

# How to purchase and install SSL certificates

- How to purchase SSL certificate
- How to generate a CSR file
  - Using LINUX operating system
  - Using Windows operating system
- How to install SSL certificates
  - Apache
  - Apache 2
  - Microsoft IIS

## How to purchase SSL certificate

1. You can purchase an SSL certificate from a domain registrar, a web-host or direct from a trusted Certificate Authority. There are several types of certificates, each with different issuance processes and for different purposes.

Certificate type	Description
Domain validated certificate	Domain validated certificates are the most basic and at the lower cost end of SSL certificates out there. Once the Certificate Authority has confirmed that the requester has control over the domain (via confirmation email, adding a DNS record, or by adding a text to the hosted website), the certificate is immediately generated and sent to the requester.
Organization validated certificate	Organization validated certificates include an additional vetting process by the Certificate Authority to verify the legitimacy of the organization. For example, the Certificate Authority may contact the person listed as the organization's primary contact during business hours or ask for documents supporting the authenticity of the organization. Unlike DV certificates, OV certificates contain legitimate business information. This is best used by commercial or public facing website whereby visitor trust is essential.
Extended validated certificate	Extended validation certificates provide the highest trust recognition for an organization. All requests for this type of certificate will go through extensive vetting of the organization by the Certificate Authority, which may result in a longer processing time. With extended validation certificates, visitors to the website will see the address bar of the browser turn green, giving visitors immediate assurance that an organization's legal and physical existence was verified according to strict industry standards. This is best used by companies who highly value consumer trust for their business and websites that deal with sensitive customer information such as payment details.
Wildcard certificate	Wildcard certificates allow customers to protect a single domain and all of its subdomains under a single SSL certificate. For example, a wildcard certificate can be used to secure <i>mydomain.com</i> , <i>mail.mydomain.com</i> and <i>login.mydomain.com</i> . This is particularly useful for websites with a list of subdomains that will change over time as the certificate automatically covers all of the website's subdomains.
SAN certificate	SAN supported certificates allow you to protect other domains other than the primary domain using a single SSL certificate. For example, a single SAN supported certificate can be used to protect <i>mydomainone.com</i> , <i>mydomaintwo.com</i> , <i>mydomainthree.com</i> etc.

2. Before you can continue with your SSL certificate purchase, you must first generate a certificate signing request (CSR). See 'How to generate a CSR file' for instructions.
3. Together with the CSR, provide all required information and complete the purchase transaction. Once completed, the certificate request is sent to the Certificate Authority to validate and process the request. This may take a few minutes or up to a week, depending on the type of certificate purchased.
4. Once validated, the SSL certificate is sent to you and you can then install it to your server. See 'How to install SSL certificates' for instructions.

## How to generate a CSR file

### Using LINUX operating system

1. Create a private key (if you're ordering an EV certificate, you should use 2048-bit encryption instead of 1024 bit)

```
openssl genrsa -out subdomain.mydomain.com.key 1024
```

2. Create a CSR based on the previously created private key

```
openssl req -new -key subdomain.mydomain.com.key -out  
subdomain.mydomain.com.csr
```

3. Fill out the required fields as prompted. Please note that when creating a CSR for a wildcard certificate, Common Name should be *\*.mydomain.com* instead of a *subdomain.mydomain.com*.

Field	Description	Example
Country Name	2 Letter country code	CA
State or Province	Full state name	British Columbia
Locality	Full city name	Vancouver
Organization	Entity's legal name	
Organizational Unit	Optional, eg a department	
Common Name	Domain or entity name	mydomain.com

4. To review the provided information,

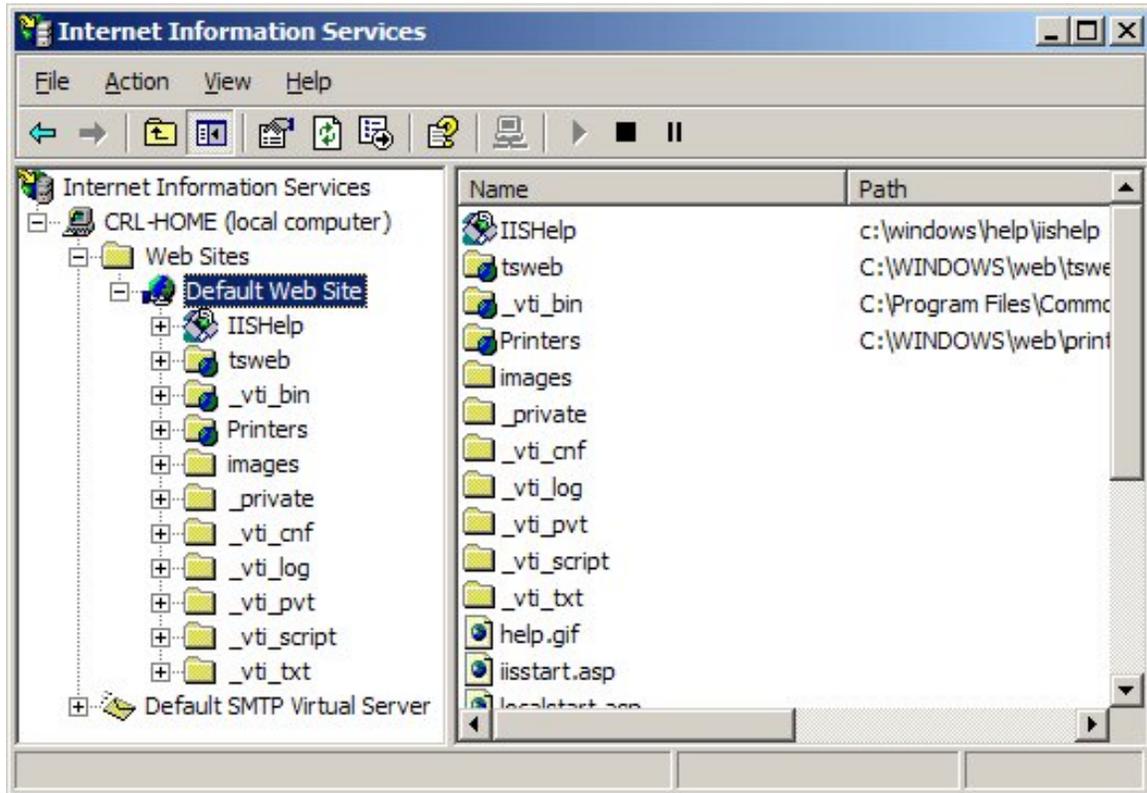
```
openssl req -noout -text -in subdomain.mydomain.com.csr
```

5. Your CSR is now available

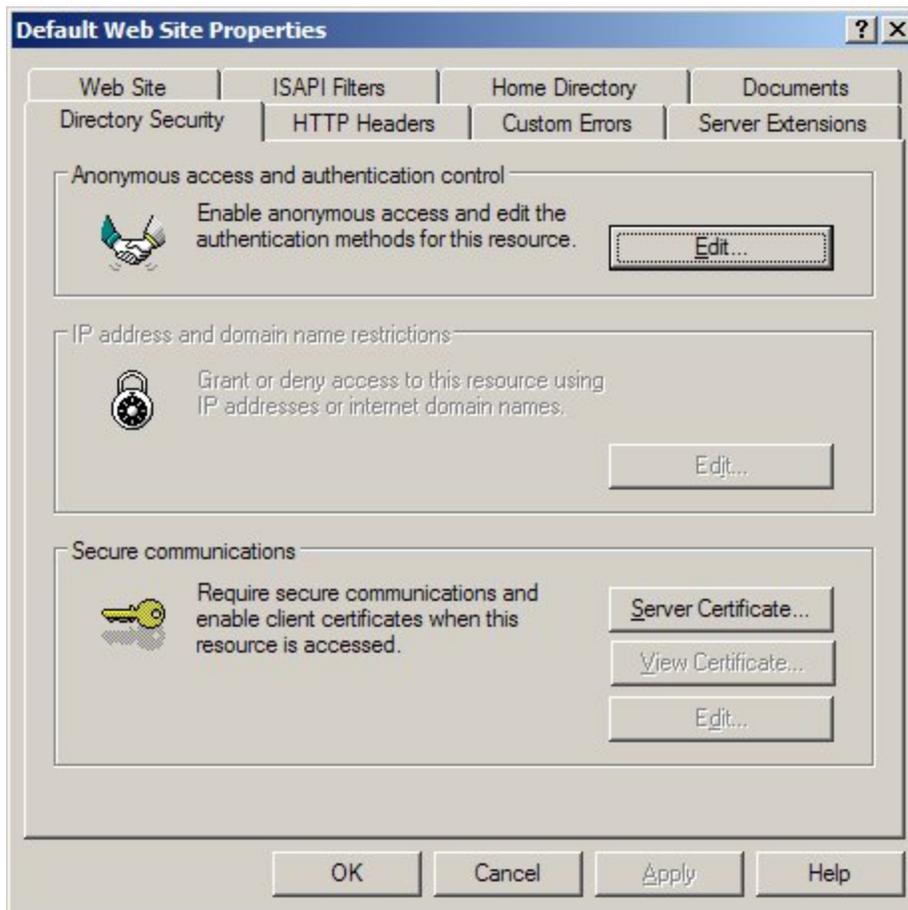
```
cat subdomain.mydomain.com.csr
```

## Using Windows operating system

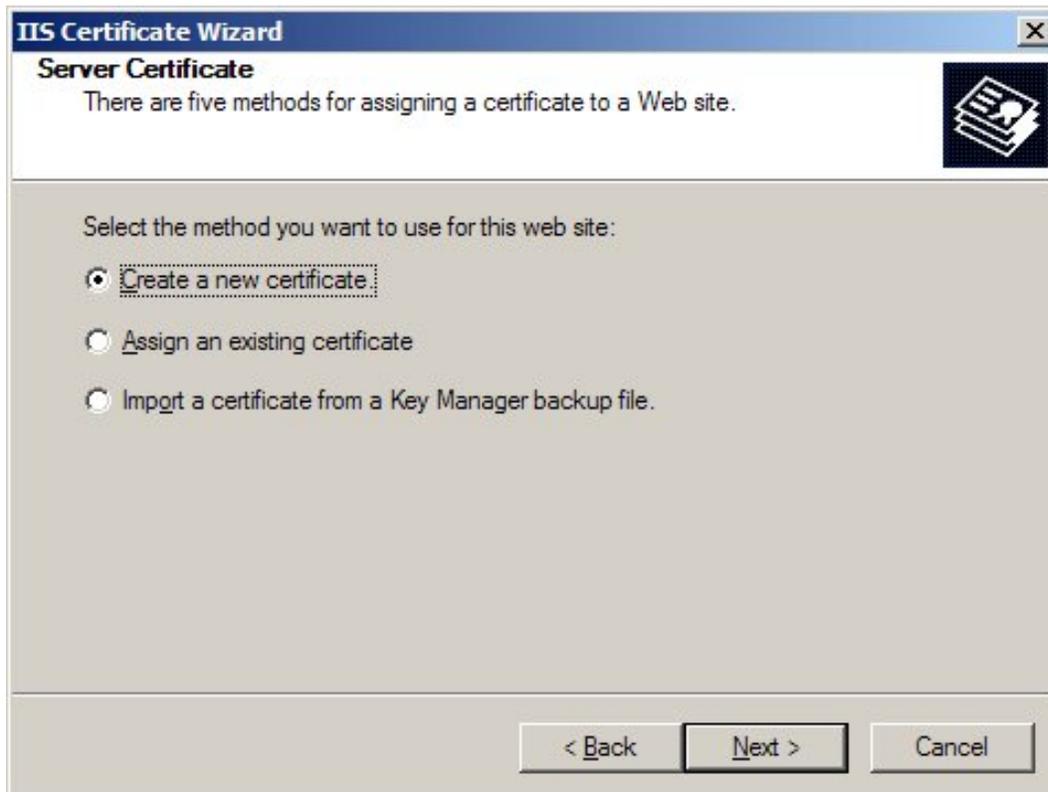
1. Select **Administrative Tools**.
2. Start **Internet Services Manager**.



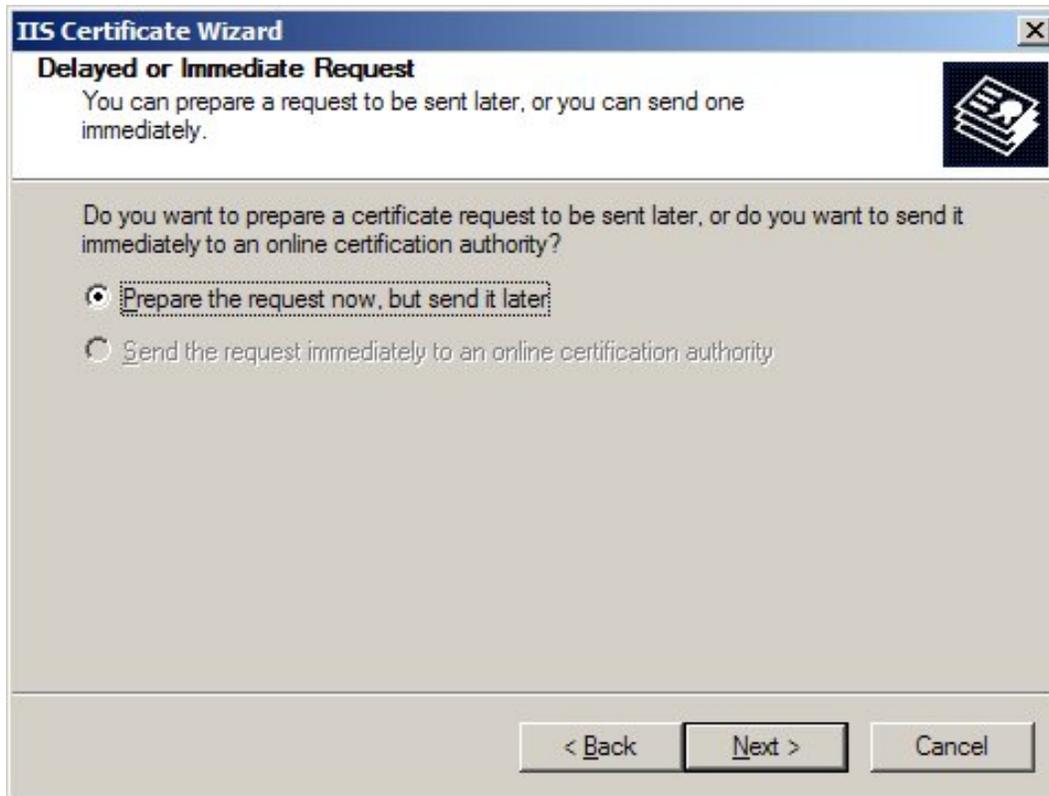
3. Open the properties window for the website the CSR is for. You can do this by right clicking on the Default Website and selecting Properties from the menu.
4. Open Directory Security by right clicking on the Directory Security tab.



5. Click **Server Certificate**. The following wizard will appear:



6. Click **Create a new certificate** and click **Next**.



**IIS Certificate Wizard** [X]

**Delayed or Immediate Request**

You can prepare a request to be sent later, or you can send one immediately.

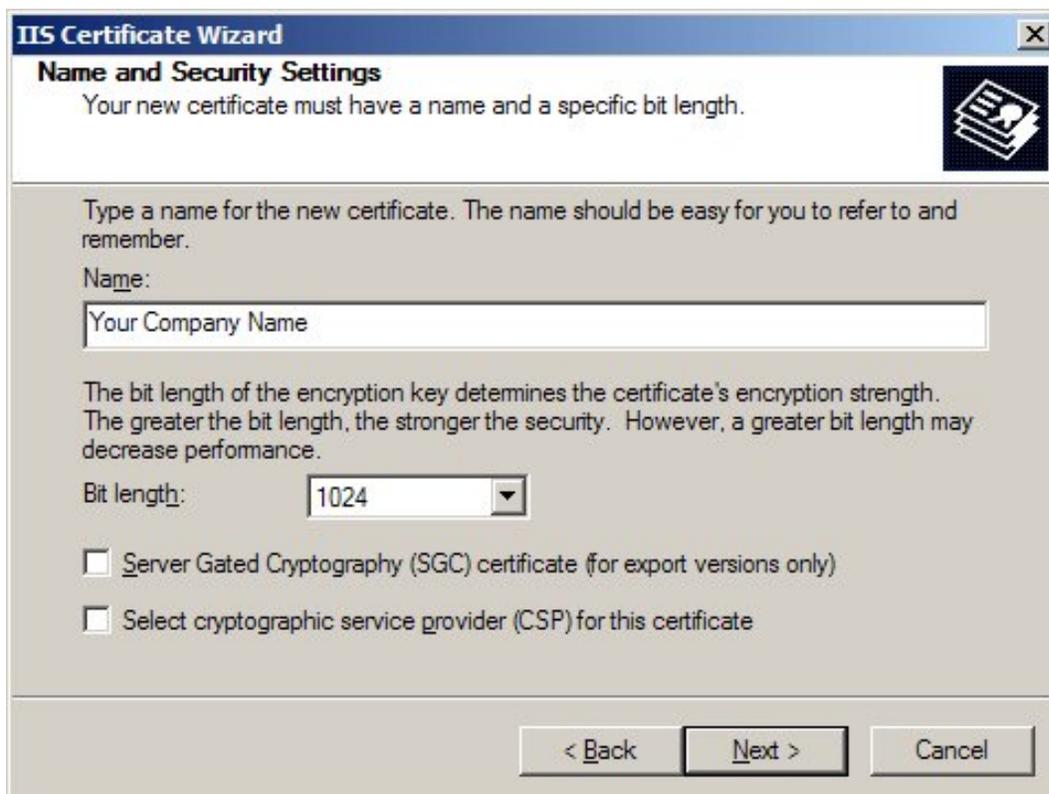
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

Prepare the request now, but send it later.

Send the request immediately to an online certification authority.

< Back   Next >   Cancel

7. Select Prepare the request and click **Next**.



**IIS Certificate Wizard** [X]

**Name and Security Settings**

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

Your Company Name

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

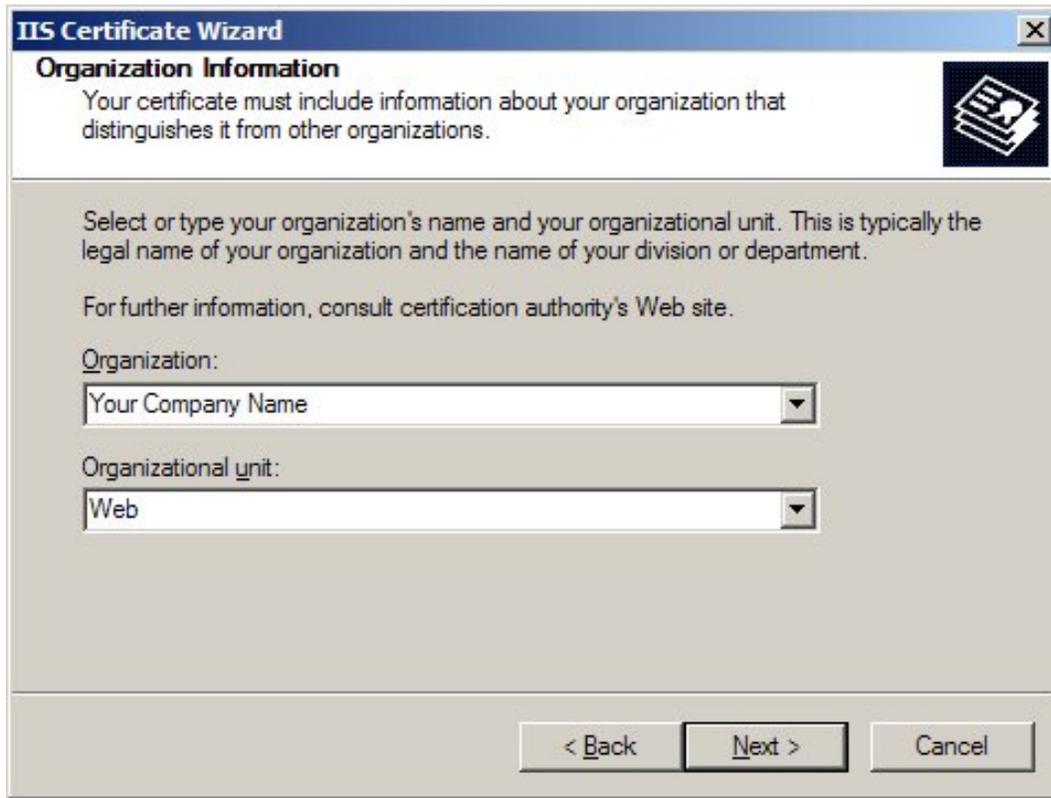
Bit length: 1024

Server Gated Cryptography (SGC) certificate (for export versions only)

Select cryptographic service provider (CSP) for this certificate

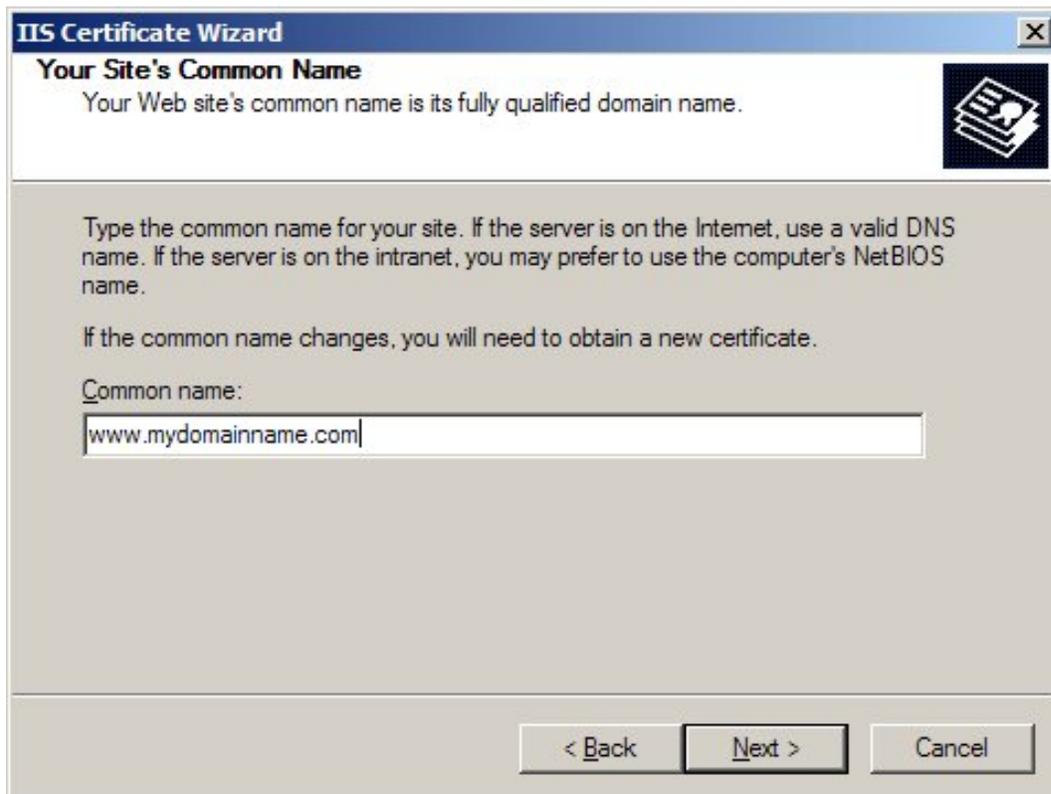
< Back   Next >   Cancel

8. Provide a name for the certificate, this needs to be easily identifiable if you are working with multiple domains. This is for your records only.
9. If your server is 40 bit enabled, you will generate a 512 bit key. If your server is 128 bit you can generate up to 1024 bit keys. We recommend you stay with the default of 1024 bit key if the option is available. Click **Next**.



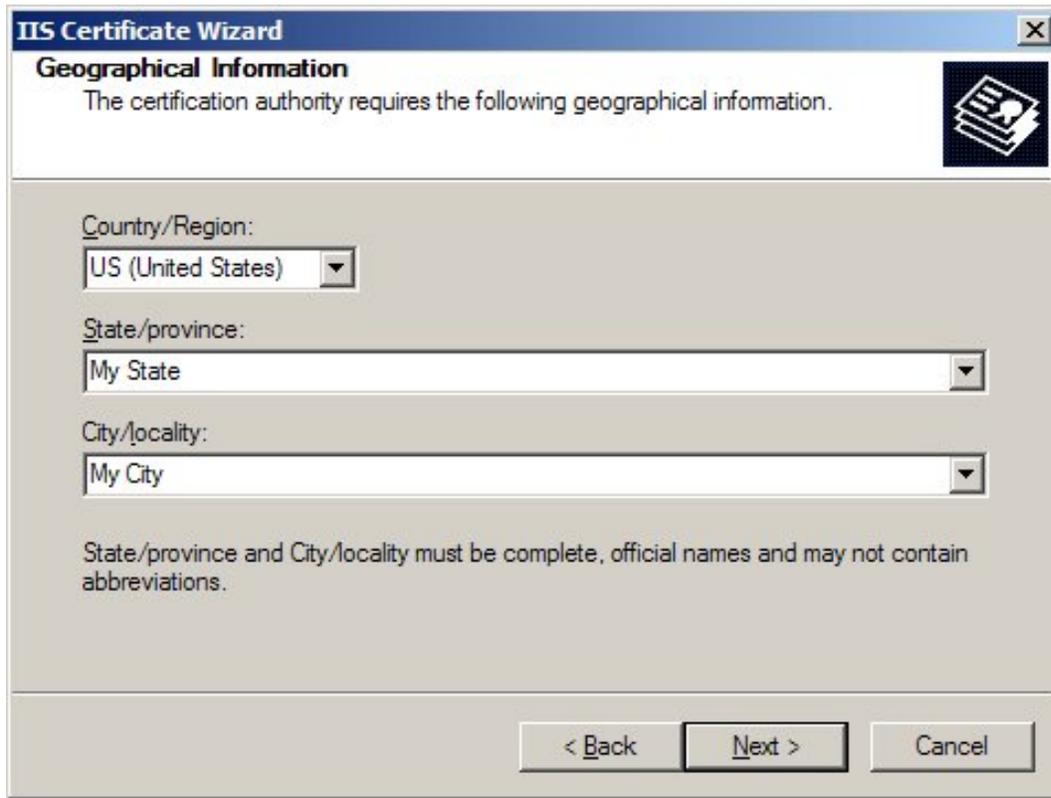
The screenshot shows the 'IIS Certificate Wizard' window at the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the section is titled 'Organization Information' with a sub-header 'Your certificate must include information about your organization that distinguishes it from other organizations.' To the right of this text is an icon of a certificate. The main area contains instructions: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' and 'For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization:' with the value 'Your Company Name' and 'Organizational unit:' with the value 'Web'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

10. Enter **Organization** and **Organization Unit**, these are your company name and department respectively. Click **Next**.



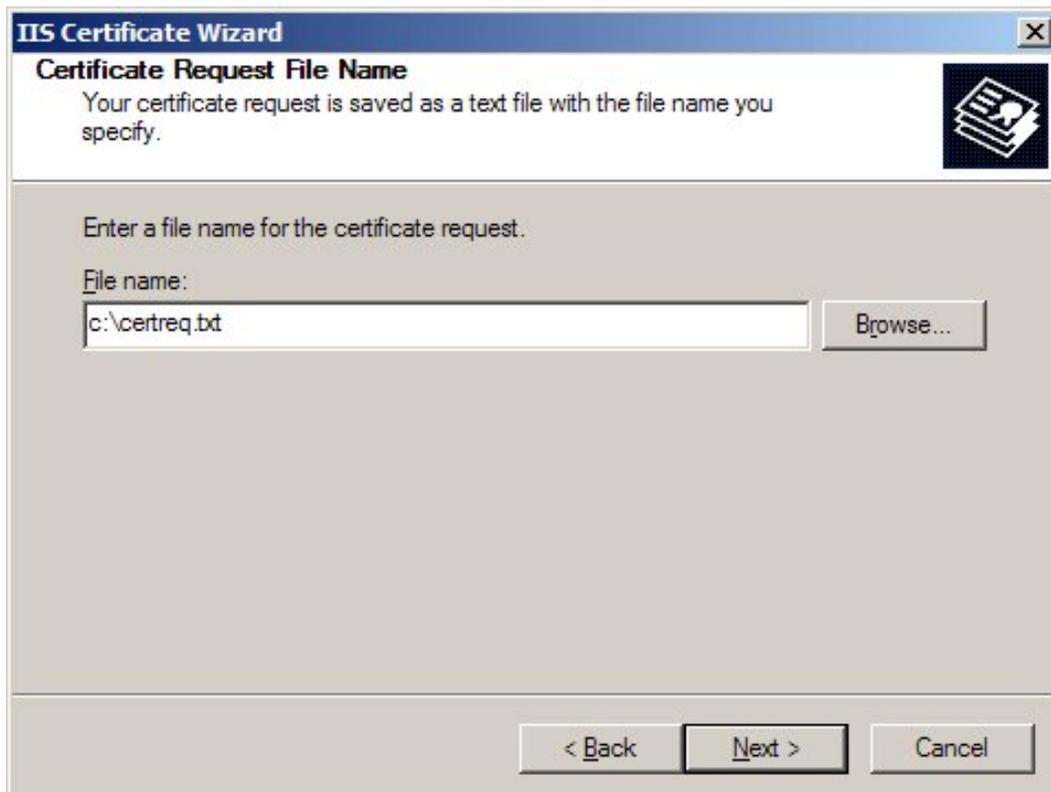
The screenshot shows the 'IIS Certificate Wizard' window at the 'Your Site's Common Name' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the section is titled 'Your Site's Common Name' with a sub-header 'Your Web site's common name is its fully qualified domain name.' To the right of this text is an icon of a certificate. The main area contains instructions: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.' and 'If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' containing the text 'www.mydomainname.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

11. The Common Name field should be the Fully Qualified Domain Name (FQDN) or the web address for which you plan to use your IIS SSL Certificate, e.g. the area of your site you wish customers to connect to using SSL certificate. Click **Next**.



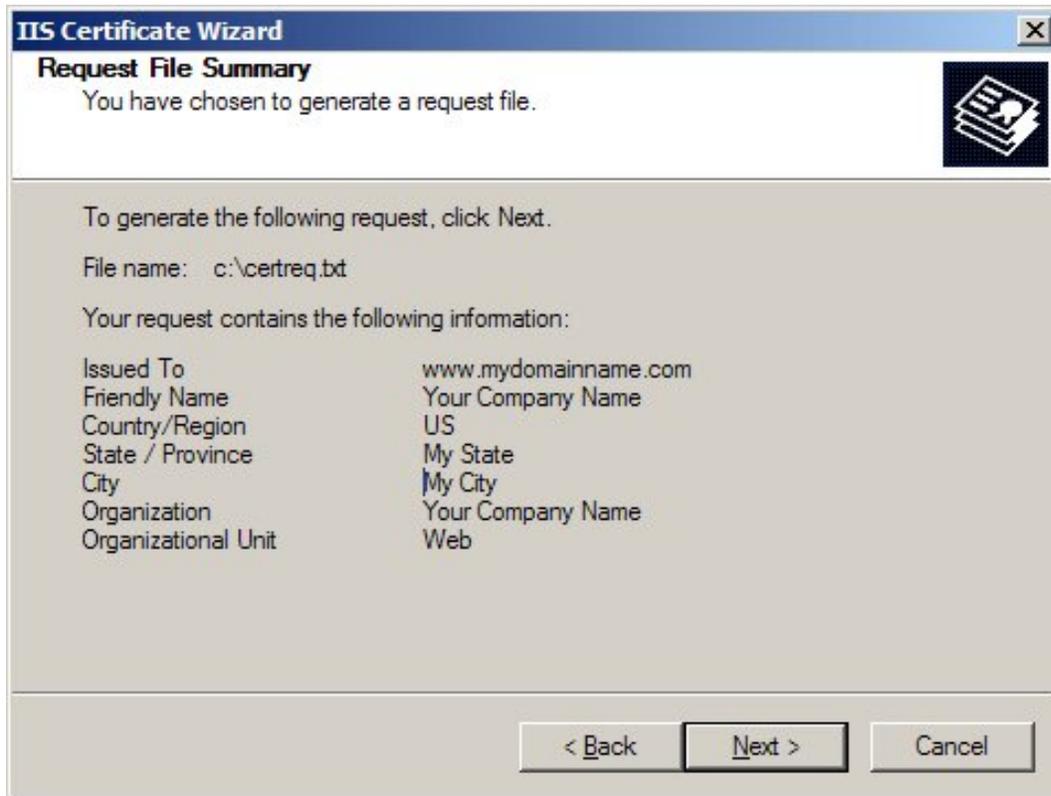
The screenshot shows the 'IIS Certificate Wizard' window at the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard' and the window has a close button. The main heading is 'Geographical Information' with a sub-heading 'The certification authority requires the following geographical information.' and an icon of a certificate. Below this, there are three dropdown menus: 'Country/Region:' with 'US (United States)', 'State/province:' with 'My State', and 'City/locality:' with 'My City'. A note states: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

12. Enter your **country**, **state** and **city**. Click **Next**.



The screenshot shows the 'IIS Certificate Wizard' window at the 'Certificate Request File Name' step. The title bar reads 'IIS Certificate Wizard' and the window has a close button. The main heading is 'Certificate Request File Name' with a sub-heading 'Your certificate request is saved as a text file with the file name you specify.' and an icon of a certificate. Below this, there is a text input field with the prompt 'Enter a file name for the certificate request.' and the text 'c:\certreq.txt'. To the right of the input field is a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

13. Enter a filename and location to save your CSR. You will need this CSR to enroll for your IIS SSL Certificate. Click **Next**.



14. Check the details you have entered. If you have made a mistake click **Back** and amend the details. Be especially sure to check the domain name the Certificate is to be "Issued To". Your IIS SSL Certificate will only work on this domain. Click **Next** when you are happy the details are absolutely correct.
15. When you make your application, make sure you include the CSR in its entirety into the appropriate section of the enrollment form - including

```
-----BEGIN CERTIFICATE REQUEST-----
```

to

```
-----END CERTIFICATE REQUEST-----
```

16. Click **Next**.
17. Confirm your details in the enrollment form.
18. To save your private key
- Go to **Certificates snap** in the MMC
  - Select **Requests > All tasks > Export**.

## How to install SSL certificates

### Apache

Note that the location of webserver configuration file may be different than what is specified below as it may vary depending on your operating system

1. Add the SSL certificate file to the designated directory. For example, `/usr/local/apache/conf/ssl.crt` or `/etc/httpd/conf/ssl.crt`.
2. Open **httpd.conf** file in a text editor.
3. Locate the secure virtual host pertaining to your order. You should have the following directives within this virtual host (otherwise, please add them).

```
SSLCertificateFile /usr/local/apache/conf/ssl.crt/mydomain.com.crt
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/mydomain.com.key
```

For Comodo certificates:

```
SSLCertificateChainFile /usr/local/apache/conf/ssl.key/mydomain.com.ca
```

4. Save the changes and exit the editor.
5. Restart your Apache web server (*Default: `/usr/local/apache/bin/apachectl startssl` or `/usr/local/apache/bin/apachectl restart`*).
6. Test your SSL certificate by connecting to your server. Use the https protocol directive (for example, <https://yourserver/>).

## Apache 2

Note that the location of webserver configuration file may be different than what is specified below as it may vary depending on your operating system

1. Add the SSL certificate file to the designated directory. For example, `/usr/local/apache2/conf/ssl.crt`.
2. Open **apache2.conf** file in a text editor.
3. Locate the secure virtual host pertaining to your order. You should have the following directives within this virtual host (otherwise, please add them).

```
SSLCertificateFile /usr/local/apache2/conf/ssl.crt/mydomain.com.crt
SSLCertificateKeyFile /usr/local/apache2/conf/ssl.key/mydomain.com.key
```

For Comodo certificates,

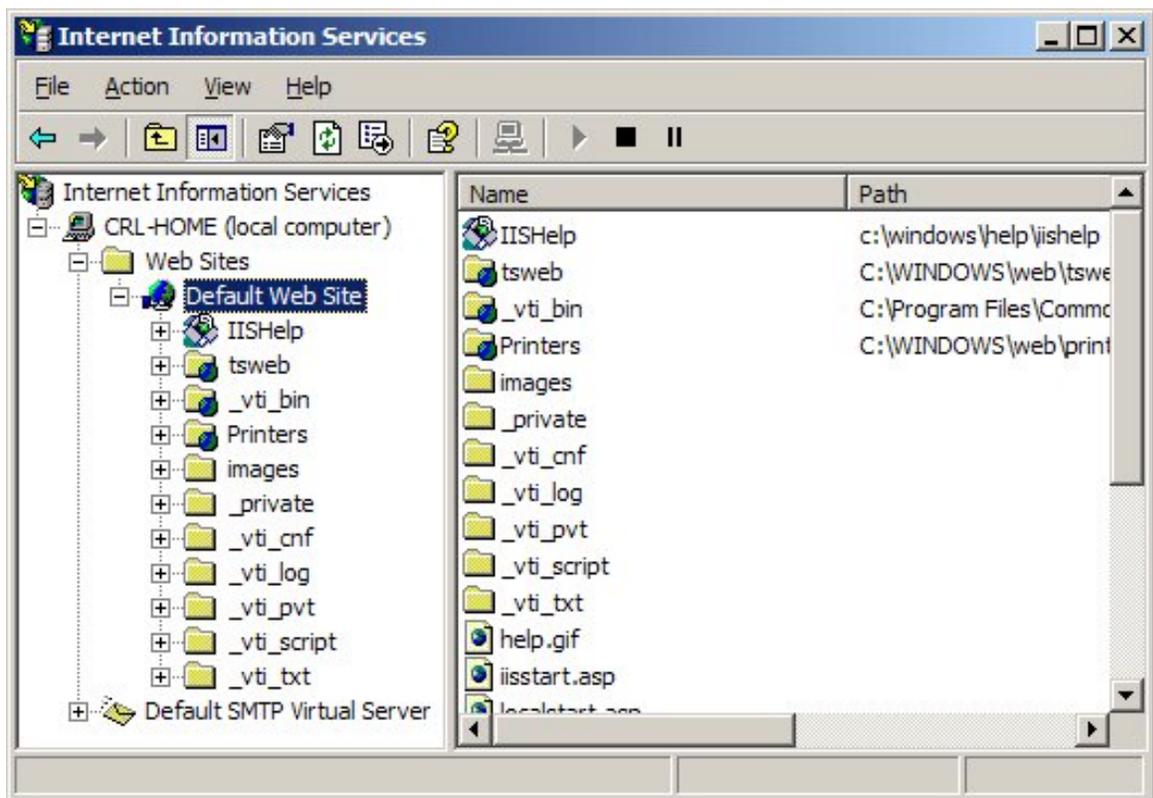
```
SSLCertificateChainFile /usr/local/apache/conf/ssl.key/mydomain.com.ca
```

4. Save the changes and exit the editor.
5. Restart your apache web server (*Default: `/usr/local/apache2/bin/apachectl stop` and `/usr/local/apache2/bin/apachectl start`*).
6. Test your SSL certificate by connecting to your server. Use the https protocol directive (for example, <https://yourserver/>).

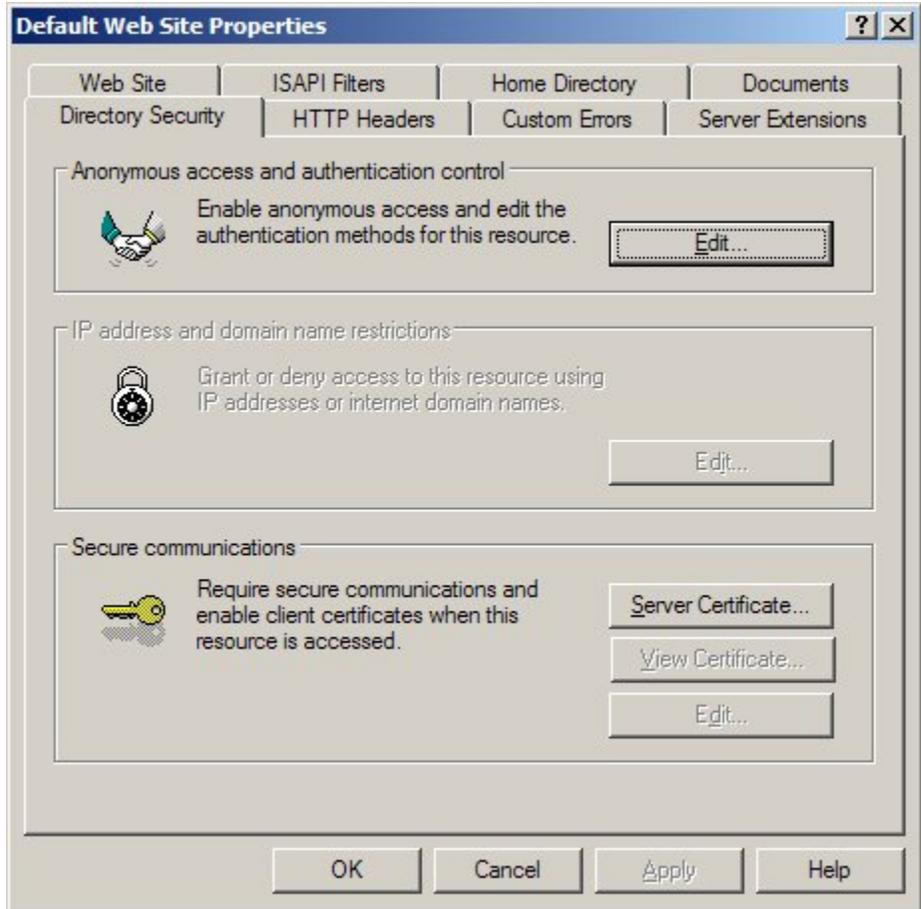
Further information can be found in the [official apache documentation](#).

## Microsoft IIS

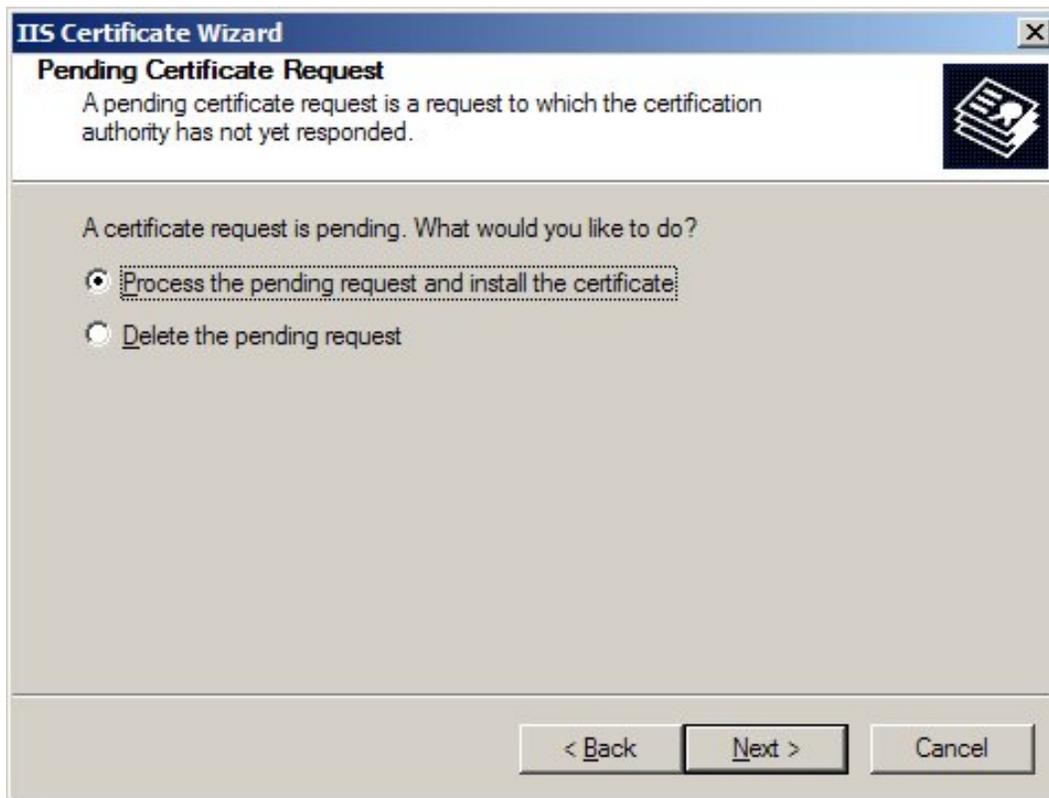
1. Select **Administrative Tools**.
2. Select **Internet Services Manager**.



3. Right click on Default Website and select Properties from the menu.
4. Right click on **Directory Security** tab.



5. Click on **Server Certificate**. The following wizard will appear:



6. Select Process the pending request and install the certificate option. Click Next.
7. Select the location of your SSL certificate and click **Next**.
8. Make sure that you are processing the right SSL certificate and all information is accurate. Click **Next**.
9. You will see a confirmation screen. When you have read the information, click **Next**.
10. Your SSL certificate is now installed on your server.

Note that you must restart your computer to complete the installation process.