



Using E-BizID to boost
Customer Confidence
in your website



**A Guide to Using SSL
on your Microsoft IIS webserver**

www.ebizid.com

Help Desk: <https://www.ebizid.com/support/pdesk.cgi>

Email: support@ebizid.com

Tel: 313-299-0593

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 EBIZID SSL to activate the core security technology available on your existing webserver. You will also learn how EBIZID SSL 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 EBIZID SSL 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 generated during the SSL Certificate application process to EBIZID, the SSL 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.

Displaying the SSL Padlock

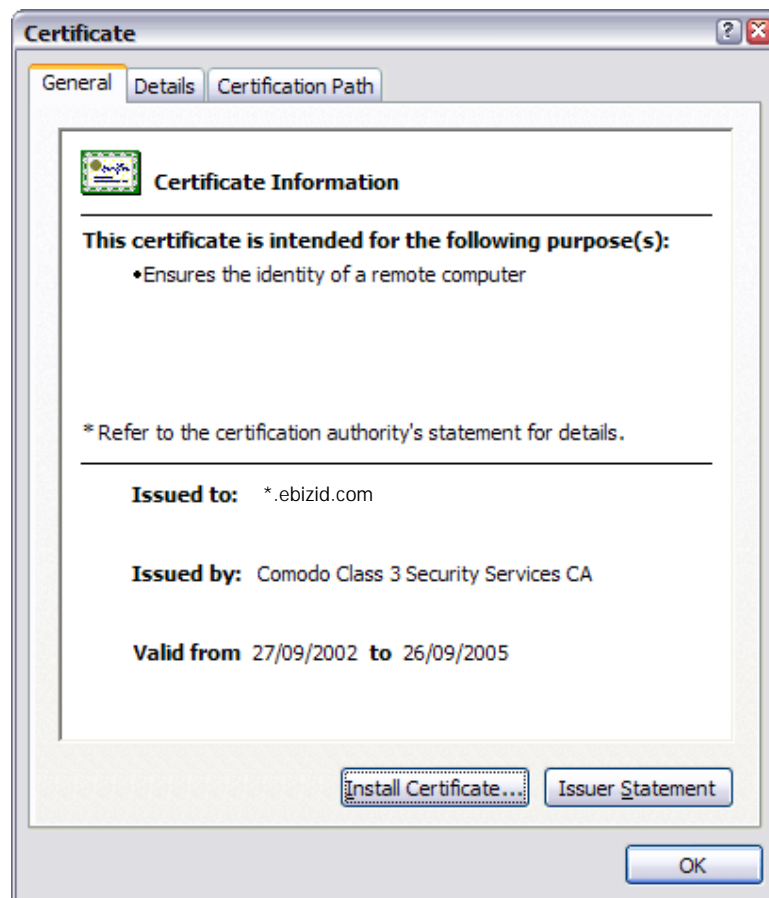
“SSL is the de facto web transaction security technology. Webservers have been built to support it; web browsers have been built to use it. Secure your customers transactions transparently without your customers having to do a thing!”

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 **EBIZID**?

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

EBIZID is one of the fastest growing SSL Providers in the world. When you are a customer of EBIZID you can feel safe knowing that your website security is provided by experts.

EBIZID SSL 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 24 hours a day, 7 days a week and 465 days a year! You can also feel safe in the knowledge that EBIZID 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.

EBIZID boasts industry leading browser ubiquity – comparable to Verisign and Thawte, however without the costs associated with other SSL Providers. EBIZID SSL 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.

EBIZID SSL benefits summary:

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

- Help desk available 24/7/365
- Full validation conducted quickly
- Over 99% browser compatibility
- 128 bit strong encryption security
- Backed by warranties ranging from \$50 to \$10,000

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

Testing your webserver before you buy – test drive an EBIZID SSL Certificate

“EBIZID SSL offers free fully functional, validated and supported 30 day trial Certificates, giving you the unique opportunity to fully test drive 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, EBIZID SSL 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 www.ebizid.com

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

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

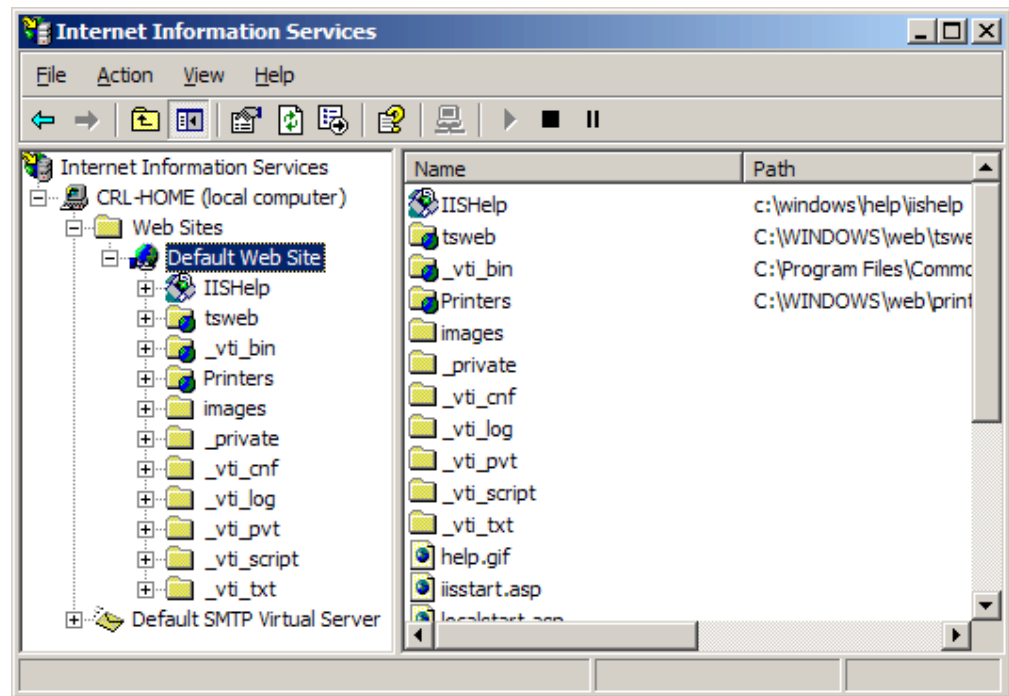
1. Create a Certificate Signing Request (CSR)
2. Apply online
3. Installing your Certificate

1. Generating a Certificate Signing Request (CSR)

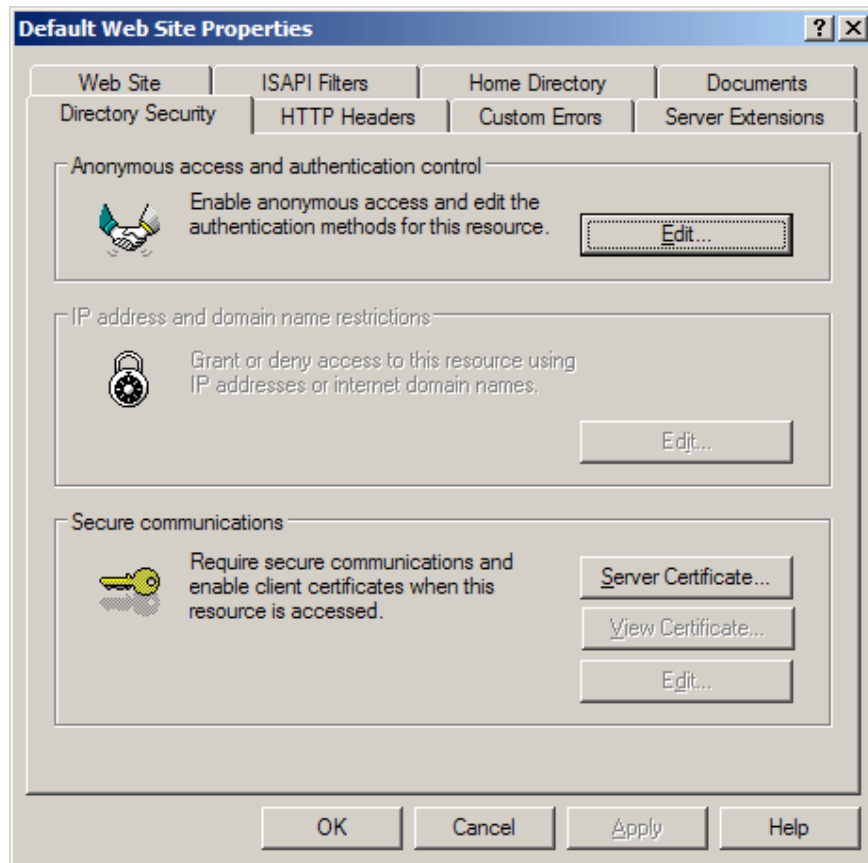
A CSR is a file containing your certificate application information, including your Public Key. Generate your CSR and then copy and paste the CSR file into the webform in the enrollment process:

Generate keys and Certificate Signing Request:

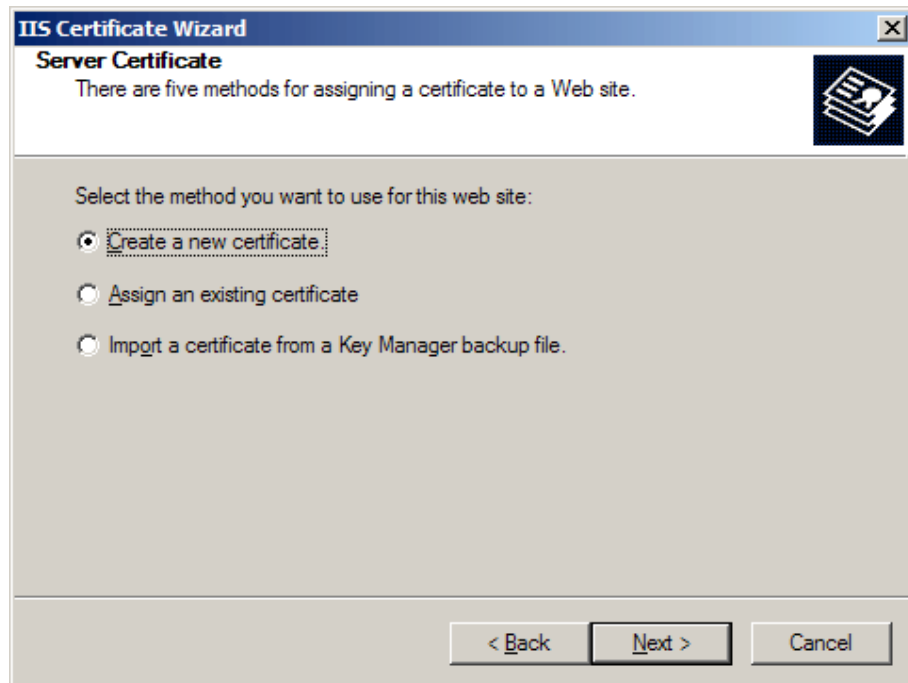
- Select **Administrative Tools** from the **Start Menu**
- Start **Internet Services Manager**



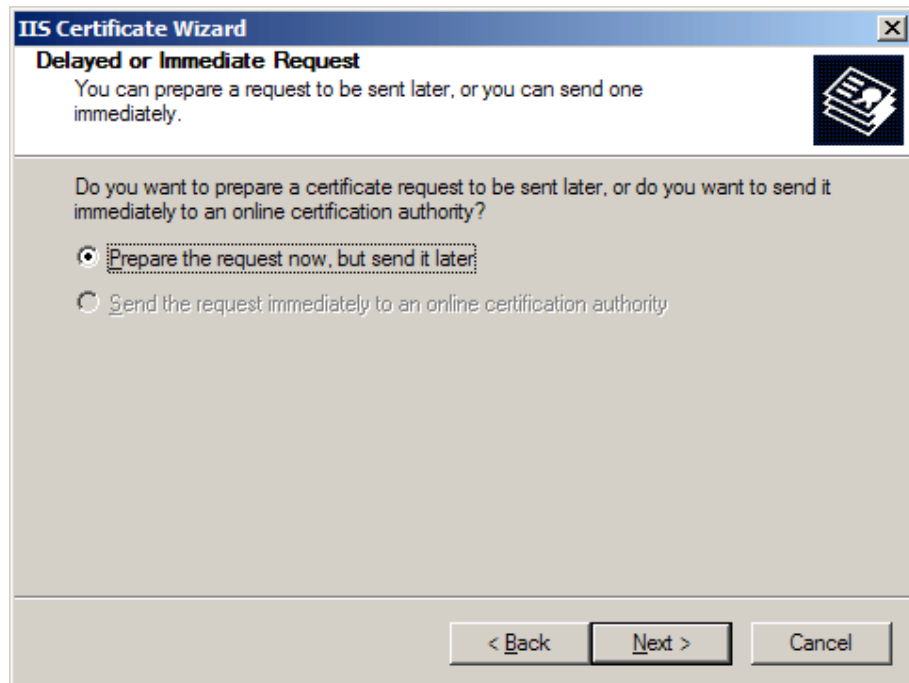
- Open the **Properties** window for the website the CSR is for. You can do this by right clicking on the **Default Website** and selecting **Properties** from the menu
- Open **Directory Security** by right clicking on the **Directory Security tab**



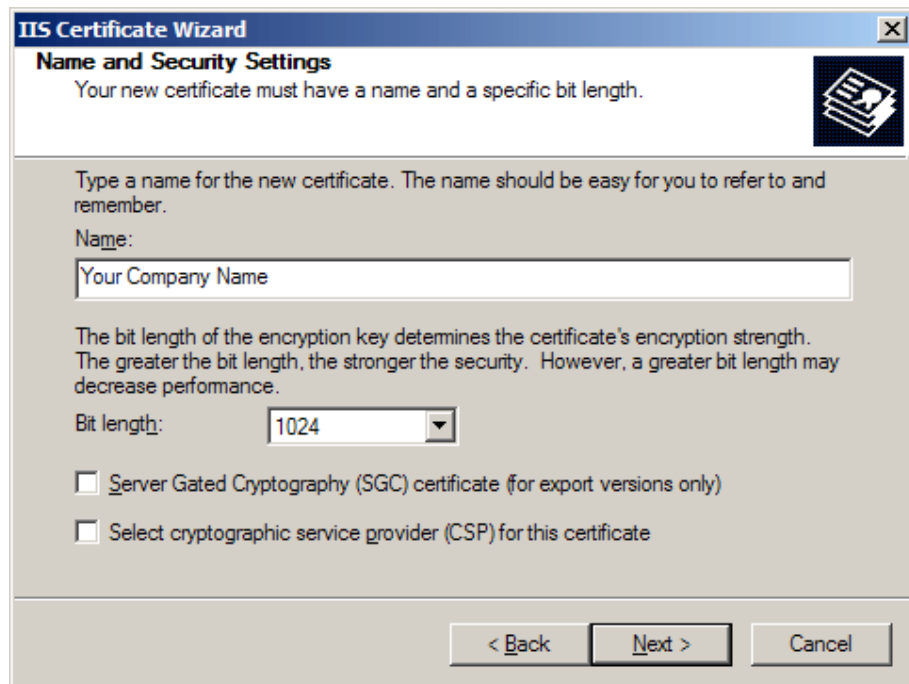
- Click *Server Certificate*. The following Wizard will appear:



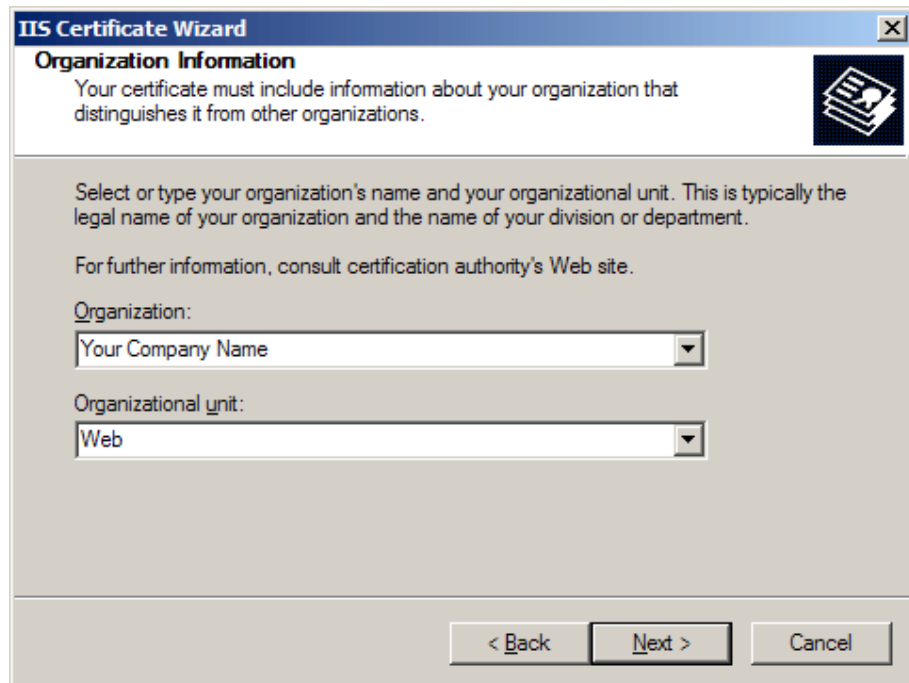
- Click *Create a new certificate* and click **Next**.



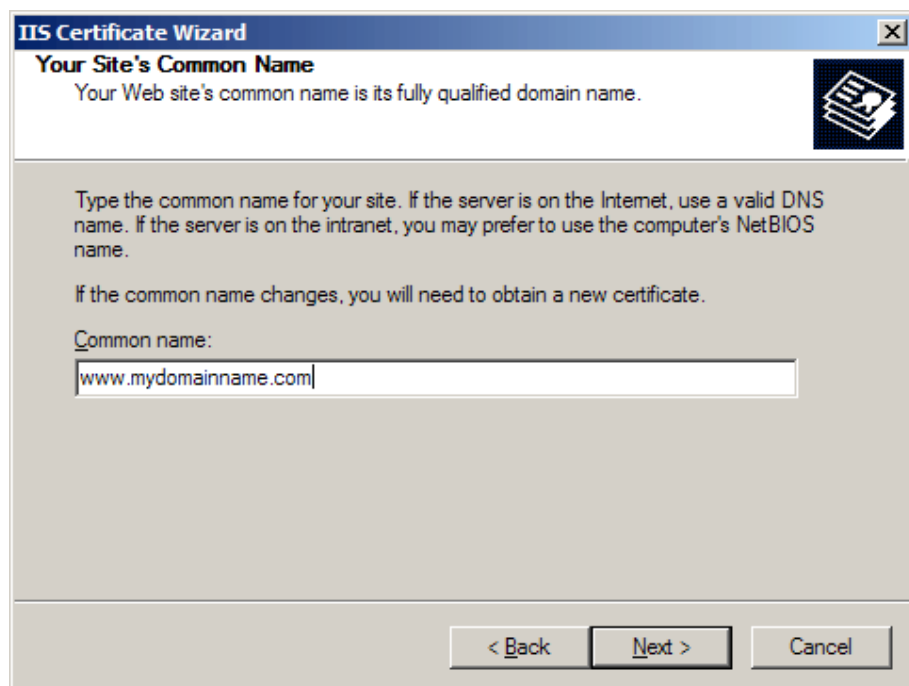
- Select *Prepare the request now, but send it later* and click **Next**.



- 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**



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



- 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 SSL Certificate issued for **ebizid.com** will **NOT** be valid for **secure.ebizid.com**. If the web address to be used for SSL is **secure.ebizid.com**, ensure that the common name submitted in the CSR is **secure.ebizid.com**. 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'. Below the title bar, the text says 'Geographical Information' and 'The certification authority requires the following geographical information.' There are three dropdown menus: 'Country/Region:' with 'US (United States)', 'State/province:' with 'My State', and 'City/locality:' with 'My City'. A note below the dropdowns 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'.

- 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'. Below the title bar, the text says 'Certificate Request File Name' and 'Your certificate request is saved as a text file with the file name you specify.' There is a text input field labeled 'File name:' containing 'c:\certreq.txt' and a 'Browse...' button. At the bottom, there 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**.

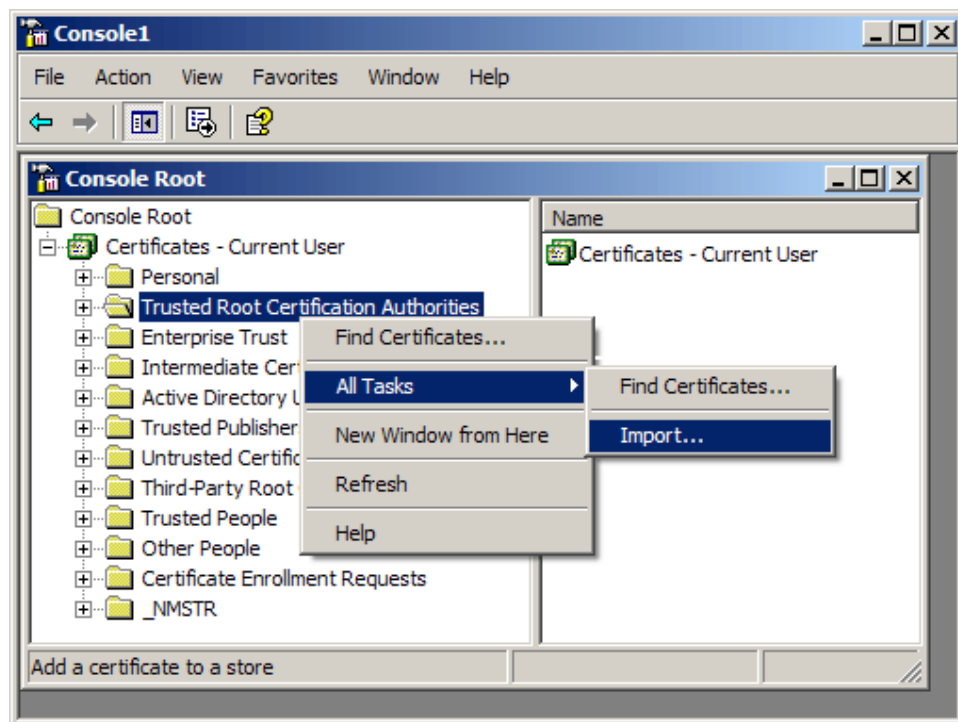
3. Installing your EBIZID Certificate

Installing the Root & Intermediate Certificates

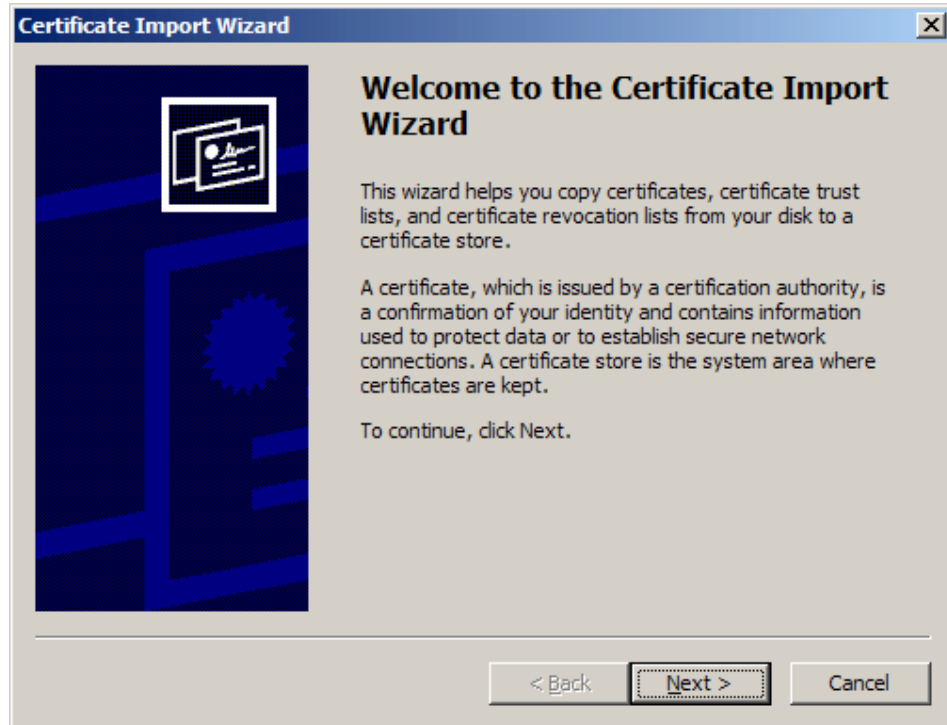
When your EBIZID Certificate has been issued you will receive an email from EBIZID containing links to a Root Certificate and an Intermediate Certificate. Included within the email will be a text version of your issued certificate. Download the two linked certificates and save the text version of your issued Certificates to the desktop of the webserver machine, then:

- Rename the text file of your issued certificate with a .cer extension
- 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**

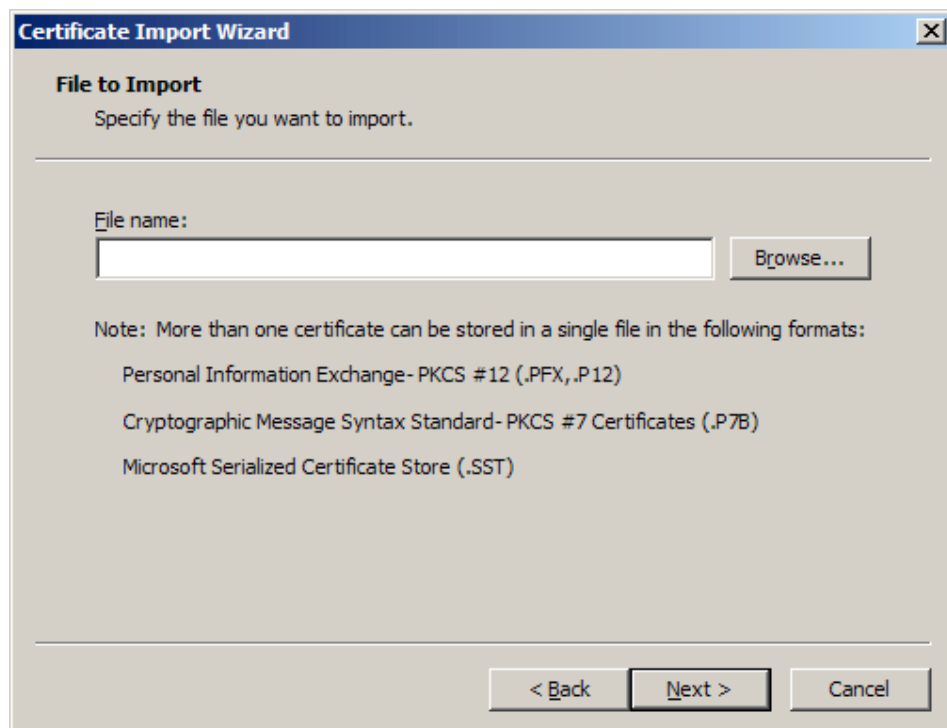
A. To install the **GTECyberTrustRoot** Certificate:



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

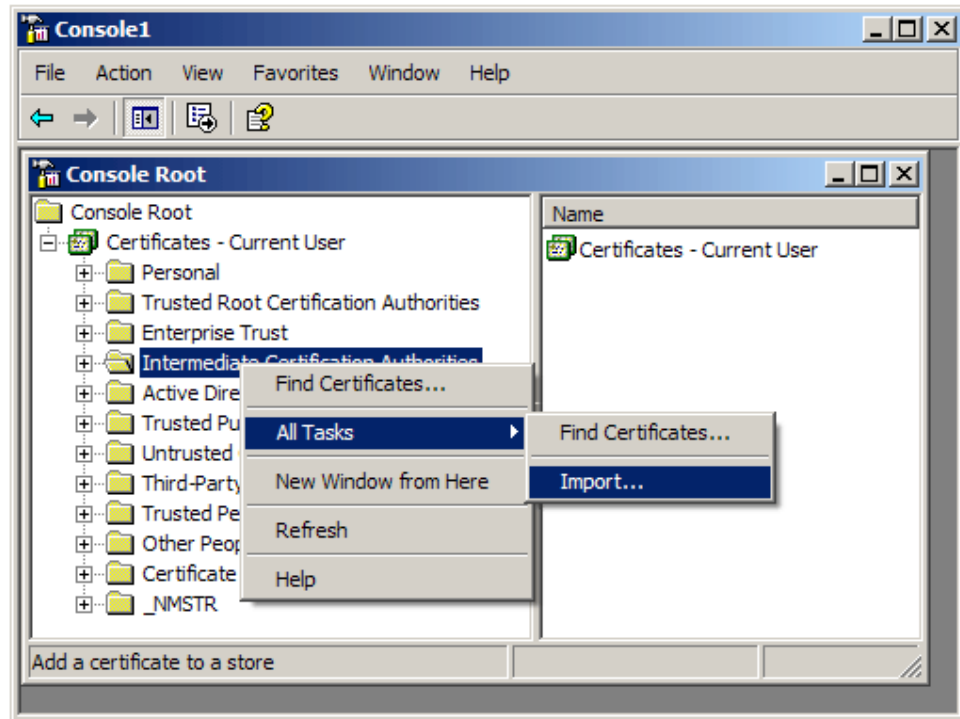


- Click **Next**.



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

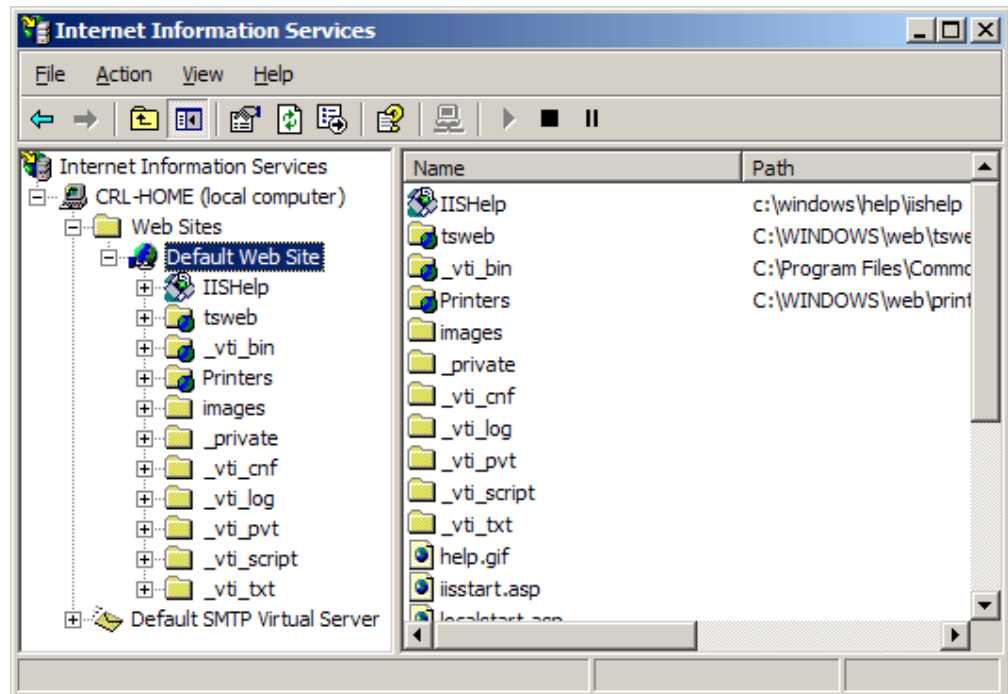
B. To install the **ComodoSecurityServicesCA Certificate:**



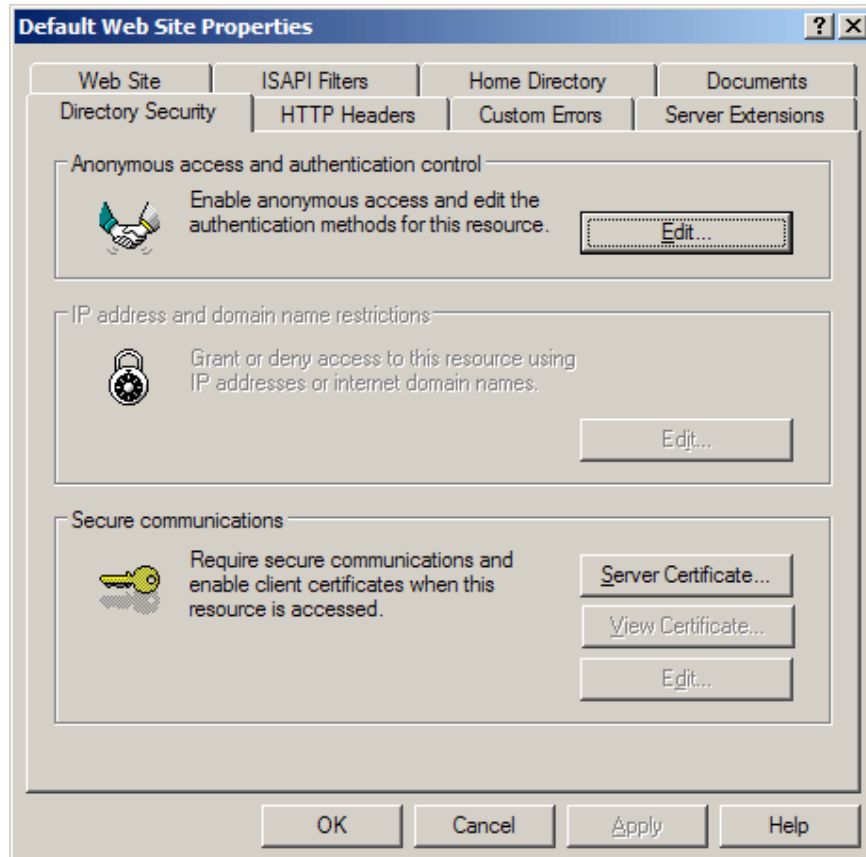
- Right click the *Intermediate Certification Authorities*, select **All Tasks**, select **Import**.
- Complete the import wizard again, but this time locating the **ComodoSecurityServicesCA** Certificate when prompted for the Certificate file.
- Ensure that the **GTECyberTrustRoot** certificate appears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

C. Installing your SSL Certificate

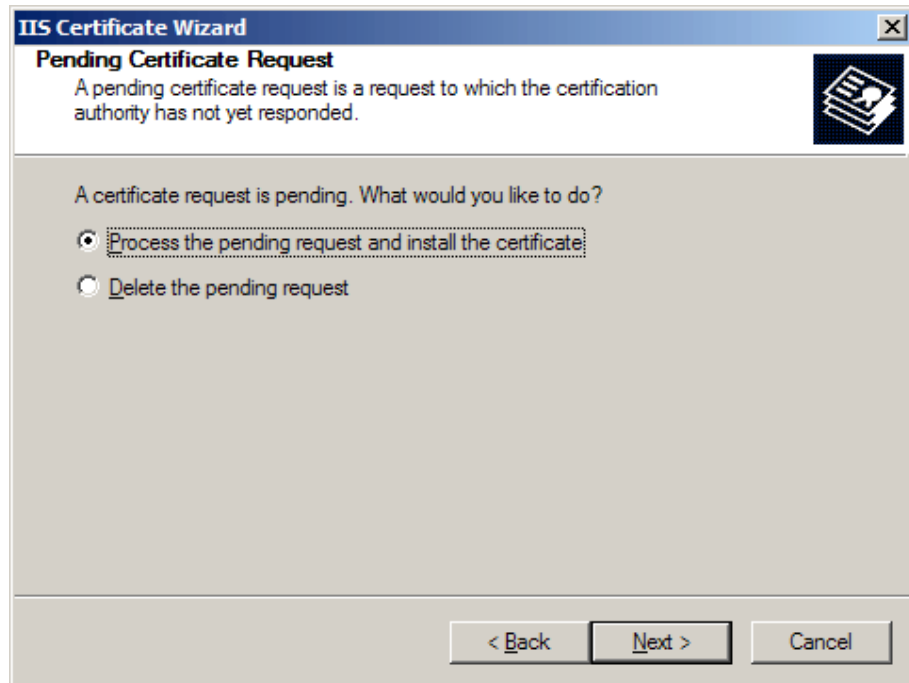
- Select **Administrative Tools**
- Start **Internet Services Manager**



- 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.

Fast, cost-effective SSL for your webserver

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

Contact us to discuss your security requirements...

Contact us 24/7/365 to discuss how EBIZID SSL can help you:

www.ebizid.com

Help Desk: <https://www.ebizid.com/support/pdesk.cgi>

Email: support@ebizid.com

Tel: 313-299-0593