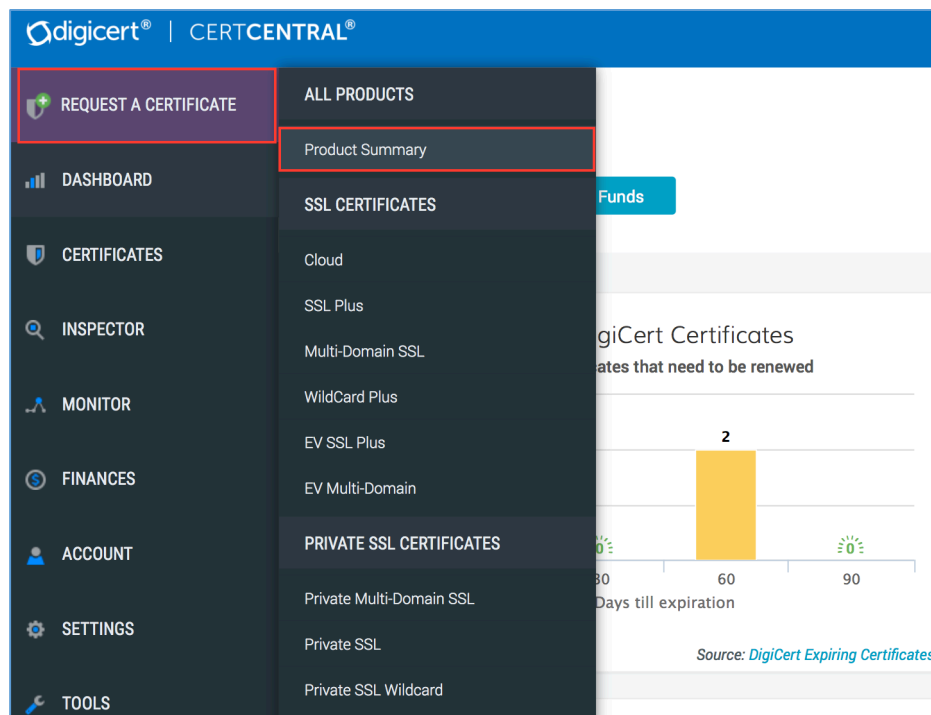
Because the form for requesting any of the Client Certificates is similar, we will provide instructions for requesting a Premium Certificate and note any differences between the Premium Certificate request form and the other types of Client Certificate request forms.

You can use this instruction for the following certificates:

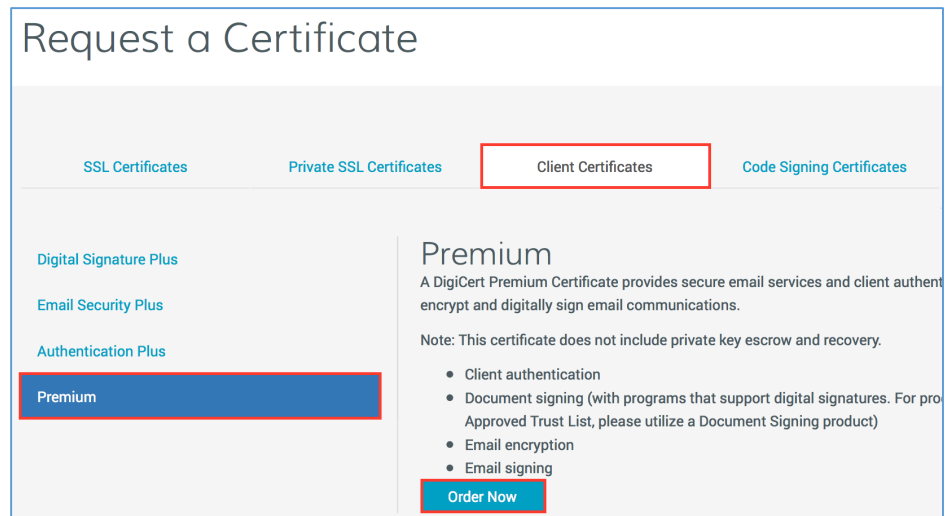
- Digital Signature Plus
- Email Security Plus
- Authentication Plus
- Premium

## How to Request a Premium Client Certificate

1. In your CertCentral account, do one for the following:
  - a. Option 1: **Unfamiliar** with certificate choices and the requesting process
    - i. In the sidebar menu, click **Request a Certificate** and then under **All Products**, click **Product Summary**.



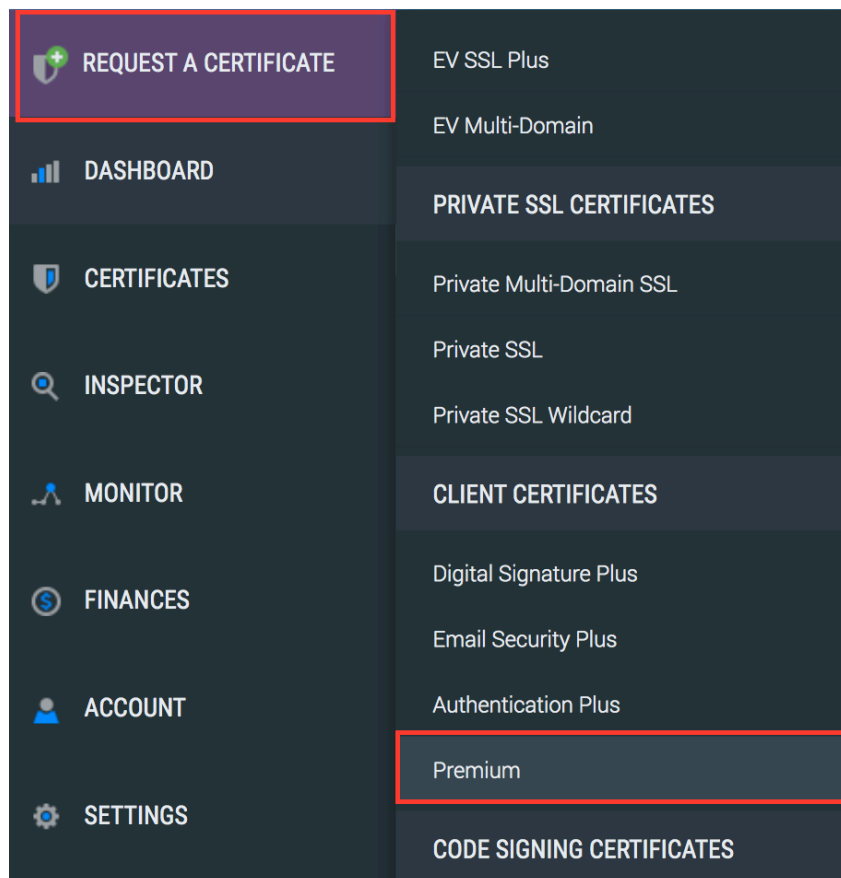
- ii. On the **Request a Certificate** page, select **Client Certificates**.



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

- b. Option 2: **Familiar** with certificate choices and the requesting process

- i. In the sidebar menu, click **Request a Certificate** and then under **Client Certificates**, select **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.

**\*Signature Hash:** In the drop-down list, select a signature hash (e.g., *SHA2*).

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

## Request a Client Certificate

For CertCentral Sales Test ▼

### Certificate Settings

Type

**Premium**

**\* Organization**

DigiCert, Inc. ▼

**Organization Unit**

**\* Signature Hash**

SHA1 ▼

SHA1 certificates have a max expiration date of December 30, 2019

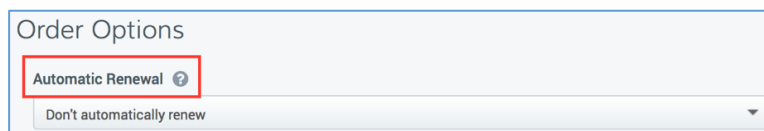
**Validity Period**

☐ 1 Year

☐ 2 Years

☒ 3 Years

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



The screenshot shows a form titled "Order Options". Inside, there is a dropdown menu labeled "Automatic Renewal" with a question mark icon. Below the dropdown, the text "Don't automatically renew" is visible, indicating the current selection.

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

**Recipient Name (Common Name)**

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

**CSR Note:** If you need to use a CSR to create your certificate, enter the fully qualified domain name (e.g., *www.example.com*).

**Recipient Email**

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

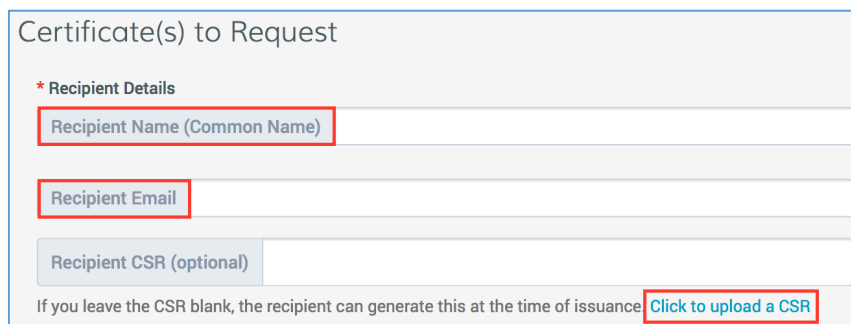
This email address is used to send the recipient an email so that they can generate their Client Certificate.

**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.



The screenshot shows a form titled "Certificate(s) to Request". Under the heading "\* Recipient Details", there are three input fields: "Recipient Name (Common Name)", "Recipient Email", and "Recipient CSR (optional)". Below these fields, there is a note: "If you leave the CSR blank, the recipient can generate this at the time of issuance". To the right of this note is a button labeled "Click to upload a CSR".

**Recipient CSR (optional)**

**(Only if required)** 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
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKEzF2b3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHdtHklRAoIVQCfjTwBWNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTmr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtASMI=/ZjaXfS1LjXurLU0nCOQQIDAQABAAWdQYJ
KoZIHvcNAQEFBQADggEBAK159goyAYOpncrQ2EvCG1izrK1kS3D8JjnAiP1NhrjB
/qdTYR+/8Dr/hMcwwUSThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEb08GA0Fc4rw
ix7vb15vSXe3shGijRGIZzHVGRoR3r7xQtIuMaDar3x1V8jHbcvZTepX0Kbq6H1G
NLA4CKsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/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**.

**+ Add Another Certificate**

## 6. 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

\*Add Order number and associated PO

Email list

Required Field 2

Country

Optional

## 7. 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

☐ Exclude from contract terms ?

Payment Method

This request will be deducted from your contract limits.

### 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.

- Check **Exclude from contract terms**.
- 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.

Payment Information

☒ Exclude from contract terms ?

Payment Method

☒ Bill to account balance ☐ Deposit Funds

☐ Bill to credit card

! You will be invoiced monthly for any negative account balance. If your account balance reaches -\$2000, your certificate requests will not be able to be approved.

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**

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

☒ Bill to credit card

Selected Card	Name on Card	Exp Date
<input checked="" type="radio"/> Client Certificate requests	Jan Doe	01/2021
<input type="radio"/> EV Certificate orders	John Doe	01/2020
<input type="radio"/> Another Credit Card		

[Manage Credit Cards](#)

2. **Add a Different Credit Card**

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

☒ Bill to credit card

Selected Card	Name on Card	Exp Date
<input type="radio"/> Client Certificate requests	Jan Doe	01/2021
<input type="radio"/> EV Certificate orders	John Doe	01/2020
<input checked="" type="radio"/> Another Credit Card		

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

- c. Then, under **Billing Information**, do one of the following:

**Use account's billing contact information**

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

**Add your billing information**

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

- d. Under **Credit Card Options**, do any or none of the following:

**Do Not Save the Credit Card**

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

**Save the Credit Card**

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

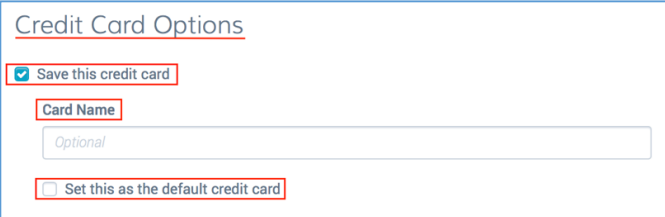
- a) Check **Save this credit card**.

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

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

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

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



Credit Card Options

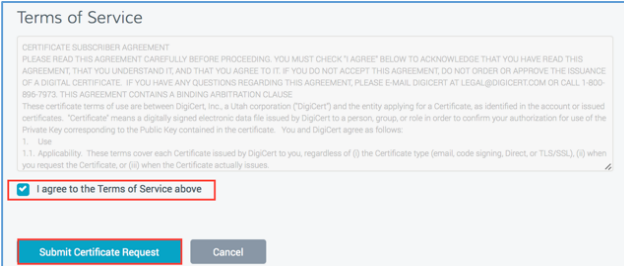
☒ Save this credit card

**Card Name**

Optional

☐ Set this as the default credit card

8. Under **Certificate Services Agreement**, read through the terms of service, making sure you understand the terms and then, check **I agree to the** Under **Certificate Services Agreement above**.



**Terms of Service**

CERTIFICATE SUBSCRIBER AGREEMENT  
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. YOU MUST CHECK "I AGREE" BELOW TO ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT ORDER OR APPROVE THE ISSUANCE OF A DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-855-7973. THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE.  
These certificate terms of use are between DigICert, Inc., a Utah corporation ("DigICert") and the entity applying for a Certificate, as identified in the account or issued certificates. "Certificate" means a digitally signed electronic data file issued by DigICert to a person, group, or role in order to confirm your authorization for use of the Private Key corresponding to the Public Key contained in the certificate. You and DigICert agree as follows:  
1. Use  
1.1. Applicability. These terms cover each Certificate issued by DigICert to you, regardless of (i) the Certificate type (email, code signing, Direct, or TLS/SSL), (ii) when you request the Certificate, or (iii) when the Certificate actually issues.

☒ I agree to the Terms of Service above

**Submit Certificate Request** Cancel

9. When you are finished, click **Submit Certificate Request**.
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 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 do not receive an email with a link to create your Client Certificate. Instead, after the recipient validates their email address(es), 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 Generating 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.

**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 (PC) or Safari (Mac).

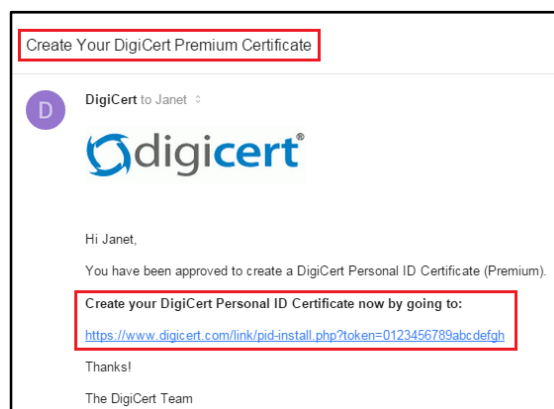
**Microsoft Edge Note:** Microsoft Edge does not support Client Certificates.

Make sure to note the browser 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.

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

### 2.1 How to Generate Your Certificate Personal ID Certificate

1. Open the **Create Your DigiCert Certificate** email.



2. To open the **Generate your DigiCert...Certificate** page, do one of the following with the **Create your DigiCert Personal ID Certificate now by going to link**:
  - i. 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**.

**digicert**

### Generate your DigiCert Premium Certificate

For technical assistance or to make corrections, contact your administrator.

**DigiCert Personal ID Details**

**Name:** Janet Van Dyne

**Email Addresses:** janet@pymsciences.com

**Organization:** Pym LLC

**Subscriber Agreement:**

CERTIFICATE SUBSCRIBER AGREEMENT

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. THE PURPOSE OF A DIGITAL CERTIFICATE IS TO BIND YOUR IDENTITY TO A PUBLIC-PRIVATE KEY PAIR. BY OBTAINING OR USING A CERTIFICATE ISSUED BY DIGICERT, YOU AGREE TO:

- PROTECT YOUR PRIVATE KEY WITH A STRONG PASSWORD AND NOT REVEAL IT TO ANYONE,
- REVIEW THE INFORMATION CONTAINED IN THE CERTIFICATE (NAME, EMAIL ADDRESS, AND ORGANIZATIONAL AFFILIATION),
- NOTIFY DIGICERT OR YOUR SPONSOR IF YOUR INFORMATION IS INCORRECT, BECOMES INCORRECT, OR IF YOU BELIEVE THAT YOUR CERTIFICATE IS NO LONGER A RELIABLE INDICATION THAT YOU POSSESS SOLE CONTROL OF THE PRIVATE KEY,

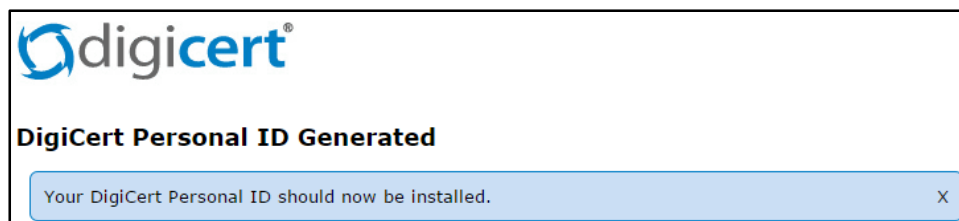
☒ I agree to the terms of the subscriber agreement

Your Personal ID will be valid for 1 year from the time it is issued. You have until April 23, 2015 to generate this certificate or you will need to contact your organization administrator to request a new email.

**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.



## 3 Managing Your Personal ID Certificate

### 3.1 (Windows) Exporting Your Personal ID Certificate

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

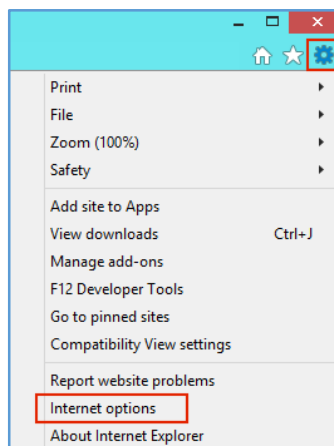
[Internet Explorer: How to Export Your Personal ID Certificate](#)

[Google Chrome: How to Export Your Personal ID Certificate](#)

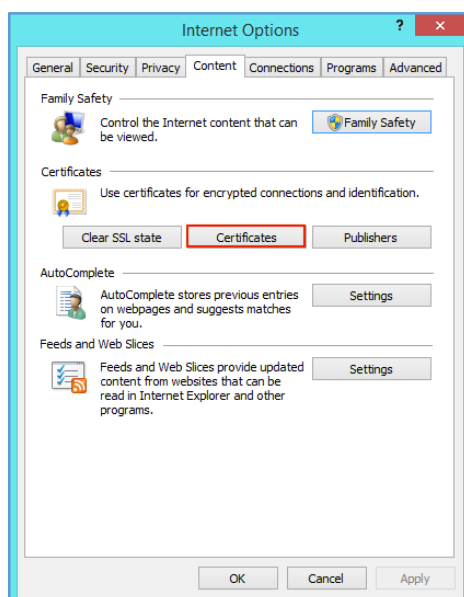
[Firefox: How to Export Your Personal ID Certificate](#)

#### 3.1.1 Internet Explorer: How to Export Your Personal ID Certificate

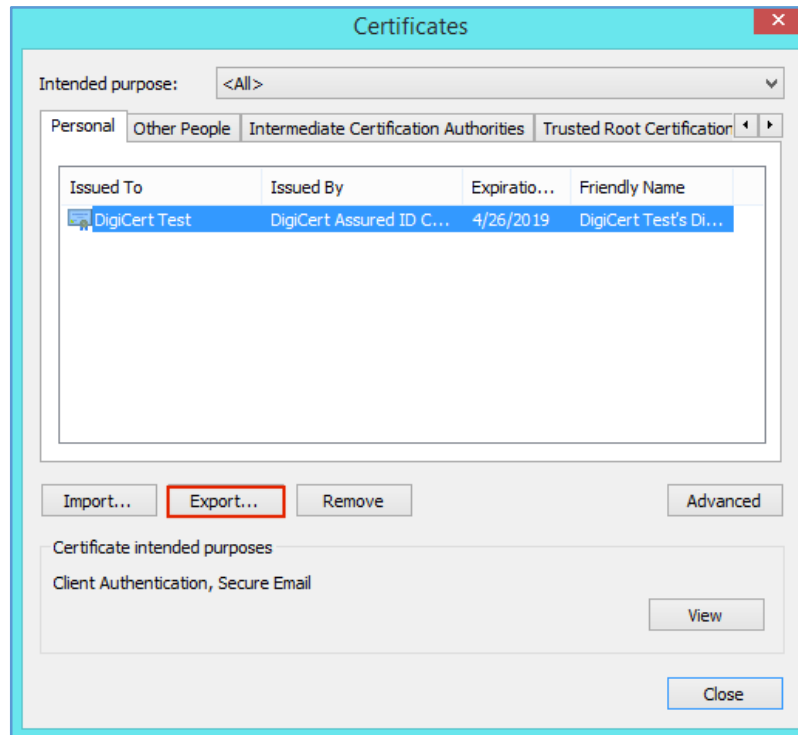
1. In Internet Explorer, go to **Internet Options**.



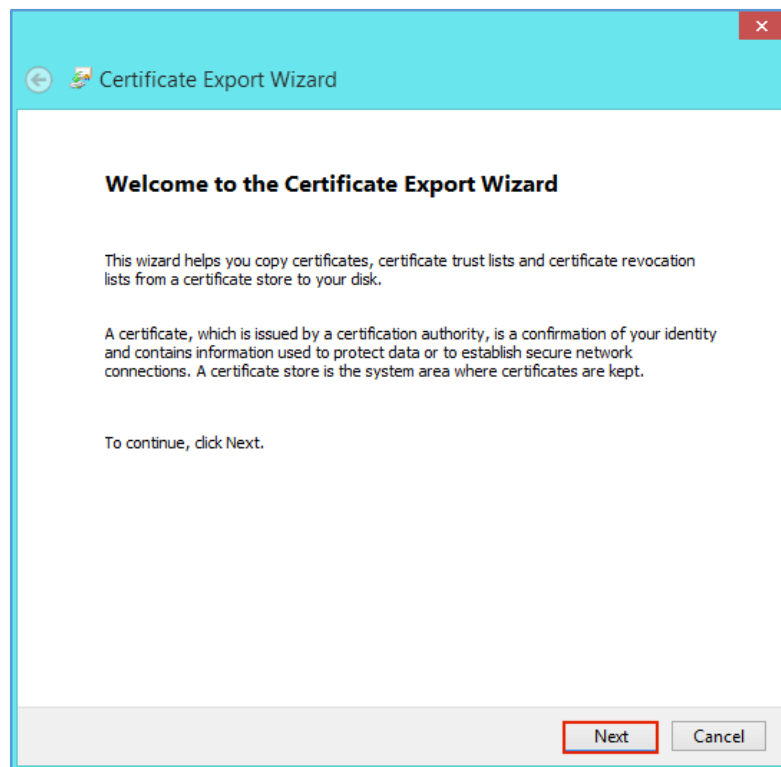
2. In the **Internet Options** window, on the **Content** tab, click **Certificates**.



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

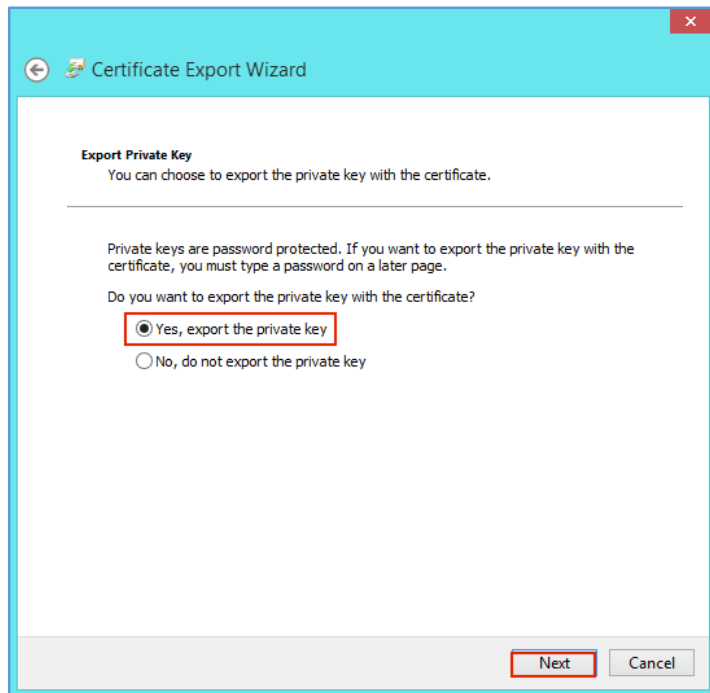


4. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.

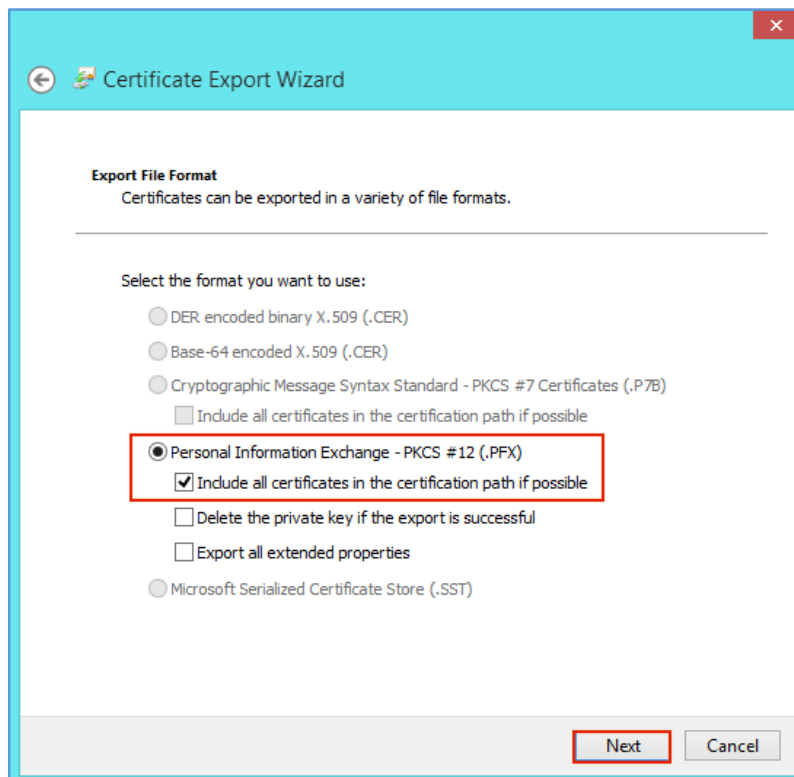




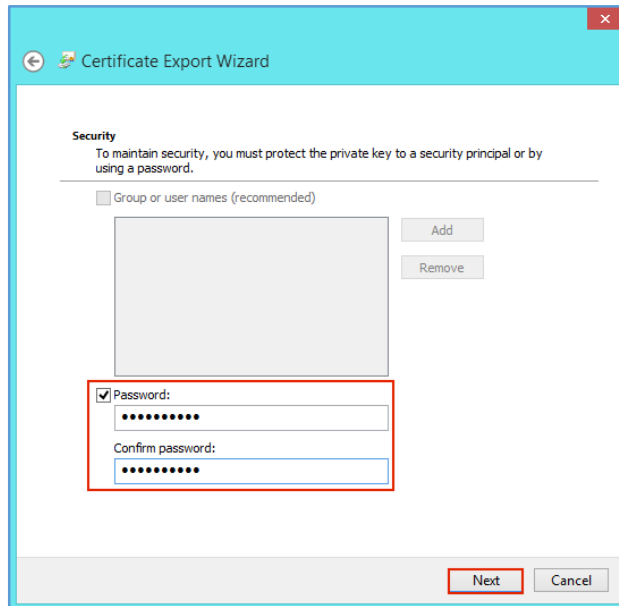
5. On the **Export Private Key** page, select **Yes, export private key** and then, click **Next**.



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**.

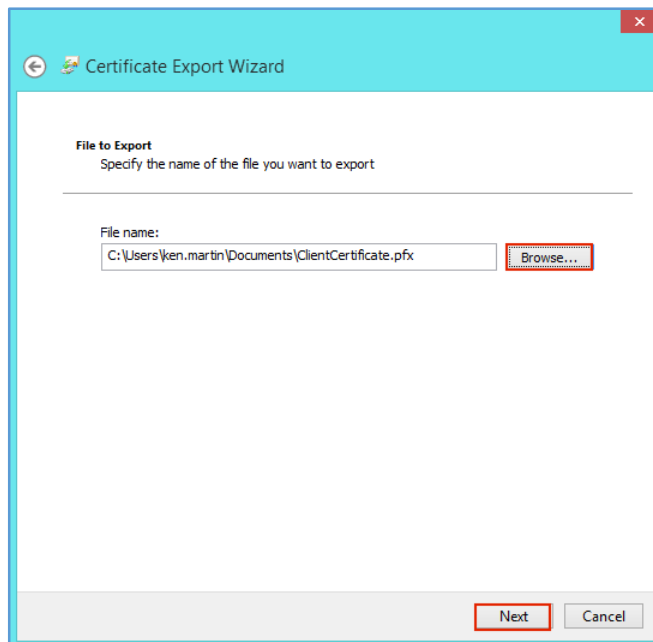


7. On the **Security** page, do the following: check **Password**.
  - i. Check **Password**.
  - ii. In the **Password** and **Confirm password** boxes, type your password.
  - iii. Click **Next**.

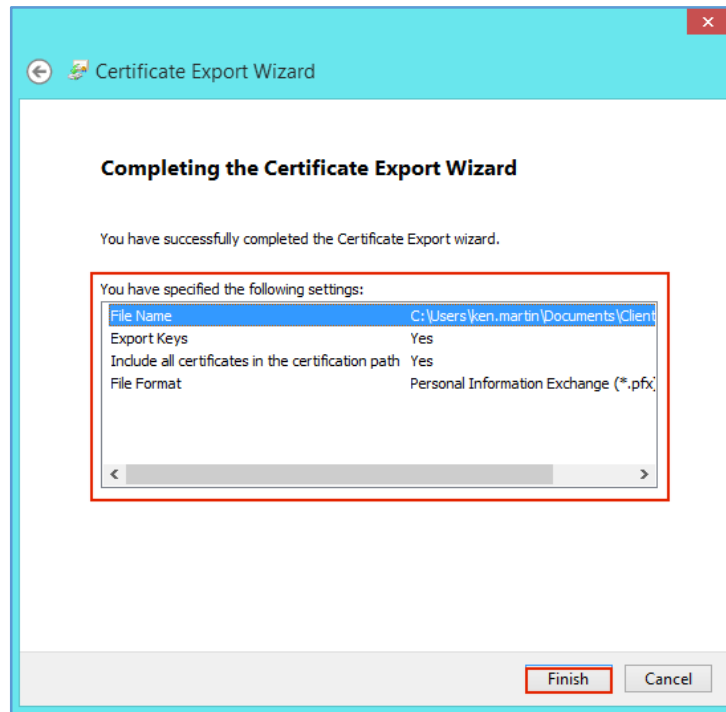


8. On the **File to Export** page, click **Browse**, locate where you want to save the Personal ID Certificate (w/private key) .pfx file, provide a file name (e.g., *myPersonalCert*), click **Save**, and then, click **Next**.

**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**.

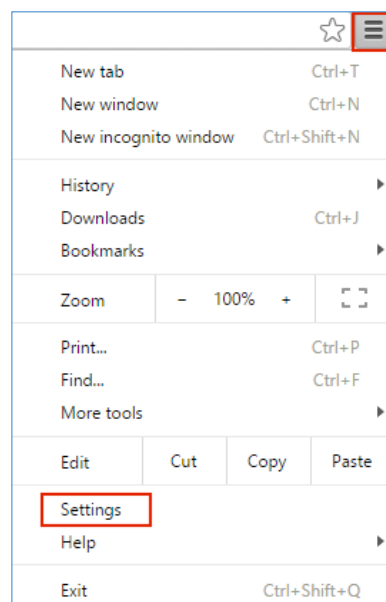


10. When you receive *"The export was successful"* message, click OK.

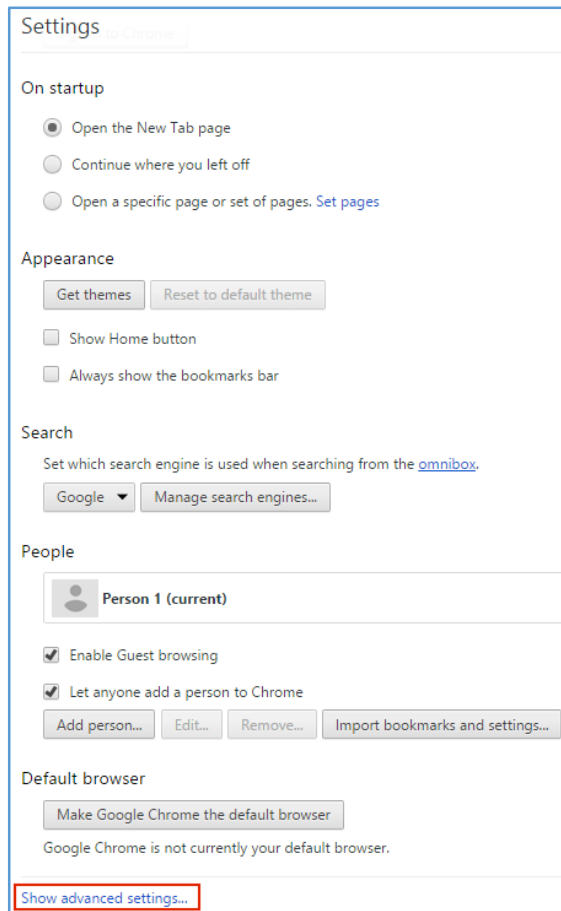
You have now exported your Personal ID Certificate w/private key as a .pfx file.

### 3.1.2 Google Chrome: How to Export Your Personal ID Certificate

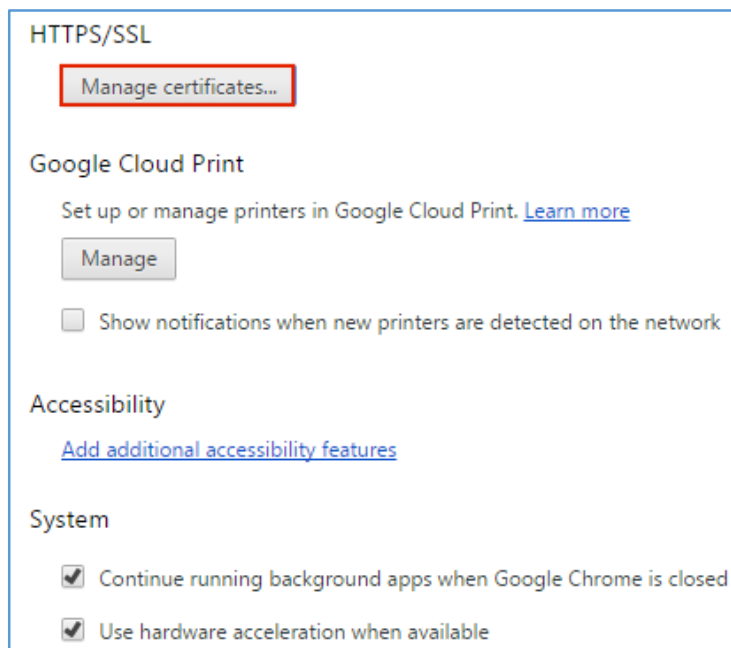
1. In Chrome, go to **Settings**.



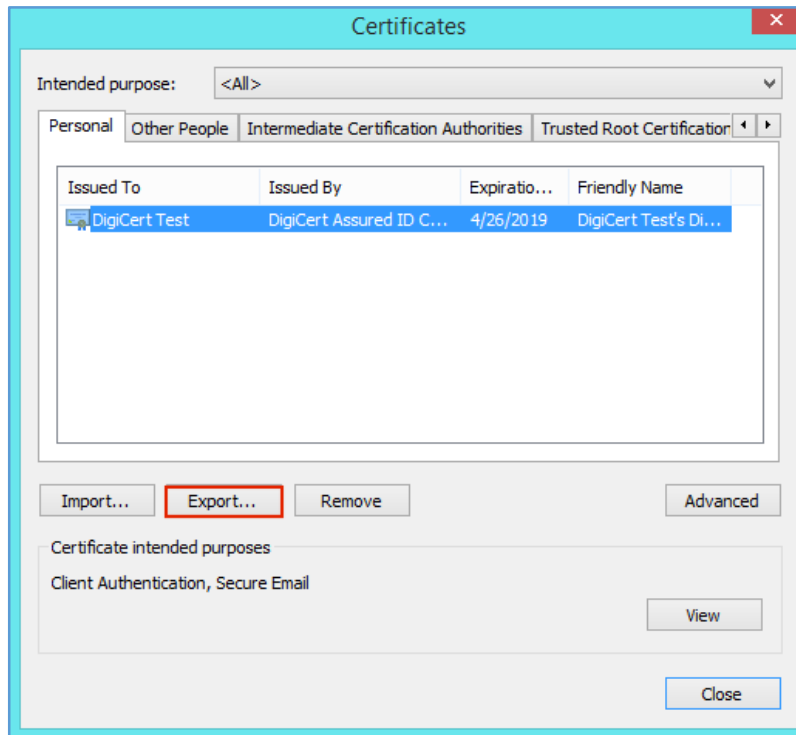
2. On the **Settings** page, below **Default browser**, click **Show advanced settings**.



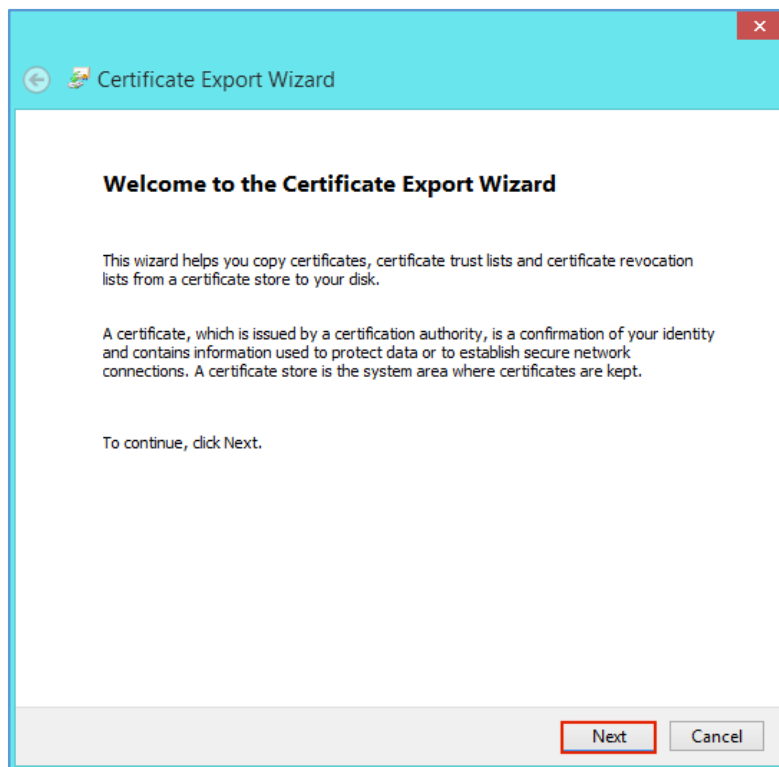
3. Under **HTTPS/SSL**, click **Manage certificates**.



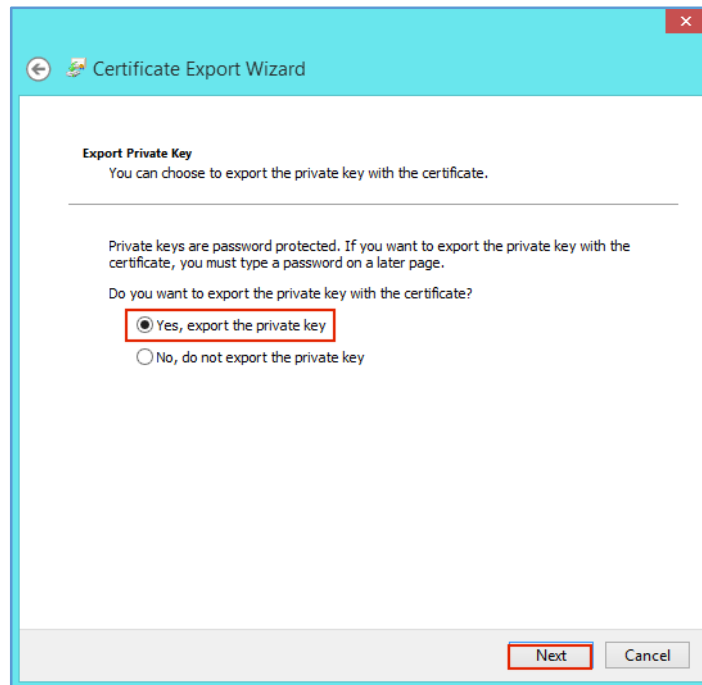
4. In the **Certificates** window, on the **Personal** tab, select your Personal ID Certificate and click **Export**.



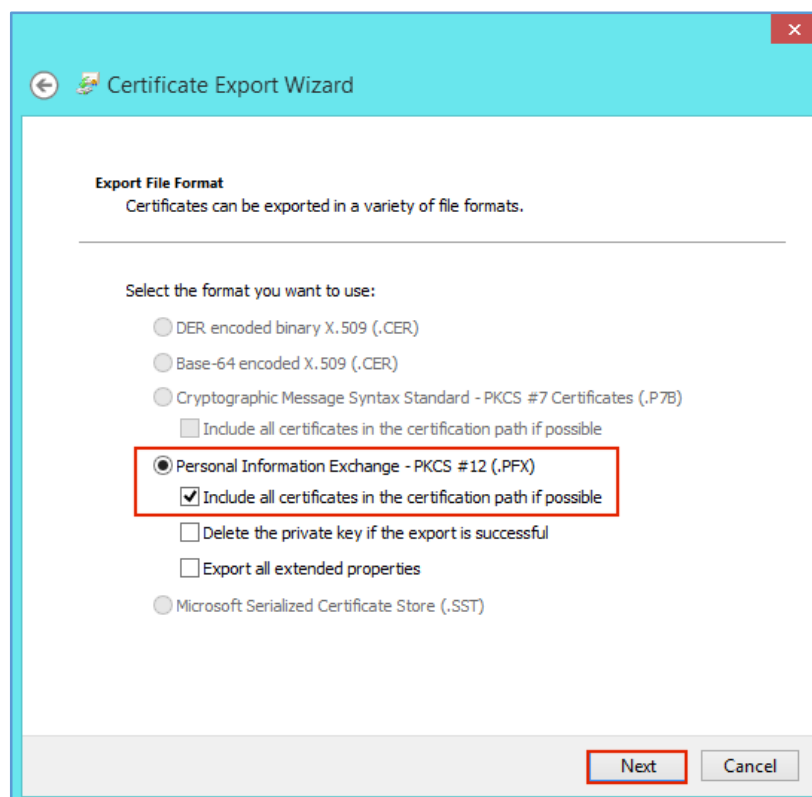
5. In the **Certificate Export Wizard**, on the **Welcome** page, click **Next**.



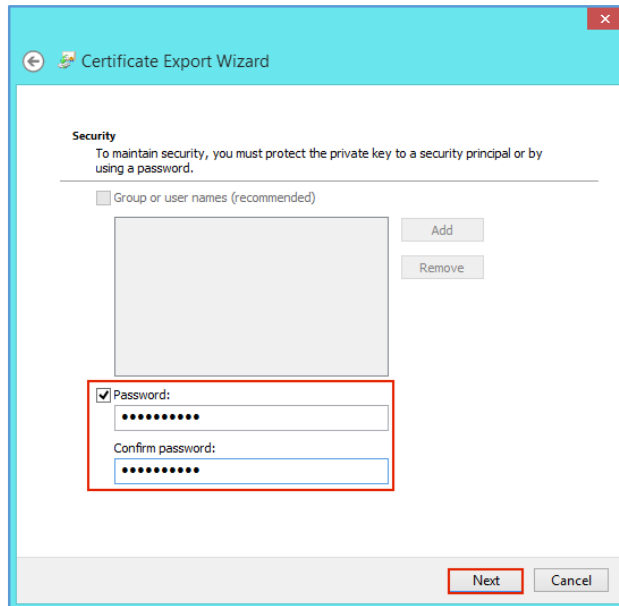
6. On the **Export Private Key** page, select **Yes, export private key** and then, click **Next**.



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**.

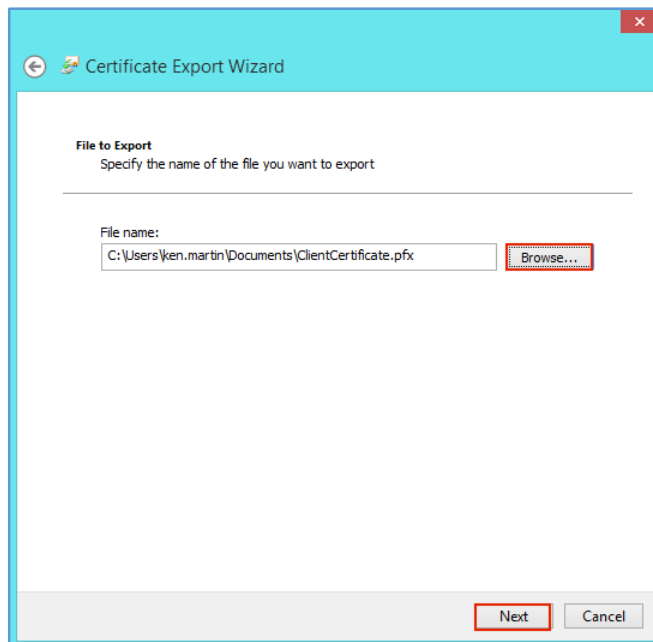


8. On the **Security** page, do the following: check **Password**.
  - i. Check **Password**.
  - ii. In the **Password** and **Confirm password** boxes, type your password.
  - iii. Click **Next**.

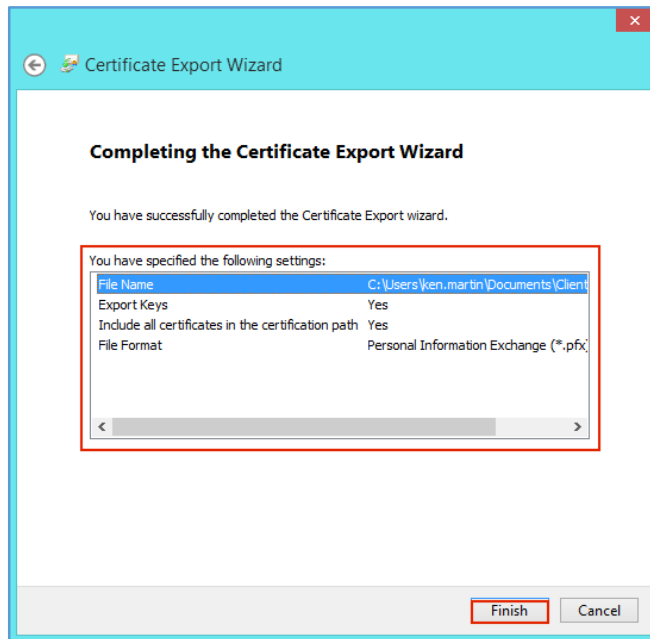


9. On the **File to Export** page, click **Browse**, locate where you want to save the Personal ID Certificate (w/private key) .pfx file, provide a file name (e.g., *myPersonalCert*), click **Save**, and then, click **Next**.

**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**.

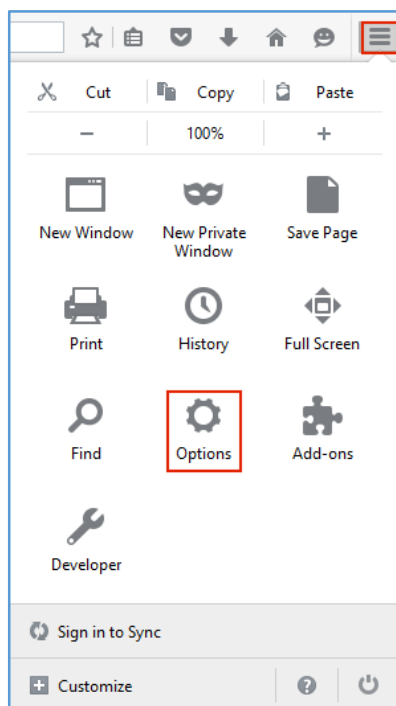


11. When you receive *"The export was successful"* message, click **OK**.

You have now exported your Personal ID Certificate w/private key as a .pfx file.

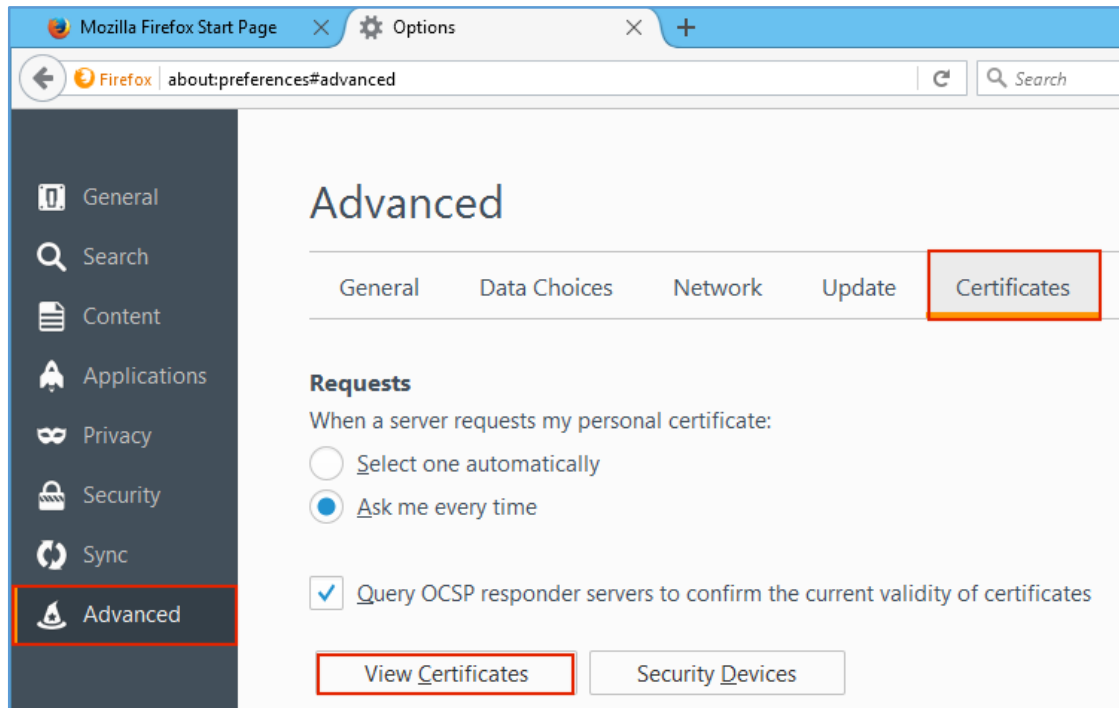
### 3.1.3 Firefox: How to Export Your Personal ID Certificate

1. In Firefox, go to **Options**.

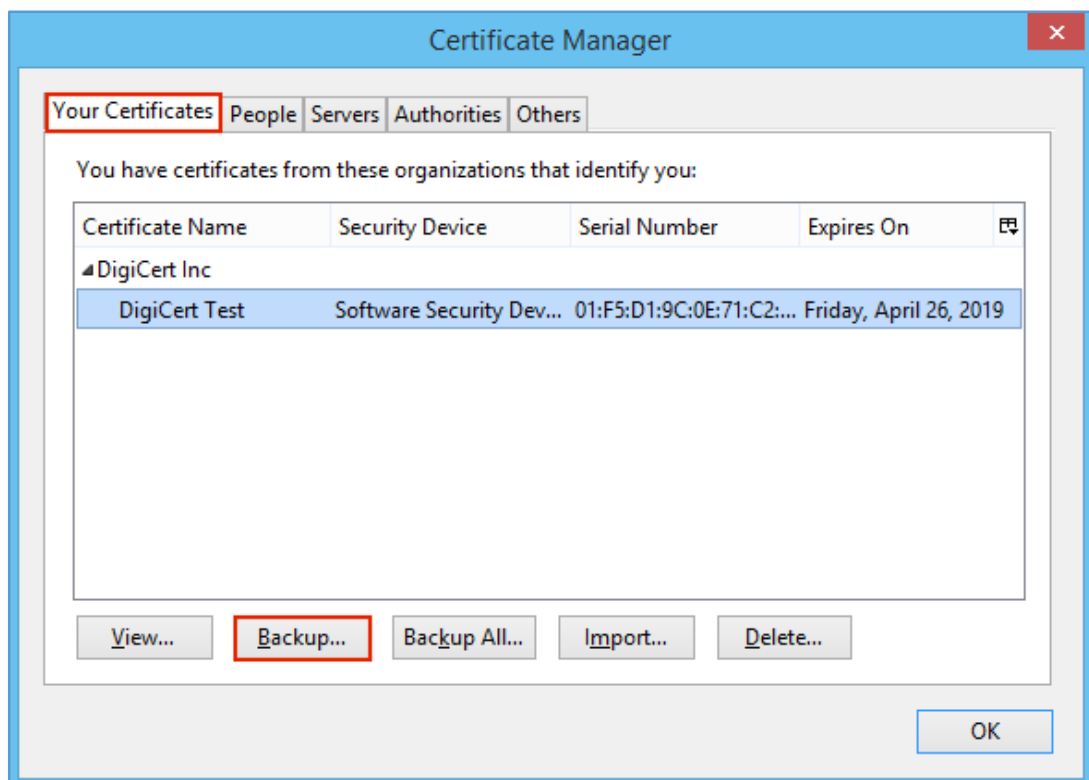




2. On the **Options** tab, in the sidebar menu, click **Advanced**, next, click the **Certificates** tab, and then, click **View Certificates**.

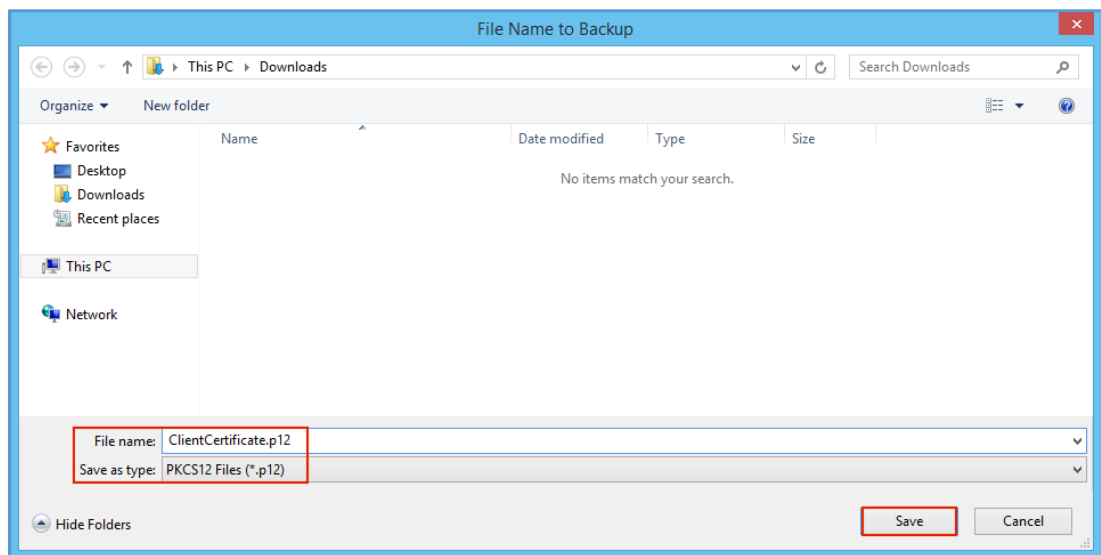


3. In the **Certificate Manager** window, on the **Your Certificates** tab, select your Personal ID Certificate and click **Backup**.

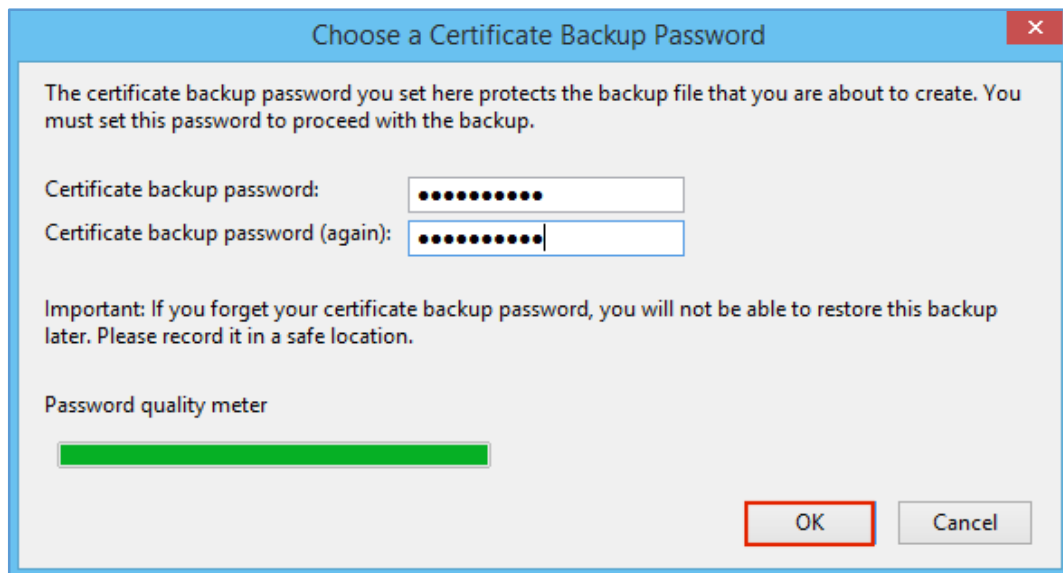


4. In the **File Name to Backup** window, go to where you want to save the Personal ID Certificate (w/private key) .p12 file, provide a file name (e.g., *myPersonalCertificate*), and then click **Save**.

**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**.



6. When you receive the *"Successfully backed up your security certificate(s) and private key(s)"* message, click **OK**.

You have now exported your Personal ID Certificate w/private key as a .p12 file.

## 3.2 (Windows) Importing 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.

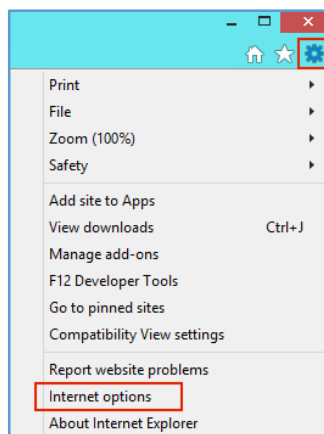
[Internet Explorer: How to Import Your Personal ID Certificate](#)

[Google Chrome: How to Import Your Personal ID Certificate](#)

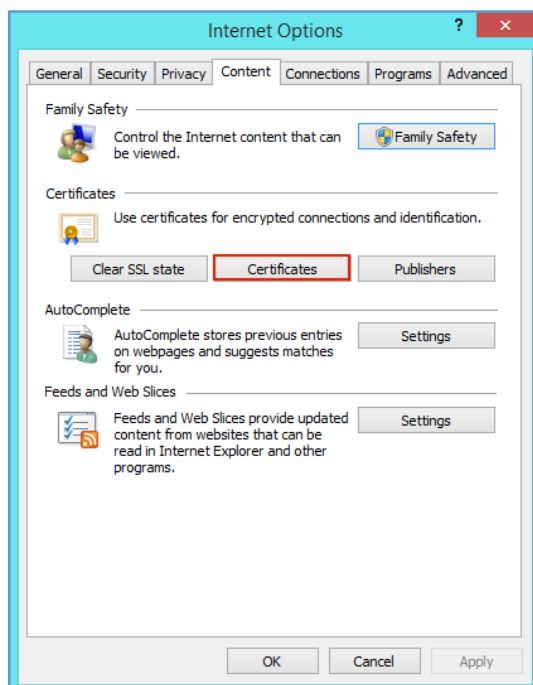
[Mozilla Firefox: How to Import Your Personal ID Certificate](#)

### 3.2.1 Internet Explorer: How to Import Your Personal ID Certificate

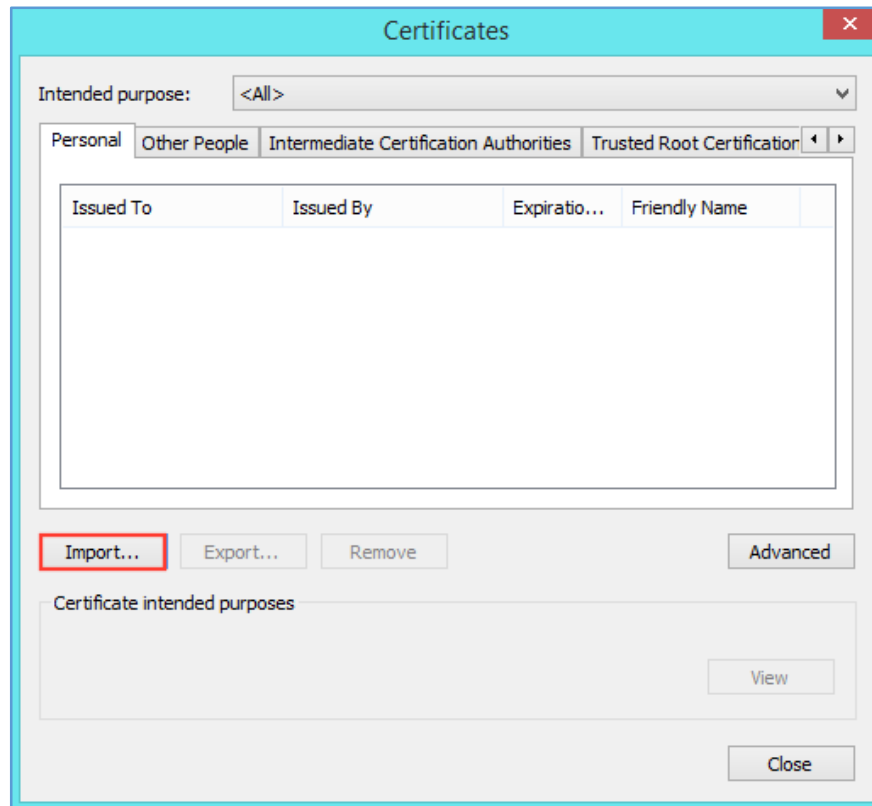
1. In Internet Explorer, go to **Internet Options**.



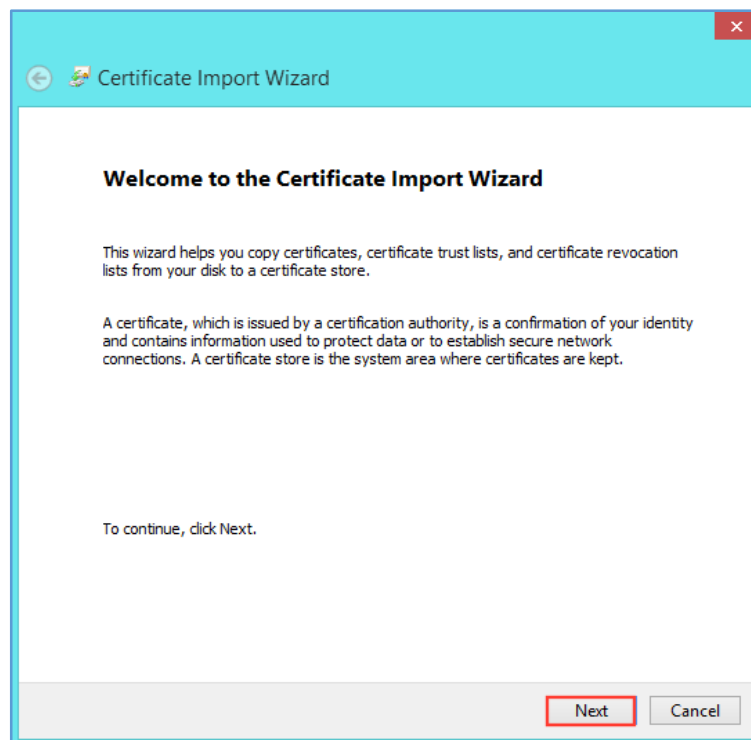
2. In the **Internet Options** window, on the **Content** tab, click **Certificates**.



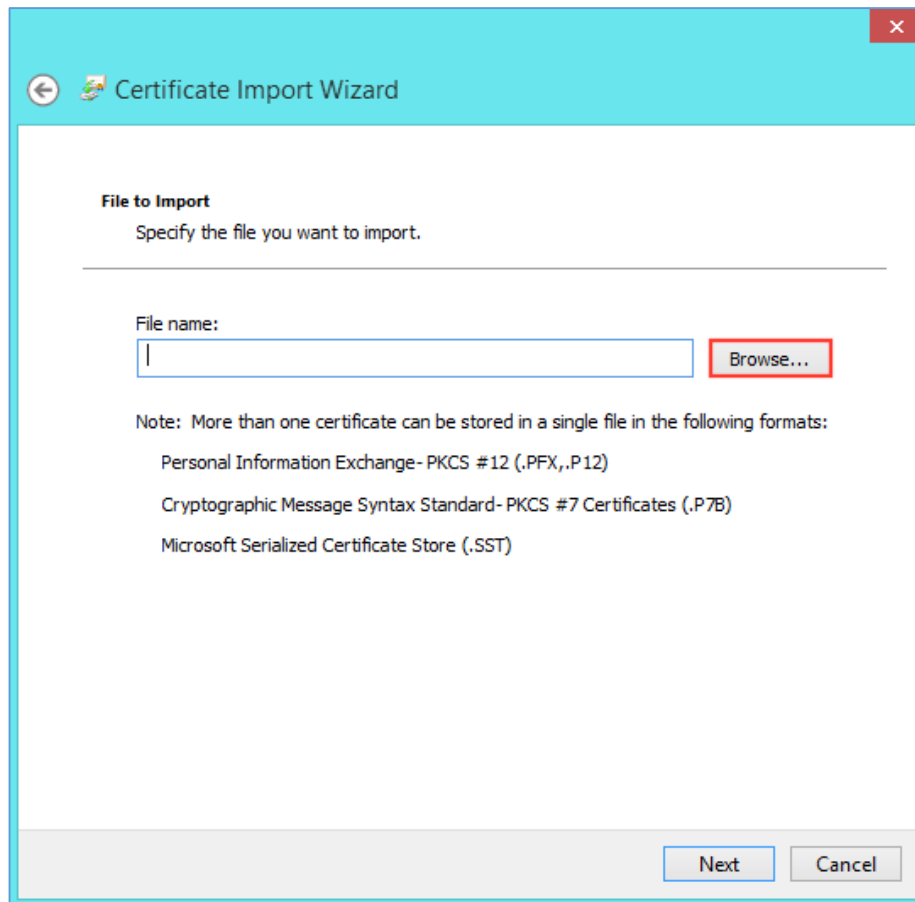
3. In the **Certificates** window, on the **Personal** tab, click **Import**.



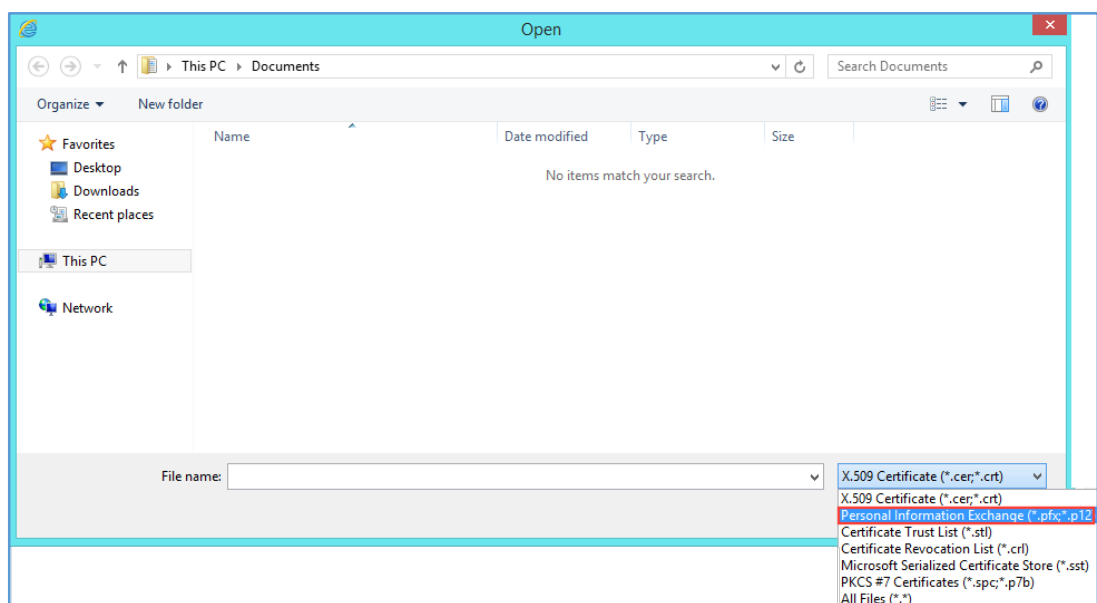
4. In the **Certificate Import Wizard**, on the **Welcome** page, click **Next**.



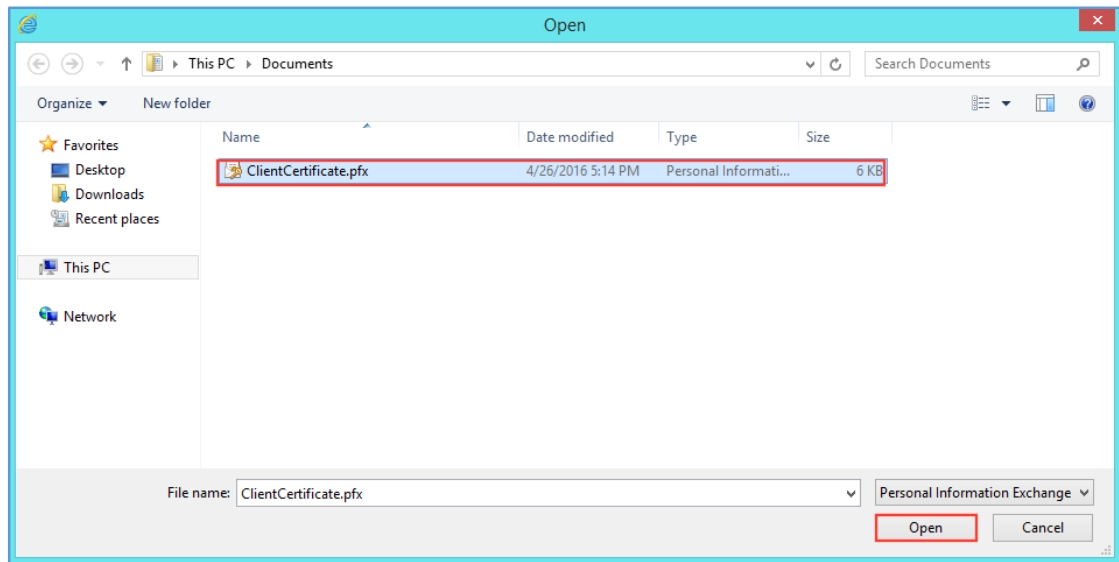
5. On the **File to Import** page, click **Browse**.



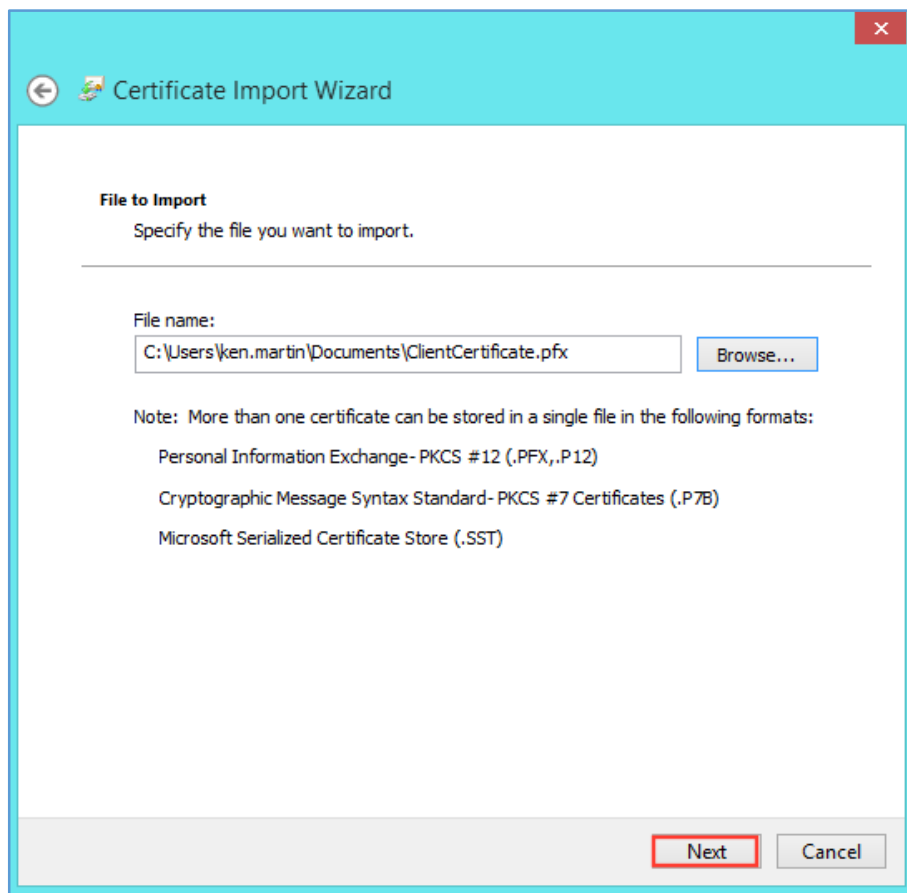
6. In the File Explorer **Open** window, in the file type drop-down list, select **Personal Information Exchange (\*.pfx;\*.p12)**.



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

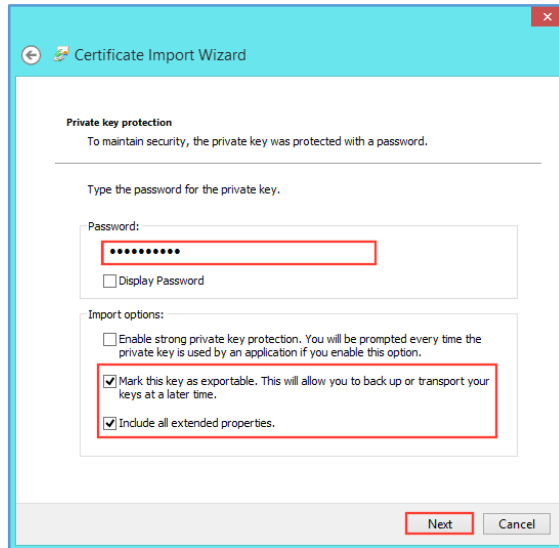


8. On the **File to Import** page, click **Next**.



9. On the **Private key protection** page, check **Mark this key as exportable** and **Include all extended properties**.

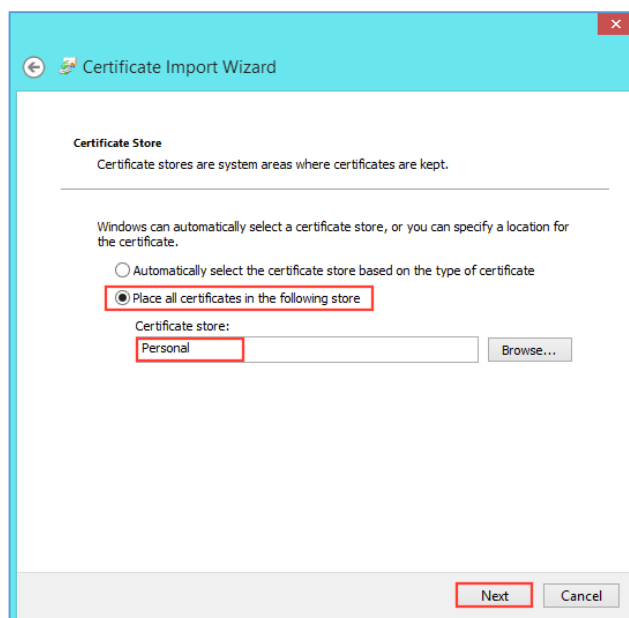
The **Mark this key as exportable** option enables you to export your Personal ID Certificate w/private key should you need to in the future.



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.



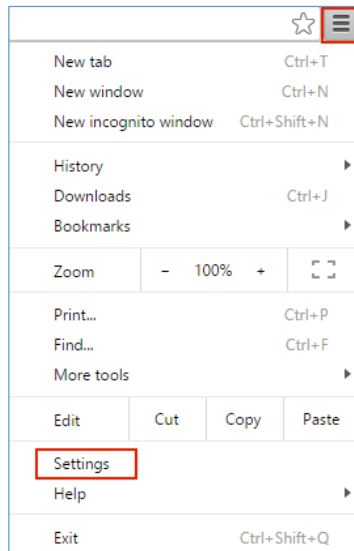
12. On the **Completing the Certificate Import Wizard** page, review the settings and then, click **Finish**.

13. When you receive *"The import was successful"* message, click **OK**.

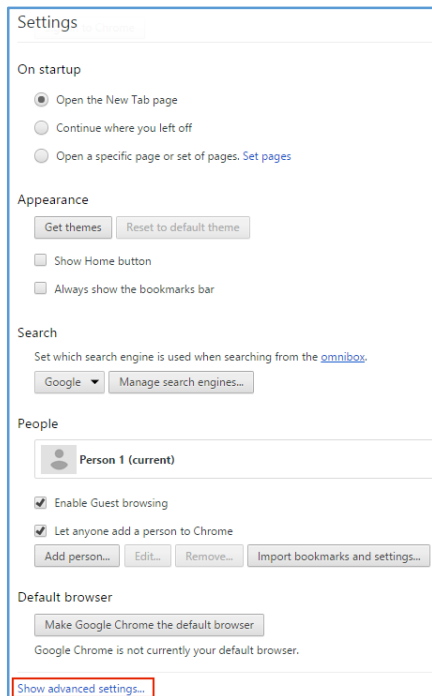
You have now imported your Personal ID Certificate w/private key in to the Windows Certificate store, and you can use Internet Explorer and Chrome to log in to your account(s).

### 3.2.2 Google Chrome: How to Import Your Personal ID Certificate

1. In Chrome, go to **Settings**.

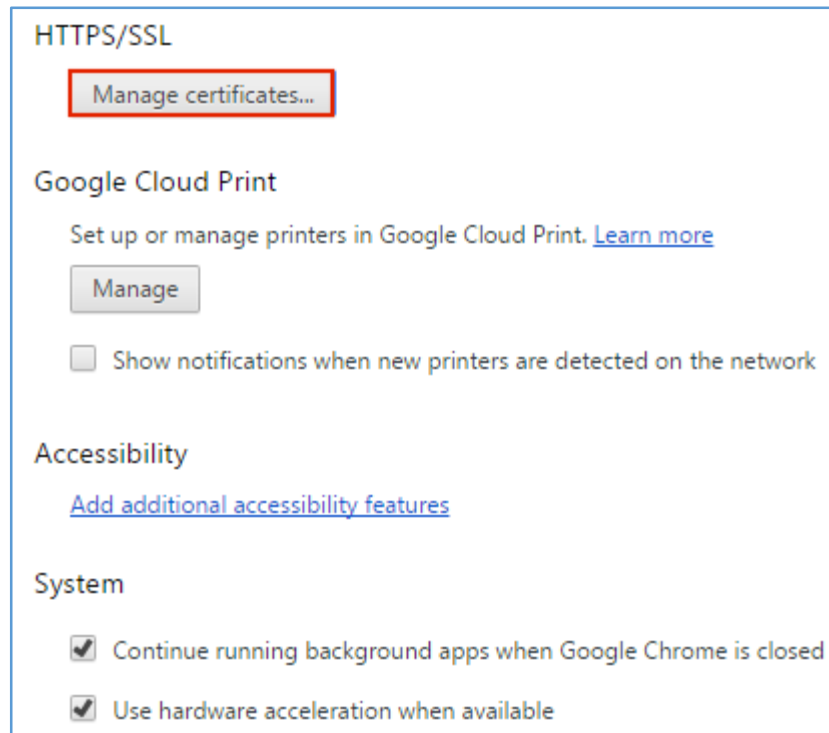


2. On the **Settings** page, below **Default browser**, click **Show advanced settings**.

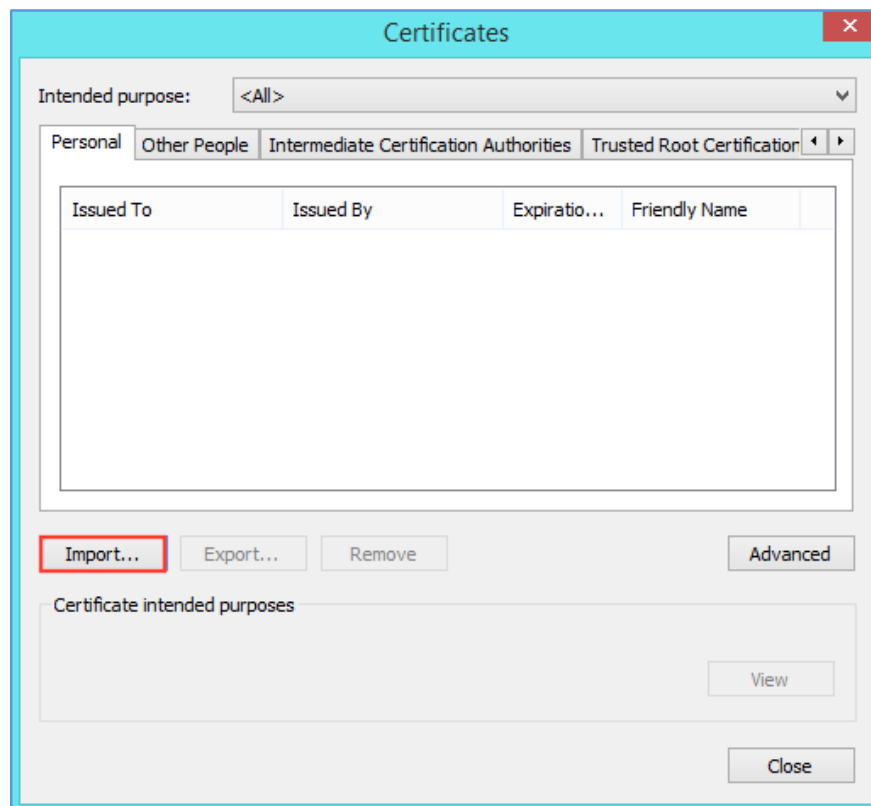




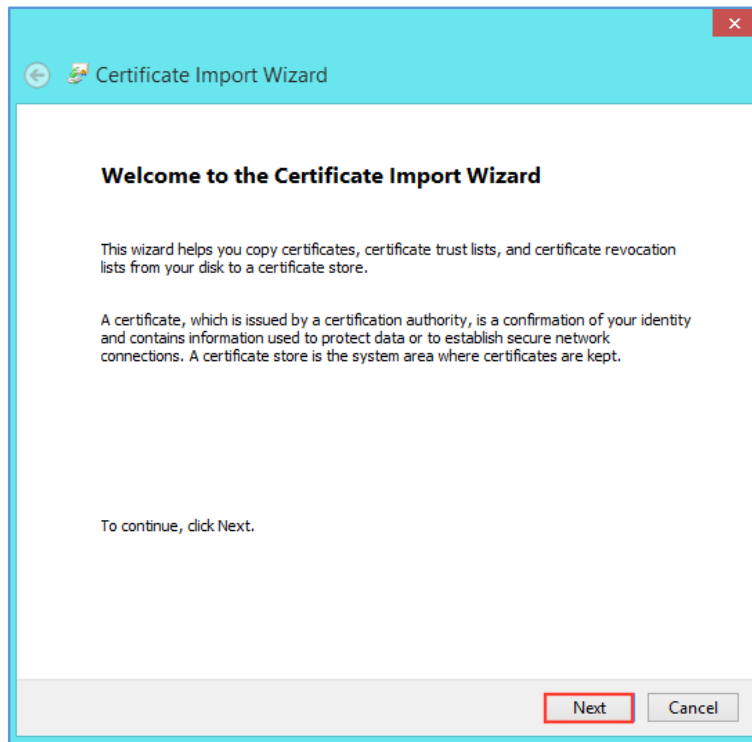
3. Under HTTPS/SSL, click **Manage certificates**.



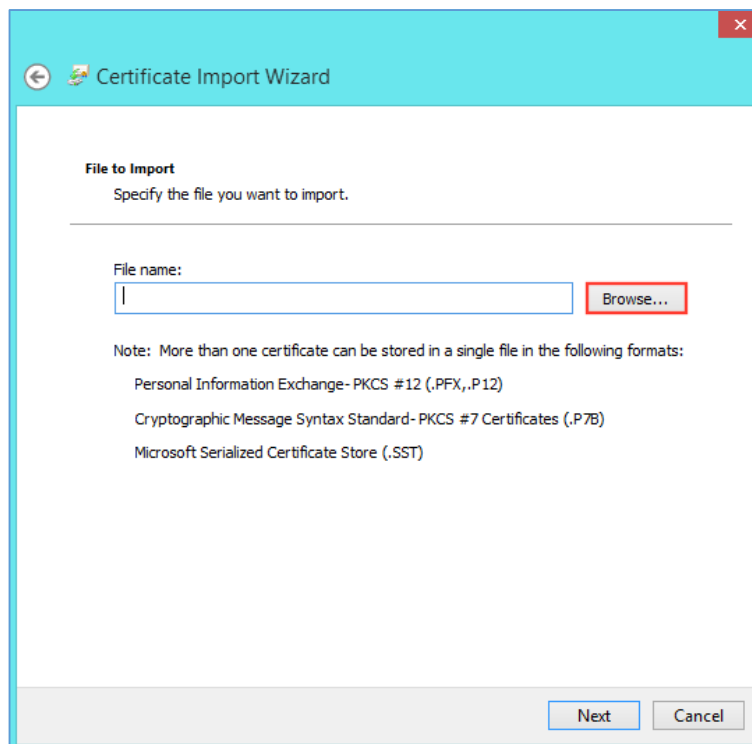
4. In the **Certificates** window, on the **Personal** tab, click **Import**.



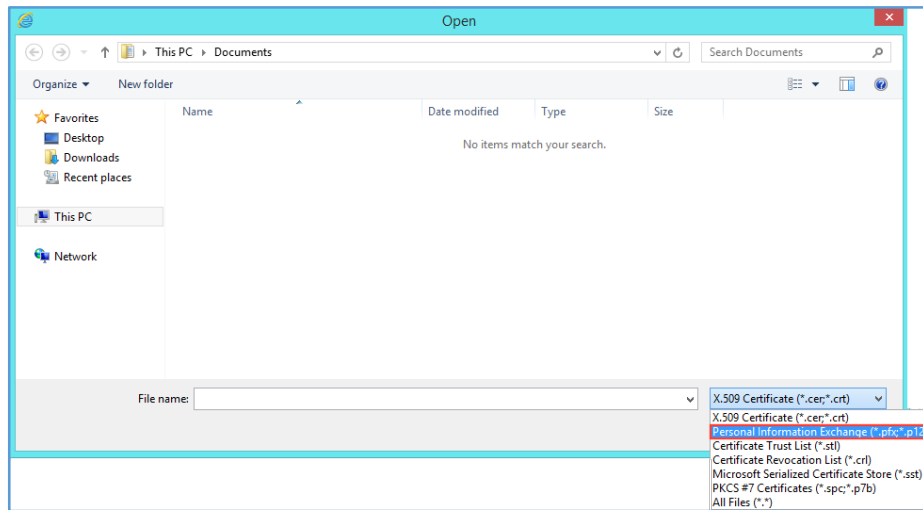
5. In the **Certificate Import Wizard**, on the **Welcome** page, click **Next**.



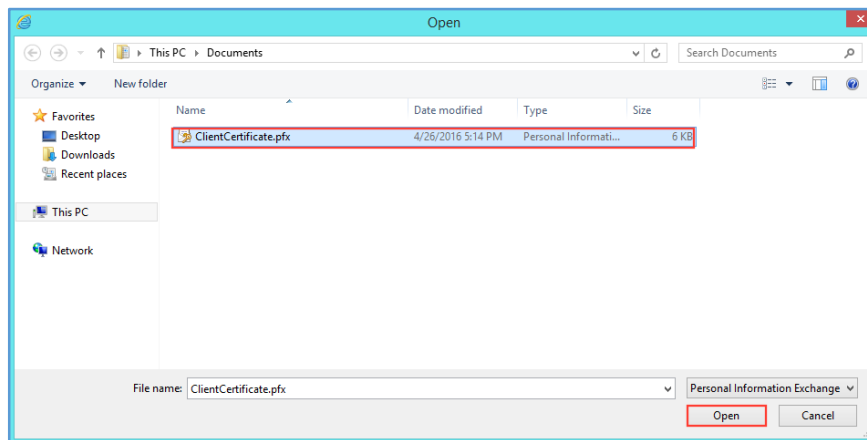
6. On the **File to Import** page, click **Browse**.



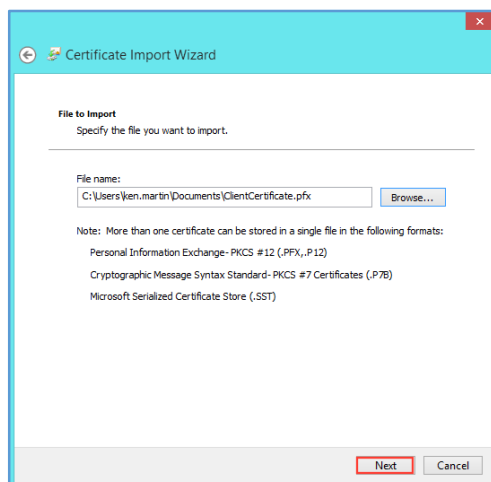
7. In the File Explorer **Open** window, in the file type drop-down list, select **Personal Information Exchange (\*.pfx;\*.p12)**.



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

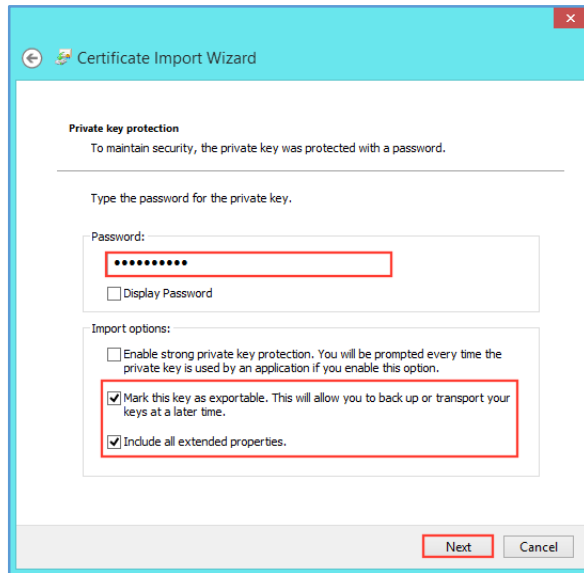


9. On the **File to Import** page, click **Next**.



10. On the **Private key protection** page, check **Mark this key as exportable** and **Include all extended properties**.

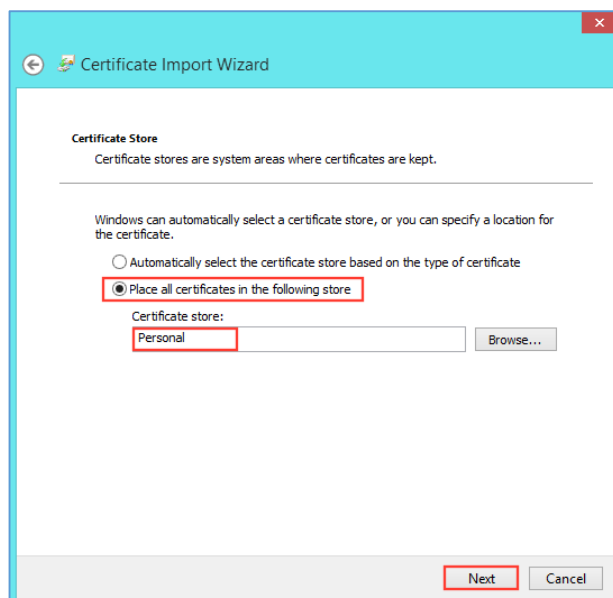
The **Mark this key as exportable** option enables you to export your Personal ID Certificate w/private key should you need to in the future.



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.

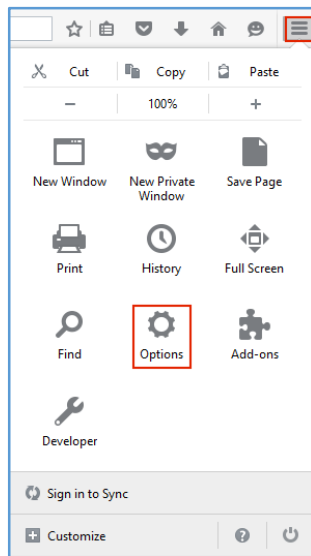


13. On the **Completing the Certificate Import Wizard** page, review the settings and then, click **Finish**.
14. When you receive *"The import was successful"* message, click **OK**.

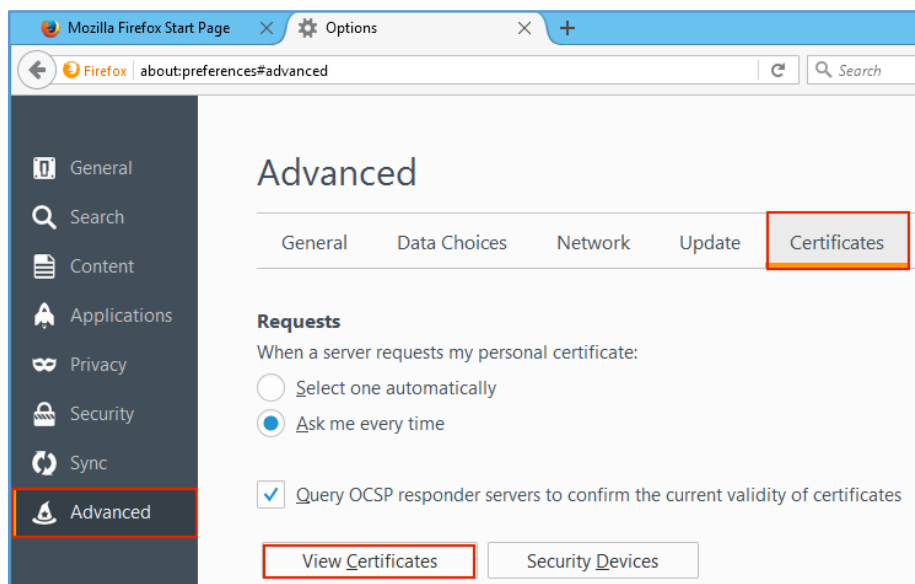
You have now imported your Personal ID Certificate w/private key in to the Windows Certificate store, and you can Chrome and use Internet Explorer to log in to your account(s).

### 3.2.3 Mozilla Firefox: How to Import Your Personal ID Certificate

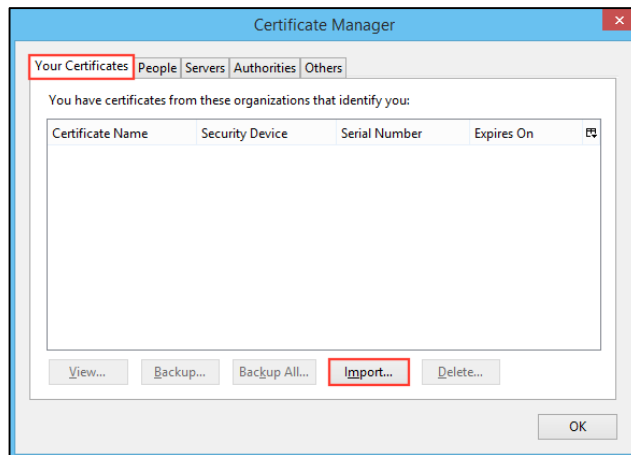
1. In Firefox, go to **Options**.



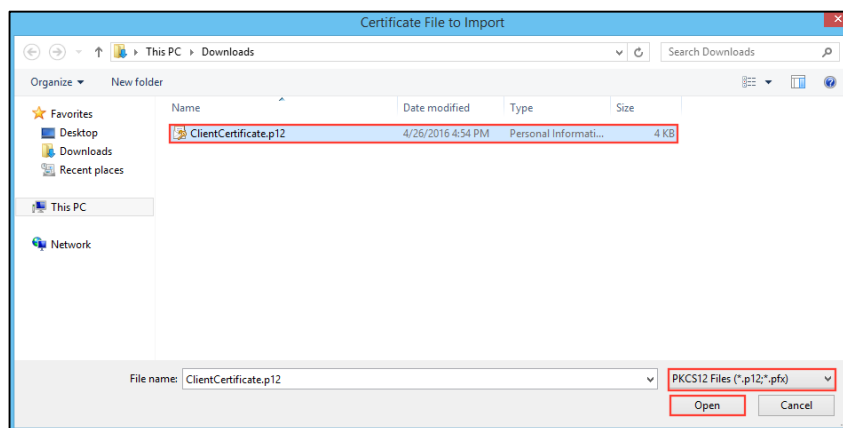
2. On the **Options** tab, in the sidebar menu, click **Advanced**, next, click the **Certificates** tab, and then, click **View Certificates**.



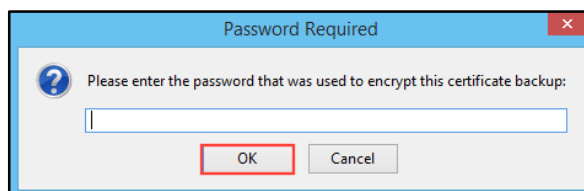
3. In the **Certificate Manager** window, on the **Your Certificates** tab, click **Import**.



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**.



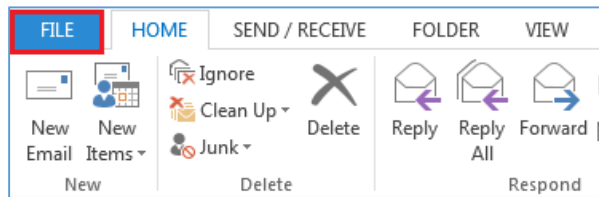
7. When you receive the *"Successfully restored your security certificate(s) and private key(s)"* message, click **OK**.

You have now imported your Personal ID Certificate w/private key in to the Firefox Certificate Store, and you can use Firefox to log into your account(s).

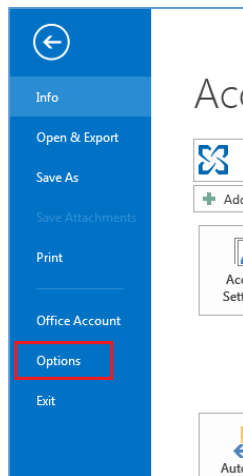
## 4 Configuring Outlook 2013 to Use Your Email Security Plus Personal ID Certificate

After you export your Personal ID Certificate, you can then configure Microsoft Outlook to use it to sign and encrypt emails.

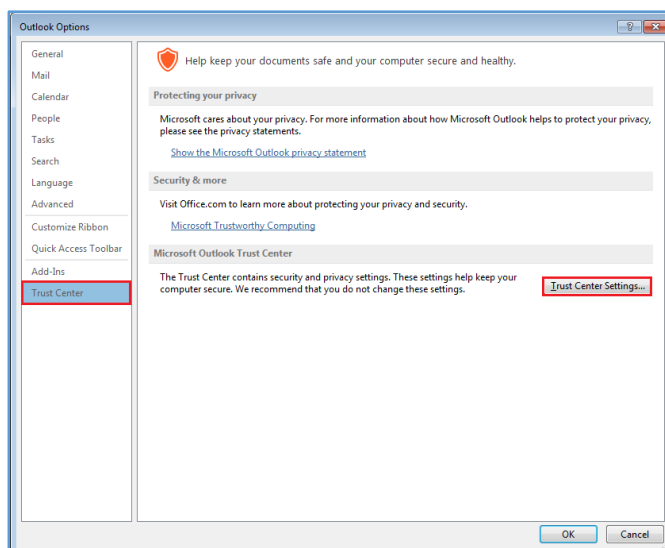
1. In Outlook 2013, click **File**.



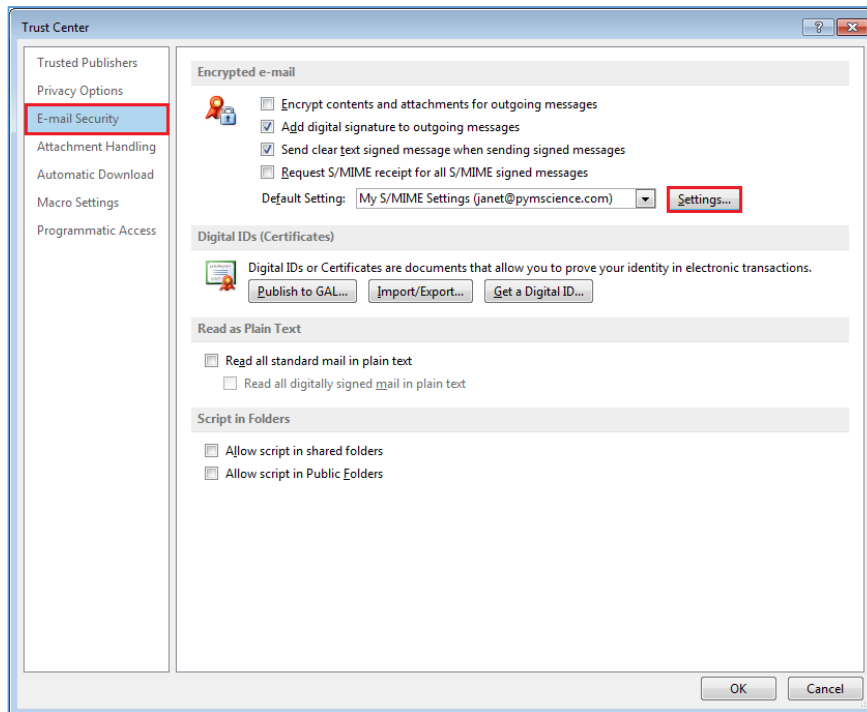
2. On the **File** page, in the sidebar menu, click **Options**.



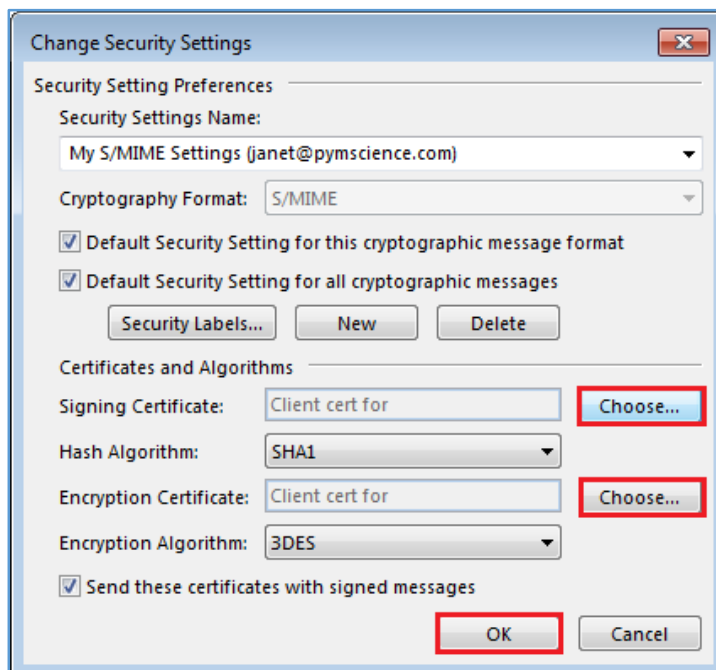
3. In the **Outlook Options** window, in the sidebar menu, click **Trust Center**.



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.

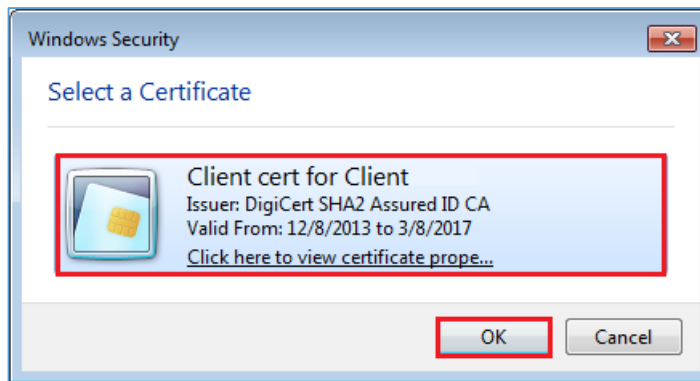


6. On the E-mail Security page, in the Encrypted e-mail section, click Settings.
7. In the Change Security Settings window, for Signing Certificate, click Choose.





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



9. Next, in the **Change Security Settings** window, for **Encryption Certificate**, click **Choose**.
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 configure Outlook 2013 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](mailto:SALES@DIGICERT.COM)

© 2017 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.

