How to Install an SSL Certificate

An SSL certificate (short for Secure Socket Layer) is a way that websites and services are authenticated to encrypt the data sent between them and their customers. SSL is also used to verify that you're connected to the correct service you want (for example, am I really signed in to my email service provider or is this just a phishing copy?). If you are providing a website or service that requires a secure connection, it may be necessary to install an SSL certificate to verify your trust. Take a look at the following article to learn how.

Using Microsoft Internet Information Services (IIS)

Initialize the CSR authentication request code (short for Certificate Signing Request). Before you can purchase and install an SSL certificate, you need to generate a CSR code on the server. This file contains the server and public key information and is required to generate the private key. You can generate a CSR code in IIS 8 in just a few clicks:

Open Server Manager.

Click Tools and select Internet Information Services (IIS) Manager.

Select the workstation where you are installing the certificate from below the Connections list.

Open the Server Certificates tool.

Click the Create Certificate Request link in the upper-right corner, below the Actions list.

Fill in the Request Certificate wizard. You'll need to enter your two-digit country code, state or province, city or town name, full company name, industry name (for example, IT or Marketing), and website address (usually called name). domain).

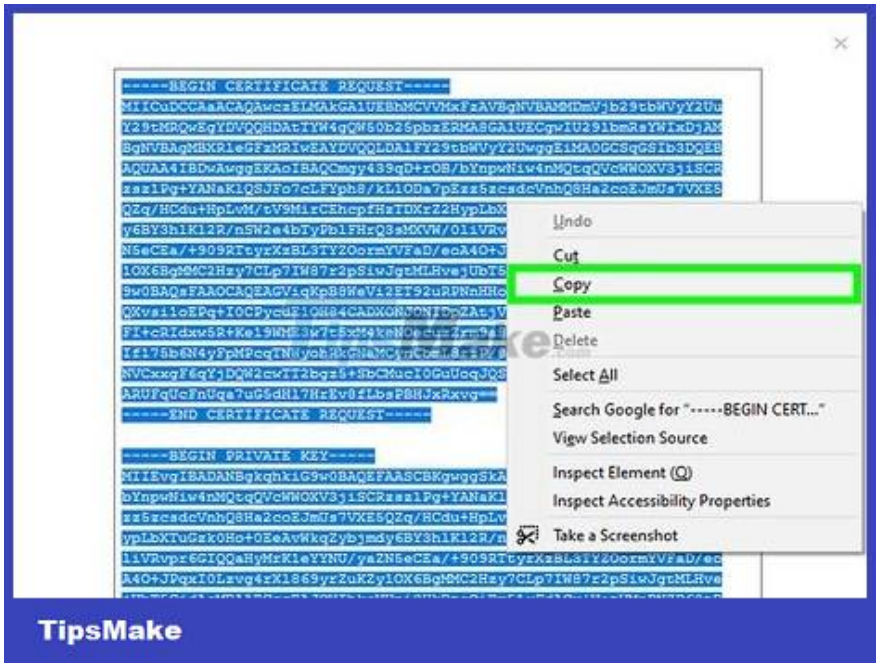
Leave the 'Cryptographic service provider' field as default.

Set 'Bit length' to '2048'.

Name the file that requires the certificate. It doesn't matter what the filename is, as long as you can find the word in your archive.

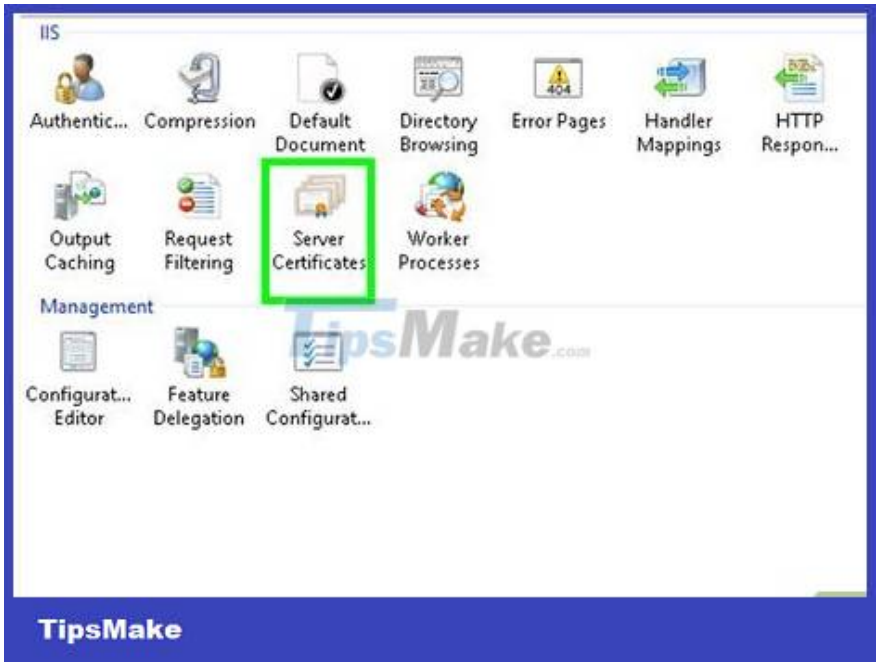
Order an SSL certificate. There are various online services that provide SSL certificates. You need to choose a reputable service to ensure the safety of your website and all customers. Popular services include: DigiCert, Symantec, GlobalSign, and more. The most appropriate service will depend on your needs (multiple certifications, enterprise solutions, etc.).

You need to upload the CSR file to the certificate service. This file will be used to generate the certificate for your server. Providers often ask us to upload files, some services just need to copy the content of the CSR file.

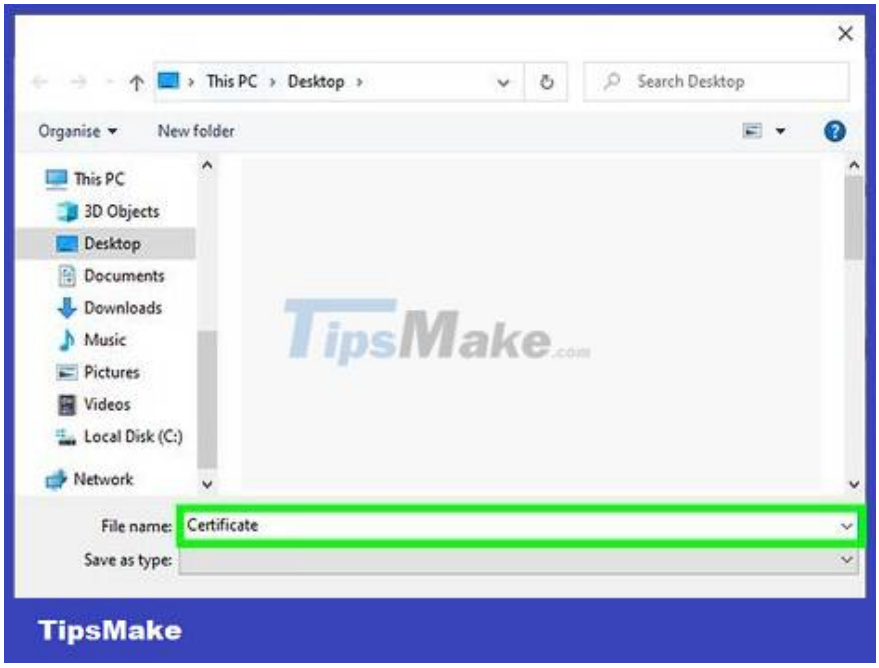


Download the certificate. The intermediate certificate needs to be downloaded from the service from which you ordered the certificate. The Primary Certificate will be sent to you via email or the client area of ??the website.

Rename the master certificate to 'website.cer'.

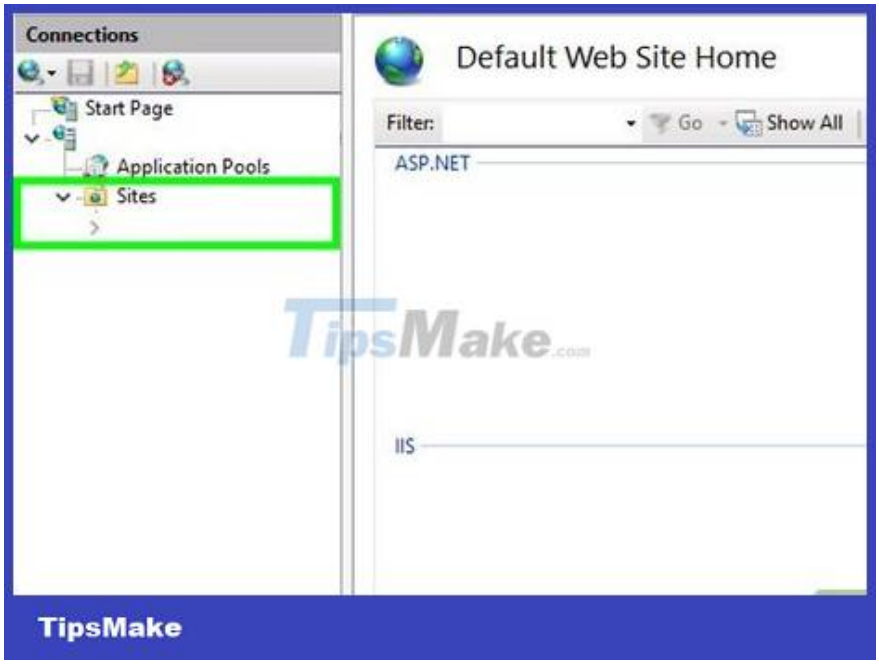


Open the Server Certificates tool in IIS again. Here, click the 'Complete Certificate Request' link below the 'Create Certificate Request' link that you clicked to initiate the CSR earlier.



Browse for the certificate file. After locating the file on the computer, you need to give the file a close name to easily identify the certificate on the server. Please save the certificate in the 'Personal' personal store, then click OK to install the certificate.

The certificate will appear in the list. If you don't see it, make sure you're using the same server where you generated the CSR code.



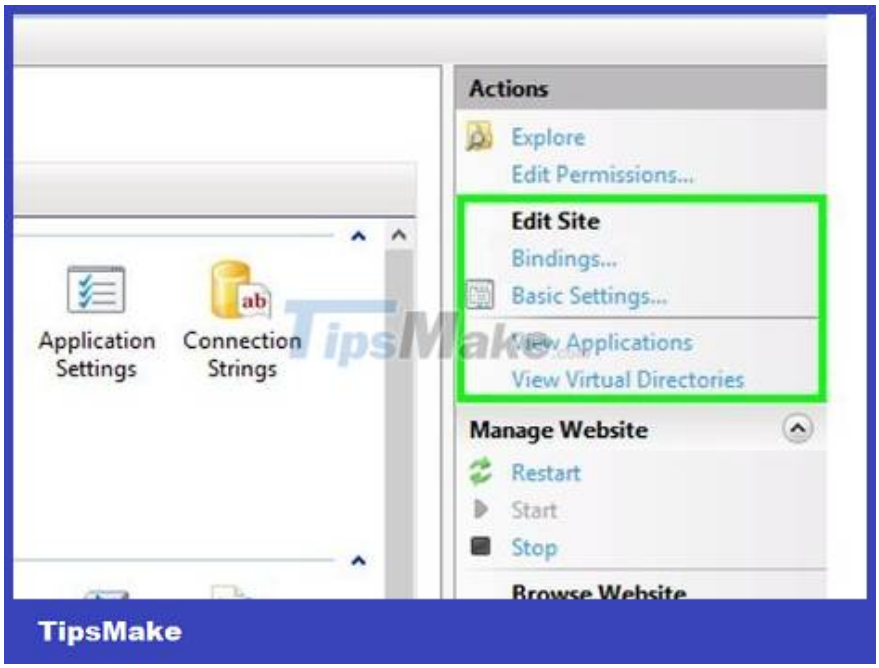
Link the certificate to the website. Now after the certificate has been installed, proceed to link to the website you want to protect. Expand the 'Sites' folder in the Connections list and click on the website that needs to be protected.

Click the Bindings link in the Actions list.

Click the Add button in the Site Bindings window that appears.

Select 'https' from the 'Type' drop-down menu, then select the installed certificate from the 'SSL certificate' drop-down menu.

Click OK and then select Close.

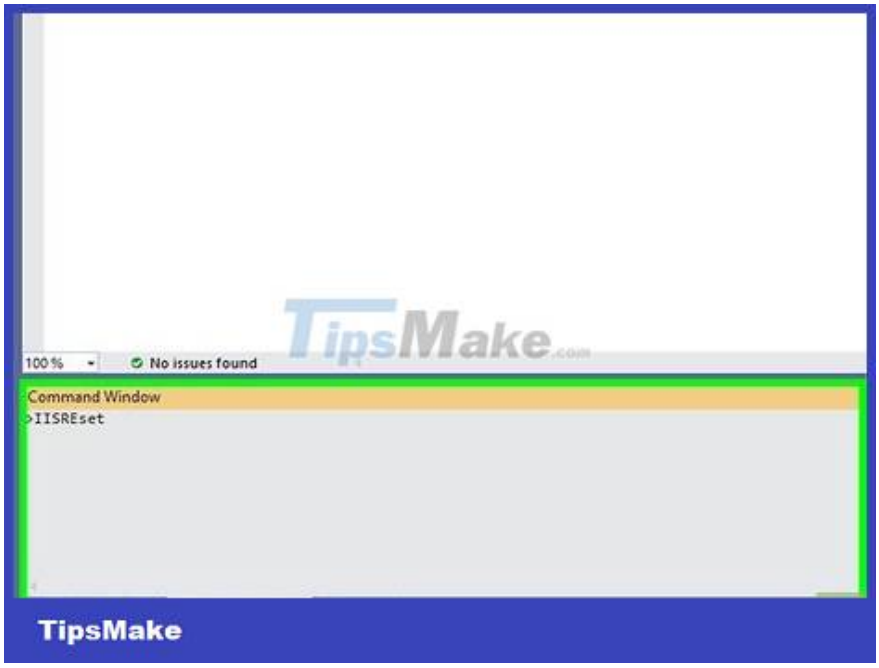


Install the Intermediate certificate. Find the intermediate certificate you downloaded from your service provider. Some services only provide one certificate that needs to be installed, others offer more. Copy these certificates to the dedicated folder on the server.

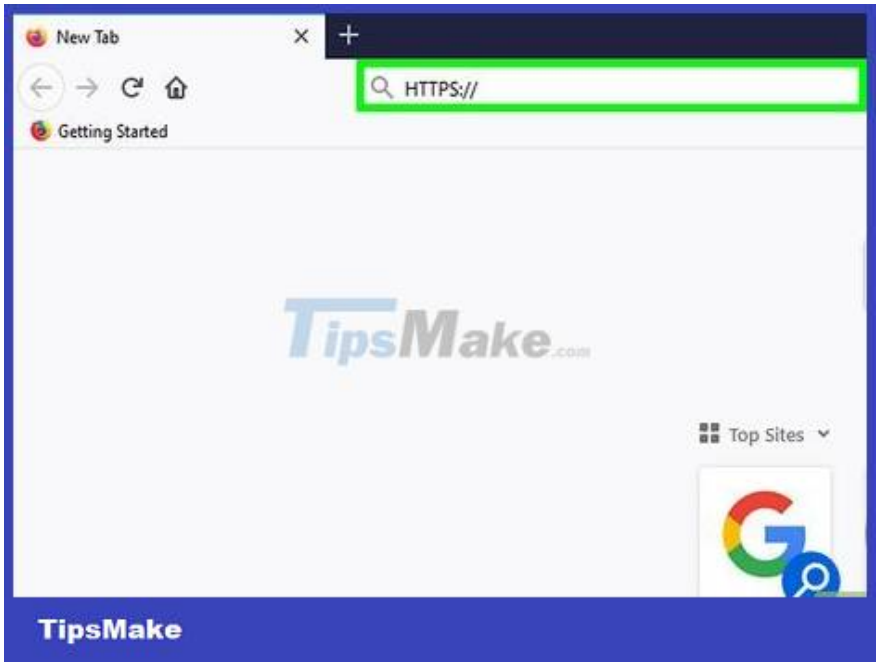
Once the certificate has been copied, you need to double-click to open the Certificate Details.

Click the General tab. Click the 'Install Certificate' button at the bottom of the window.

Select 'Place all certificates in the following store' and browse for the local store. You can find the local storage by checking the 'Show physical stores' box, then selecting Intermediate Certificates and then clicking Local Computer.

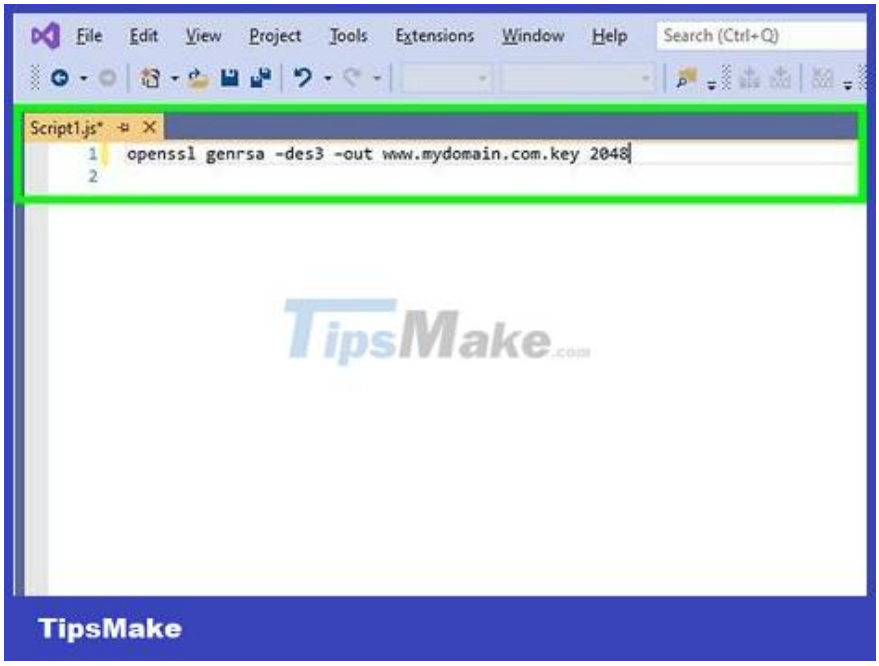


Restart IIS. Before you start distributing certificates, you need to restart the IIS server. To restart IIS, click Start and select Run. Type the command 'IISREset' and press Enter. The Command Prompt will open up and show the restart status of IIS.



Check the certificate. Use different web browsers to check if the certificate is working properly. Connect to your website using the 'https://' protocol to force an SSL connection. A padlock icon will appear in the address bar, usually on a green background.

Using Apache



Generate CSR code. Before you can purchase and install an SSL certificate, you need to generate a CSR code on the server. This file contains the server and public key information and is required to generate the private key. You can generate the CSR code directly from the Apache command line:

Start the OpenSSL utility. You can find it at /usr/local/ssl/bin/

Generate the key pair by entering the following command:

```
openssl genrsa –des3 –out www.mydomain.com.key 2048
```

Create a passphrase. You will enter this passphrase every time you interact with the key pair.

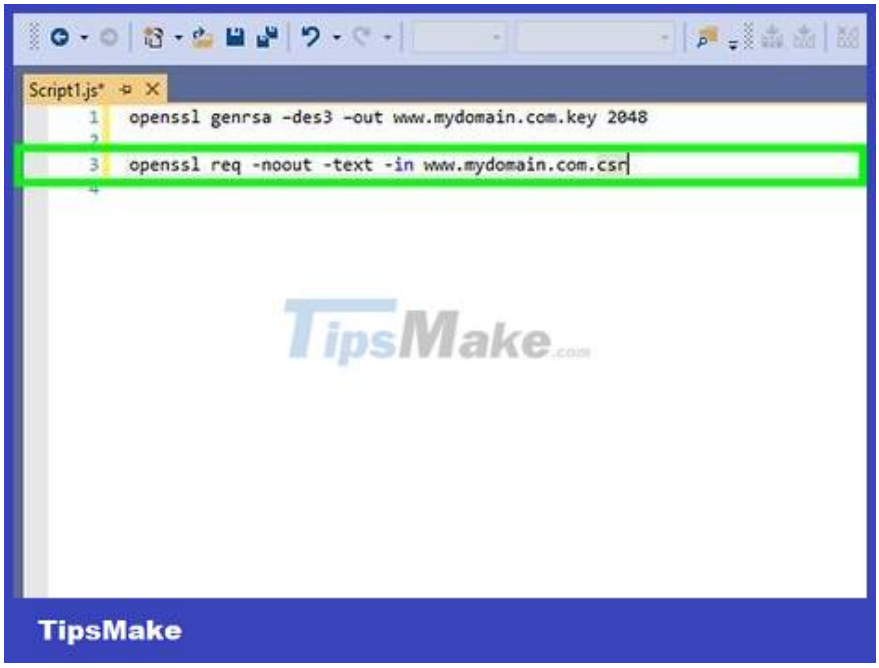
Start the CSR initialization process. Enter the following command when asked to create the CSR file:

```
openssl req –new –key www.mydomain.com.key –out www.mydomain.com.csr
```

Fill in the requested information. You'll need to enter your two-digit country code, state or province, city or town name, full company name, industry name (for example, IT or Marketing), and website address (usually called name). domain).

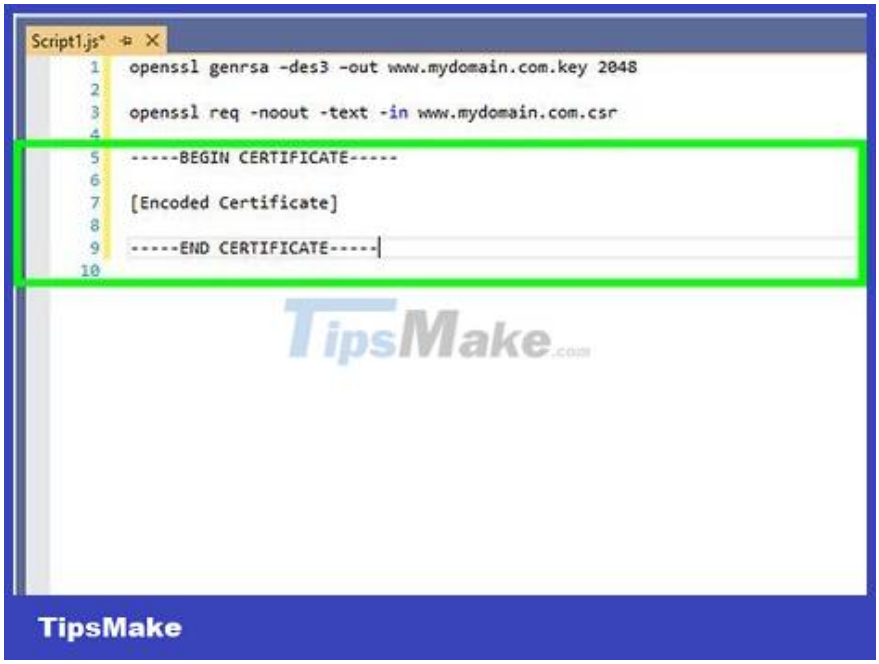
Generate CSR file. After entering the information, launch the following command to initialize the CSR file on the server:

```
openssl req -noout -text -in www.mydomain.com.csr
```



Order an SSL certificate. There are various online services that provide SSL certificates. You need to choose a reputable service to ensure the safety of your website and all customers. Popular services include: DigiCert, Symantec, GlobalSign, and more. The most appropriate service will depend on your needs (multiple certifications, enterprise solutions, etc.).

You need to upload the CSR file to the certificate service. This file will be used to generate the certificate for your server.

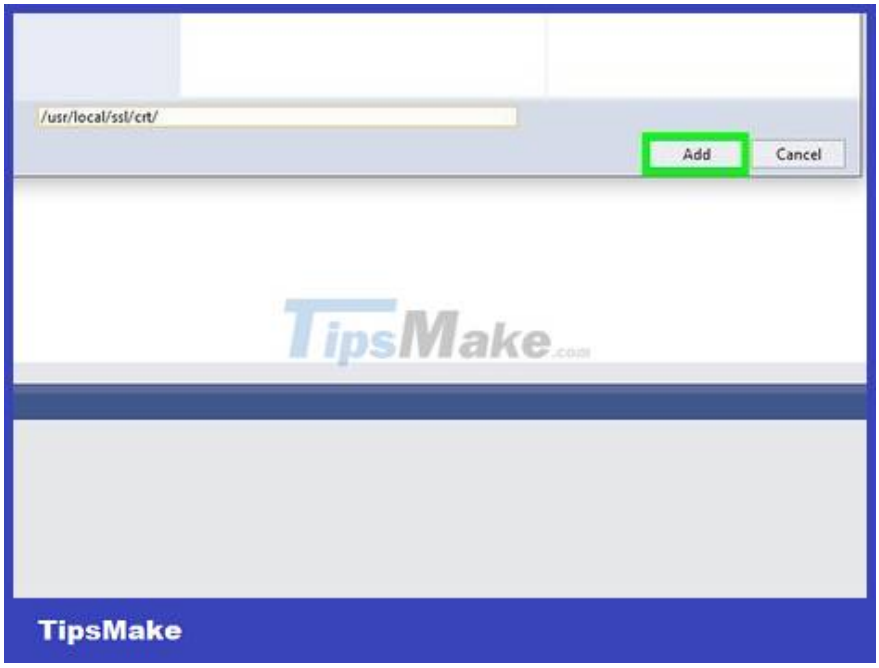


Download the certificate. The intermediate certificate needs to be downloaded from the service from which you ordered the certificate. The master certificate will be sent via email or the client area of ??the website. Your key should look similar to this:

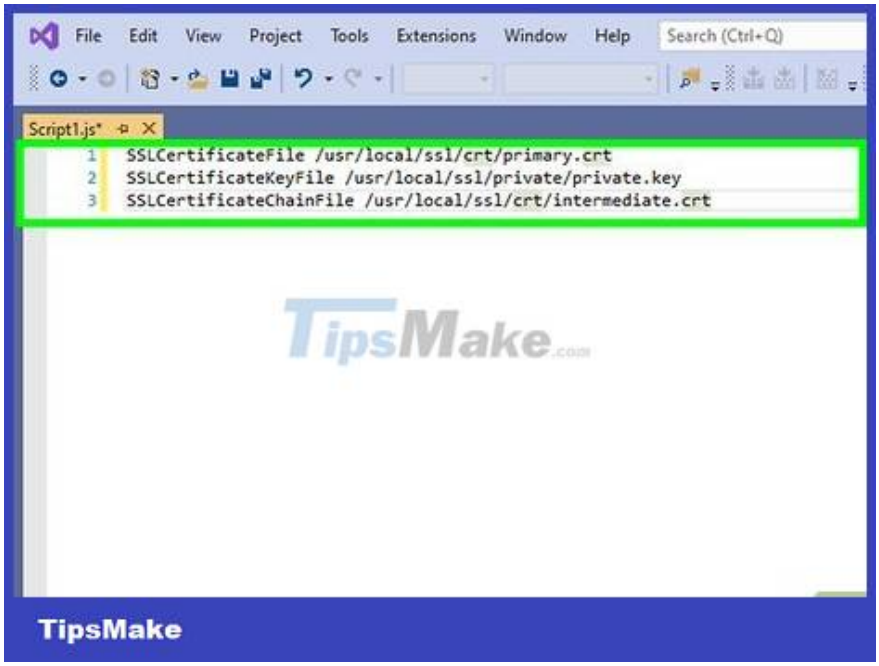
```
-----BEGIN CERTIFICATE----- [Encoded Certificate] -----END CERTIFICATE-----
```

If the certificate is in a text file, you need to change the file extension to .CRT before uploading

Check the key that you have loaded. There will be 5 hyphens '-' on either side of the BEGIN CERTIFICATE and END CERTIFICATE lines. Also you need to check to make sure that no extra spaces or line breaks are inserted in the key.



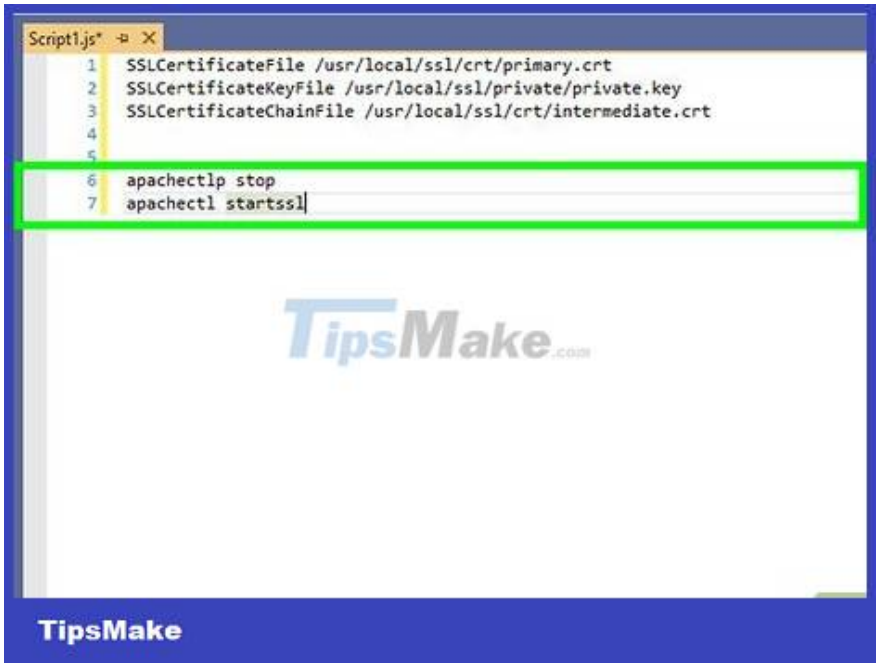
Upload the certificate to the server. The certificate will be in a folder dedicated to the key and certificate files. For example, /usr/local/ssl/crt/. All certificates need to be saved in the same folder.



Open the file 'httpd.conf' in a text editor. Some versions of Apache have an 'ssl.conf' file for SSL certificates. You only need to edit one file if you have both. Add the following lines to the Virtual Host section:

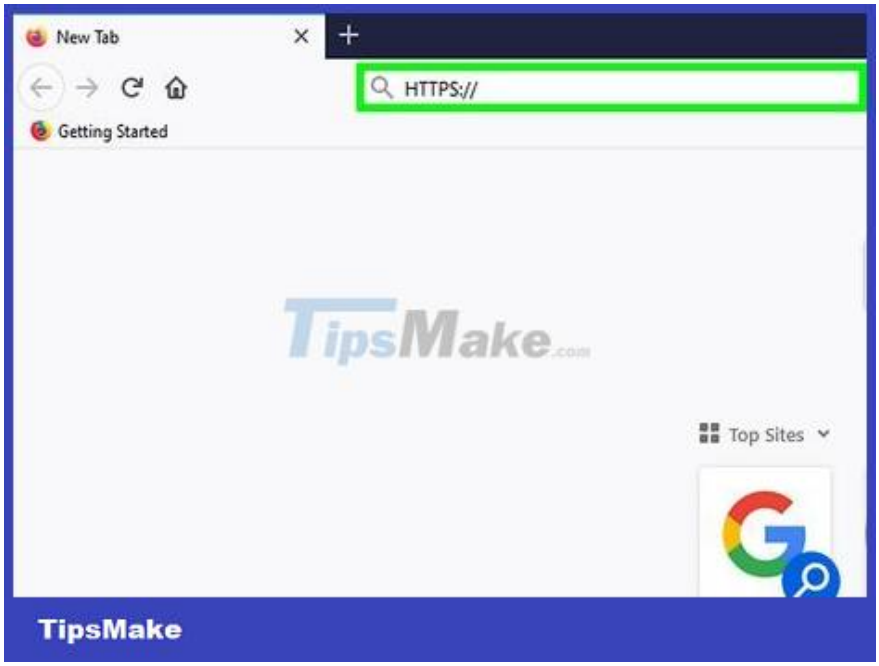
```
SSLCertificateFile /usr/local/ssl/crt/primary.crt SSLCertificateKeyFile /usr/loca
```

Save the changes to the file when finished. Re-upload the file to the server if necessary.



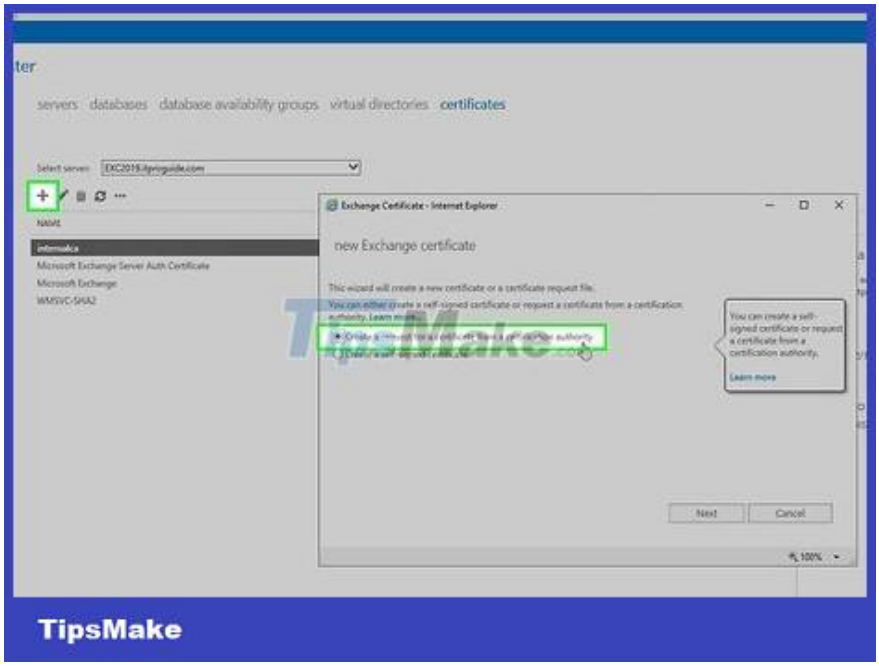
Restart the server. After changing the file, you can start using the SSL certificate by restarting the server. Most instances can be restarted by entering the following command:

```
apachectlp stop apachectl startssl
```



Check the certificate. Use different web browsers to check if the certificate is working properly. Connect to your website using the 'https://' protocol to force an SSL connection. A padlock icon will appear in the address bar, usually on a green background.

Using Exchange



Generate CSR code. Before you can purchase and install an SSL certificate, you need to generate a CSR code on the server. This file contains the server and public key information and is required to generate the private key.

Open Exchange Management Console. Click Start > Programs > Microsoft Exchange 2010 > Exchange Management Console.

After the program launches, click the Manage Databases link in the middle of the window.

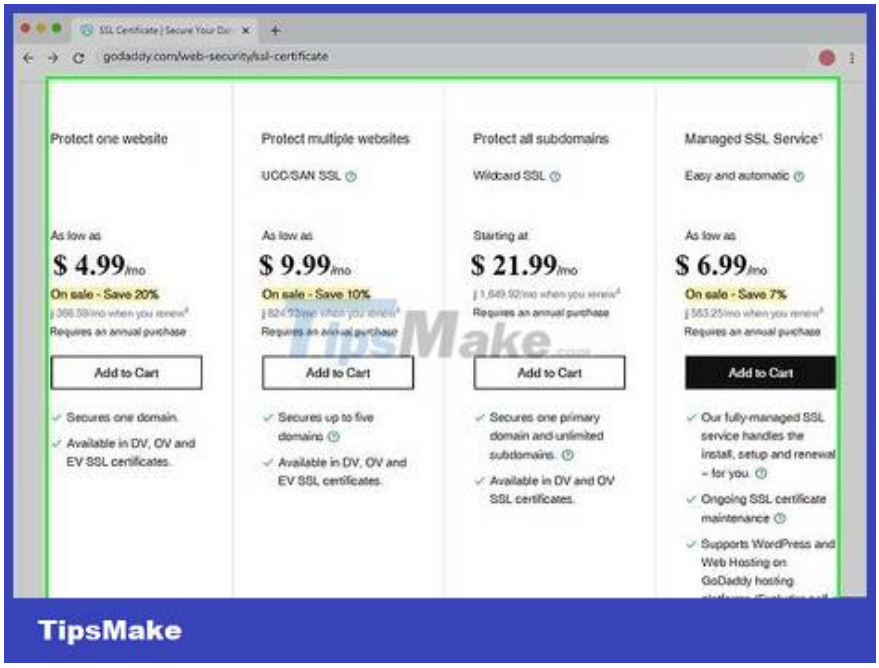
Select 'Server Configuration'. This option is in the left pane. Click the 'New Exchange Certificate' link in the Actions list on the right side of the screen.

Enter a memorable name for the certificate. This is optional if it's convenient for you (doesn't affect the certificate).

Enter configuration information. Exchange will automatically select the appropriate service, but if the server does not, you need to set it up yourself. Make sure all services for which you need protection are selected.

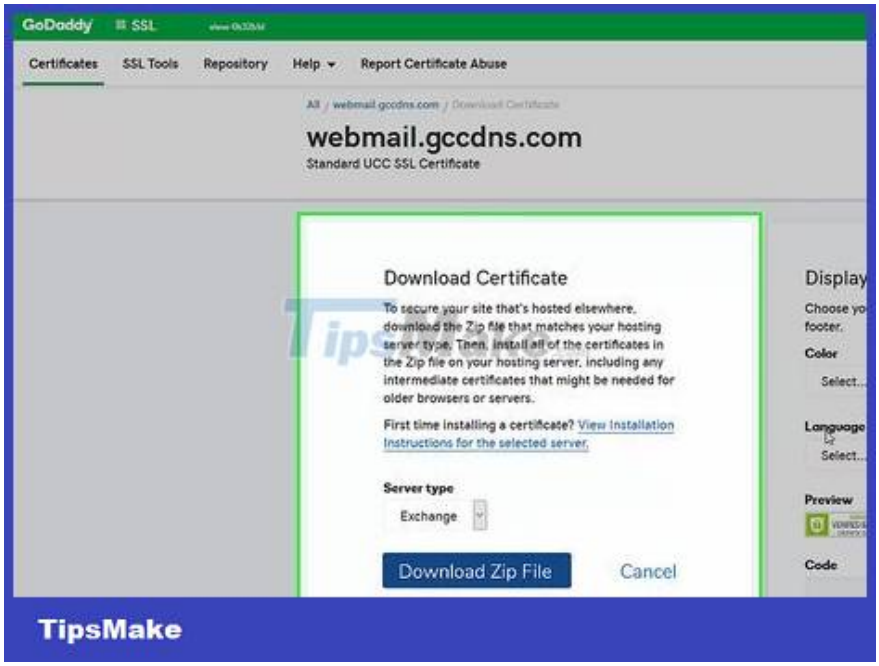
Enter organization information. You'll need to enter your two-digit country code, state or province, city or town name, full company name, industry name (for example, IT or Marketing), and website address (usually called name). domain).

Choose a location and name for the CSR file you are about to create. Make a note of where this file is saved for the next certificate ordering process.



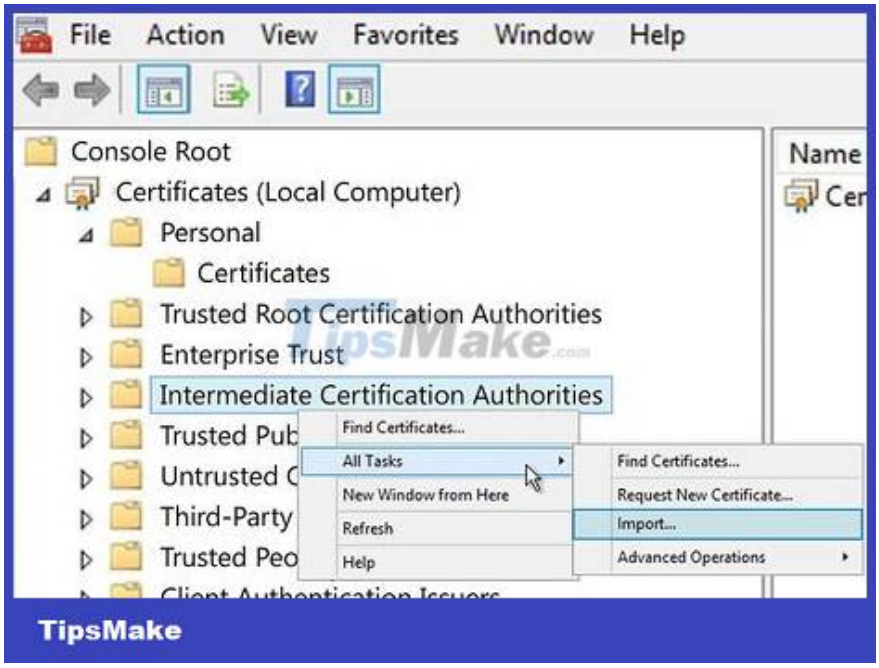
Order an SSL certificate. There are various online services that provide SSL certificates. You need to choose a reputable service to ensure the safety of your website and all customers. Popular services include: DigiCert, Symantec, GlobalSign, and more. The most appropriate service will depend on your needs (multiple certifications, enterprise solutions, etc.).

You need to upload the CSR file to the certificate service. This file will be used to generate the certificate for your server. Providers often ask us to upload files, some services just need to copy the content of the CSR file.



Download the certificate. The intermediate certificate needs to be downloaded from the service from which you ordered the certificate. The master certificate will be sent via email or the client area of ??the website.

Copy the certificate file you received to the Exchange server.



Install the intermediate certificate. In most cases you can copy the provided certificate data to a text document and save it as 'intermediate.cer'. Proceed to open Microsoft Manage Console (MMC) by clicking Start, selecting Run and then typing 'mmc'.

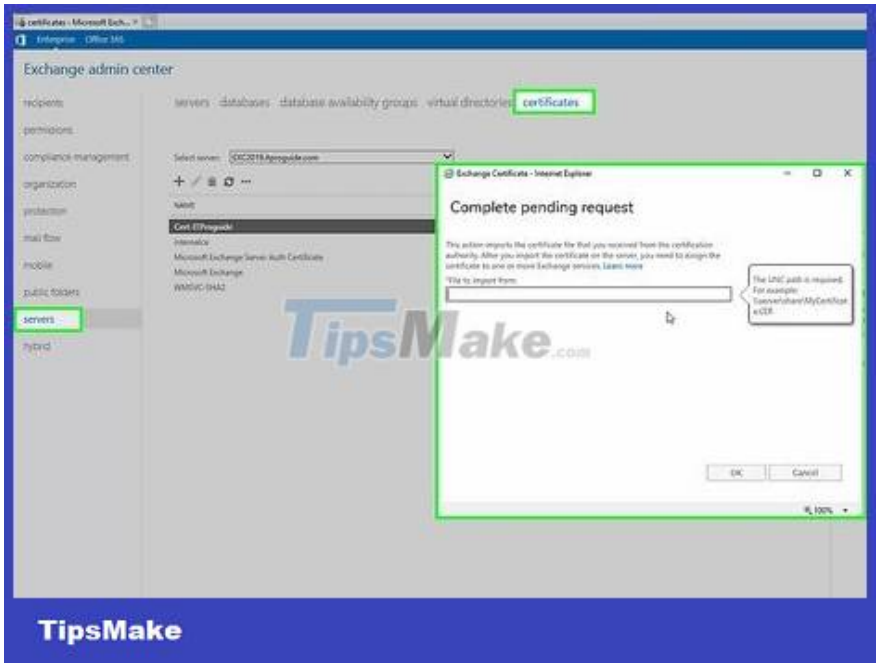
Click File and select Add/Remove Snap In.

Click Add, select Certificates and then click Add again.

Select Computer Account and click Next. Select Local Computer as the storage location. Click Finish, and then click OK. You will return to MMC.

Select Certificates in the MMC. Select 'Intermediate Certification Authorities' and select Certificates.

Right-click Certificates, select All Tasks, and then select Import. Use the wizard to load the intermediate certificate that you downloaded from your service provider.



Open the 'Server configuration' section in the Exchange Management Console. See step 1 again for how to open 'Server configuration'. Then, click on the certificate in the center of the window and then click the 'Complete Pending Request' link in the Actions list.

Browse for the main certificate file and click Complete. After the certificate is uploaded, click Finish.

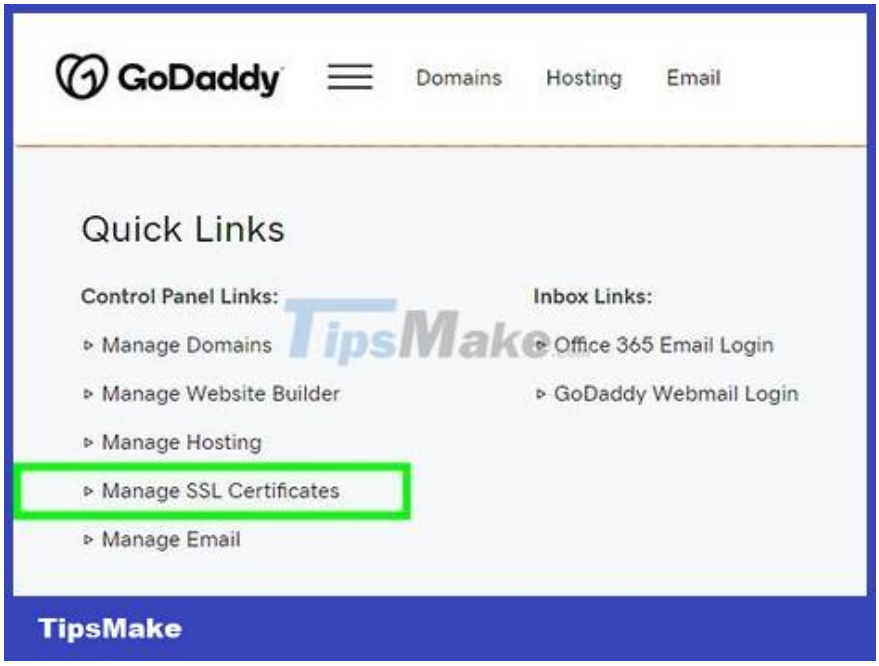
Ignore any error that the process failed; This is a common error.

Activate the certificate. After installing the certificate, click the 'Assign Services to Certificate' link located towards the bottom of the Actions list.

Select the server from the list that appears and click Next.

Select the server that you want to protect with the certificate. Click Next, then Assign, and then click Finish.

Using cPanel



Generate CSR code. Before you can purchase and install an SSL certificate, you need to generate a CSR code on the server. This file contains the server and public key information and is required to generate the private key.

Login to cPanel. Open control panel and find SSL/TLS Manager.

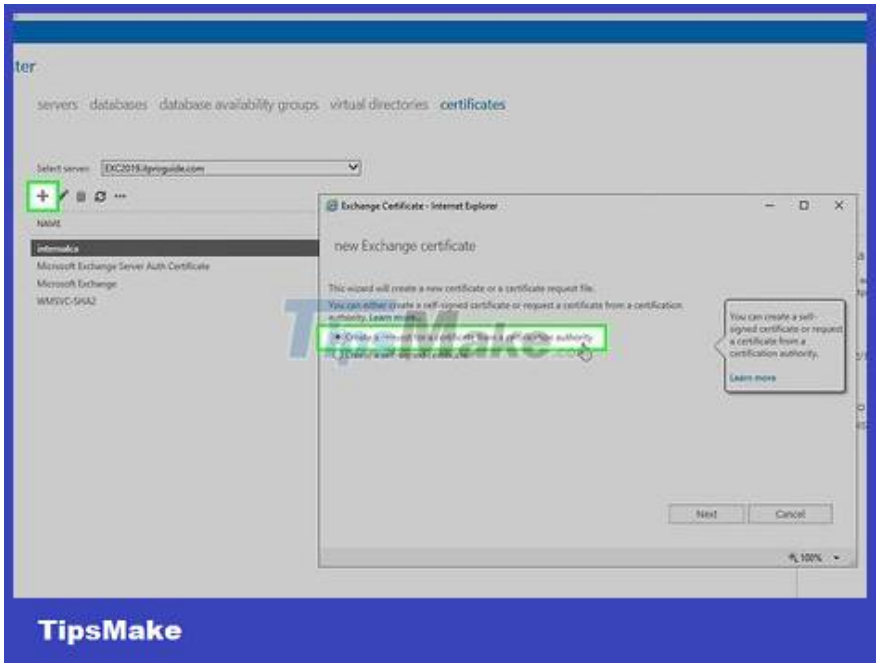
Click the 'Generate, view, upload, or delete your private keys' link.

Scroll down to the 'Generate a New Key' section. Enter the domain name or choose from the drop-down menu. Select 2048 for 'Key Size'. Click the Generate button.

Click 'Return to SSL Manager'. From the main menu, select the 'Generate, view, or delete SSL certificate signing requests' link.

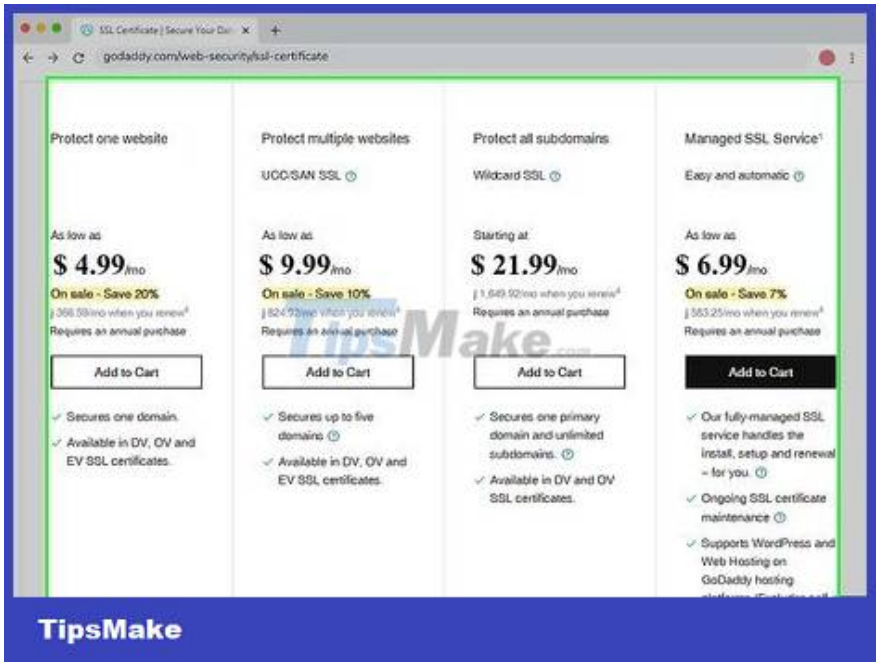
Enter organization information. You'll need to enter your two-digit country code, state or province, city or town name, full company name, industry name (for example, IT or Marketing), and website address (usually called name). domain).

Click the Generate button. The CSR code will appear. You can proceed to copy and enter this code into the certificate order form. If the service requires a CSR file, copy the code into a text editor and save it as a .CSR file.

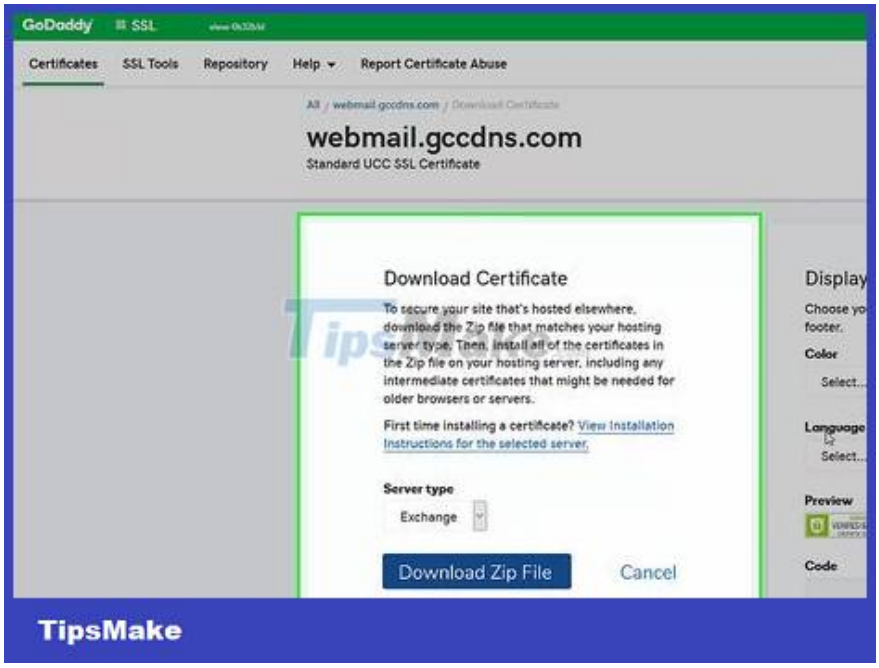


Order an SSL certificate. There are various online services that provide SSL certificates. You need to choose a reputable service to ensure the safety of your website and all customers. Popular services include: DigiCert, Symantec, GlobalSign, and more. The most appropriate service will depend on your needs (multiple certifications, enterprise solutions, etc.).

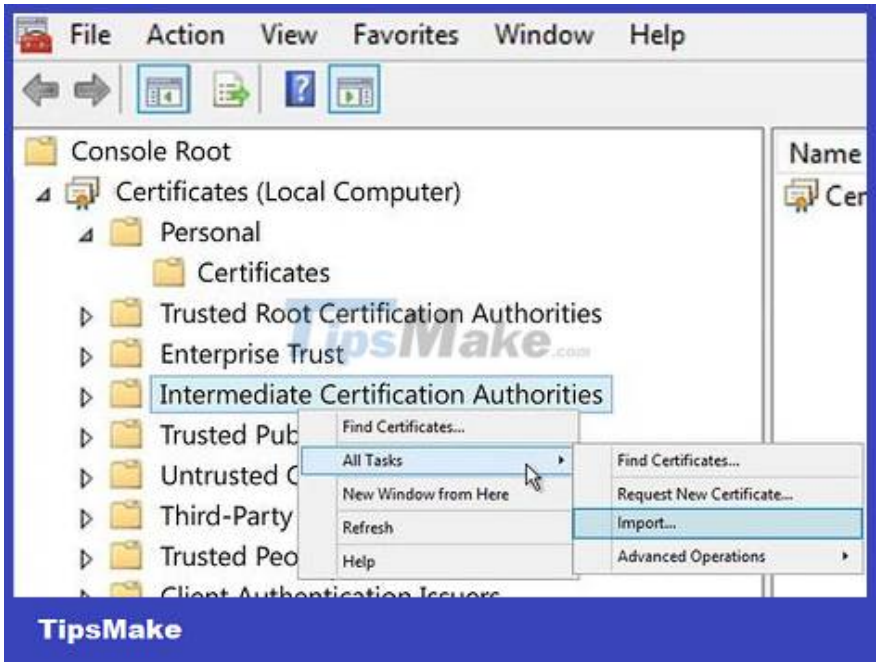
You need to upload the CSR file to the certificate service. This file will be used to generate the certificate for your server. Providers often ask us to upload files, some services just need to copy the content of the CSR file.



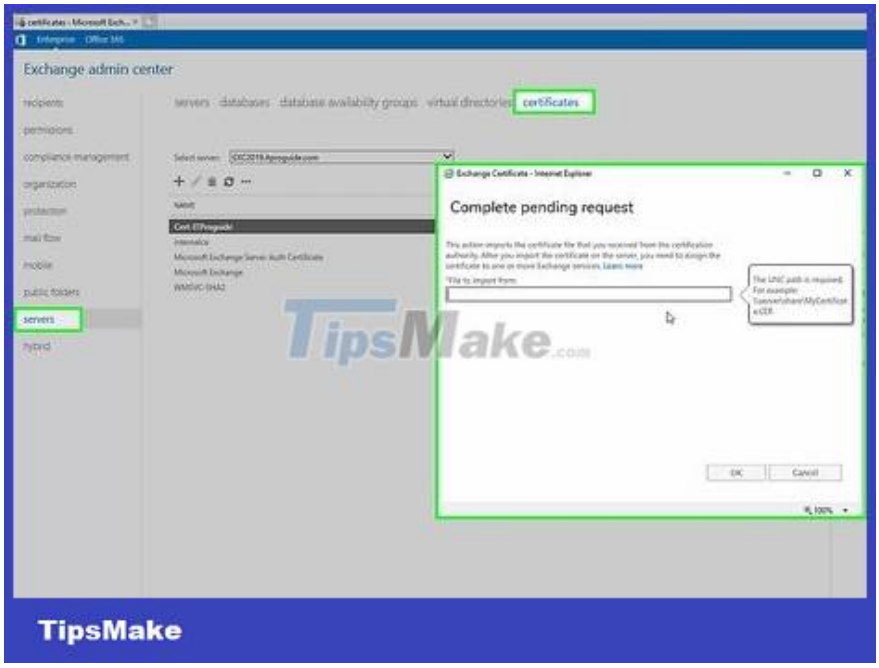
Download the certificate. The intermediate certificate needs to be downloaded from the service from which you ordered the certificate. The master certificate will be sent via email or the client area of ??the website.



Open the SSL Manager menu in cPanel again. Click the 'Generate, view, upload, or delete SSL certificates' link. Click the Upload button to browse for the certificate you received from your service provider. If the certificate was downloaded as text, paste the certificate content into the browser's frame.



Click the 'Install SSL Certificate' link. The SSL certificate installation will be complete. The server will restart and the certificate will be distributed.



Check the certificate. Use different web browsers to check if the certificate is working properly. Connect to your website using the 'https://' protocol to force an SSL connection. A padlock icon will appear in the address bar, usually on a green background.

You finished reading the article "**How to Install an SSL Certificate**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
