Search guides

How to install an SSL on a Windows server when the CSR was generated elsewhere

April 21, 2020

SSL Installation instructions (https://www.ssls.com/knowledgebase/category/ssl-installation-instructions/)

This article explains the SSL installation process for Windows-based servers when the CSR (Certificate Signing Request) and the corresponding Private Key were not generated on the server where the SSL needs to be installed.

To successfully install the certificate, you need to have the Private Key file. If the Private Key file is missing, you can search for it, or generate a new CSR and Private Key and reissue your SSL certificate.

When activating a certificate on SSLs.com, you have two options for submitting the CSR:

1. Using the “Auto-activate” option, where the CSR is generated in-browser
2. Manually entering the CSR code you generated on your hosting server

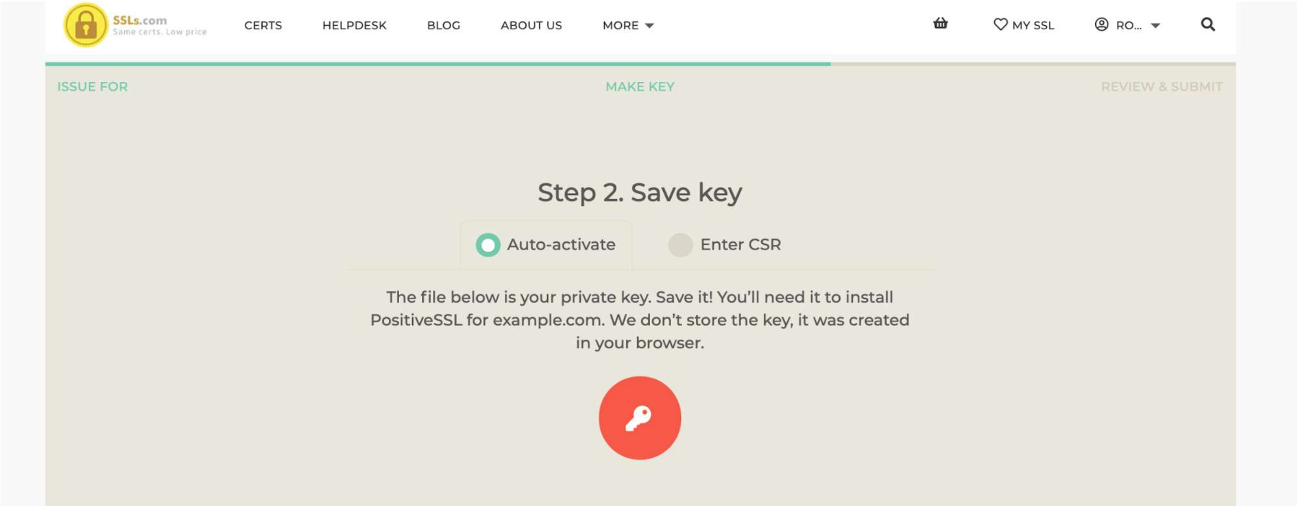
In this article, we’ll describe the most convenient way to install the certificate on a Windows-based server if you chose the first option or if the CSR was generated elsewhere, such as an online CSR generator.

Prepare the Private Key

Method 1: The Auto-activate feature

With the “Auto-activate” feature, the Private Key file is generated and saved during the activation process. Make sure to save it somewhere on your device that you’ll remember later.

1. Click on the “**key**” button in **Step 2** to **save the Private Key** during the SSL activation:



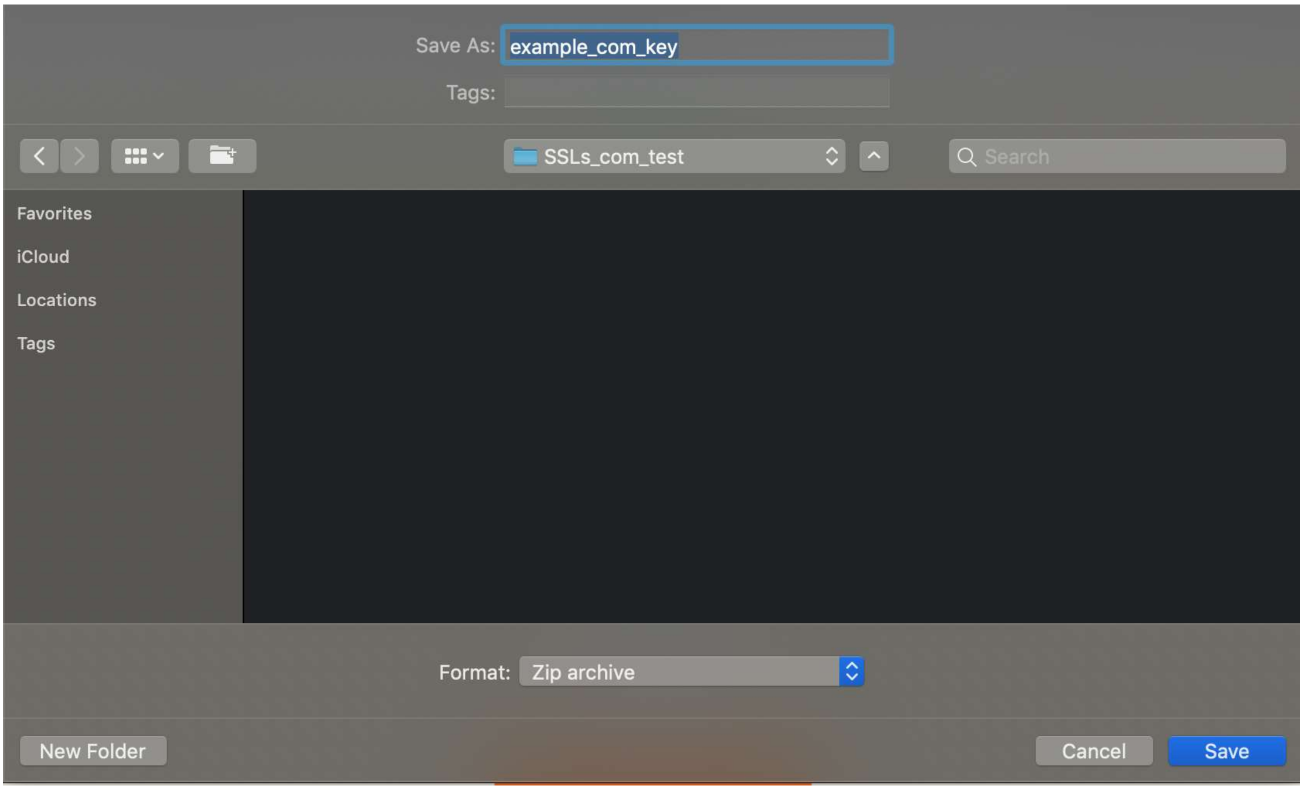
Step 2. Save key

● Auto-activate ○ Enter CSR

The file below is your private key. Save it! You’ll need it to install PositiveSSL for example.com. We don’t store the key, it was created in your browser.

2. Save the file to your device.

***Note**: It is typically saved in the “Downloads” folder. If you change the location/name of the key file, take note of the new details.*



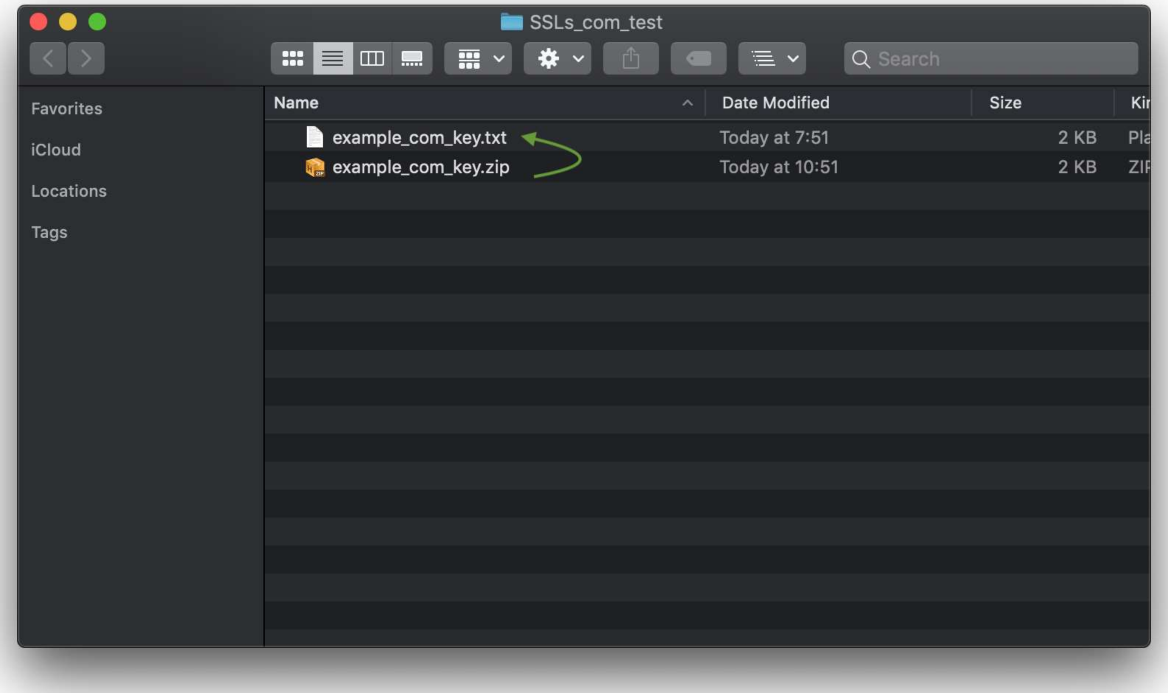
Save As: example_com_key

Tags:

Format: Zip archive

3. Extract the Private Key file from the downloaded archive file.

The archive file will contain a **.txt** file with the **Private Key** code:



Name	Date Modified	Size	Ki
example_com_key.txt	Today at 7:51	2 KB	Pla
example_com_key.zip	Today at 10:51	2 KB	ZIF

4. The archive file will contain a .txt file with the Private Key code:

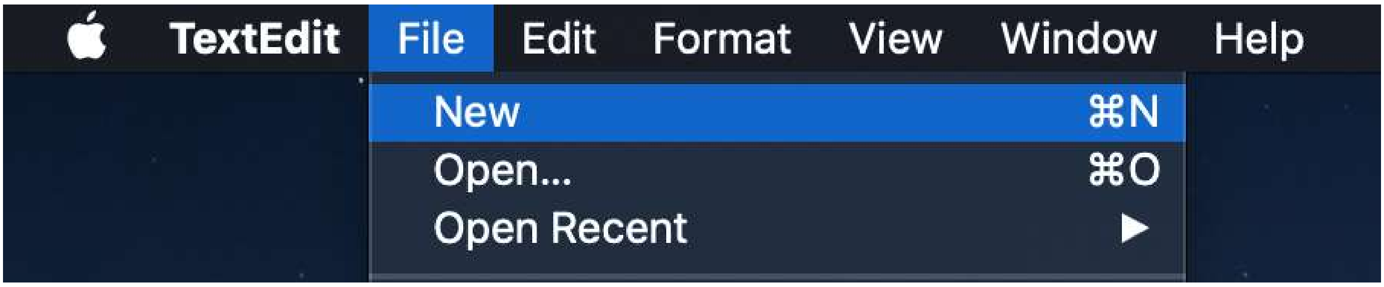
Method 2: The CSR code was generated elsewhere

If the CSR code was not generated using Auto-activate or on your Windows-based server, you will need to find the Private Key code and prepare the Private Key file manually. We have covered this process in this blog post.

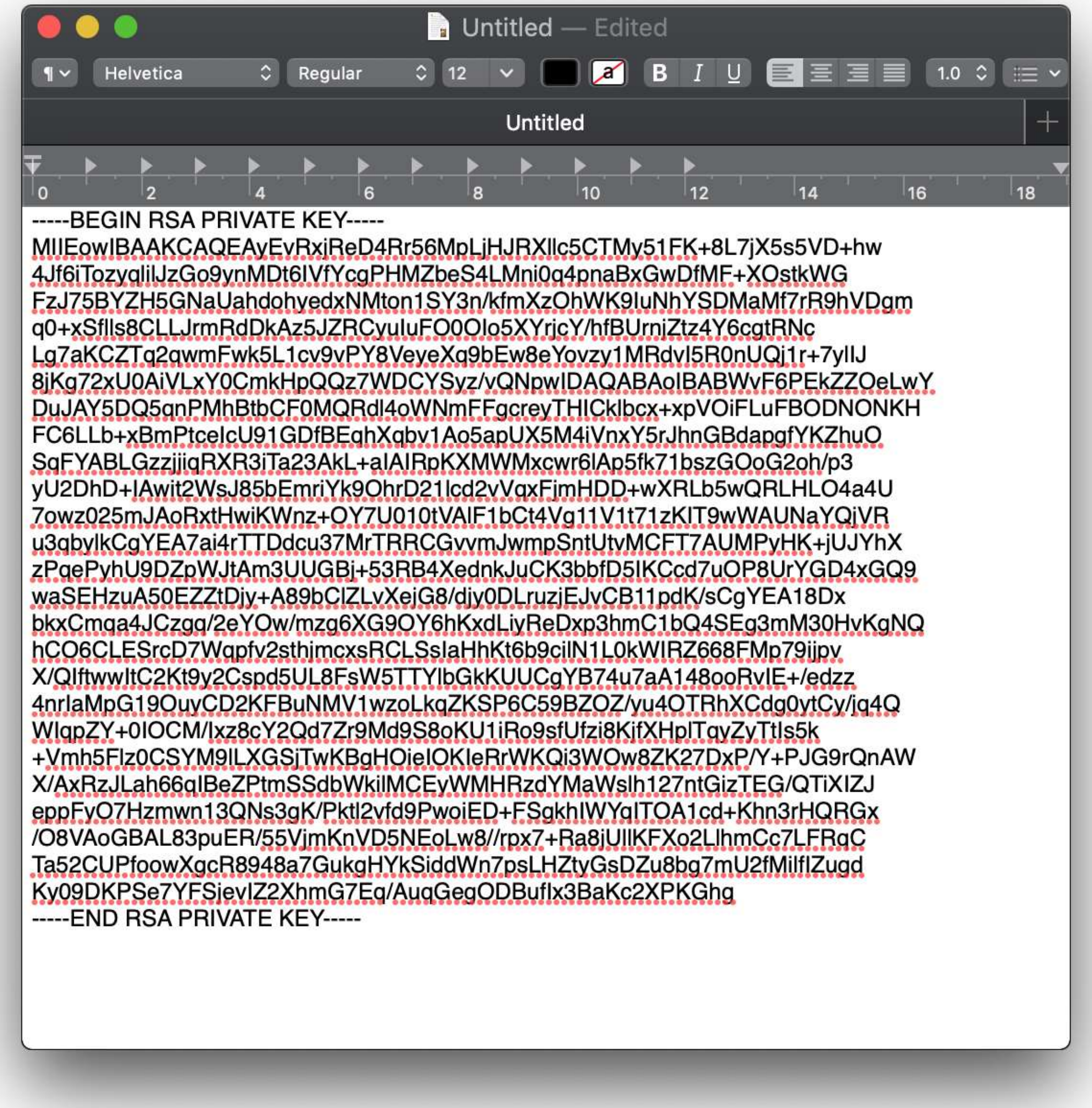
When the Private Key code is found, feel free to save it in a **.txt** file.

On Windows, you can do this by using the built-in “Notepad” application. Make sure to use “Notepad” and not “WordPad” or “MS Word” in order to save the key in plain text by default.

On MacOS, the Private Key can be saved using the “**TextEdit**” application. Open “**TextEdit**” and select **File** >> **New**:

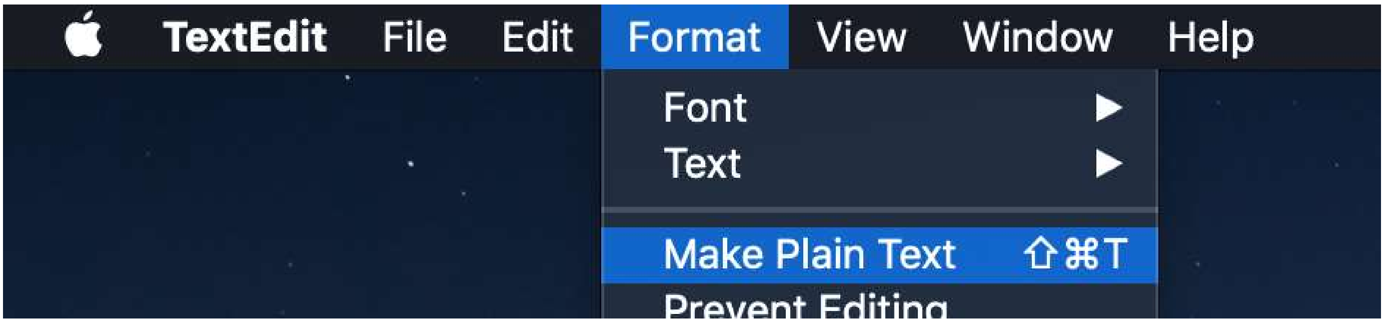


Then, paste the Private Key:

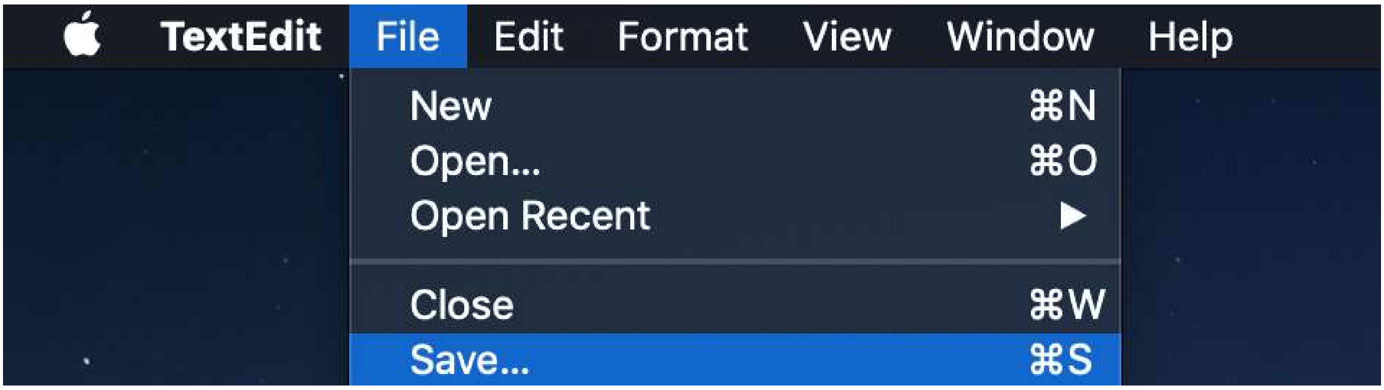


```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAyEvRxjReD4Rr56MpLjHJRXllc5CTMy51FK+8L7jX5s5VD+hw
4Jf6iTozyqliIJzGo9ynMDt6lVfYcgPHMZbeS4LMni0q4pnaBxGwDfMF+XOstkWG
FzJ75BYZH5GNaUahdohyedxNMton1SY3n/kfmXzOhWK9IuNhYSDMaMf7rR9hVDgm
q0+xSflls8CLLJrmRdDkAz5JZRCyuIuFO0OIo5XYrjcY/hfBUrnjZtz4Y6cgtRNc
Lg7aKCZTq2qwmFwk5L1cv9vPY8VeyeXq9bEw8eYovzy1MRdvI5R0nUQj1r+7ylIJ
8jKg72xU0AiVLxY0CmkHpQQz7WDCYSyz/vQNpwIDAQABAoIBABWvF6PEkZZOeLwY
DuJAY5DQ5qnPMhBtbCF0MQRdl4oWNmFFgcreyTHICklbcx+xpVOiFLuFBODNONKH
FC6LLb+xBmPtceIcU91GDfBEqhXqbv1Ao5apUX5M4iVnxY5rJhnGBdapgfYKZhuO
SqFYABLGzzjjiqRXR3iTa23AkL+aIAIRpKXMWMxcwr6lAp5fk71bszGOoG2oh/p3
yU2DhD+IAwit2WsJ85bEmriYk9OhrD21lcd2vVqxFjmHDD+wXRLb5wQRLHLO4a4U
7owz025mJAoRxtHwiKWnz+OY7U010tVAlF1bCt4Vg11V1t71zKIT9wWAUNaYQjVR
u3qbylkCgYEA7ai4rTTDdcu37MrTRRCGvvmJwmpSntUtvMCFT7AUMPyHK+jUJYhX
zPqePyhU9DZpWJtAm3UUGBj+53RB4XednkJuCK3bbfD5IKCcd7uOP8UrYGD4xGQ9
waSEHzuA50EZZtDjy+A89bClZLvXejG8/djy0DLruzjEJvCB11pdK/sCgYEA18Dx
bkxCmqa4JCzgq/2eYOw/mzg6XG9OY6hKxdLiyReDxp3hmC1bQ4SEg3mM30HvKgNQ
hCO6CLESrcD7Wqpfv2sthjmcxsRCLSslaHhKt6b9cilN1L0kWIRZ668FMp79ijpv
X/QIftwwItC2Kt9y2Cspd5UL8FsW5TTYlbGkKUUCgYB74u7aA148ooRvIE+/edzz
4nrlaMpG19OuyCD2KFBuNMV1wzoLkqZKSP6C59BZOZ/yu4OTRhXCdg0ytCy/jq4Q
WIqpZY+0IOCM/lxz8cY2Qd7Zr9Md9S8oKU1iRo9sfUfzi8KifXHplTqyZyTtIs5k
+Vmh5Flz0CSYM9lLXGSjTwKBgHOieIOKIeRrWKQi3WOw8ZK27DxP/Y+PJG9rQnAW
X/AxRzJLah66qIBeZPtmSSdbWkilMCEyWMHRzdYMaWslh127ntGizTEG/QTiXIZJ
eppFyO7Hzmwn13QNs3gK/Pktl2vfd9PwoiED+FSgkhIWYqITOA1cd+Khn3rHQRGx
/O8VAoGBAL83puER/55VjmKnVD5NEoLw8//rpx7+Ra8jUllKFXo2LlhmCc7LFRqC
Ta52CUPfoowXgcR8948a7GukgHYkSiddWn7psLHZtyGsDZu8bg7mU2fMilfIZugd
Ky09DKPSe7YFSjevIZ2XhmG7Eq/AuqGegODBuflx3BaKc2XPKGhg
-----END RSA PRIVATE KEY-----
```

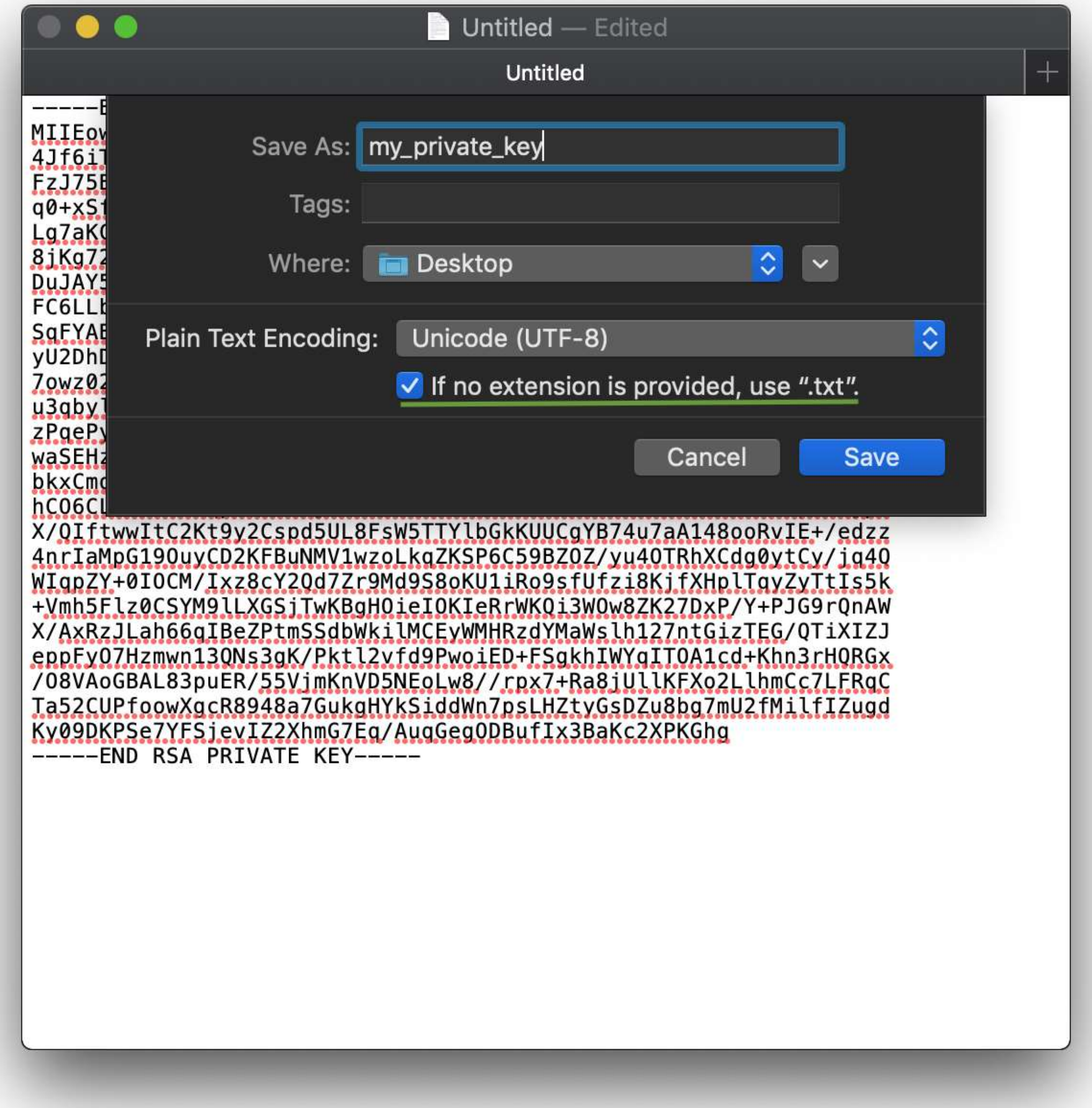
After that, select **Format** >> **Make Plain Text**:



Then, select **File** >> **Save**:



You can name your file whatever you like. We recommend avoiding spaces in the file name to prevent issues with the installation. Additionally, make sure that you have checked the "*If no extension is provided, use "**.txt**"*" checkbox. Finally, click the **Save** button.



Save As: my_private_key

Tags:

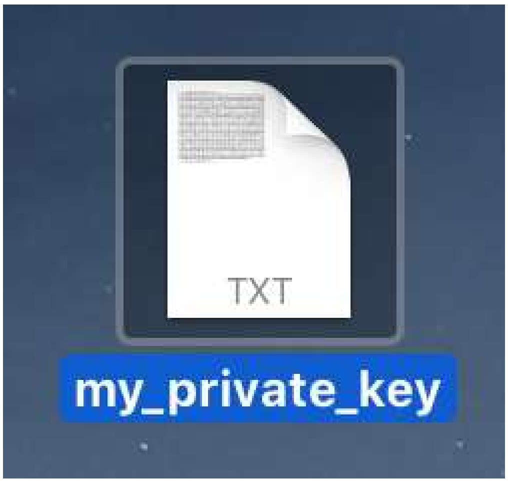
Where: Desktop

Plain Text Encoding: Unicode (UTF-8)

☑ If no extension is provided, use ".txt".

```
-----B
MIIEow
4Jf6iT
FzJ75E
q0+xSt
Lg7aKC
8jKg7z
DuJAY5
FC6LLb
SqFYAE
yU2DhD
7owz02
u3qbyl
zPqePy
waSEHz
bkxCmd
hC06CL
X/QIftwwItC2Kt9y2Cspd5UL8FsW5TTYlbGkKUUCgYB74u7aA148ooRvIE+/edzz
4nrIaMpG19OuyCD2KFBuNMV1wzoLkqZKSP6C59BZOZ/yu4OTRhXCdg0ytCy/jq4O
WIqpZY+0IOCM/Ixz8cY2Qd7Zr9Md9S8oKU1iRo9sfUfzi8KjfXHplTqyZyTtIs5k
+Vmh5Flz0CSYM9lLXGSjTwKBgHOieIOKIeRrWKQi3WOw8ZK27DxP/Y+PJG9rQnAW
X/AxRzJLah66qIBeZPtmSSdbWkilMCEyWMHRzdYMaWslh127ntGizTEG/QTiXIZJ
eppFyO7Hzmwn13QNs3gK/Pktl2vfd9PwoiED+FSgkhIWYqITOA1cd+Khn3rHQRGx
/O8VAoGBAL83puER/55VjmKnVD5NEoLw8//rpx7+Ra8jUllKFXo2LlhmCc7LFRqC
Ta52CUPfoowXgcR8948a7GukgHYkSiddWn7psLHZtyGsDZu8bg7mU2fMilfIZugd
Ky09DKPSe7YFSjevIZ2XhmG7Eq/AuqGegODBufIx3BaKc2XPKGhg
-----END RSA PRIVATE KEY-----
```

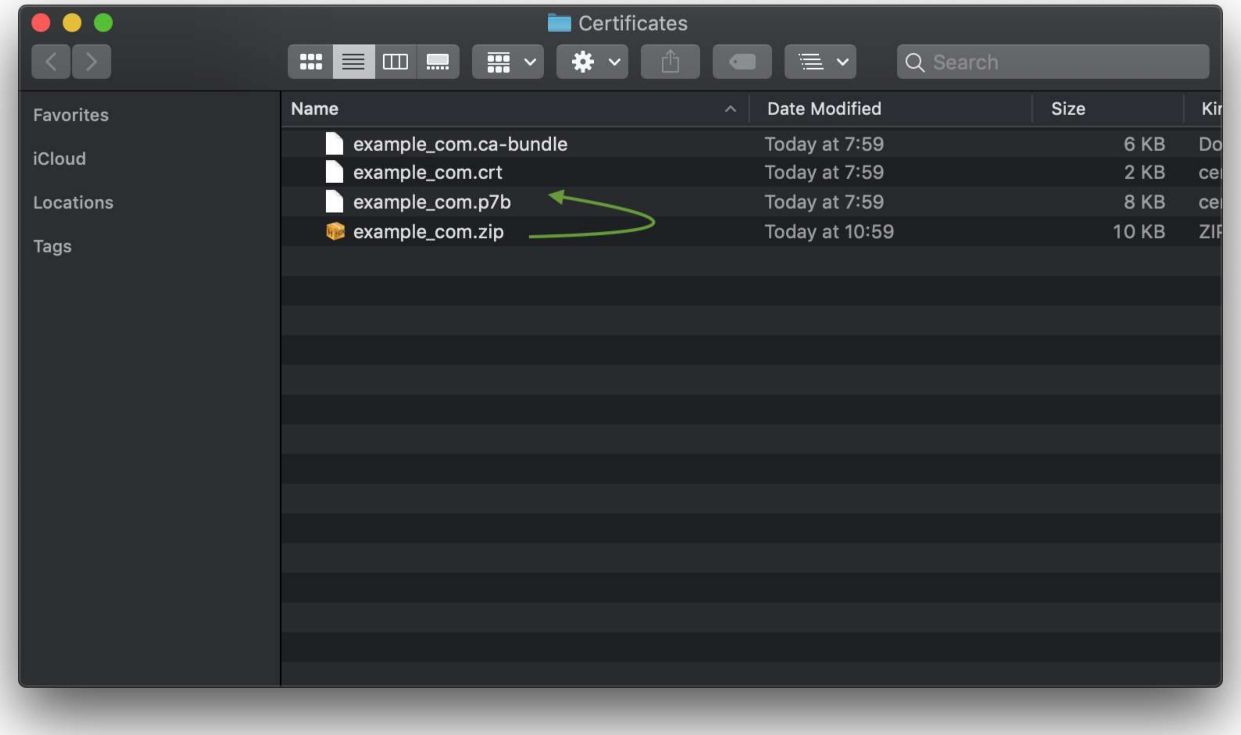
Done! The Private Key file is prepared.



Download the certificate files

Once the certificate is issued, download your SSL files using the **Download** button in the top-right corner of the certificate details page.

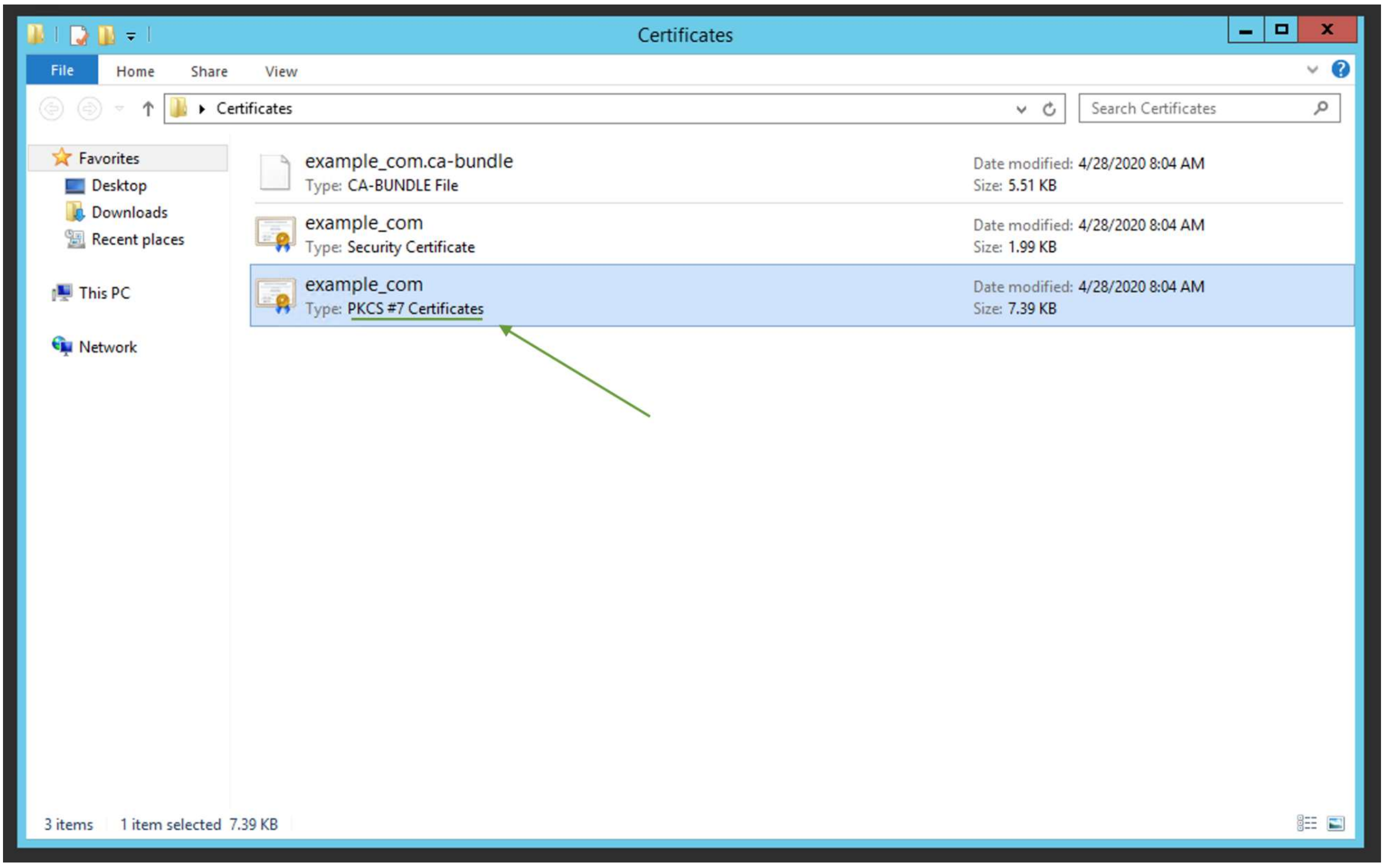
Extract the files from the downloaded archive. The archive should contain the certificate in 2 formats: PEM (.crt and .ca-bundle) and PKCS#7 (.p7b):



Name	Date Modified	Size	Kir
example_com.ca-bundle	Today at 7:59	6 KB	Do
example_com.crt	Today at 7:59	2 KB	ce
example_com.p7b	Today at 7:59	8 KB	ce
example_com.zip	Today at 10:59	10 KB	ZIF

We will use the PKCS#7 (.p7b) file in this guide because it includes both the certificate and the CA certificates bundled in one file.

If your system does not show the file extensions, you can check the certificate file type by looking at the Windows file type description.



example_com.ca-bundle
Type: CA-BUNDLE File
Date modified: 4/28/2020 8:04 AM
Size: 5.51 KB

example_com
Type: Security Certificate
Date modified: 4/28/2020 8:04 AM
Size: 1.99 KB

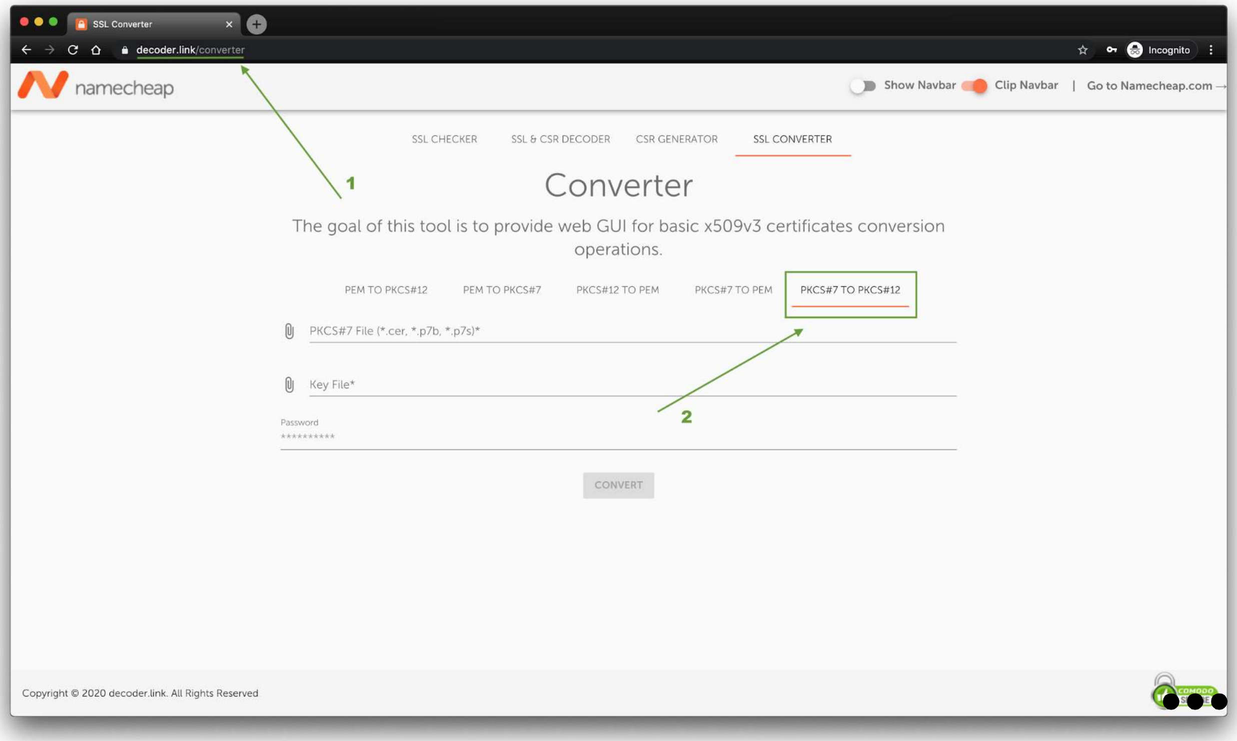
example_com
Type: PKCS #7 Certificates
Date modified: 4/28/2020 8:04 AM
Size: 7.39 KB

3 items 1 item selected 7.39 KB

Create the PFX file

Since Windows does not support Private Key import, you'll need to combine the certificate with the Private Key into a single file: **PKCS#12-type certificate** (also called **PFX**) with a **.pfx** extension.

1. To do that, open the online converter and select the **PKCS#7 to PKCS#12** tab:



Converter

The goal of this tool is to provide web GUI for basic x509v3 certificates conversion operations.

PKCS#7 File (*.cer, *.p7b, *.p7s)*

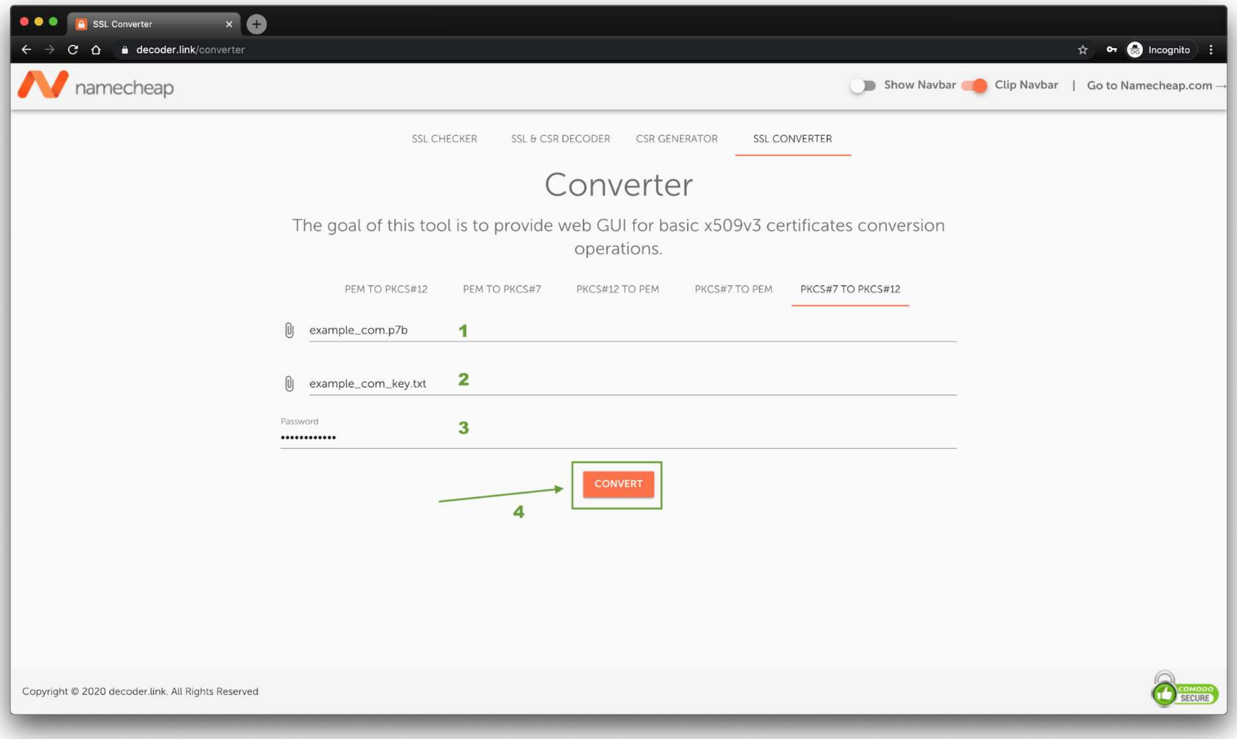
Key File*

Password
****

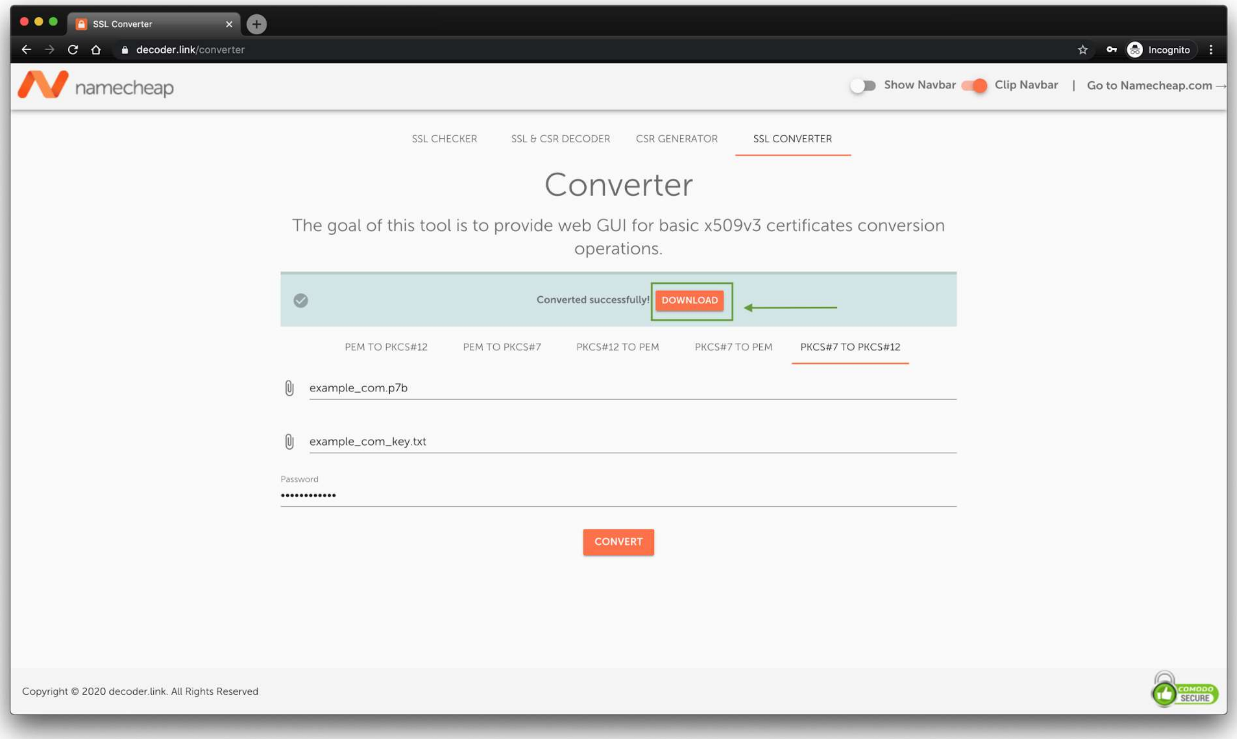
Copyright © 2020 decoder.link. All Rights Reserved

2. After that, upload both files: the PKCS#7-type certificate file and the Private Key file.

   ***Important note**: Make sure to **set a password for the file**. It should contain alphanumeric characters only. Otherwise, the generated PFX file will be corrupted.*



3. Finally, click **Convert** to confirm the action.
4. In the pop-up notification, click **Download** to save the converted certificate on your device. After that, extract the file from the downloaded archive.



Converter

The goal of this tool is to provide web GUI for basic x509v3 certificates conversion operations.

Converted successfully!

example_com.p7b

example_com_key.txt

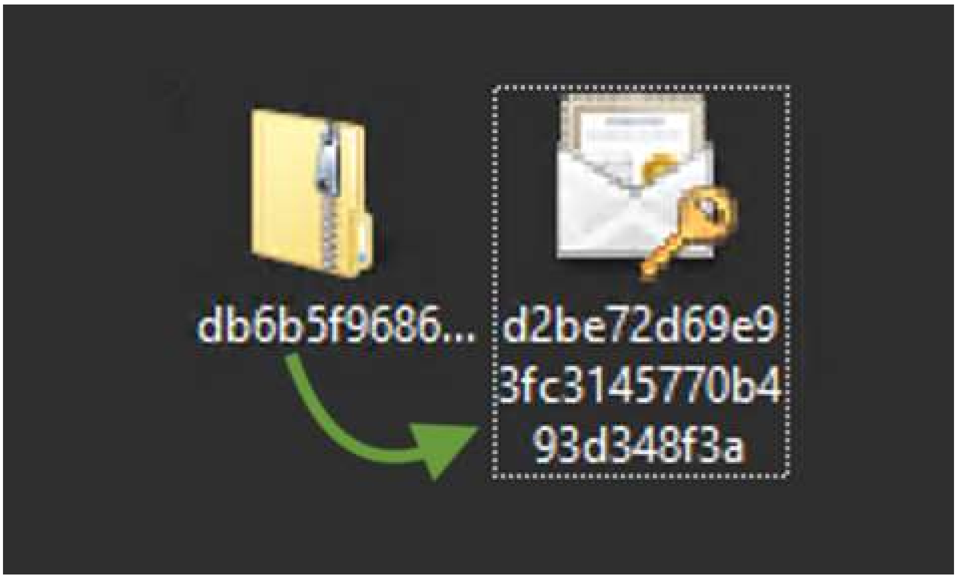
Copyright © 2020 decoder.link. All Rights Reserved

Import the PFX file

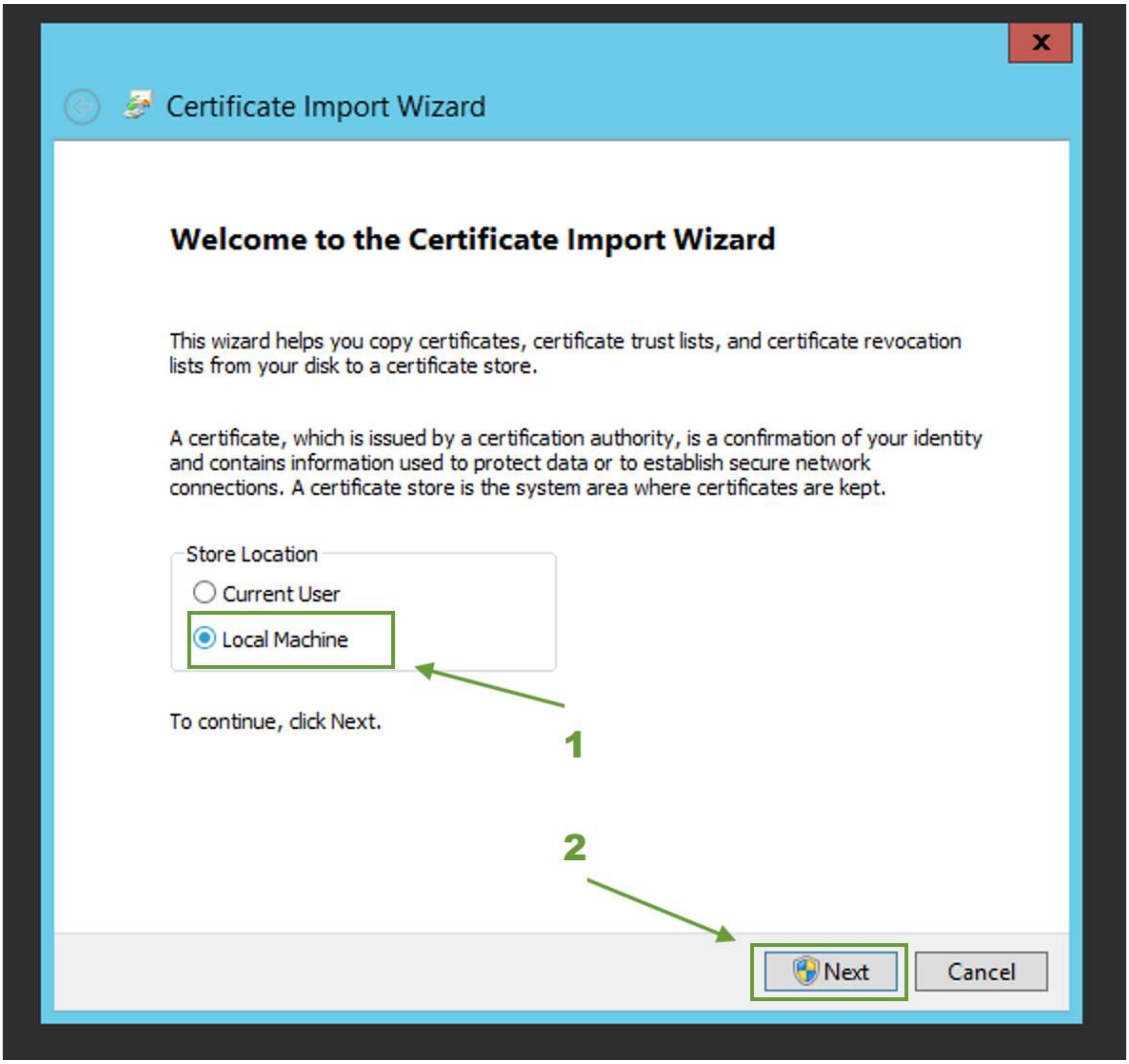
Note that the below steps are applicable on IIS servers. For the Exchange server, please use the following guidelines.

Once done, you can proceed with importing the PFX file to your Windows server:

1. Double-click the file to open the certificate import wizard or right-click on the file and select "*Install PFX*".



2. Select **Local Machine** to make the certificate accessible from all of the accounts in the system. Then, click **Next**.



Welcome to the Certificate Import Wizard

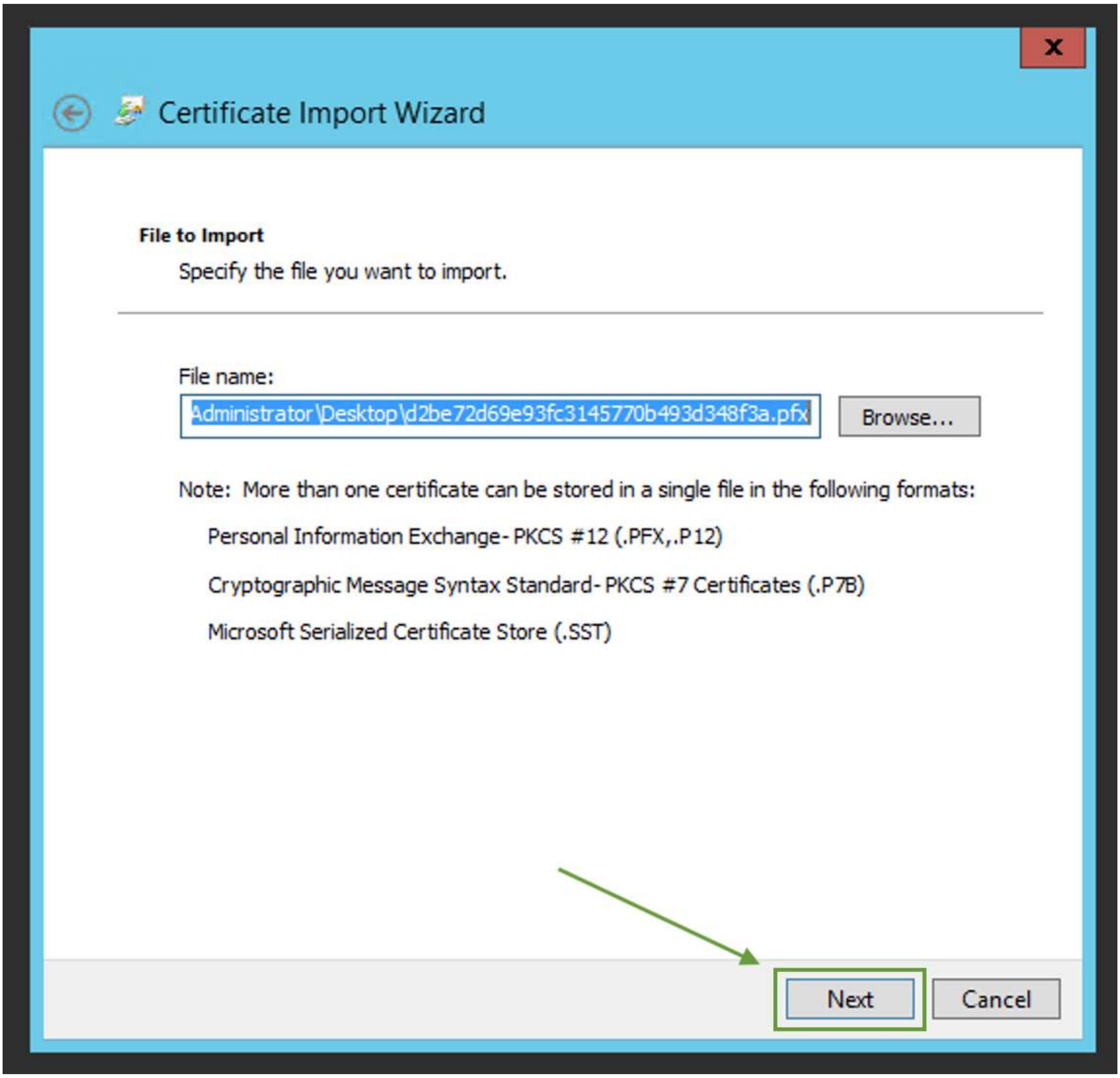
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

3. In the following prompt, click **Next** once again to confirm the file location.



File to Import

Specify the file you want to import.

File name:

Administrator\Desktop\d2be72d69e93fc3145770b493d348f3a.pfx

Note: More than one certificate can be stored in a single file in the following formats:

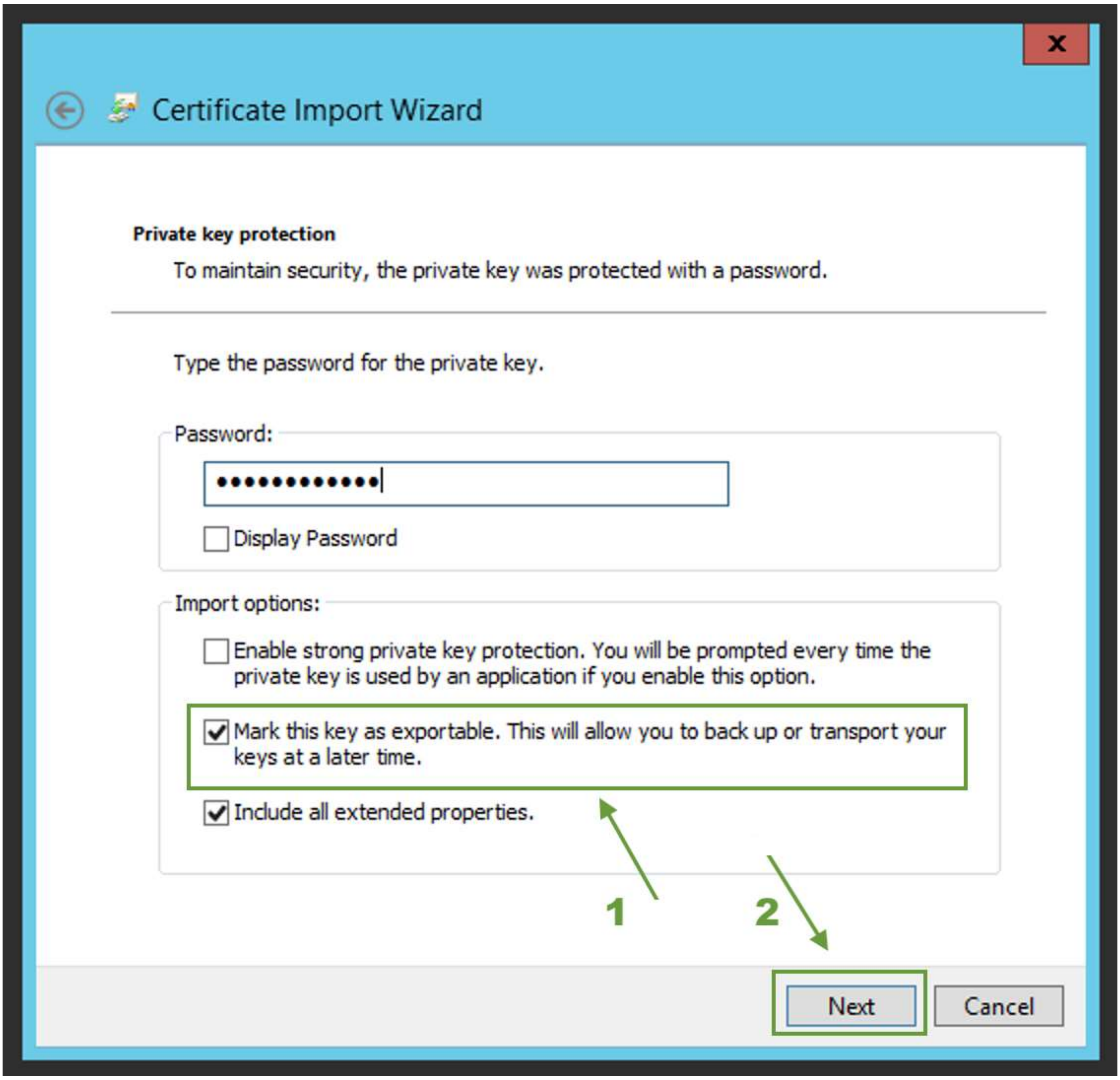
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

4. Enter the password you set for the PFX file. Make sure to tick off the "*Mark this key as exportable*" option, so that the Private Key can be exported later.

   Important note*: If the provided password is incorrect or lost, feel free to re-generate a new .pfx file.*



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

•••••••••••••

□ Display Password

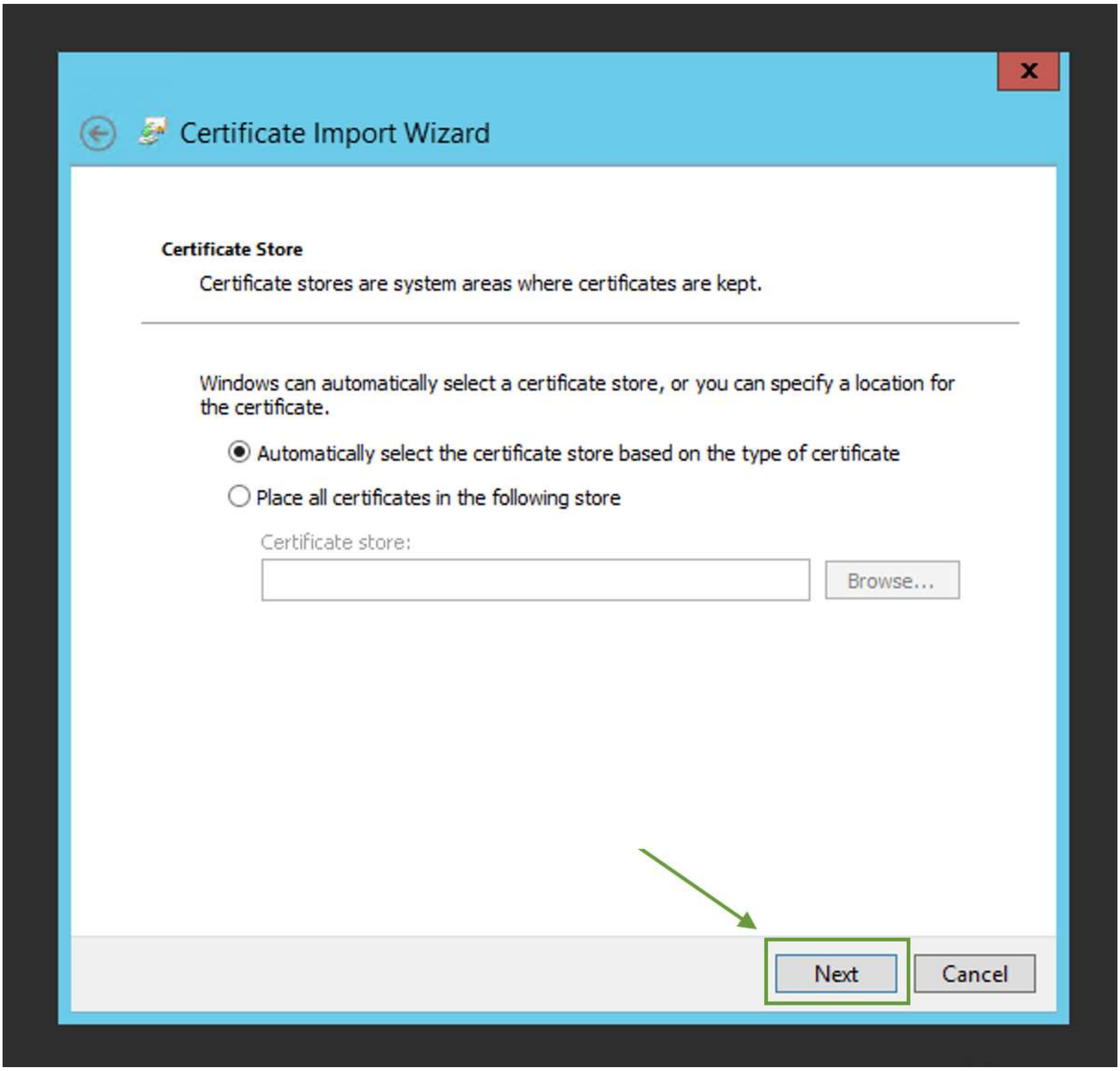
Import options:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

5. In the next prompt, you can choose the automatic option to let the Certificate Import Wizard take care of it. Click **Next** to proceed.



Certificate Store

Certificate stores are system areas where certificates are kept.

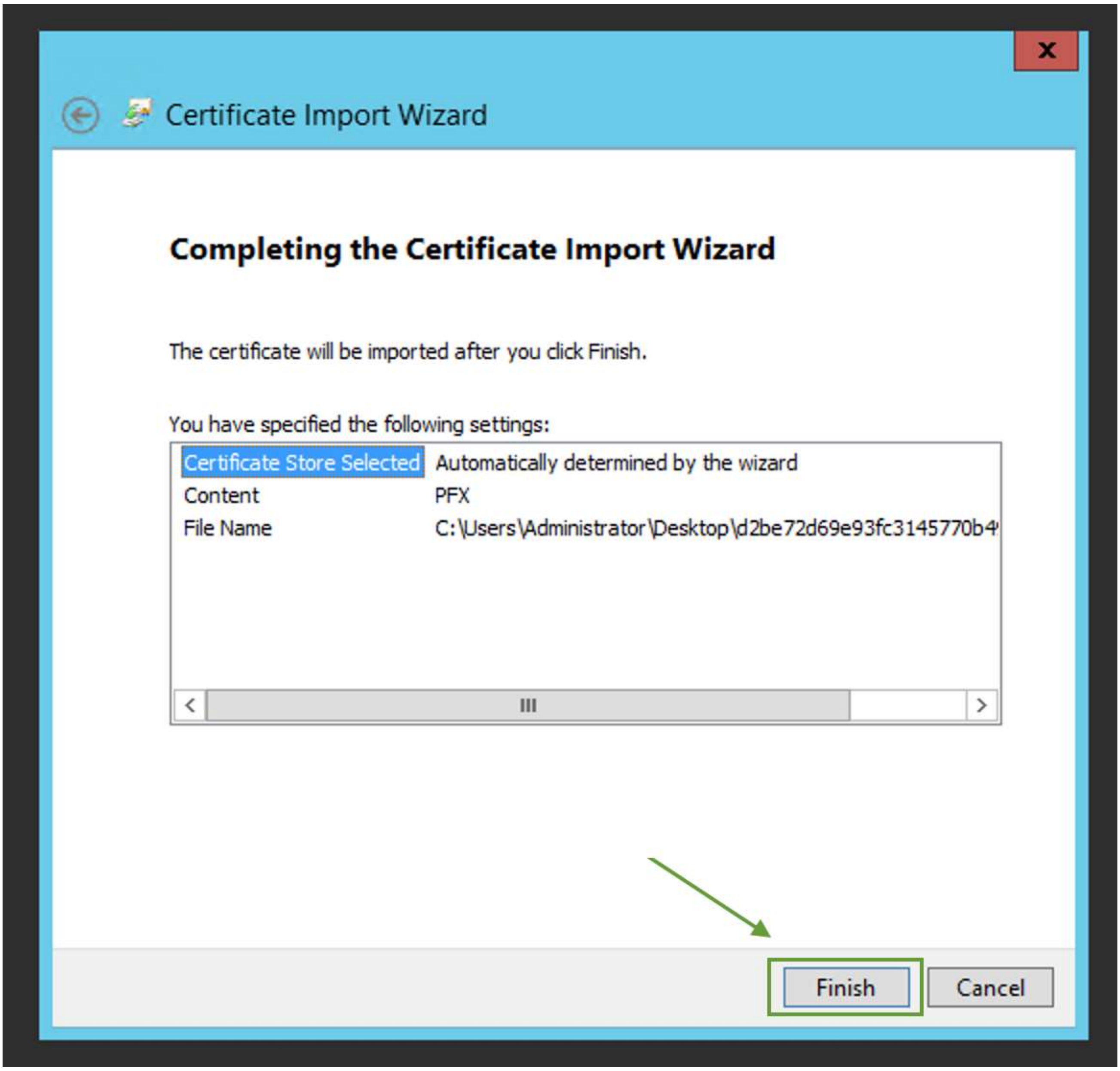
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

6. Then, click **Finish** to confirm the certificate import.



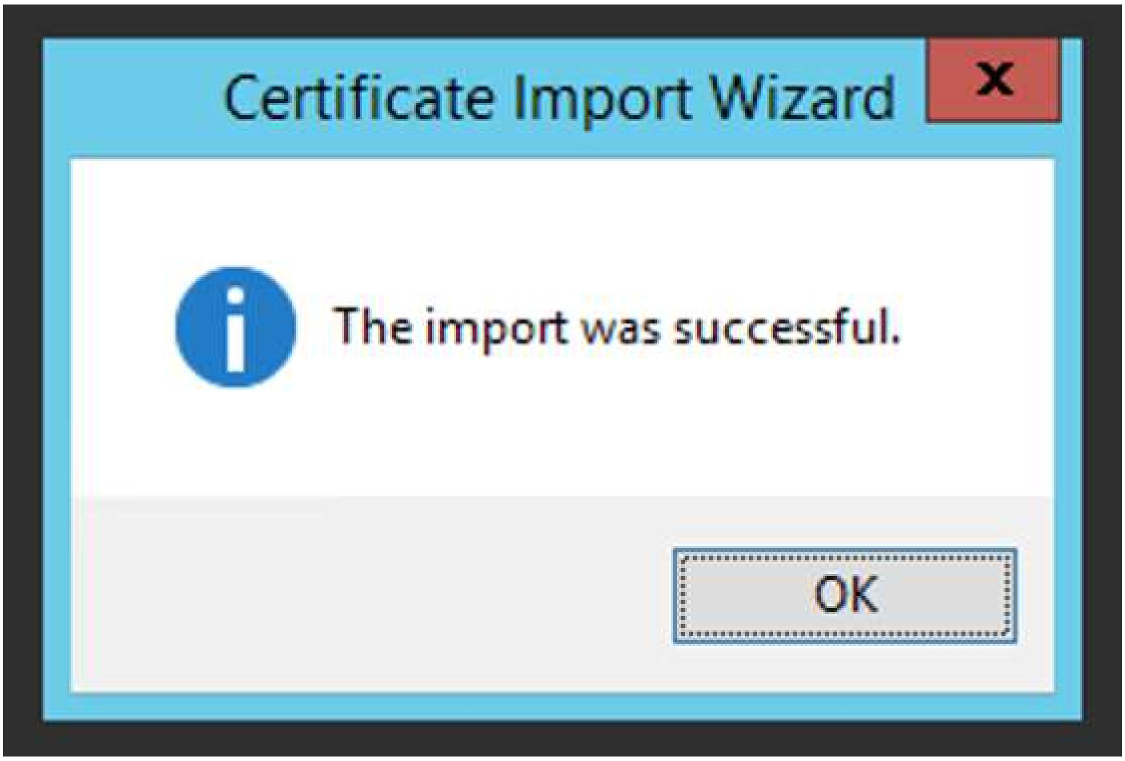
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\Users\Administrator\Desktop\d2be72d69e93fc3145770b4

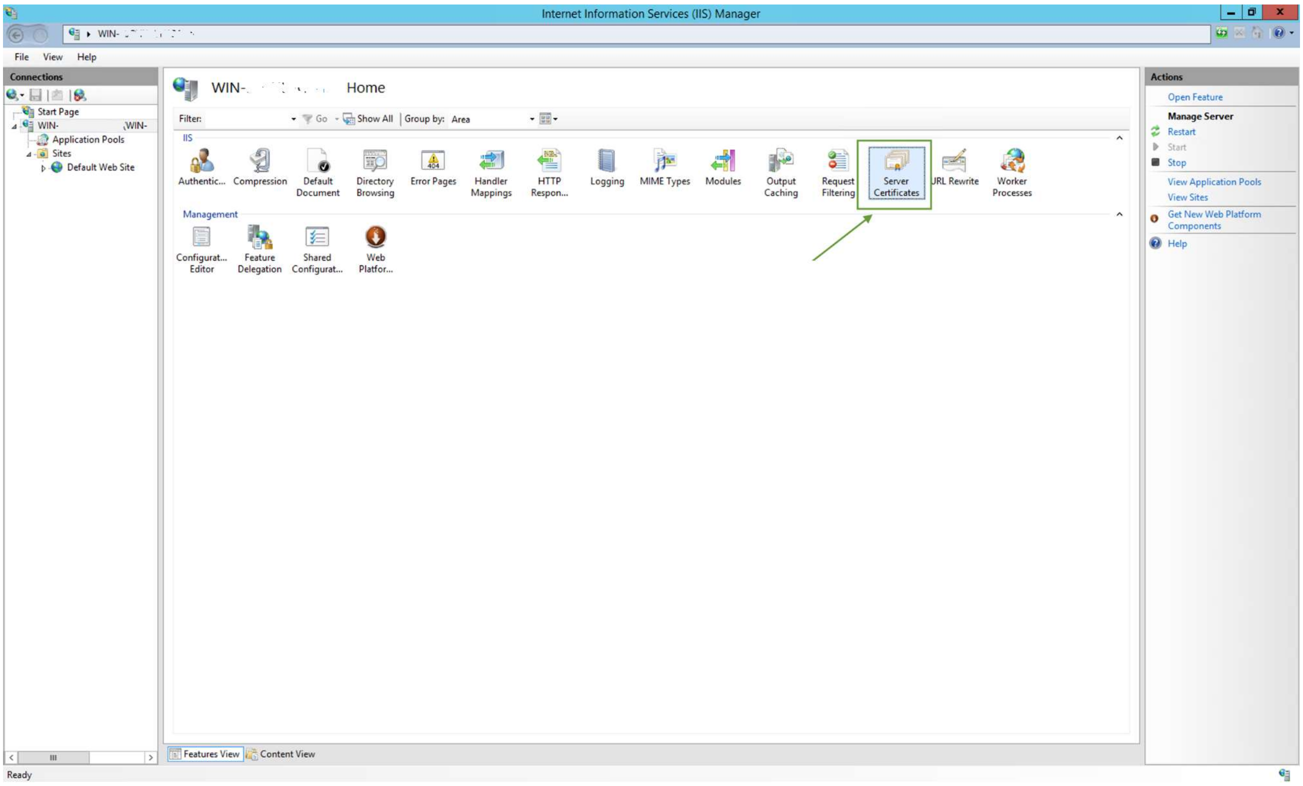
7. The following window should appear after that:

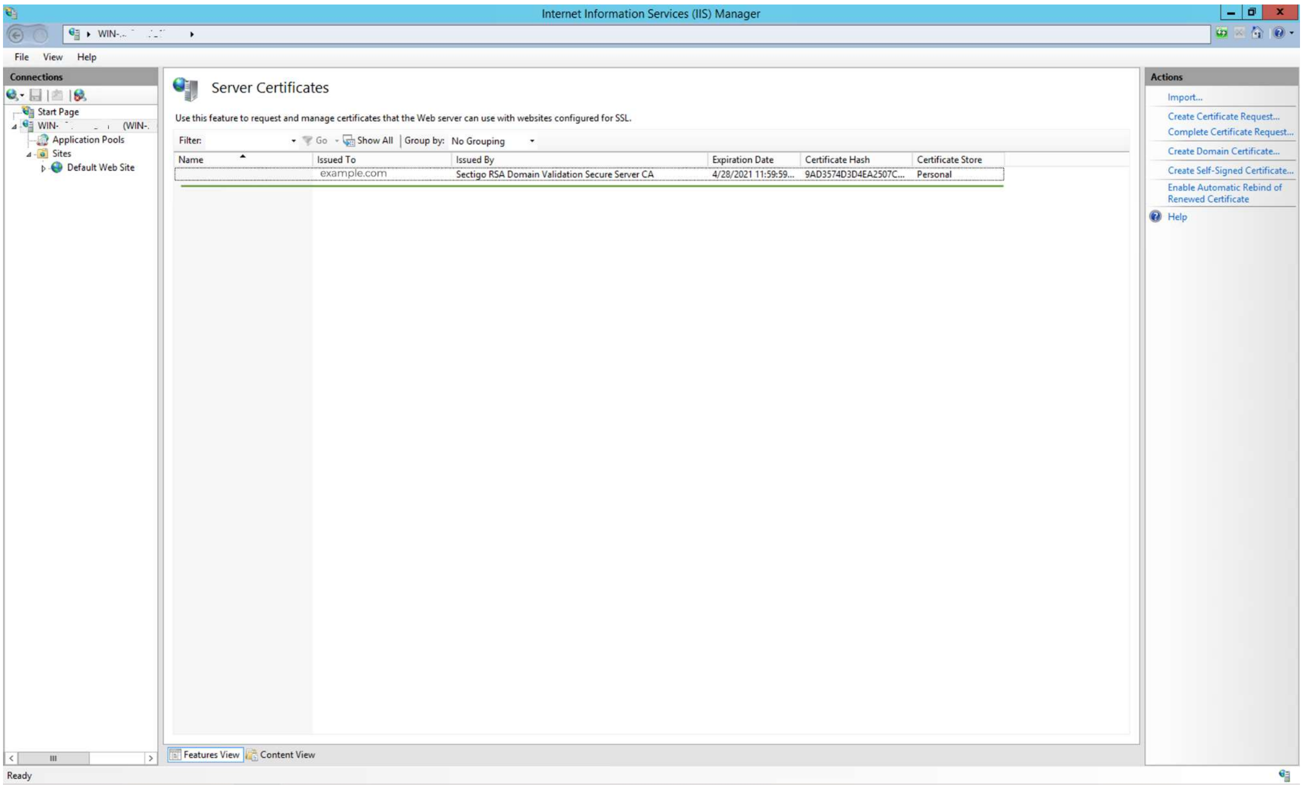


Certificate Import Wizard

The import was successful.

The certificate will also be displayed in the IIS console (**PC Name** >> **Server Certificates**):




Internet Information Services (IIS) Manager
File View Help
Connections
Start Page
WIN-
Application Pools
Sites
Default Web Site
Server Certificates
Filter:
Go
Show All
Group by: No Grouping
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
	example.com	Sectigo RSA Domain Validation Secure Server CA	4/28/2021 11:59:59...	9AD3574D3D4EA2507C...	Personal

The certificate will not have the “Name” parameter. Instead, it will display the domain name of the website as its name during the binding process. It is advisable to remove old certificates from the console to avoid confusion.

Install the certificate

To enable the certificate for your domain, you should set up certificate bindings. The installation should be straightforward from this point. Here are the guides outlining the procedure for every IIS version available:

IIS 7

IIS 8

IIS 10

Note*: On IIS 5 and 6, there's no need to add site bindings.*

You may need to restart your IIS sites to apply the changes.

<< How to install an SSL certificate on Ubiquiti Unifi (https://www.ssls.com/knowledgebase/installing-an-ssl-certificate-on-ubiquiti-unifi/)

Sectigo Root Certificate expiring May 30, 2020 >> (https://www.ssls.com/knowledgebase/sectigo-root-certificate-expiring-may-30-2020/)

Categories

Affiliate Program (https://www.ssls.com/knowledgebase/category/affiliate-program/)

CSR and certificate installation related questions (https://www.ssls.com/knowledgebase/category/csr-and-certificate-installation-related-questions/)

CSR generation instructions (https://www.ssls.com/knowledgebase/category/csr-generation-instructions/)

General Questions (https://www.ssls.com/knowledgebase/category/general-questions/)

Getting started and activating your SSL (https://www.ssls.com/knowledgebase/category/getting-started-and-activating-your-ssl/)

Multi-domain certificates FAQ (https://www.ssls.com/knowledgebase/category/multi-domain-certificates/)

News (https://www.ssls.com/knowledgebase/category/news/)

Renewal, Reissue and Refund related questions (https://www.ssls.com/knowledgebase/category/renewal-reissue-and-refund-related-questions/)

Site Seals (https://www.ssls.com/knowledgebase/category/site-seals/)

SSL Installation instructions (https://www.ssls.com/knowledgebase/category/ssl-installation-instructions/)

Troubleshooting errors (https://www.ssls.com/knowledgebase/category/troubleshooting-errors/)

f (https://www.facebook.com/SSLsCom)

(https://twitter.com/SSLscom)

Powered by SSLs.com (/) DMCA PROTECTED (https://www.dmca.com/Protection/Status.aspx?ID=b1971cab-a804-4f40-94c8-149f36985a27&refurl=https://www.ssls.com/knowledgebase/how-to-install-an-ssl-on-a-windows-server-when-the-csr-was-generated-elsewhere/)