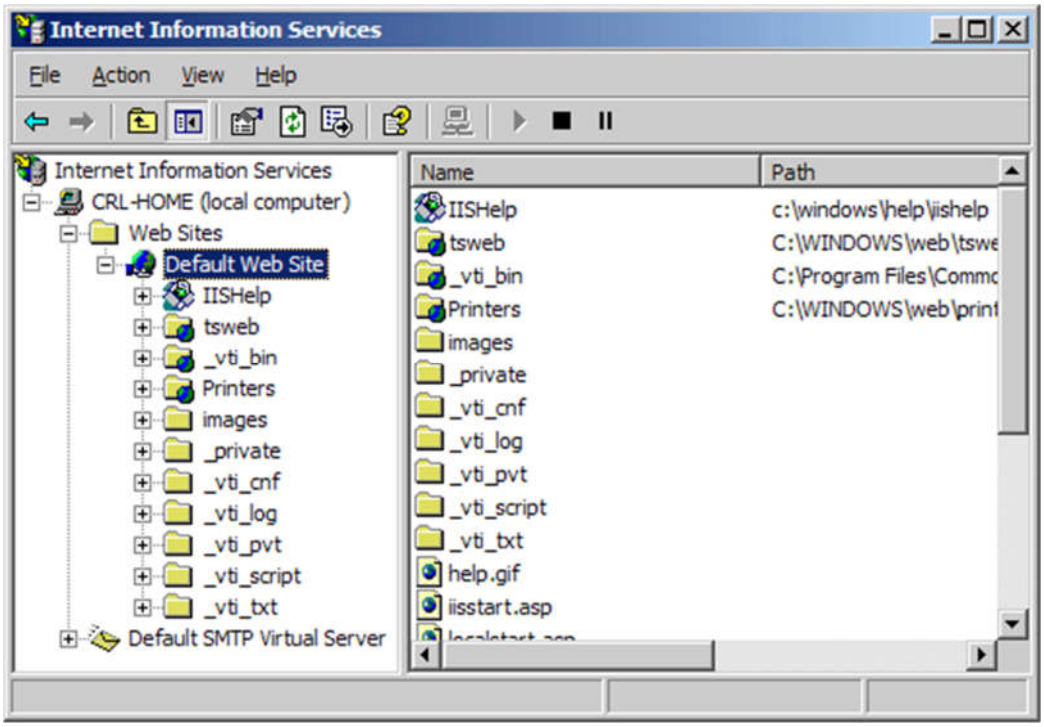
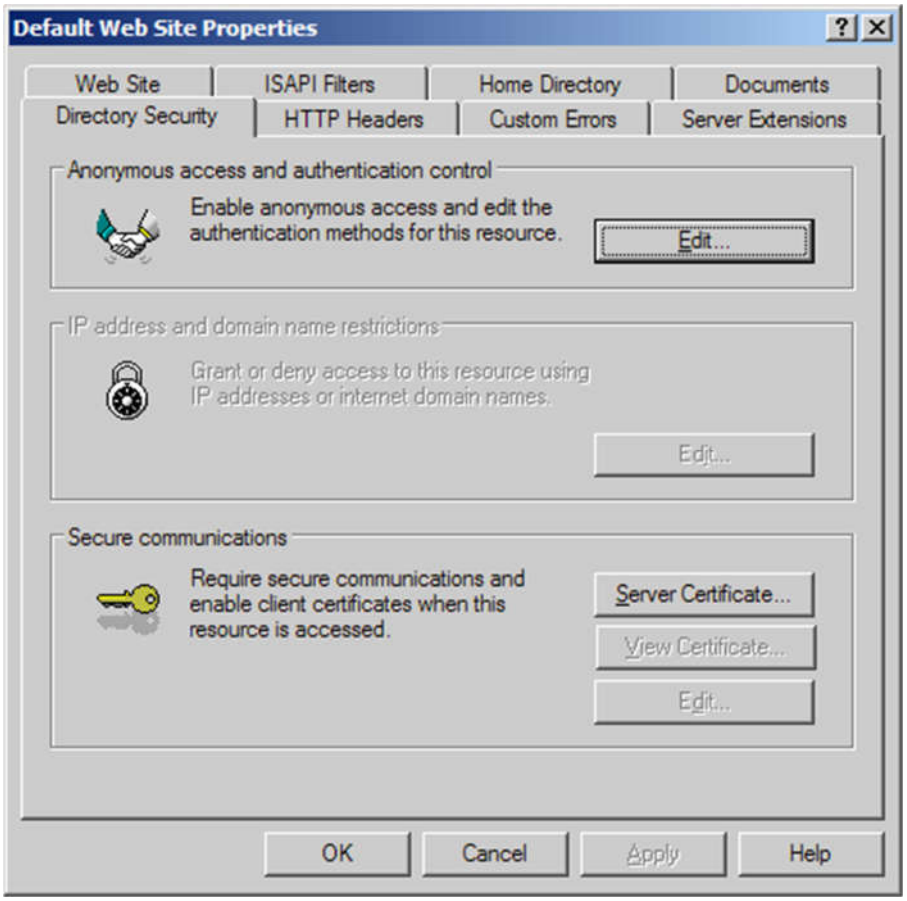
IIS 5-6 Web Server CSR Creation and Installation

How to generate a CSR in IIS 5.x or 6.x Web Server

1. From the Administrative Tools in the Control Panel, run Internet Information Services.

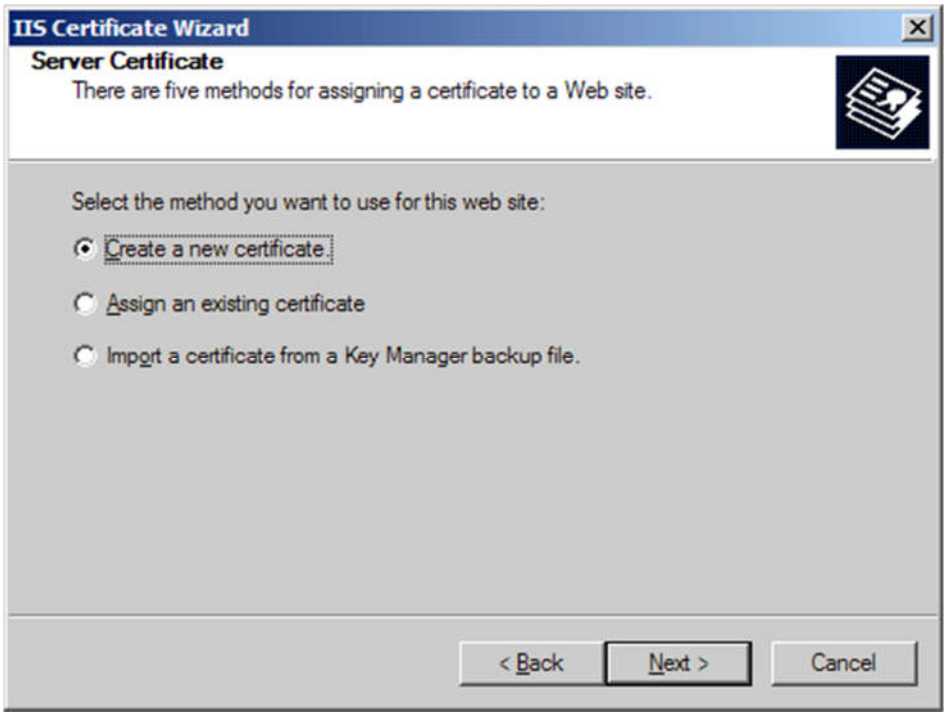


2. Right-click on the website you are securing, and select Properties. Click on the Directory Security tab, and hit the Server Certificate button.

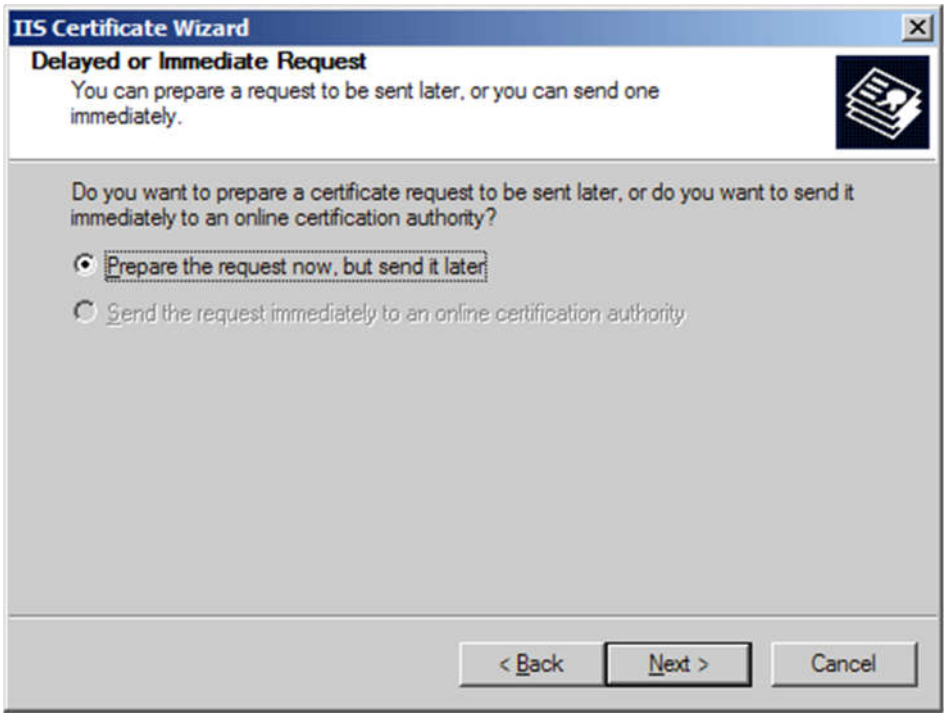


3. Click next. Choose 'Create a new certificate' and hit next.

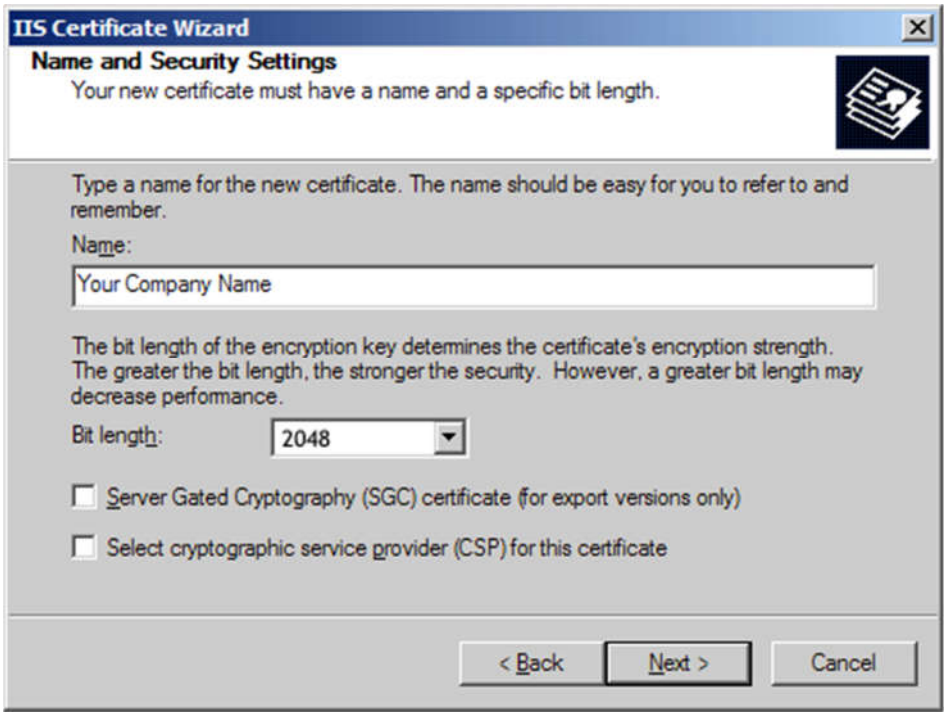
   If you are renewing an existing certificate, you will instead see the option to Renew, Remove, or Replace your certificate. Choose the option to Renew and skip over steps 5-8.



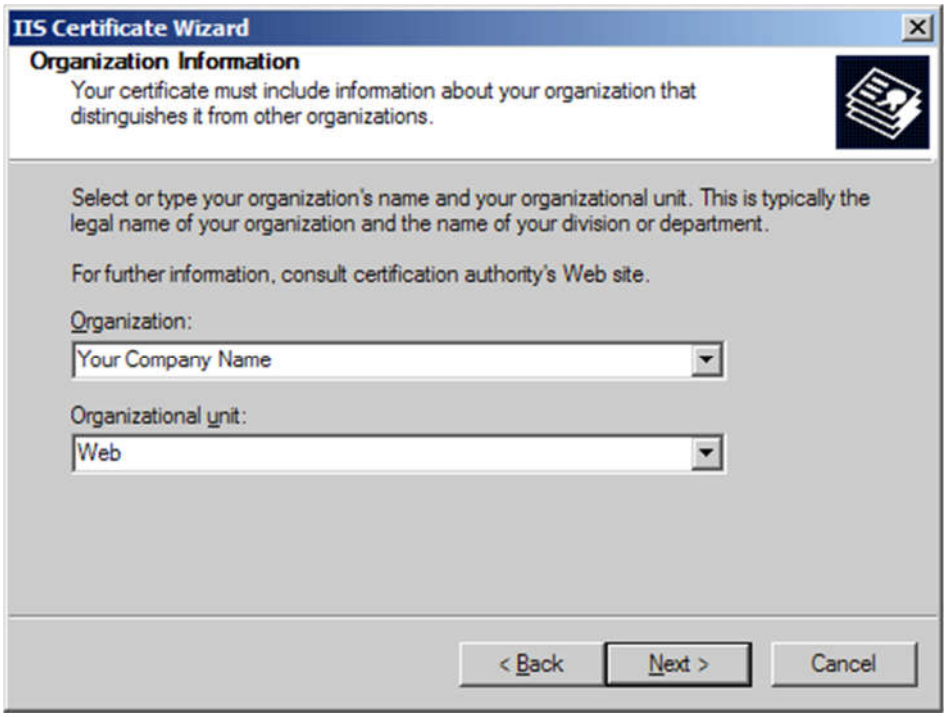
4. Choose 'Prepare the request now, but send it later' and hit next.



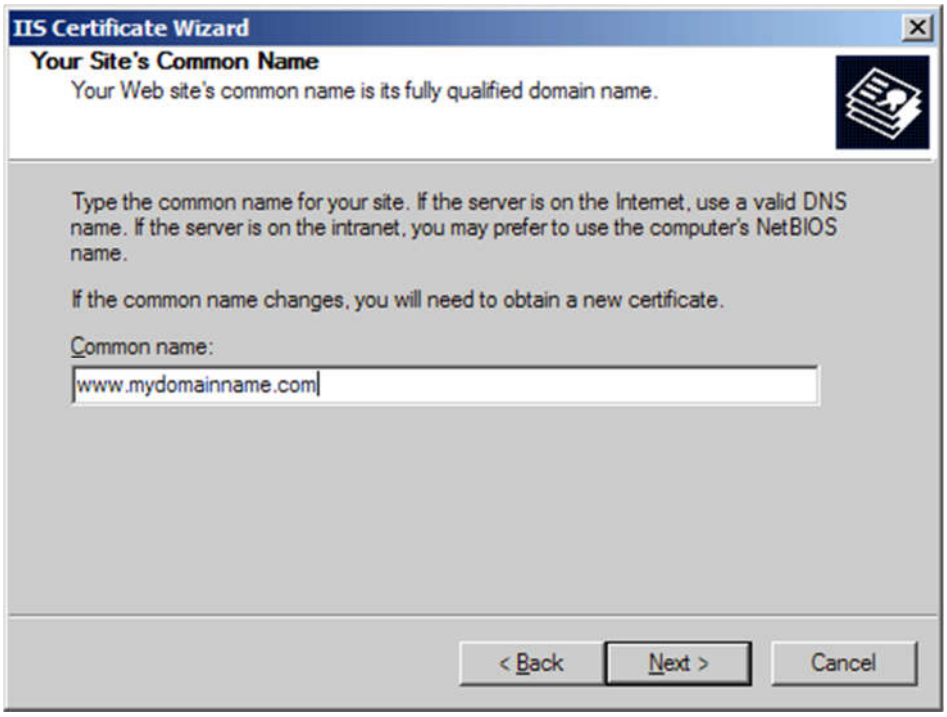
5. Enter a name for the certificate that you can identify on your server. Choose a bit-length of 2048. Leave the other boxes un-checked.



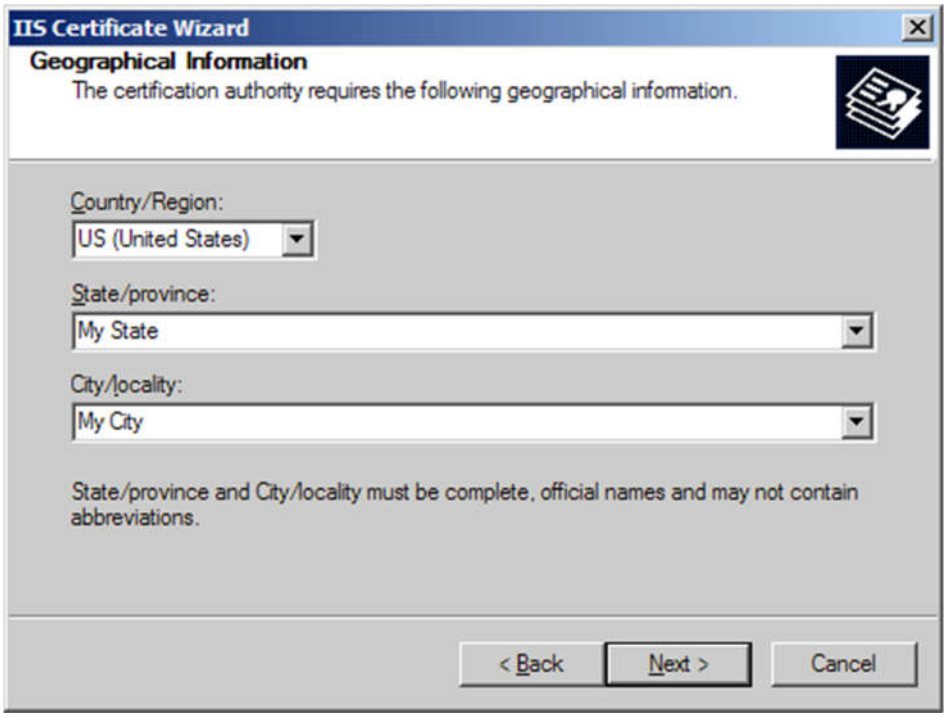
6. Enter the full legal name of your company. Enter a department such as 'Security' or 'IT' in the organizational unit.



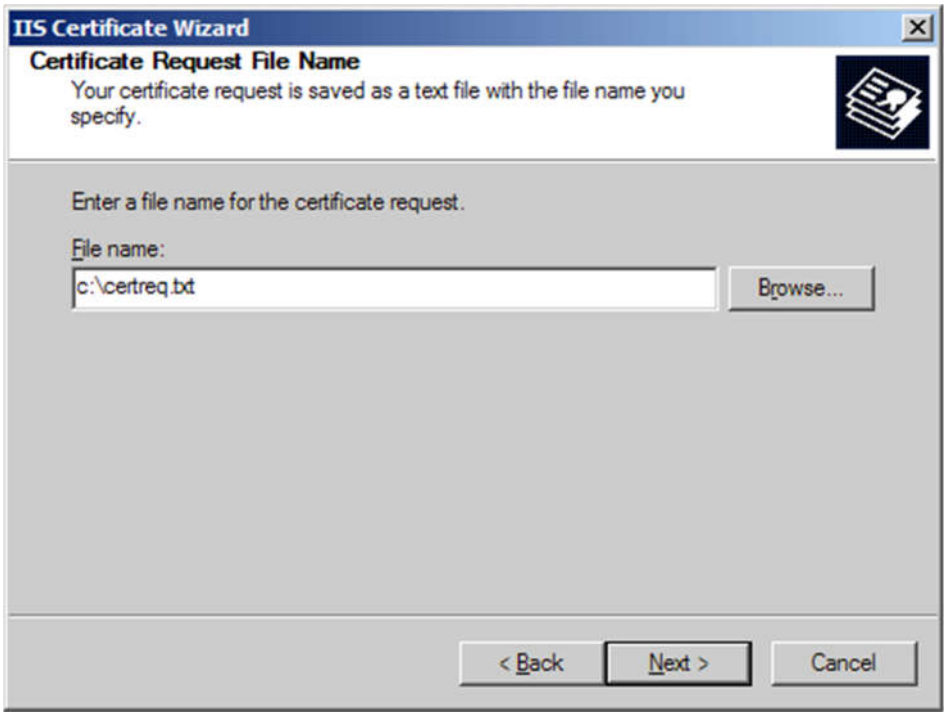
7. Enter the fully qualified domain name of your site (ex: www.yourdomain.com)



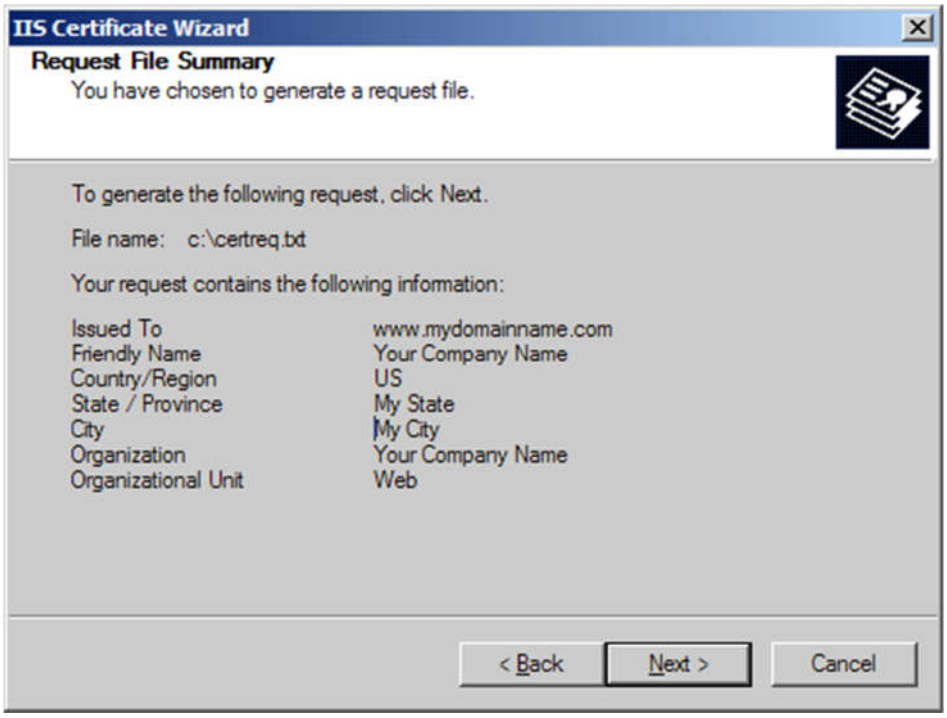
8. Enter the location of your organization: Country, State, and City.



9. Choose a file name and a location to save your SSL Certificate Signing Request (CSR). The file should be saved as a text file (.txt)



10. Click next to generate the file.



11. Please send the CSR file to us for our process.

**** Important ** - When you have completed the steps above a "pending request" will be created on your website. This "pending request" MUST NOT BE DELETED. Later, when your certificate is**

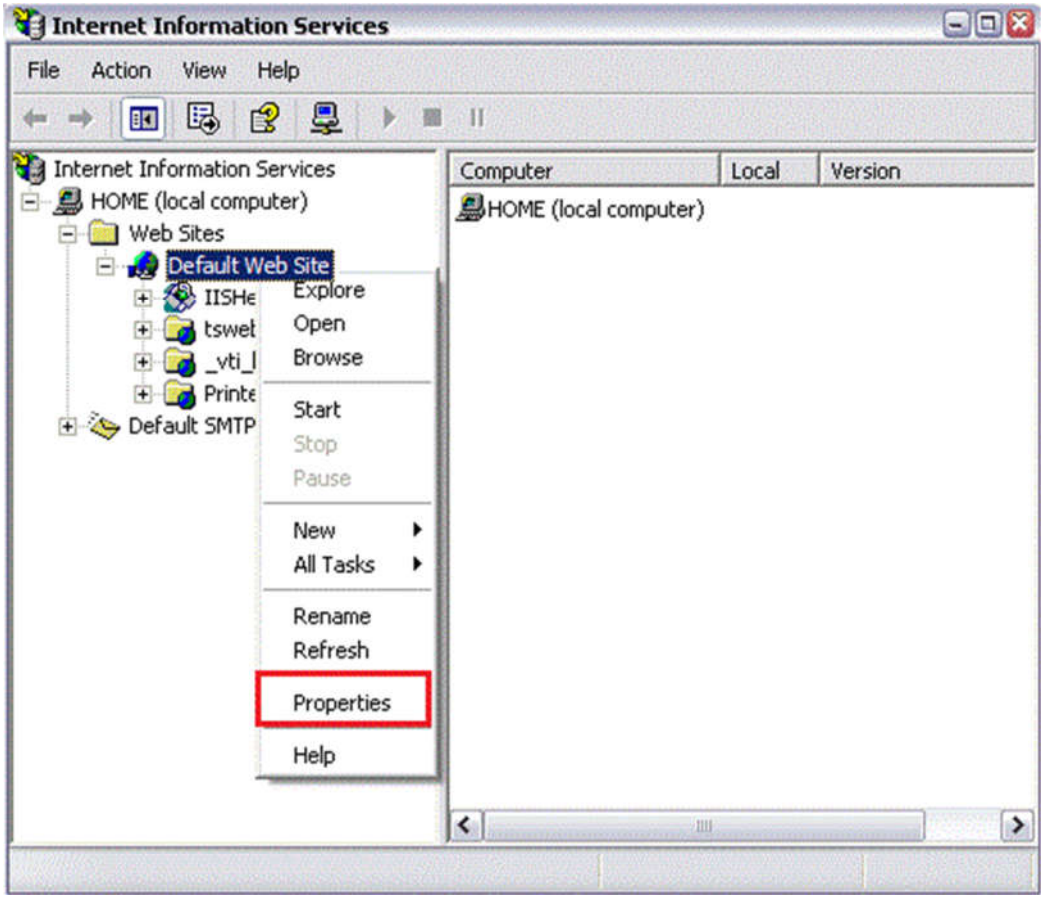
issued, you must install the certificate to this exact pending request or the certificate will not be functional.

How to install your SSL Certificate to your IIS 5 & 6

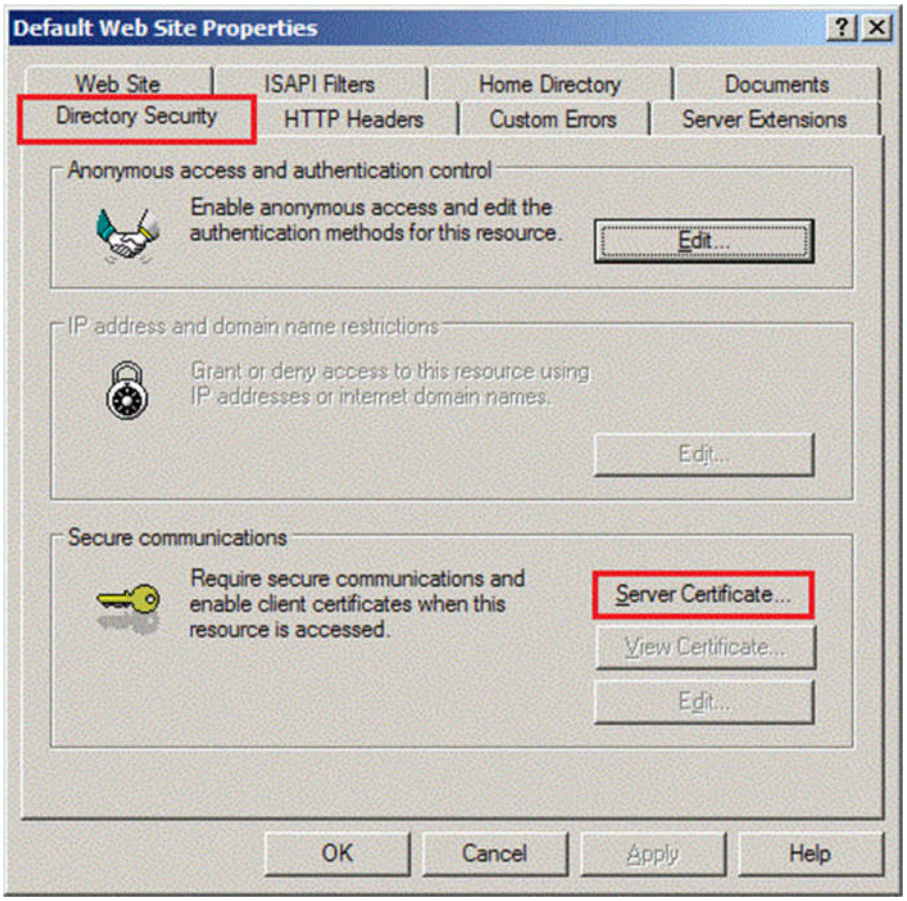
Install your Certificate:

1. Open the ZIP file containing your certificate and copy the file named your_domain_name.cer to the desktop of the web server you are securing.

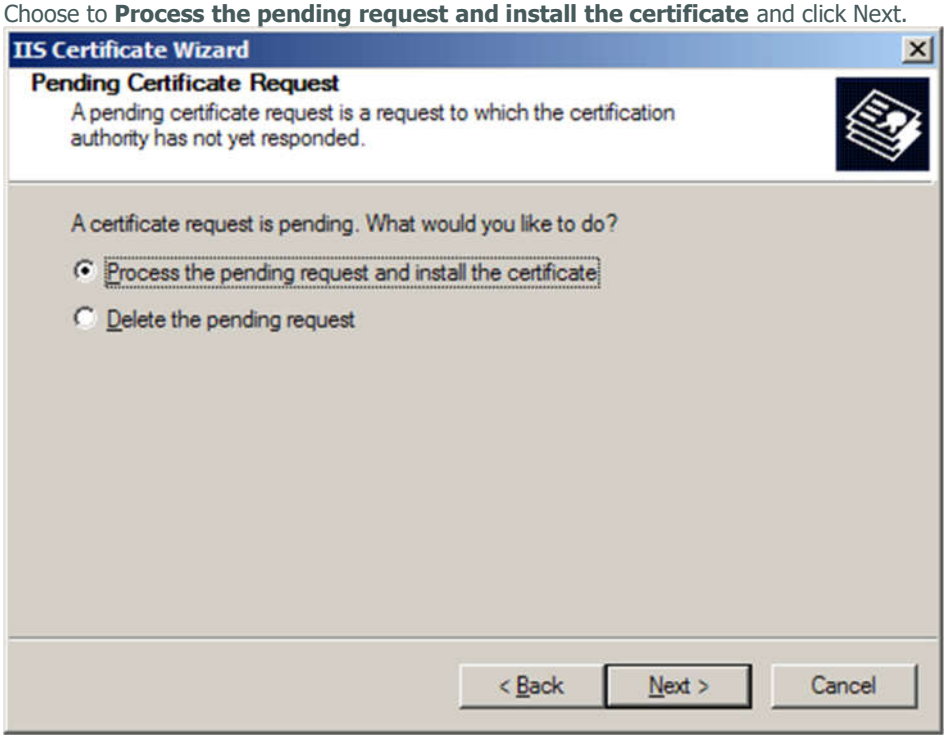
2. Go to your Administrative Tools, and Open the Internet Services Manager. Right-Click on the Default Website or the website that the CSR was created on and select Properties. The certificate will only be able to be installed on the same website that you created the CSR on.



3. Go to the Directory Security panel. Click on the "Server Certificate..." button. This will start the certificate wizard. Click "Next".



4. Choose to **Process the pending request and install the certificate** and click Next.



5. "Browse" for your SSL Certificate. Locate your_domain_name.cer, then Click Next. Follow the rest of the wizard steps until finished.

Test your certificate

The best way to test your certificate using a browser is to visit its secure URL with a browser other than Internet Explorer. We recommend this because Internet Explorer is able to verify your site is trusted with or without the intermediate certificate, but most other browsers cannot do this. If other browsers complain about your site not being trusted, but Internet Explorer does not, then you most likely need to install the intermediate certificate (instructions below).

Note for ISA users: If you are using ISA 2004 or 2006 and your server is not sending the intermediate certificate, you need to fully reboot your server. We have confirmed this to be true with many customers: ISA server will not properly send the intermedate certificate chain until after a full reboot.

If you notice that the server continues to use an old certificate or the server will not load https at all then you may need to shutdown and restart the server.

Backup the certificate and private key (Recommended)

It is always good to keep a backup of your certificate and private key in case your server crashes. You must backup your certificate from your server in order to include a backup of your private key. The private key is not included in your certificate files, and the certificate is not functional without the private key.

To backup your SSL Certificate and private key, we recommend you refer to our PFX export instructions or help backing up your certificates and private key as a .pfx file.

Import the Intermediate Certificate (Not required for most installations)

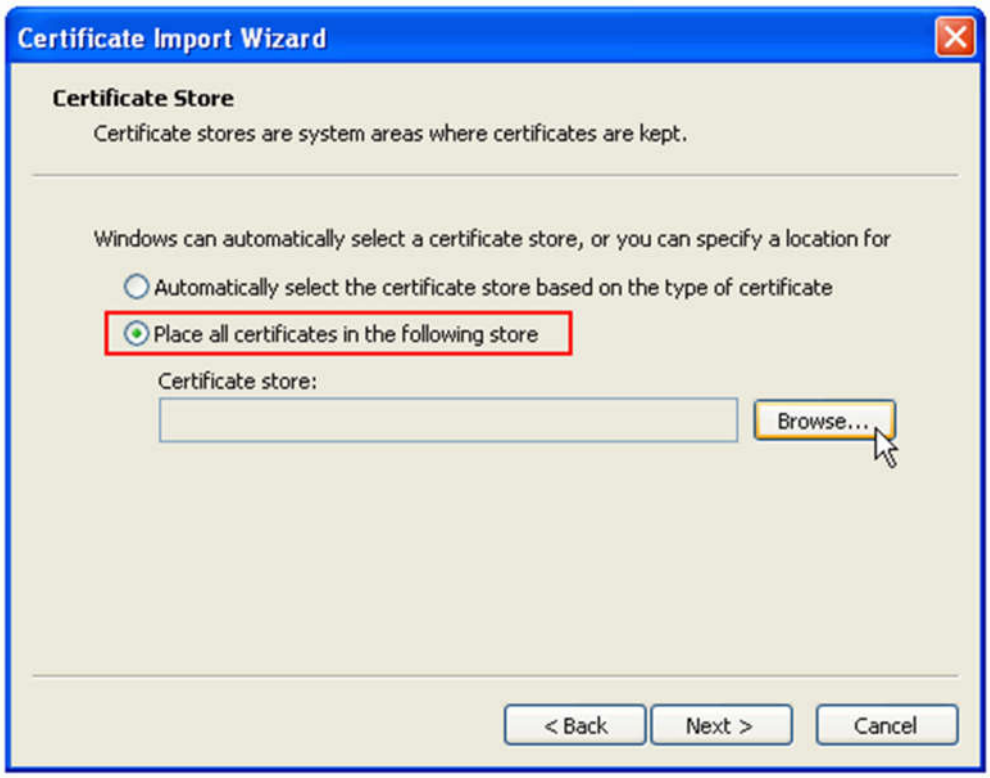
Because the Intermediate Certificate is built into your_domain_name.cer, this step should not be necessary for most installations. When the certificate is correctly installed to your server browsers will not display any certificate warnings whatsoever. However, if your clients are getting a warning stating that the certificate was issued by a company that you have not chosen to trust, then the following procedure will fix that problem.

1. Save the IntermediateCA.crt to your desktop.

2. Double-click the certificate. This will open the certificate to view.

3. At the bottom of the General tab, click the "Install Certificate..." button. This will start the certificate import wizard. Click "Next".

4. Choose to "Place all certificates in the following store", and click "Browse".



5. First, click the "Show physical stores" box, then expand the Intermediate Certification Authorities folder, select the underlying Local Computer folder, and click ok. Hit "Next", then "Finish"

6. Your intermediate certificate is now installed. You may need to restart your server.