

Using **InstantSSL** to boost
Customer Confidence in your web services

For Microsoft IIS5 webserver

www.instantssl.com
www.comodogroup.com

support@comodogroup.com



Tel: (877) COMODO-5

Tel: +44 (0) 161 874 7070

Why you need **security** for your website

The Internet has created many new global business opportunities for enterprises conducting online commerce. However, the many security risks associated with conducting e-commerce have resulted in security becoming a major factor for online success or failure.

Over the past 7 years, consumer magazines, industry bodies and security providers have educated the market on the basics of online security. The majority of consumers now expect security to be integrated into any online service they use, as a result they expect any details they provide via the Internet to remain confidential and integral. For many customers, the only time they will ever consider buying your products or services online is when they are satisfied their details are secure.

This guide explains how you can utilize InstantSSL to activate the core security technology available on your existing webserver. You will also learn how InstantSSL allows you to protect your customer's transactions and provide visitors with proof of your digital identity – essential factors in gaining confidence in your services and identity.

Using InstantSSL Certificates to secure your online transactions tells your customers you take their security seriously. They will visibly see that their online transaction will be secure, confidential and integral and give them the confidence that you have removed the risk associated with trading over the Internet.

Using Security helps you realize the benefits of online commerce:

- Cost effectiveness of online operations and delivery
- Open global markets – gain customers from all over the world
- New and exciting ways of marketing directly to your customers
- Offer new data products and services via the Web

Only if you have visibly secured your site with SSL security technology will your customers have confidence in your online operations. Read on to learn how SSL helps you achieve the confidence essential to successful e-commerce.

What is SSL?

Secure Sockets Layer, SSL, is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an SSL Certificate.

When you choose to activate SSL on your webserver you will be prompted to complete a number of questions about the identity of your website (e.g. your website's URL) and your company (e.g. your company's name and location). Your webserver then creates two cryptographic keys – a Private Key and a Public Key. Your Private Key is so called for a reason – it must remain private and secure. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) – a data file also containing your details. You should then submit the CSR during the SSL Certificate application process Comodo, the InstantSSL Certification Authority, who will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL.

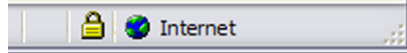
Your webserver will match your issued SSL Certificate to your Private Key. Your webserver will then be able to establish an encrypted link between the website and your customer's web browser.

For detailed application and installation instructions please refer to section "Step by step instructions to set up SSL on your webserver" of this guide.

“SSL is the de facto web transaction security technology. Webservers have been built to support it; web browsers have been built to use it. Secure your customers transactions transparently without your customers having to do a thing!

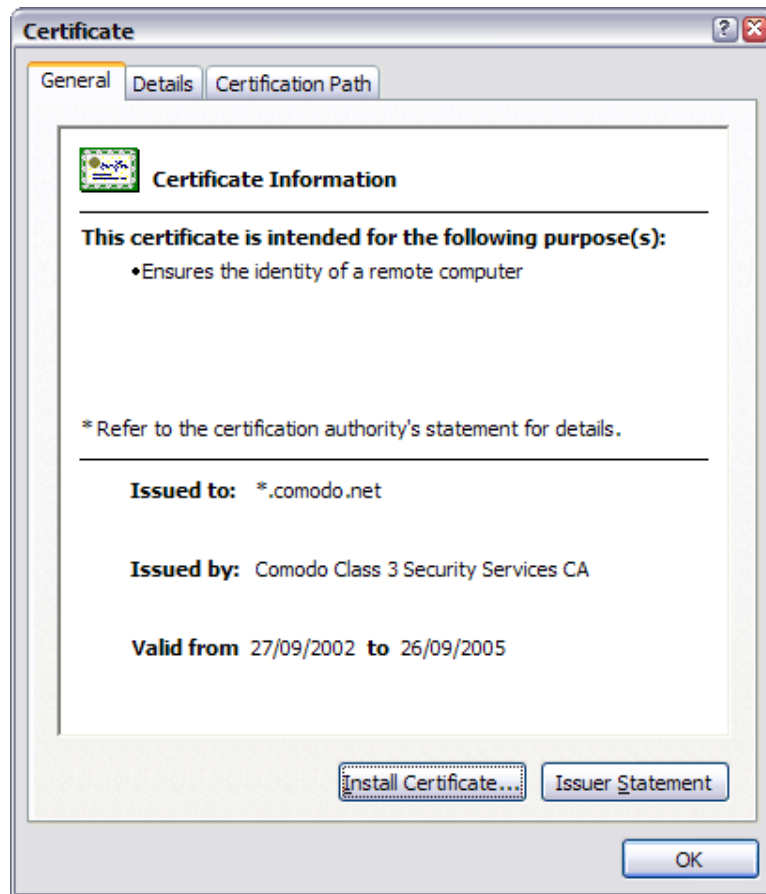
Displaying the SSL secure padlock

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session – the Padlock:



As seen by users of Internet Explorer

Clicking on the Padlock displays your SSL Certificate and your details:



As seen by users of Internet Explorer

All SSL Certificates are issued to either companies or legally accountable individuals. Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiry date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate.

When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user.

Why should you use an **InstantSSL Certificate**?

“Starting at only \$49 per year per Certificate, with additional bulk and multi-year discounts available, InstantSSL provide the most cost effective fully validated and fully supported Certificates available.”

Comodo, the Certification Authority behind InstantSSL, is the fastest growing SSL Provider in the world. Unlike other Certification Authorities, Comodo does not just provide SSL Certificates – they are a world-renowned security and cryptography service provider. When you are a customer of Comodo, you can feel safe knowing that your website security is provided by experts.

InstantSSL Certificates are the most cost-effective fully validated and fully supported 128 bit SSL Certificates you can buy today! You can contact the technical support team between 3am- 7pm EST (soon to be 24 hours). You can also feel safe in the knowledge that Comodo will validate your application in accordance with the latest digital signature legislation pertaining to Qualified Certificates. This validation is done effectively and quickly, ensuring you need not wait the traditional 3 working days normally associated with a fully validated SSL Certificate.

InstantSSL boasts industry leading browser ubiquity – comparable to Verisign and Thawte, however without the costs associated with other SSL Providers. InstantSSL Certificates are compatible with over 99% of browsers – including Internet Explorer 5.00 and above, Netscape 4.5 and above, AOL 6 and above and Opera 5.00 and above.

InstantSSL benefits summary:

InstantSSL Certificates are the most cost effective SSL Certificates you can buy which include:

- Full validation conducted quickly – in many cases you can expect your SSL Certificate to be issued within minutes
- Telephone, email, web support available 3am – 7pm EST
- Over 99% browser compatibility
- 128 bit strong encryption security
- Backed by warranties ranging from \$50 to \$10,000

InstantSSL Certificates provide you with the key to successfully using SSL on your webserver.

Testing your webserver before you buy – Try a Trial SSL Certificate for FREE

*“Only InstantSSL offers
free fully functional,
validated and supported
30 day trial Certificates,
giving you the unique
opportunity to fully test
the Certificate and your
webserver configuration
before going live.”*

Trial SSL Certificates provide full SSL functionality for 30 days and are fully supported by our expert technical support staff. Unlike test Certificates from other CAs, InstantSSL trial Certificates are issued using the same Trusted Root CA that issues our end-entity SSL Certificates and provides 99% browser ubiquity, and NOT by a different test CA. This unique service helps you fully test your system prior to your live roll out.

Trial SSL Certificates are ideal for anyone requiring proof of ease of installation, confirmation of high quality technical support and also confirmation of compatibility with the majority of the browsers that exist today. Trial SSL Certificates are also ideal for practicing with Certificates and learning about SSL implementation before committing to installing a Certificate on your live system.

Get your free 30 day trial SSL Certificate from <http://www.instantssl.com/ssl-certificate-products/free-ssl-certificate.html>

Step by step instructions to set up SSL on your Microsoft IIS 5x webserver

There are four stages to setting up SSL on your Microsoft IIS 5x webserver:

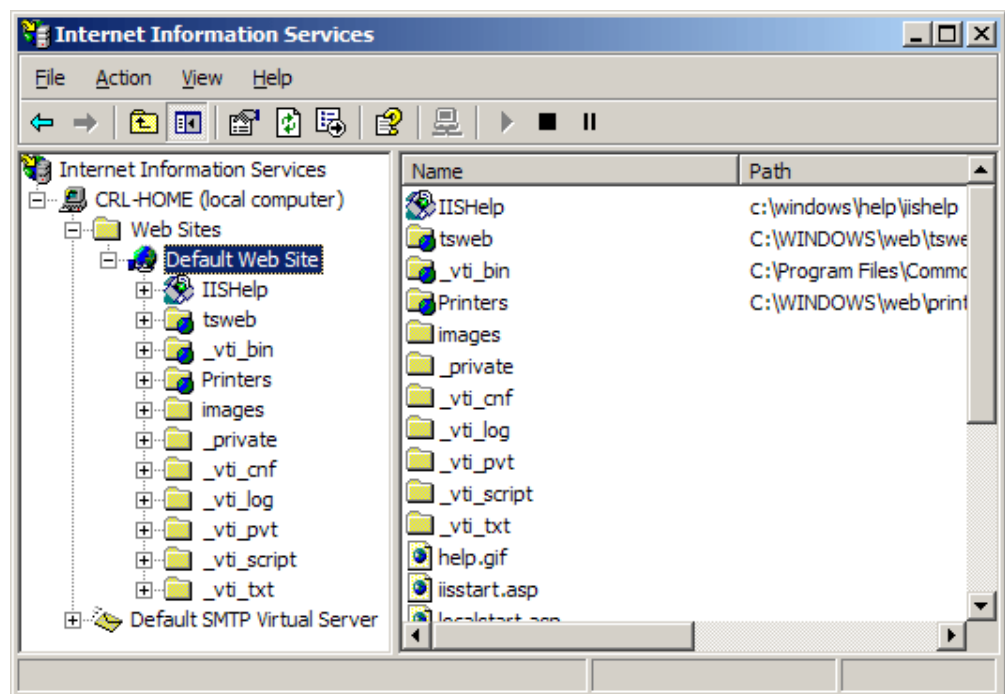
1. Create a Certificate Signing Request (CSR)
2. Apply online
3. Installing your Certificate
4. Displaying your Secure Site Seal

1. Generating a Certificate Signing Request (CSR)

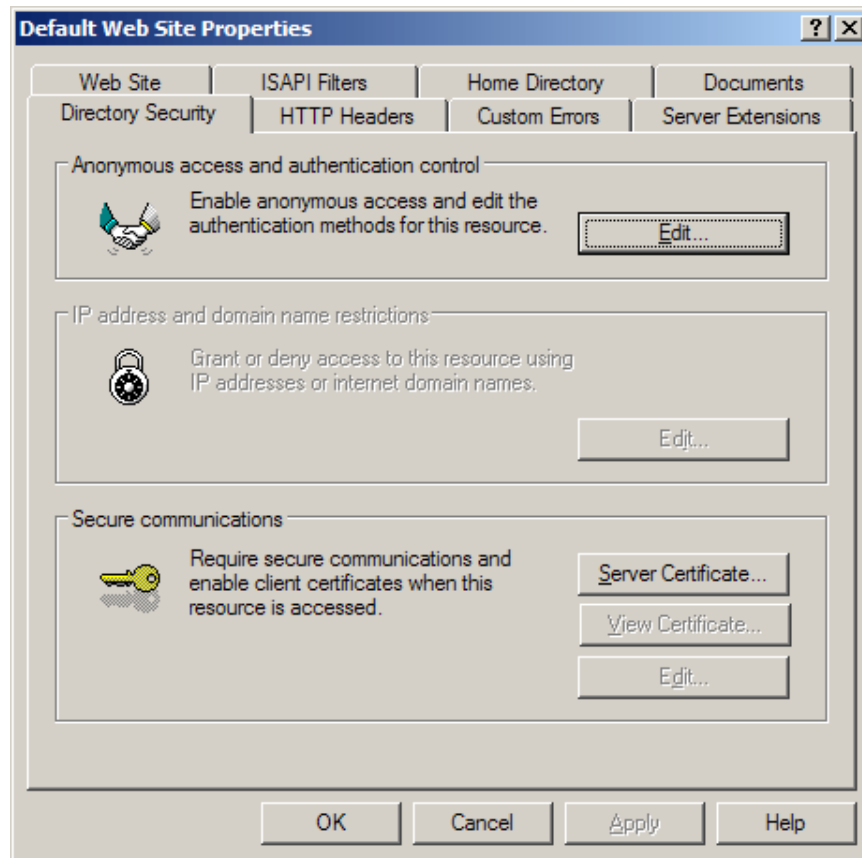
A CSR is a file containing your certificate application information, including your Public Key. Generate your CSR and then copy and paste the CSR file into the webform in the enrollment process:

Generate keys and Certificate Signing Request:

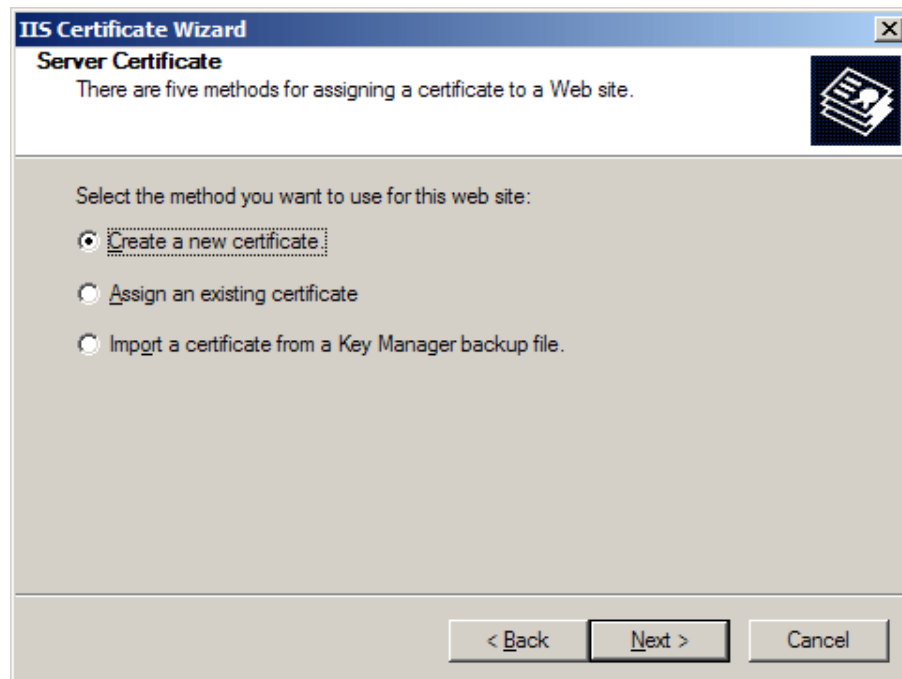
- Select **Administrative Tools** from the **Start Menu**
- Start **Internet Services Manager**



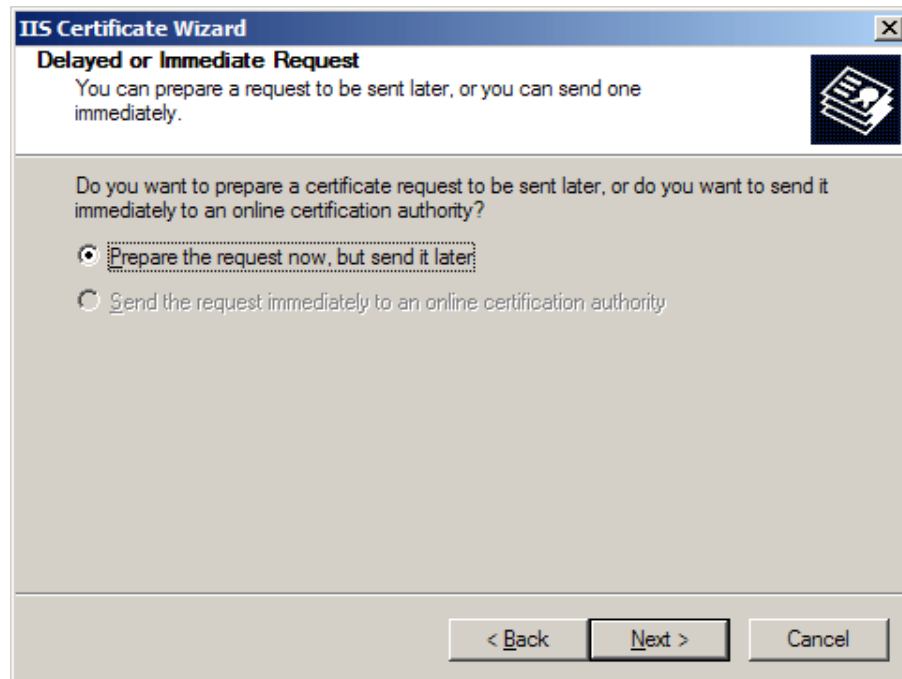
- Open the **Properties** window for the website the CSR is for. You can do this by right clicking on the **Default Website** and selecting **Properties** from the menu
- Open **Directory Security** by right clicking on the **Directory Security** tab



- Click *Server Certificate*. The following Wizard will appear:



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



IIS Certificate Wizard

Delayed or Immediate Request

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

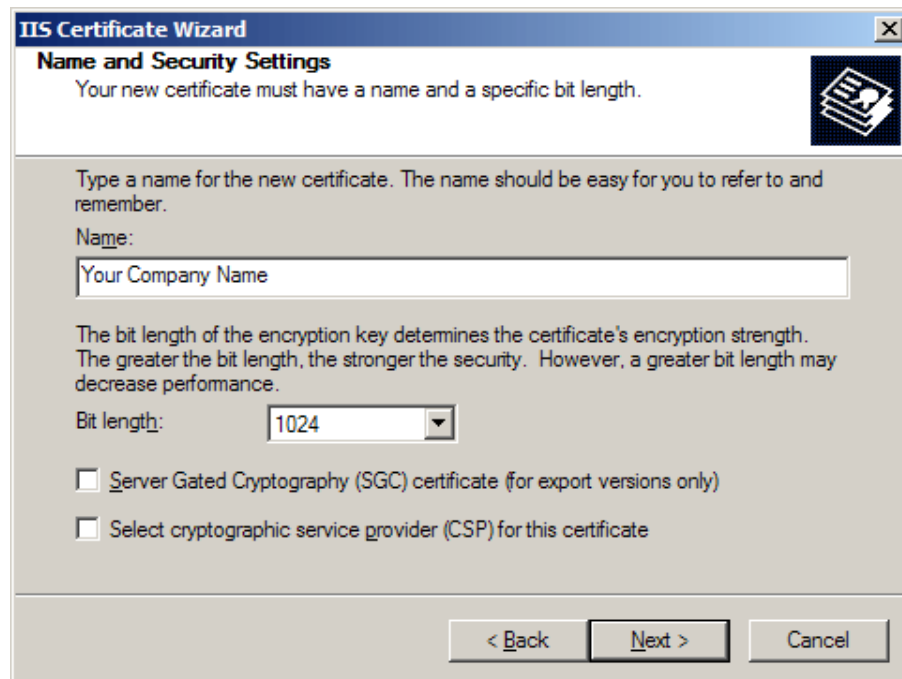
Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

☒ Prepare the request now, but send it later

☐ Send the request immediately to an online certification authority

< Back Next > Cancel

- Select *Prepare the request now, but send it later* and click **Next**.



IIS Certificate Wizard

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

- 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.
- 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**

IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

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.

For further information, consult certification authority's Web site.

Organization:

Your Company Name

Organizational unit:

Web

< Back Next > Cancel

- Enter *Organisation* and *Organisation Unit*, these are your company name and department respectively. Click **Next**.

IIS Certificate Wizard

Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

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.

If the common name changes, you will need to obtain a new certificate.

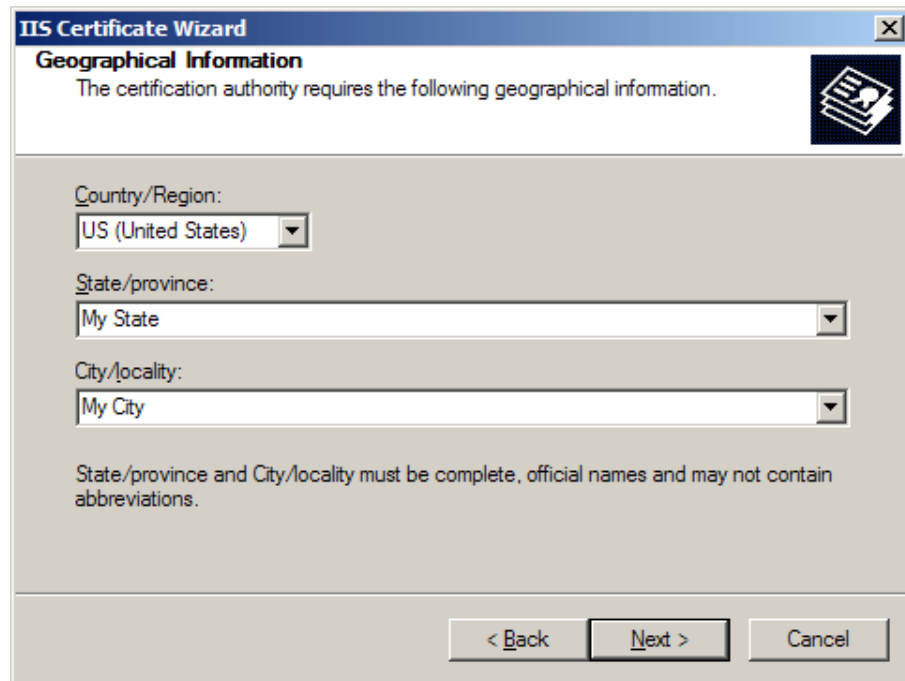
Common name:

www.mydomainname.com

< Back Next > Cancel

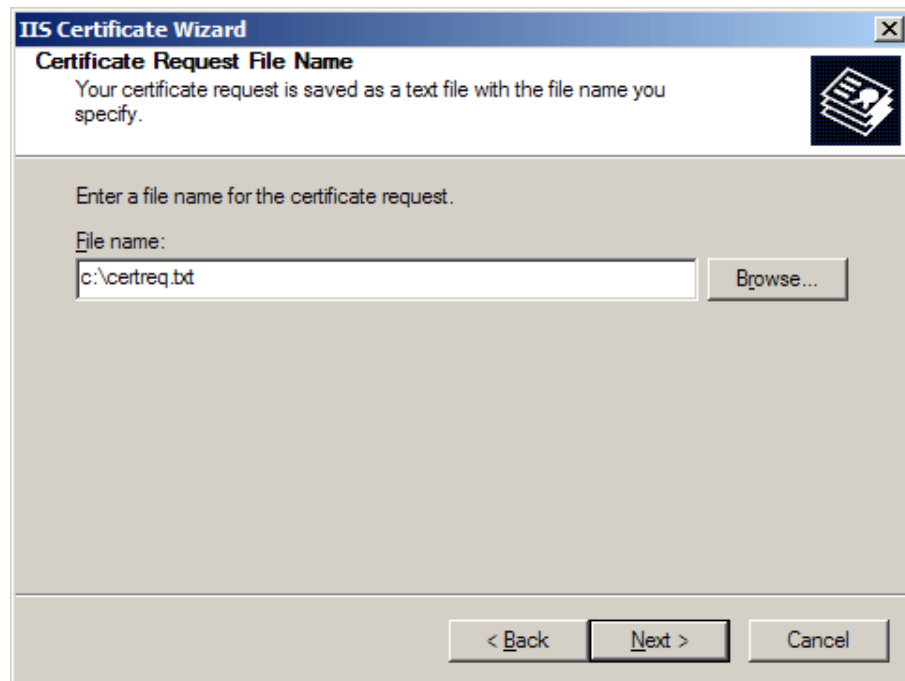
- The *Common Name* field should be the **Fully Qualified Domain Name** (FQDN) or the web address for which you plan to use your Certificate, e.g. the area of your site you wish customers to connect to using SSL. For example, an InstantSSL Certificate issued for **comodo.net** will **NOT** be valid for **secure.comodo.net**. If the web address to be used for SSL is **secure.comodo.net**, ensure that the common name submitted in the CSR is

secure.comodo.net. Note that preceding the FQDN with **https://** is **NOT** necessary. Click **Next**.



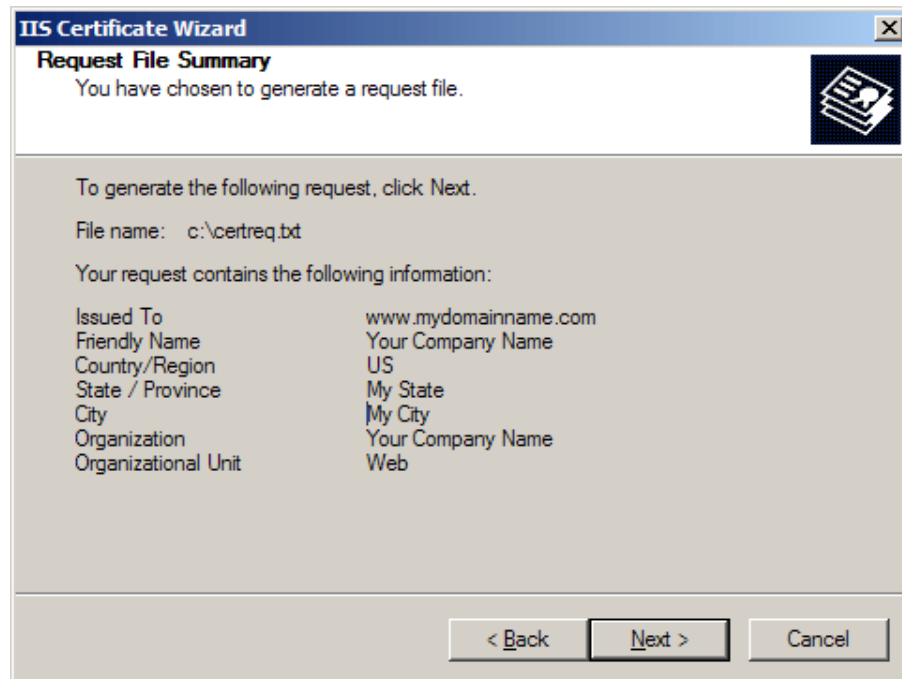
The screenshot shows the 'IIS Certificate Wizard' window at the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Geographical Information' with a subtext: 'The certification authority requires the following geographical information.' There is a small icon of a document with a checkmark in the top right corner. The form contains three dropdown menus: 'Country/Region:' with 'US (United States)' selected, 'State/province:' with 'My State' selected, and 'City/locality:' with 'My City' selected. Below these is a note: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 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'. The main heading is 'Certificate Request File Name' with a subtext: 'Your certificate request is saved as a text file with the file name you specify.' There is a small icon of a document with a checkmark in the top right corner. The form contains a text input field labeled 'File name:' with the text 'c:\certreq.txt' entered. To the right of the input field is a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

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



- 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 Certificate will only work on this domain. Click **Next** when you are happy the details are absolutely correct.

2. Applying for your InstantSSL Certificate Online

Visit www.instantssl.com and select your SSL Certificate product type. You will be required to submit the CSR into a webform. When you make your application, make sure you include the CSR in its entirety into the appropriate section of the enrollment form. When you view your CSR it will appear something like:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVjCCAr8CAQAwEzEdMBsGA1UEAxMud3d3Lm15ZG9tYWlubmFtZS5jb20xDDAK
BgNVBAsTAld1YjEAMBgGA1UEChMRWW91ciBDb21wYW55IE5hbWUxEDA0BgNVBACQ
B015IENpdHkxETAPBgNVBAGTCe15IFN0YXRlMQswCQYDVQQGEwJVUzCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lksJ0
n5r9w1EK9Np5/OJEt72r5es3nie5rTKo304yvsLovkS0vqT+i01EzVl5B4mXTEPw
fDLjEcwcNb8SCJ4ArUAhHKJWHDKJHDKDA6587568gfhjffjFHGFHFHsgGHJGJjhhj
HFD^TGFrYTrYTrfGHI&DHJKDHkjwjjkgAgcwCgYIKoZIhvcNHHKJHFrytDETR$456
AwcwEwYDVR01BAwwYIawYBOHAWjgffSCisGAQGBjcnAgIw4wgesCAQEE
WgBNAGkAYwByAG8AABwYAG8AABwYAG8AABwYAG8AABwYAG8AABwYAG8AABwYAG8A
QwByAHkAcABUAG8AZwByAGEAcABOAGkAYwAGAFAAcgbvAHYAaQBkAGUAcgOBiQCq
EH3QppP7Ewuz6oh4EUXMbKdgieAcBQ52iFSXqQ/n1xAtEpVUfjIM3exr42EhyYlr
1V7cpUKbSr/eQ6c/hjiUi17EpvleBBV0BkFWsWzJoShx0BmOKvDnKINNQC3Jya+M
N/t9axyuCdWUYJiLglNnjcBLSxL/6hovXNDLuCLgMAAAAAAAAAAAMA0GCSqGSIb3
DQEBBQUAA4GBAEQT6Pwj0BHeOUw+AROGAT30q+1OYNkr341CoumC6M7Kq1KgVZDV
tRes4uz1Yf8+WRCutVvDByreY+CdgzJzHvHqS61Aj2swx8QadclVWOkZfH//k/KE
1MiOEb6c3MplECorjIm+HRN20Qga+dnDBOowYRn7Vz+Nkar88mrJwk/
-----END NEW CERTIFICATE REQUEST-----
```

Be sure to copy the CSR text in its entirety into the application form, including the:

```
-----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----
```

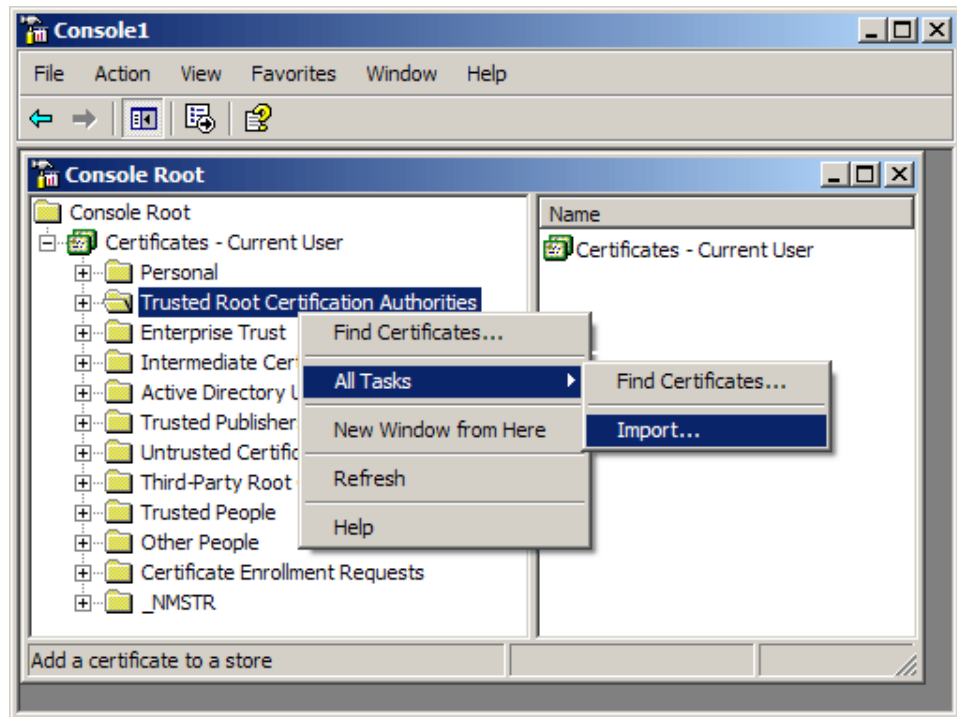
3. Installing your InstantSSL Certificate

Installing the Root & Intermediate Certificates

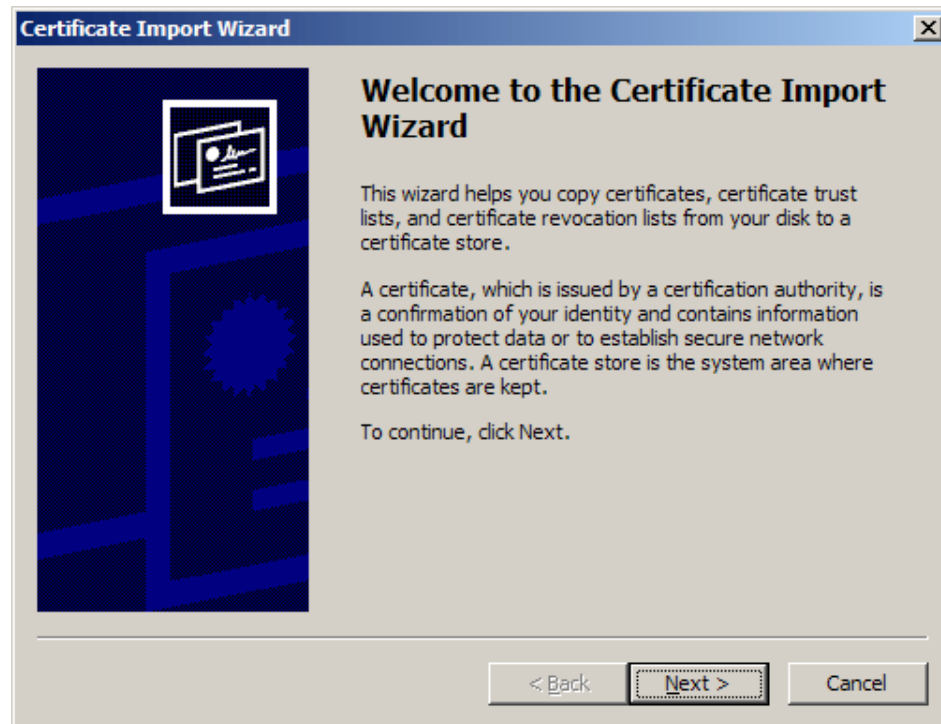
When you InstantSSL Certificate has been issued you will receive 3 Certificates via email from Comodo Security Services. Save these Certificates to the desktop of the webserver machine, then:

- Click the **Start Button** then select **Run** and type *mmc*
- Click **File** and select **Add/Remove Snap in**
- Select **Add**, select Certificates from the **Add Standalone Snap-in box** and click **Add**
- Select **Computer Account** and click **Finish**
- Close the **Add Standalone Snap-in** box, click **OK** in the **Add/Remove Snap in**
- Return to the **MMC**

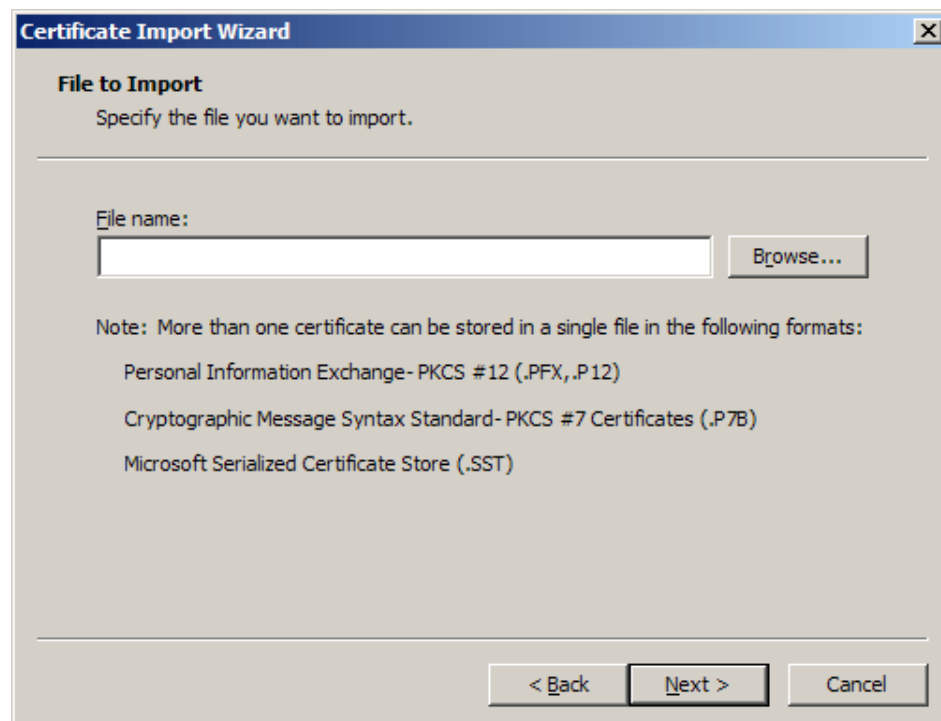
A. To install the **GTECyberTrustRoot** Certificate:



- Right click the *Trusted Root Certification Authorities* , select **All Tasks**, select **Import**.

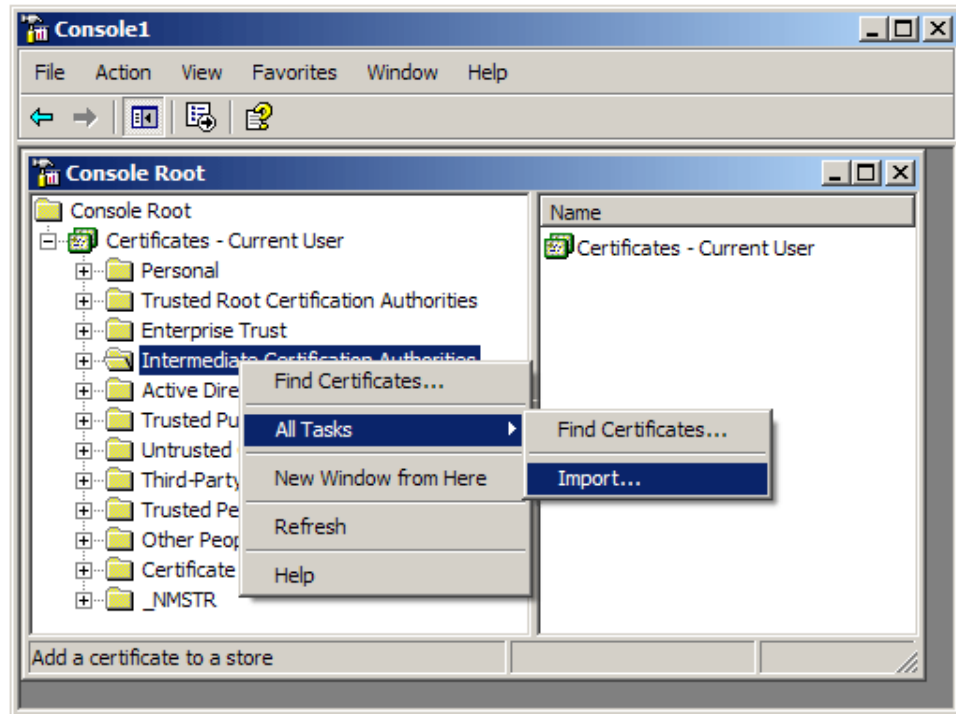


- Click **Next**.



- Locate the **GTECyberTrustRoot** Certificate and click **Next**.
- When the wizard is completed, click **Finish**.

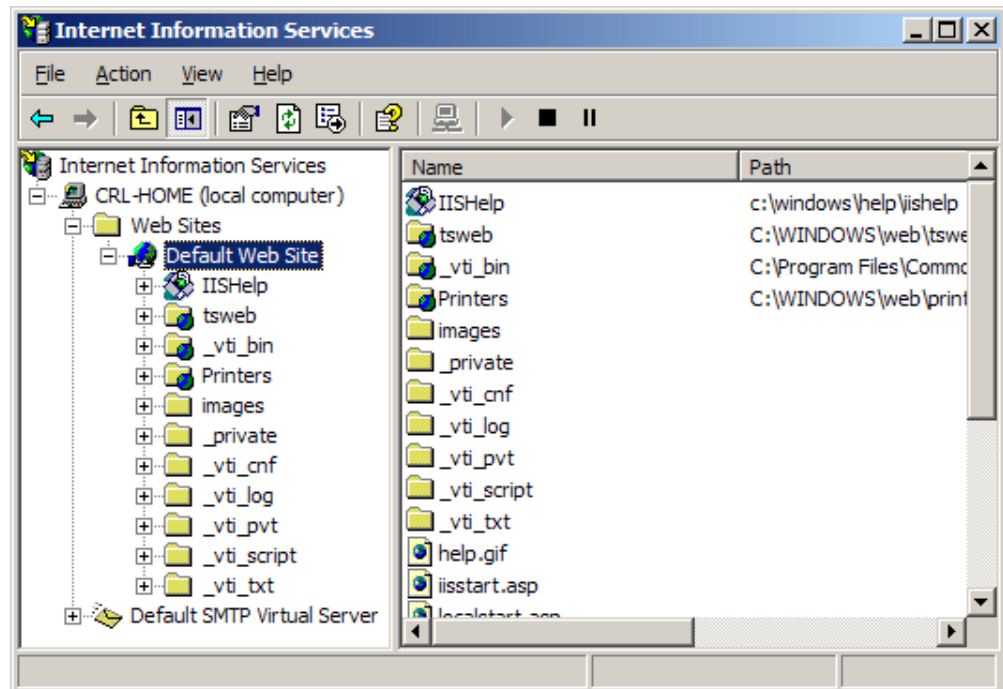
B. To install the **ComodoSecurityServicesCA Certificate:**



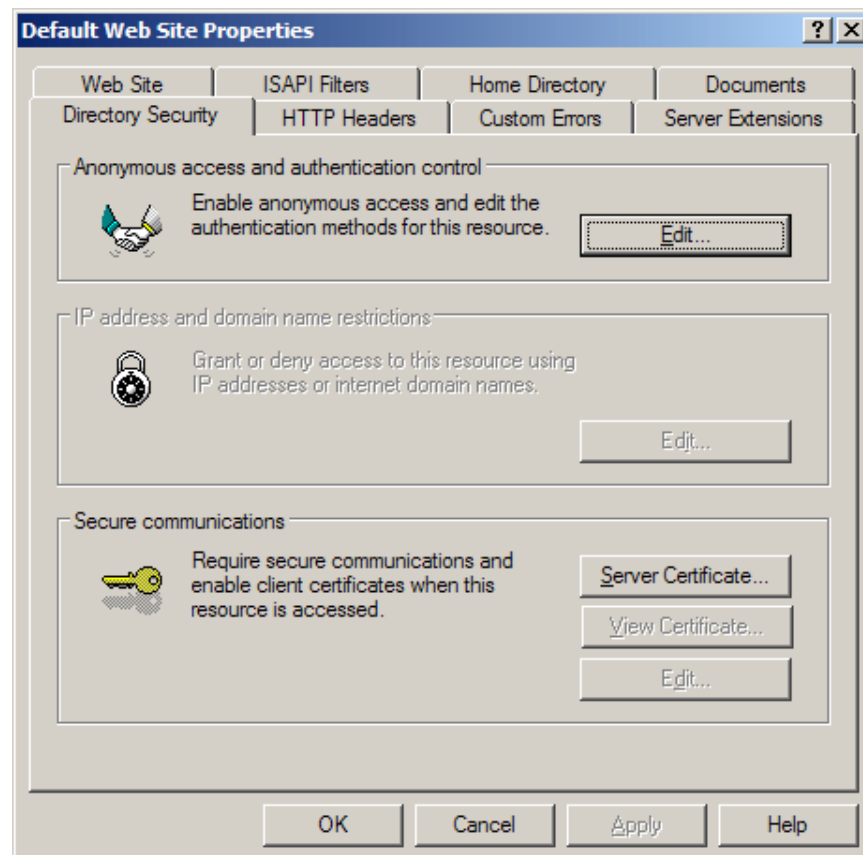
- Right click the *Intermediate Certification Authorities*, select **All Tasks**, select **Import**.
- Complete the import wizard again, but this time locating the **ComodoSecurityServicesCA** Certificate when prompted for the Certificate file.
- Ensure that the **GTECyberTrustRoot** certificate appears under *Trusted Root Certification Authorities*
- Ensure that the **ComodoSecurityServicesCA** appears under *Intermediate Certification Authorities*

C. Installing your SSL Certificate

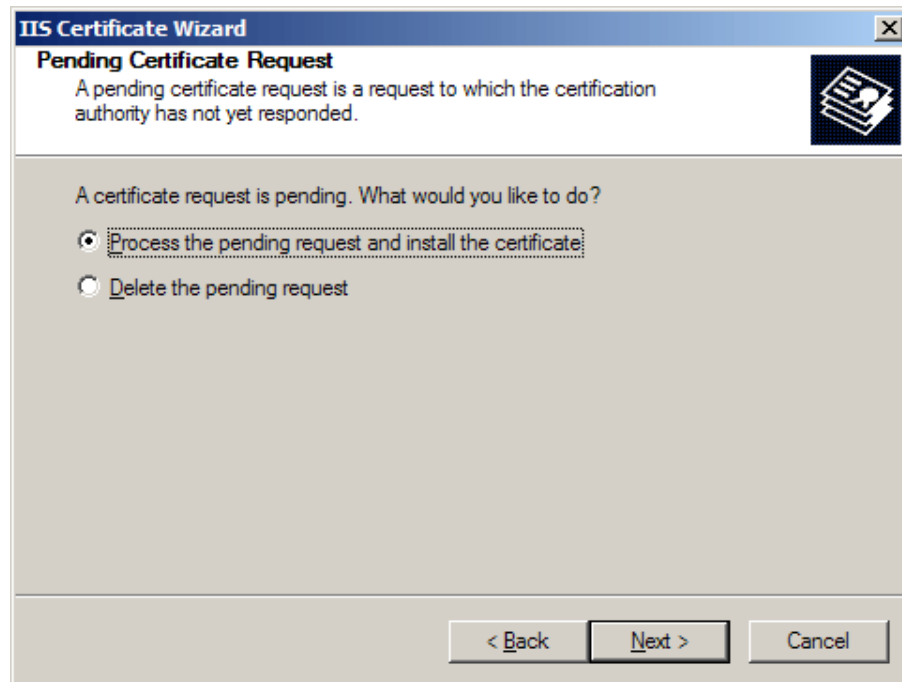
- Select **Administrative Tools**
- Start **Internet Services Manager**



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



- Click **Server Certificate**. The following Wizard will appear:



- Choose to *Process the Pending Request and Install the Certificate*. Click **Next**.
- Enter the location of your certificate (you may also browse to locate your certificate), and then click **Next**.
- Read the summary screen to be sure that you are processing the correct certificate, and then click **Next**.
- You will see a confirmation screen. When you have read this information, click **Next**.
- **You now have a server certificate installed.**

Important: You must now restart the computer to complete the install

Open the **Properties** of the default website and ensure that *SSL port* contains the number **443** (it should default to this number automatically). You may want to test the Web site to ensure that everything is working correctly. Be sure to use `https://` when you test connectivity to the site.

4. Displaying your Secure Site Seal

As a valued InstantSSL customer we encourage you to display the InstantSSL secure site seal to help promote your **secure** site to customers. The secure site seal is free to all InstantSSL customers.

Contact us to discuss our TrustLogo technology and how providing real-time identity assurance to customers to help establish even more confidence and trust with your customers.

Fast, cost-effective **SSL Security** for your webserver...


The Internet is a revolutionary medium for you to improve your sales and online services for customers. InstantSSL is the perfect solution to securing your webserver with SSL quickly, easily and cost-effectively.

Contact us to discuss your individual security requirements


Contact us between 3am and 7pm EST to discuss how InstantSSL can help you:

support@comodogroup.com

sales@comodogroup.com

Comodo 

3401 E. McDowell Rd,
Suite B, Phoenix AZ 85008.
Tel: (877) COMODO-5
Fax: (720) 863 2140
3am- 7pm EST

Comodo 

New Court, Regents Place,
Regent Road, Manchester M5 4HB,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767
8am - 12am GMT