Configuring a Secure Website with a Digital Certificate

This article will explain you different steps that can be taken to secure a web site in IIS5 with a third- party assigned certificate.

The whole practice consists of the following steps.

- Generating the CSR for a website named **Secure**.
- Requesting a trial certificate from **Verisign**.
- Obtaining the **Trial Certificate**.
- Installing the **Trial Certificate**.
- **Enforcing SSL** and Testing the **Secure Website**.

Note: This whole article assumes that you have already installed IIS 5 on your Windows 2000 computer and has configured a website named Secure.

Generating CSR:

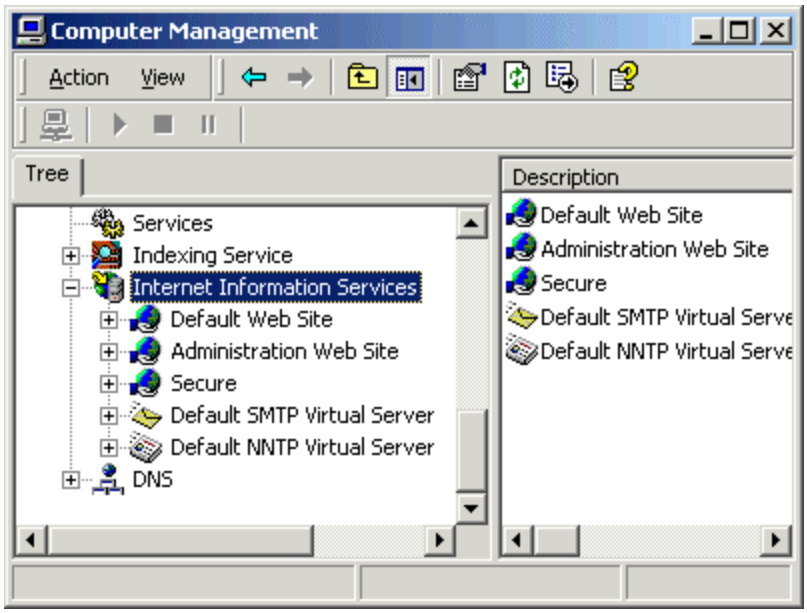
A CSR (Certificate Signing Request) is basically a certificate that you generate on your server that validates the computer-specific information about your server when you request a certificate from a third-party CA. The CSR is simply an encrypted text message that is encrypted with a public/private key pair.

Typically, a CSR contains the following information about your computer.

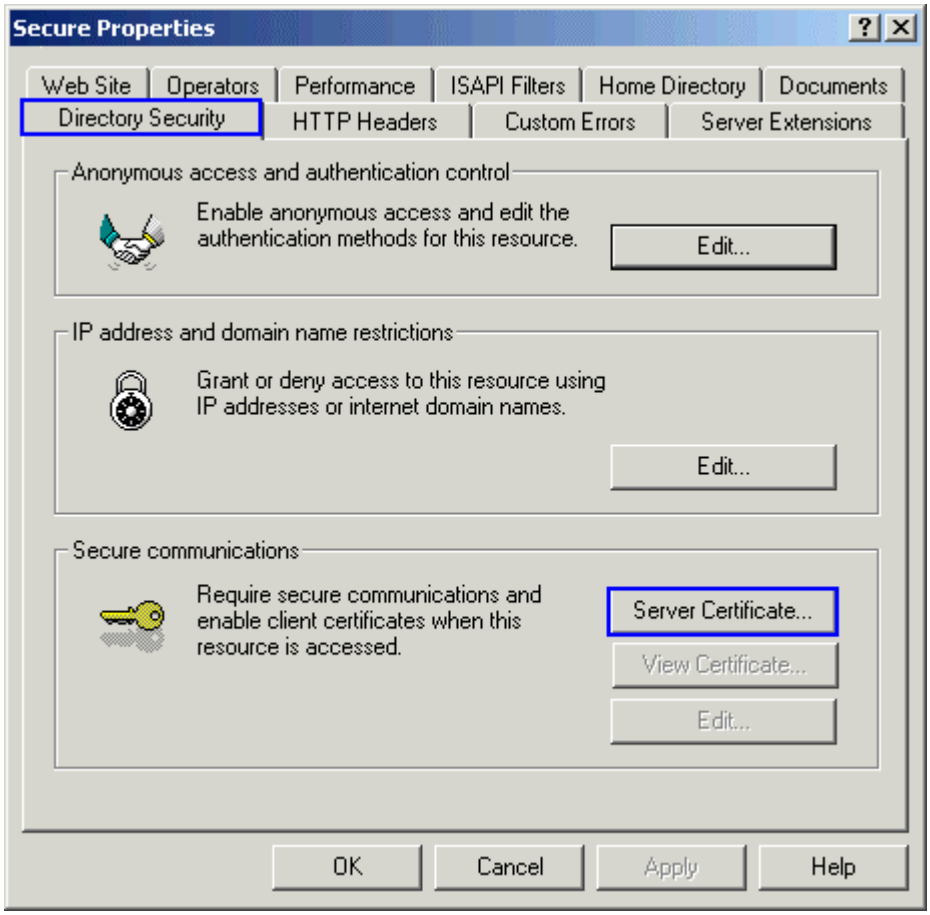
- Organization
- Organizational unit
- Country
- State
- Locality

To begin the process to obtain the certificate, you must generate a CSR. Follow these steps to generate the CSR.

1. Access the IIS Microsoft Management Console (MMC). To access it, right-click **My Computer** and click **Manage**. This opens the Computer Management Console. Expand the **Services and Application** section. Locate **Internet Information Services** and expand the IIS console.

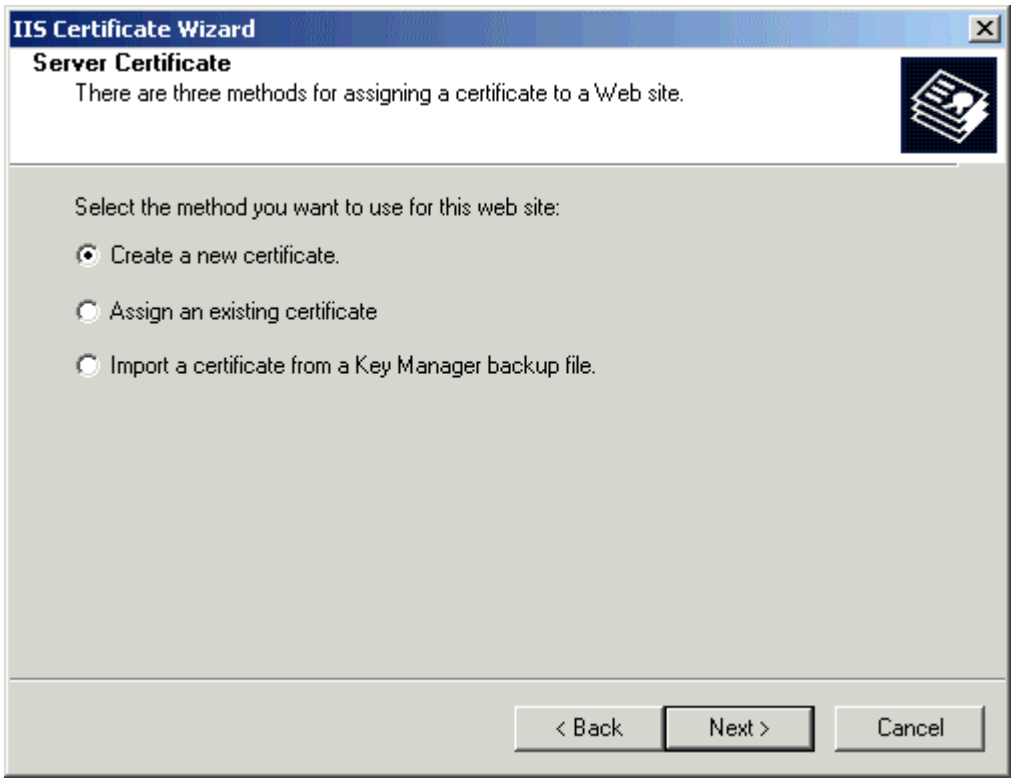


2. Select the specific Web site (Secure), right-click the site and click **Properties**.
3. Click the **Directory Security** tab. In the **Secure Communications** section, click **Server Certificate**.

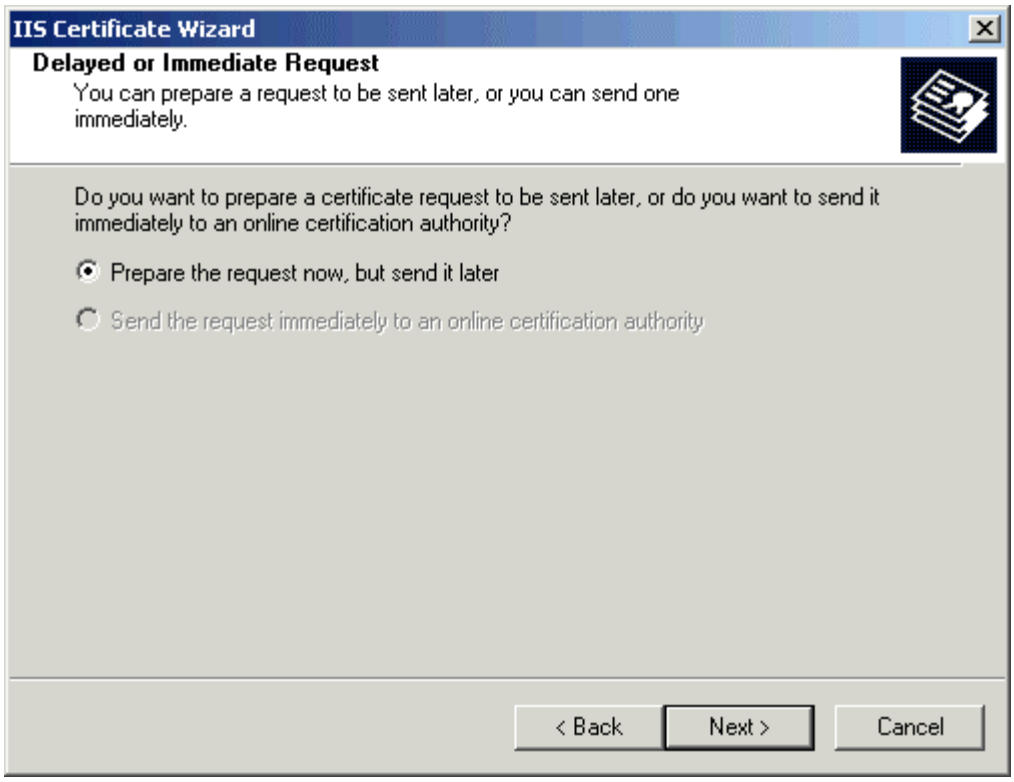


4. The Web Server Certificate Wizard will start. Click **Next**.

5. Select **Create a New Certificate** and click **Next**.

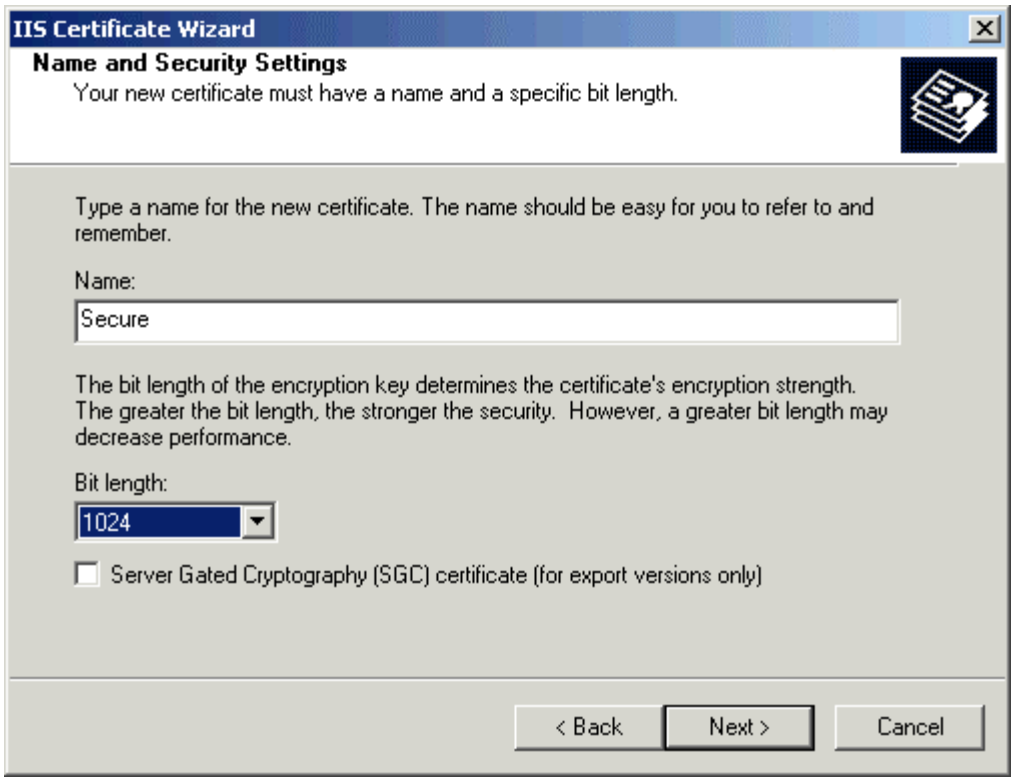


6. Select **Prepare the request now, but send it later** and click **Next**.

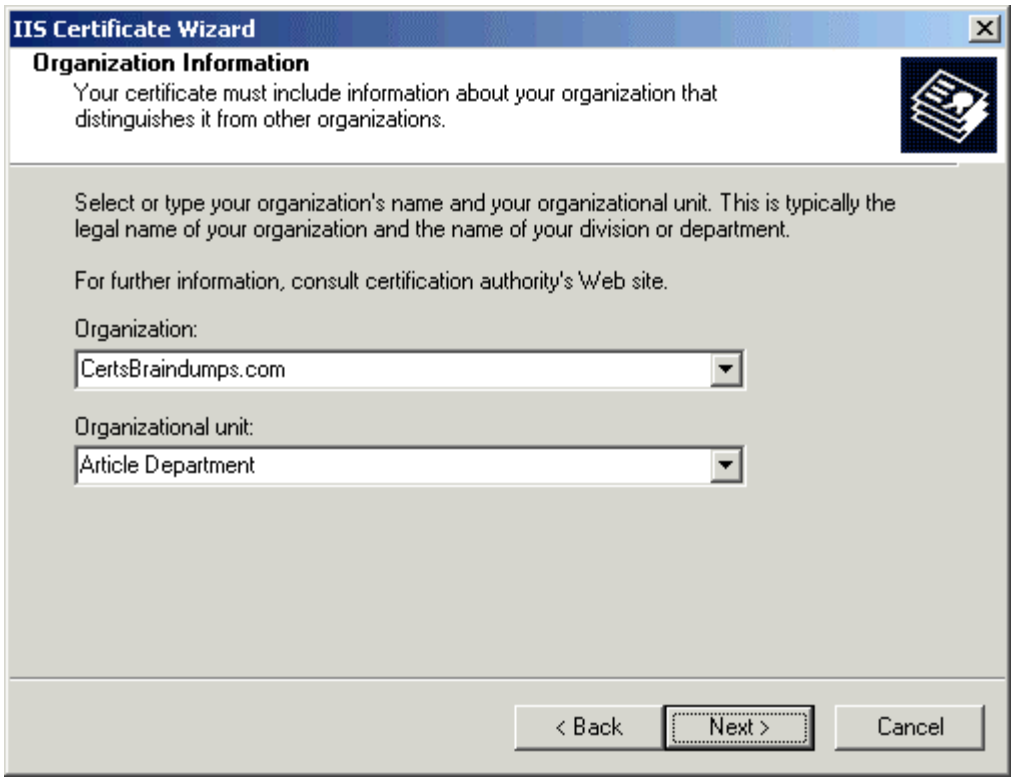


7. In the **Name** field, enter a name that you can remember. It will default to the name of the Web site for which you are generating the CSR.

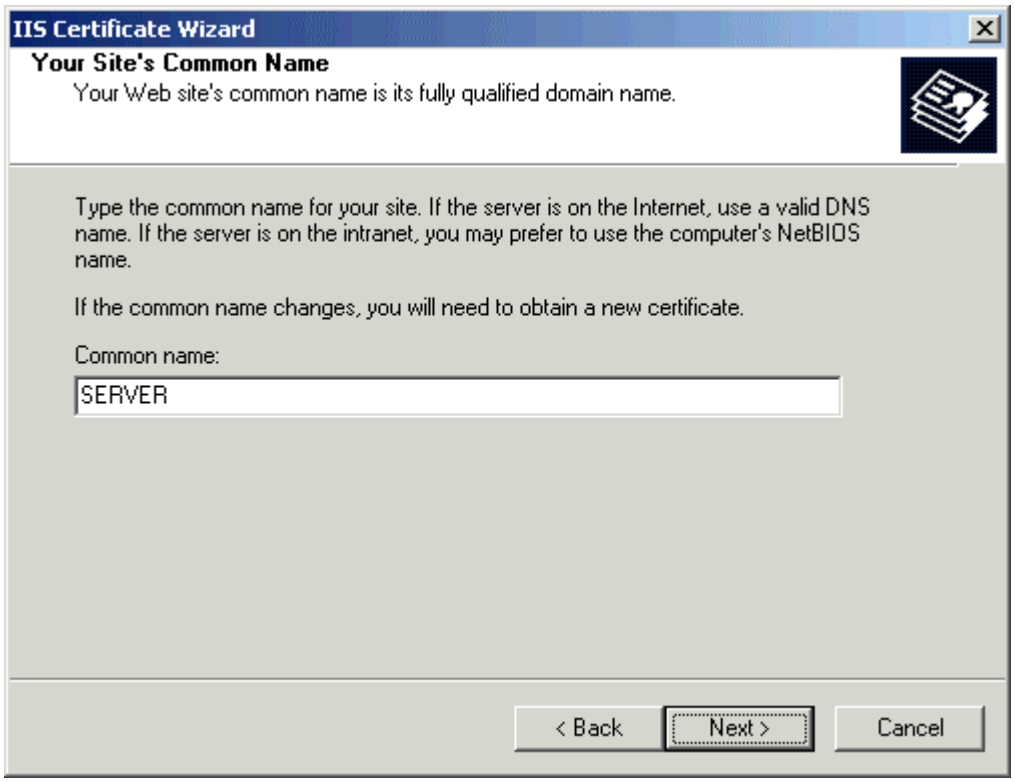
NOTE: When you generate the CSR, you need to specify a bit length. The bit length of the encryption key determines the strength of the encrypted certificate which you send to the third-party CA. The higher the bit length, the stronger the encryption. Most third-party CAs prefer a minimum of 1024 bits.



8. In the **Organization Information** section, enter your organization and organizational unit information. This must be accurate, because you are presenting these credentials to a third-party CA and you must comply with their licensing of the certificate.

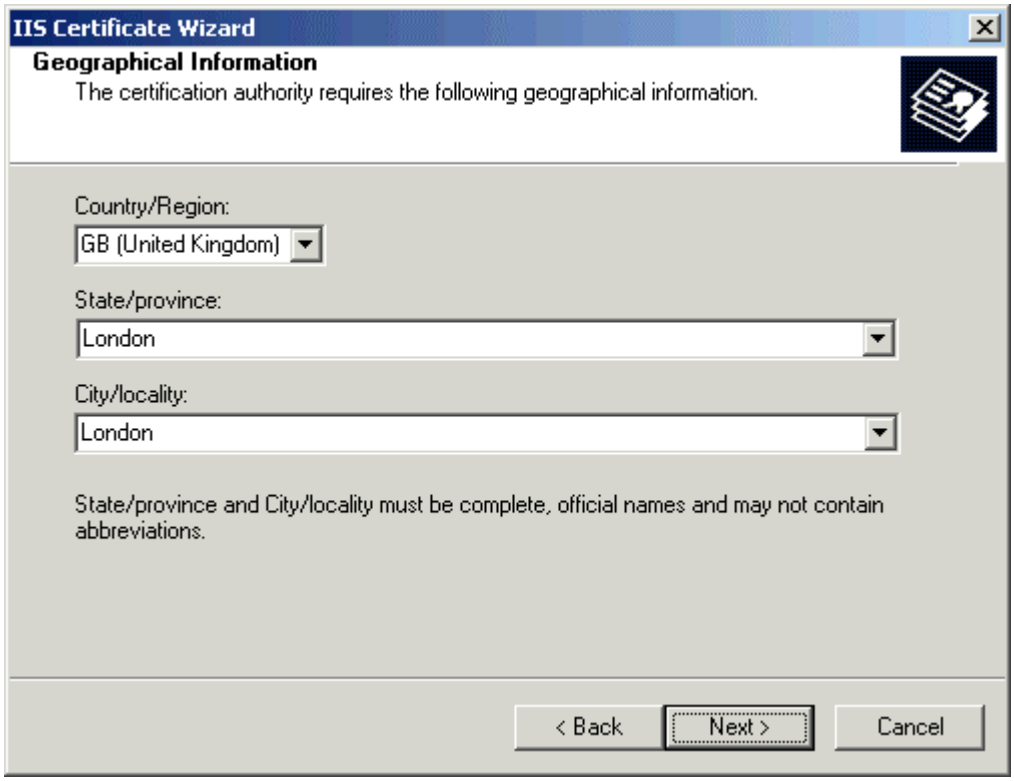


9. Click **Next** to access the **Your Site's Common Name** section.

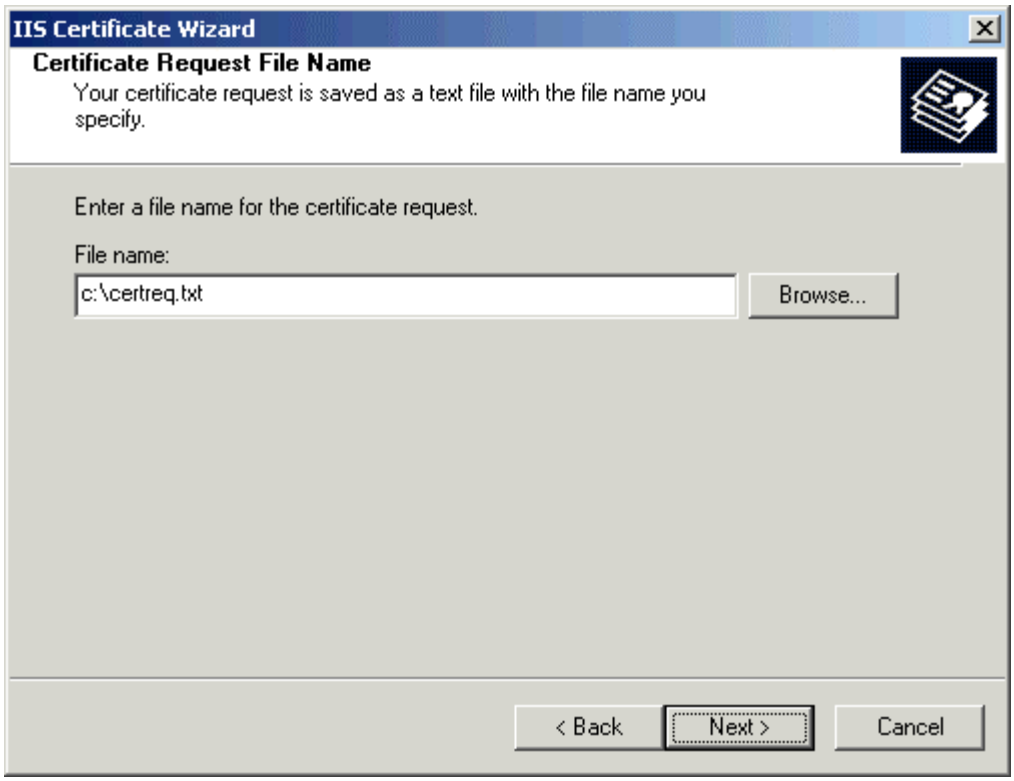


Note: The **Your Site's Common Name** section is responsible for binding the certificate to your Web site. For SSL certificates, enter the host computer name with the domain name. For Intranet servers, you may use the NetBIOS name of the computer that is hosting the site. Click **Next** to access geographical information.

10. Enter your country, state or province, and country or region information. Completely spell out your state or province and country or region; do not use abbreviations. Click **Next**.



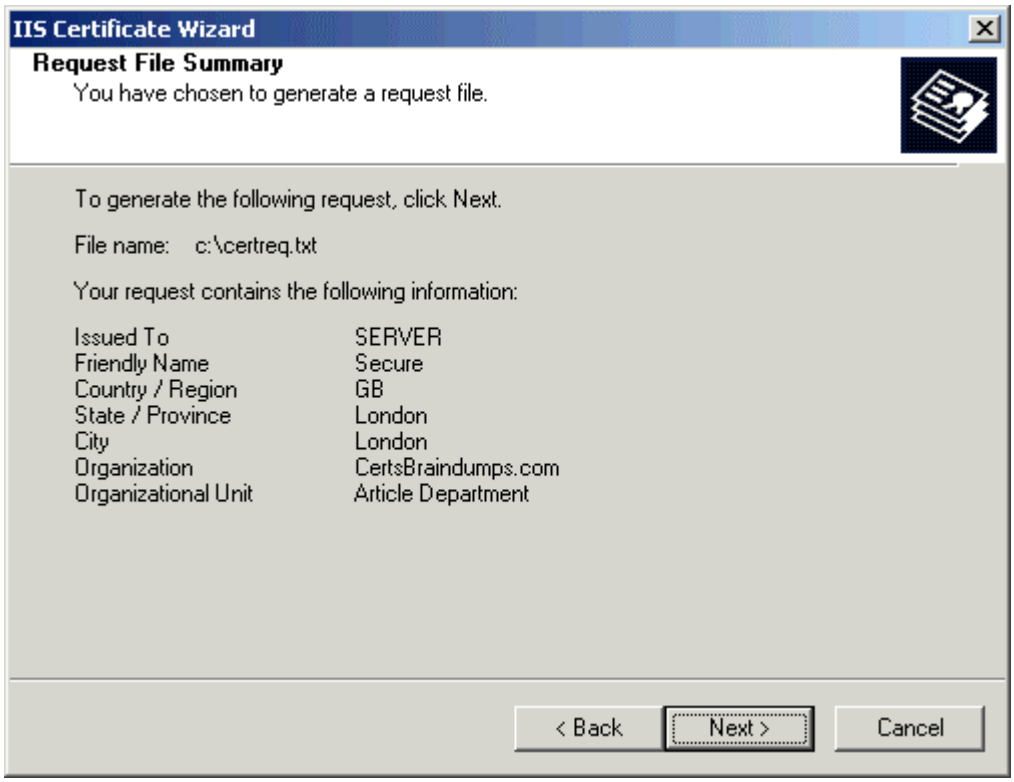
11. Save the file as a .txt file.



Note: When you actually send the request to the CA, you must paste the contents of this file into the request. This file will be encrypted and contain a header and footer for the contents. You must include both the header and footer when you request the certificate. A CSR should resemble the following:

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDATCCAmoCAQAwbDEOMAwGA1UEAxMFcGxhbjgxDDAKBgNVBAsTA1BTUzE
SMBAGA1UEChMJTWljcm9zb2Z0MRIwEAYDVQQHEwlDaGFybG90dGUxFzAVBg
NVBAgTDk5vcnRoIENhcm9saW5hMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w
0BAQEFAAOBjQAwgYkCgYEAtW1koGfdt+EoJbKdxUZ+5vE7TF1ZuT+xaK9jEWHE
Sfw11zoRKrHzHN0fASnwg3vZ0ACteQy5SiWmFaJeJ4k7YaKUb6chZXG3GqL4YiSK
FaLpJX+YRiKMtmIJzFzict5GVVGHsa1lY0BDYDO2XOAlstGlHCtENHOKpzdYdANR
g0CAwEAAaCCAVMwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMDUGCis
GAQQBgjcCAQ4xJzAlMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggrBgE
FBQcDATCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8
AZgB0ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbw
BnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByA4GJAGKa0jzBn8fkxSc
rWsdnU2eUJOMUK5Ms87Q+fjP1/pWN3PJnH7x8MBc5isFCjww6YnIjD8c3OfYfjkmW
c048ZuGoH7ZoD6YNfv/SfAvQmr90eGmKOFFiTD+hl1hM08gu2oxFU7mCvfTQ/2IbX
P7KYFGEqaJ6wn0Z5yLOByPqblQZAAAAAAAAAAAwDQYJKoZIhvcNAQEFBQADg
YEAhpzNy+aMNHAmGUXQT6PKxWpaxDSjf4nBmo7oMhfC7CIvR0McCQ+CBwuLz
D+UJxl+kjgb+qwcOUkGX2PCZ7tOWzcXWNmn/4YHQl0MGEXu0w67sVc2R9DlsHD
NzeXLIOmjUl935qy1uoIR4V5C48YNsF4ejlgjeCFsbCojJb9/2RM=
-----END NEW CERTIFICATE REQUEST-----

12. Confirm your request details. Click **Next** to finish, and exit the Web Server Certificate Wizard.

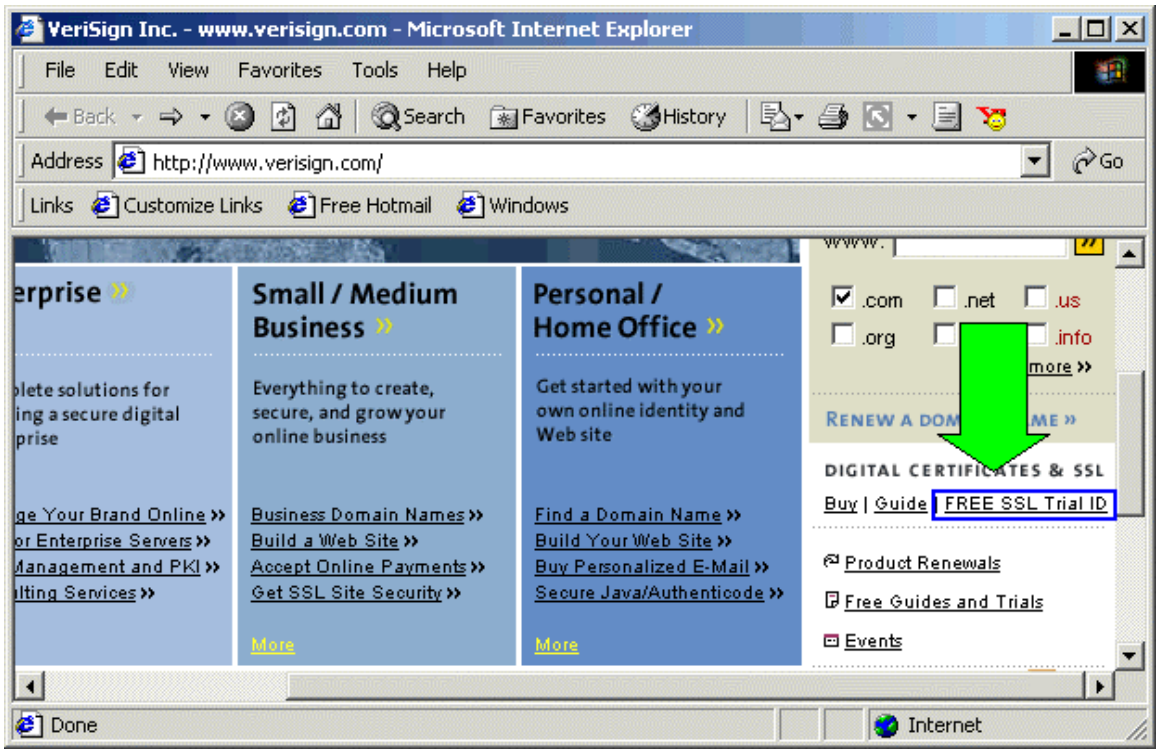


The CSR generating steps has been completed.

Requesting a Trial Certificate:

Certificates are obtained from the CA (Certificate Authorities). Different Third-Party CA(s) offer a trial certificate free of cost. Here we will request a server certificate to Verisign (a popular CA) on Internet.

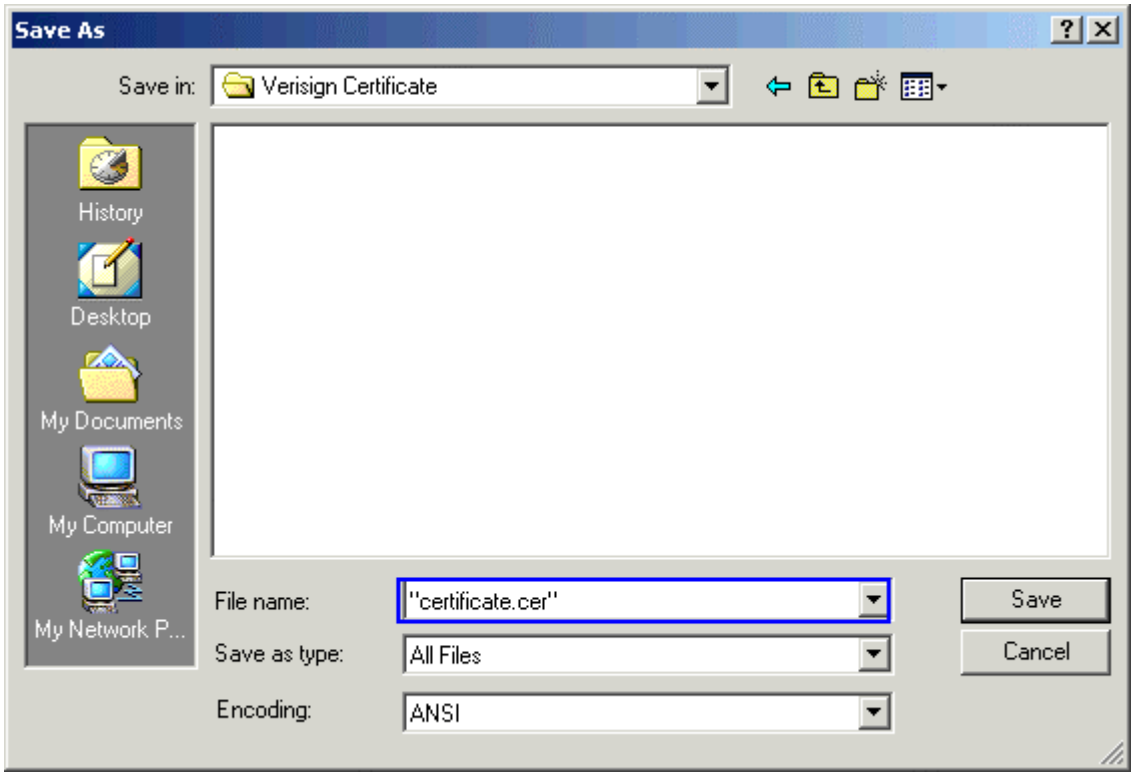
1. Launch your browser, Open www.verisign.com website and find the link for Free Trial SSL Id as shown below.



2. Fill out your Registration Information with a valid E-mail address to receive the digital certificate.
3. Follow the different steps (Normally five on Verisign) of online application to obtain the certificate.
   Note: The CA can change the whole enrollment procedure according to its own policy.
4. Verisign will mail you with your digital certificate and instruction about using it.

Obtaining the Trial Certificate:

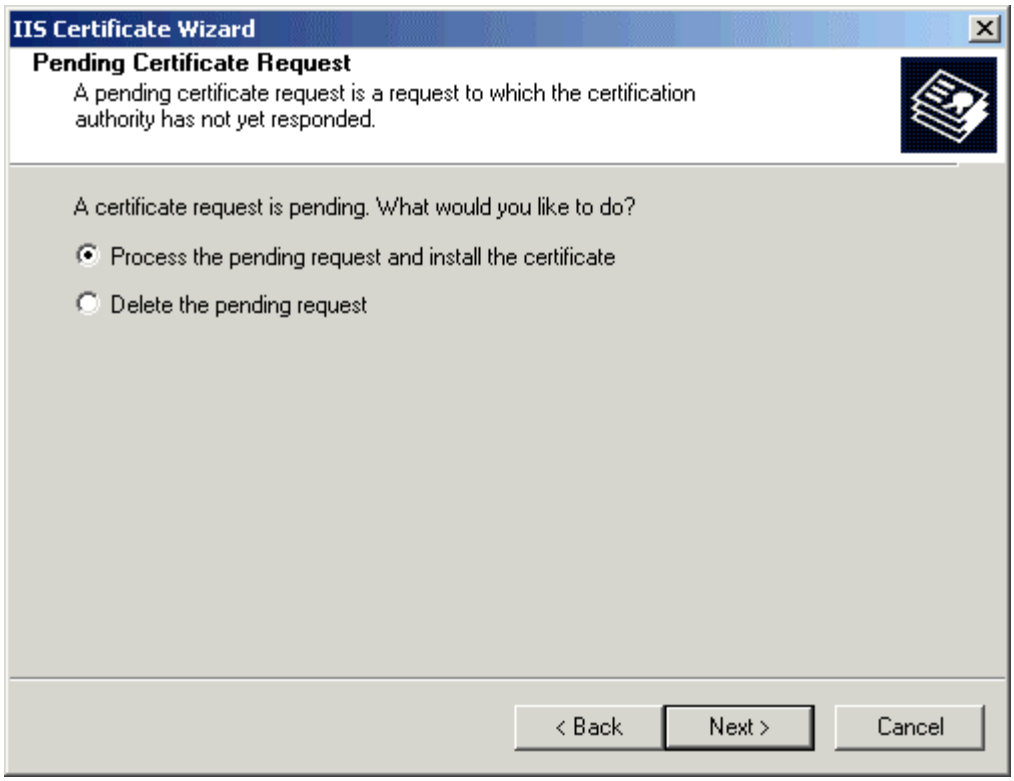
You will receive an e-mail from Verisign containing the same CSR text as you have sent it to but with a digitally signed signature. Just copy that text, paste it in a notepad and save the file with .Cer extension. Its your digital certificate.



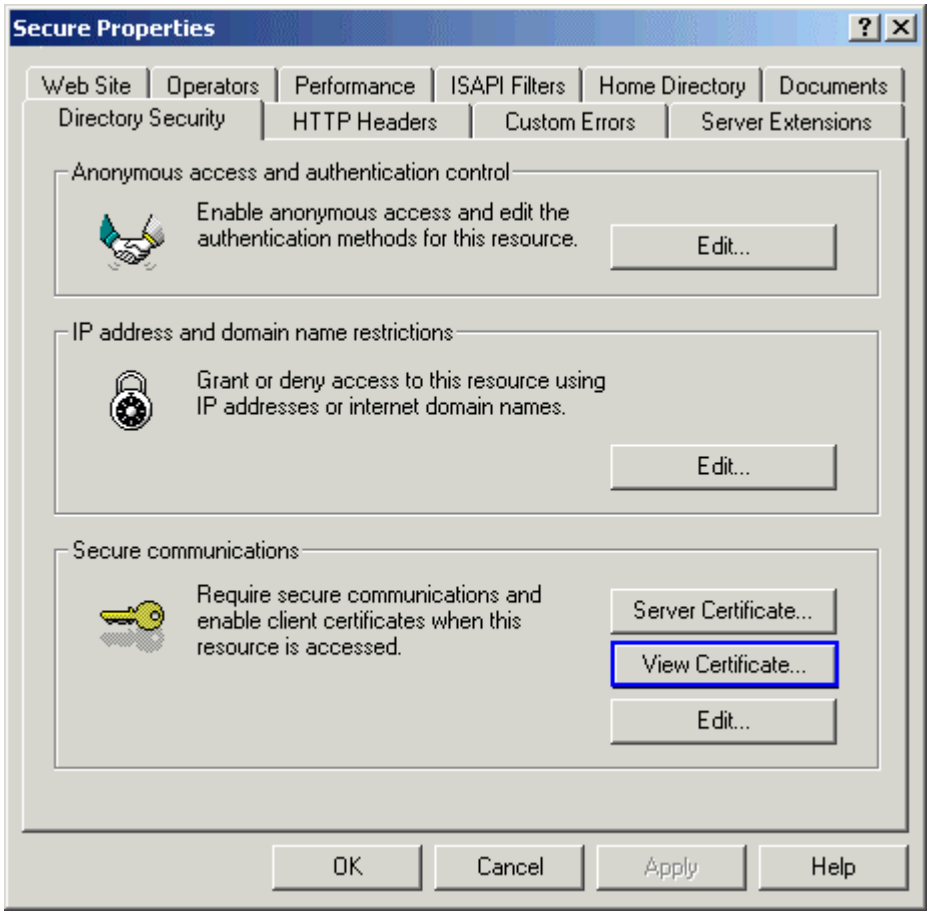
Installing the Trial Certificate:

To install the certificate, follow these steps:

1. Open the IIS MMC as described in the "Generating the CSR" section.
2. Access the **Properties** dialog box for the Web site on which you are installing the certificate.
3. Click the **Directory Security** tab and click **Server Certificate**. This starts the Web Server Certificate Wizard. Click **Next**.
4. Select **Process the Pending Request and install the certificate** and click **Next**.



5. Browse to the file that you saved in previous step with .cer extension. Verify the certificate summary, click **Next** twice, then click **Finish**.
6. After Finishing the wizard, you can view the installed certificate with the private key by clicking on the View Certificate Tab as shown below.

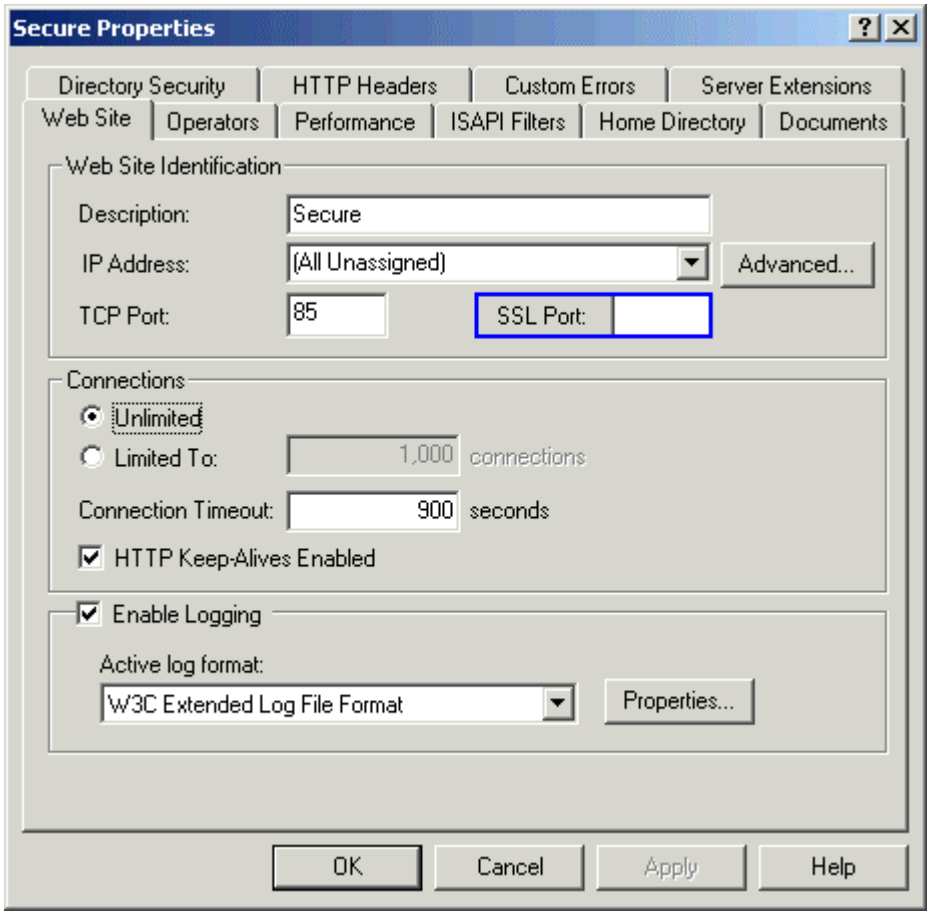


Note: This trial certificate is valid for only fifteen days

Enforcing SSL and testing secure site:

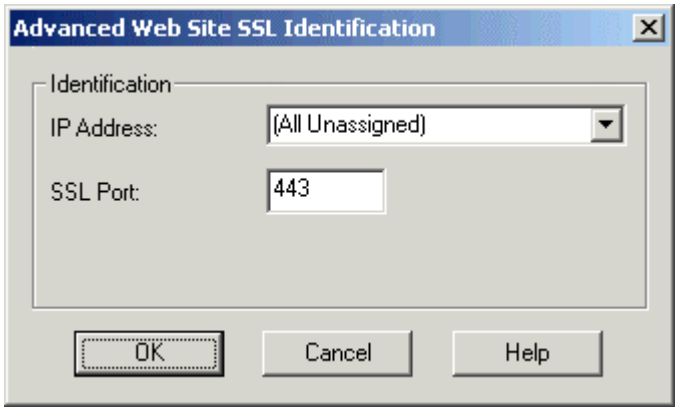
Now that the server certificate is installed, you can enforce SSL secure channel communications with clients of the Web server. First, you need to enable port 443 for secure communications with the Web site. To do this, follow these steps:

1. Right-click the secure Web site on and click **Properties**.
2. Click the **Web Site** tab. In the **Web Site Identification** section, verify that the **SSL Port** field is populated with the numeric value **443**.

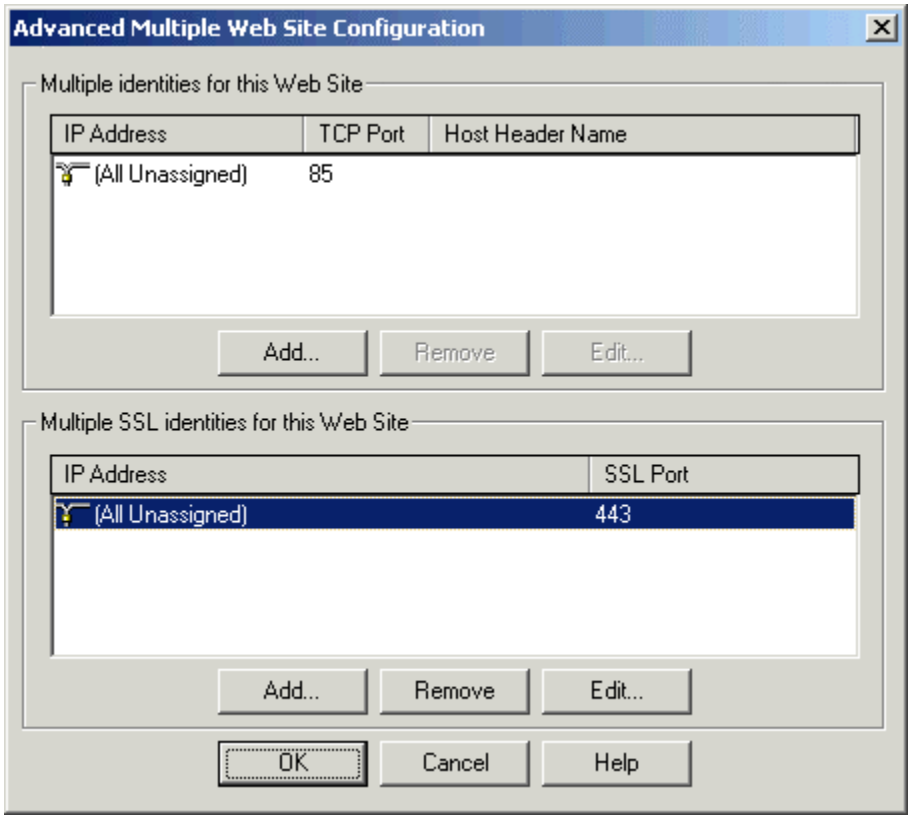


If SSL port is not populated with 443 port number, follow the next step.

3. Click **Advanced**. You should see two fields. The IP address and port of the Web site should already be listed in the **Multiple identities for this web site** field. Under the **Multiple SSL Identities for this web site** field, click **Add** if port 443 is not already listed. Select the server's IP address, and type the numeric value **443** in the **SSL Port** field. Click **OK**.

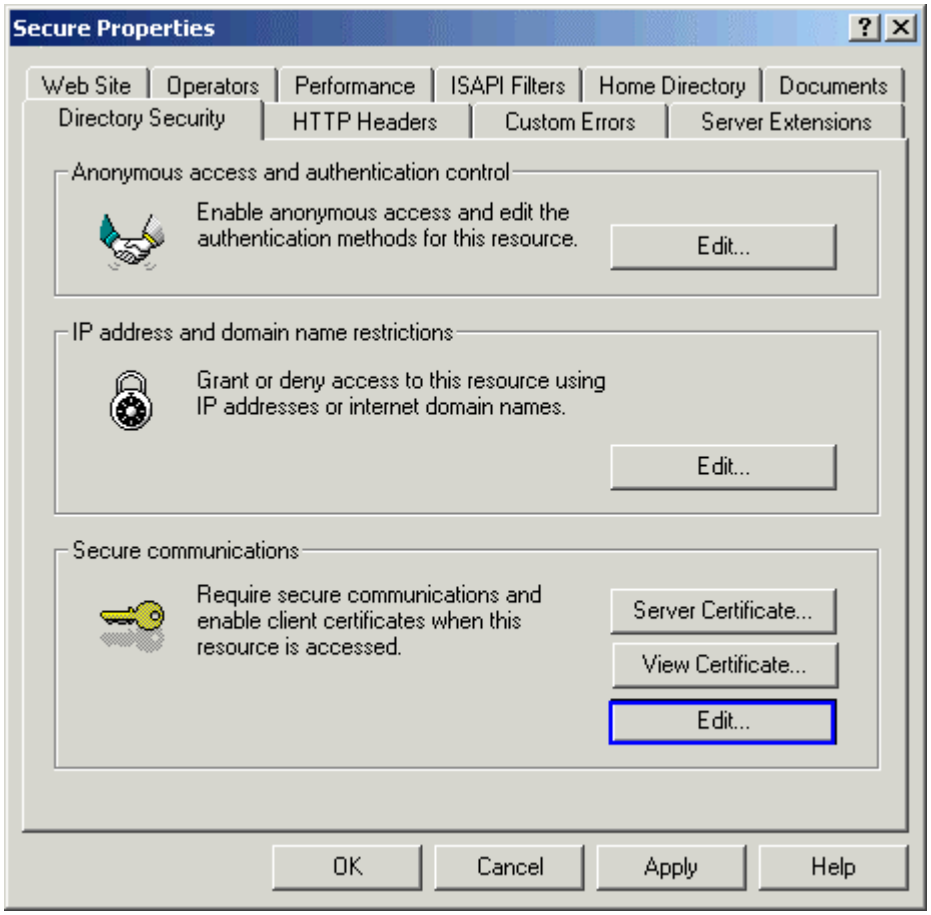


4. Click **Ok** to close the Advanced Website configuration Windows.



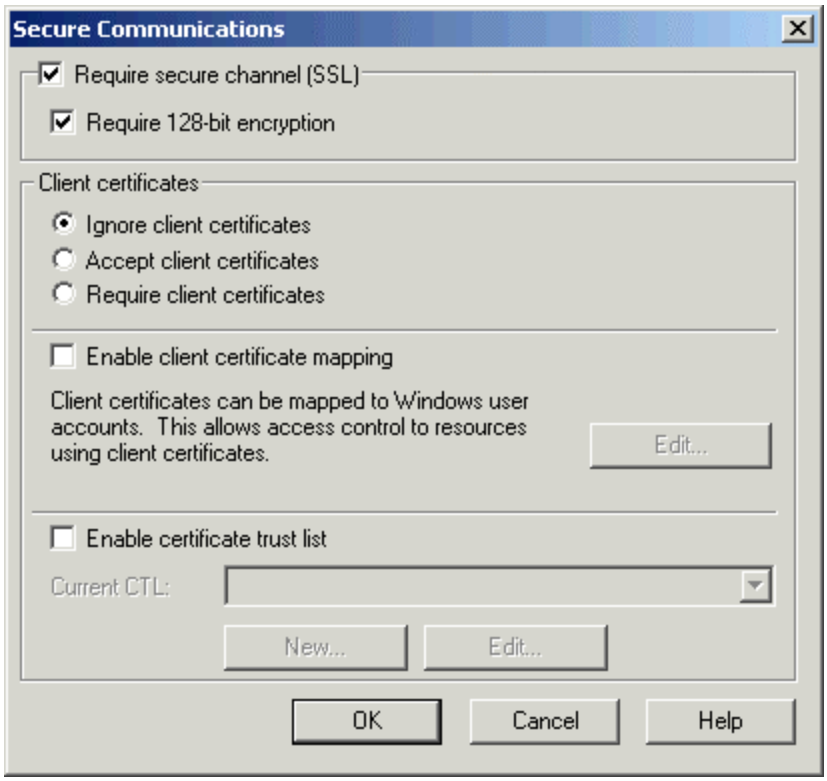
Now that port 443 is enabled, you can enforce SSL connections. To do this, follow these steps:

1. Click the **Directory Security** tab. In the **Secure Communications** section, note that **Edit** is now available. Click **Edit**.

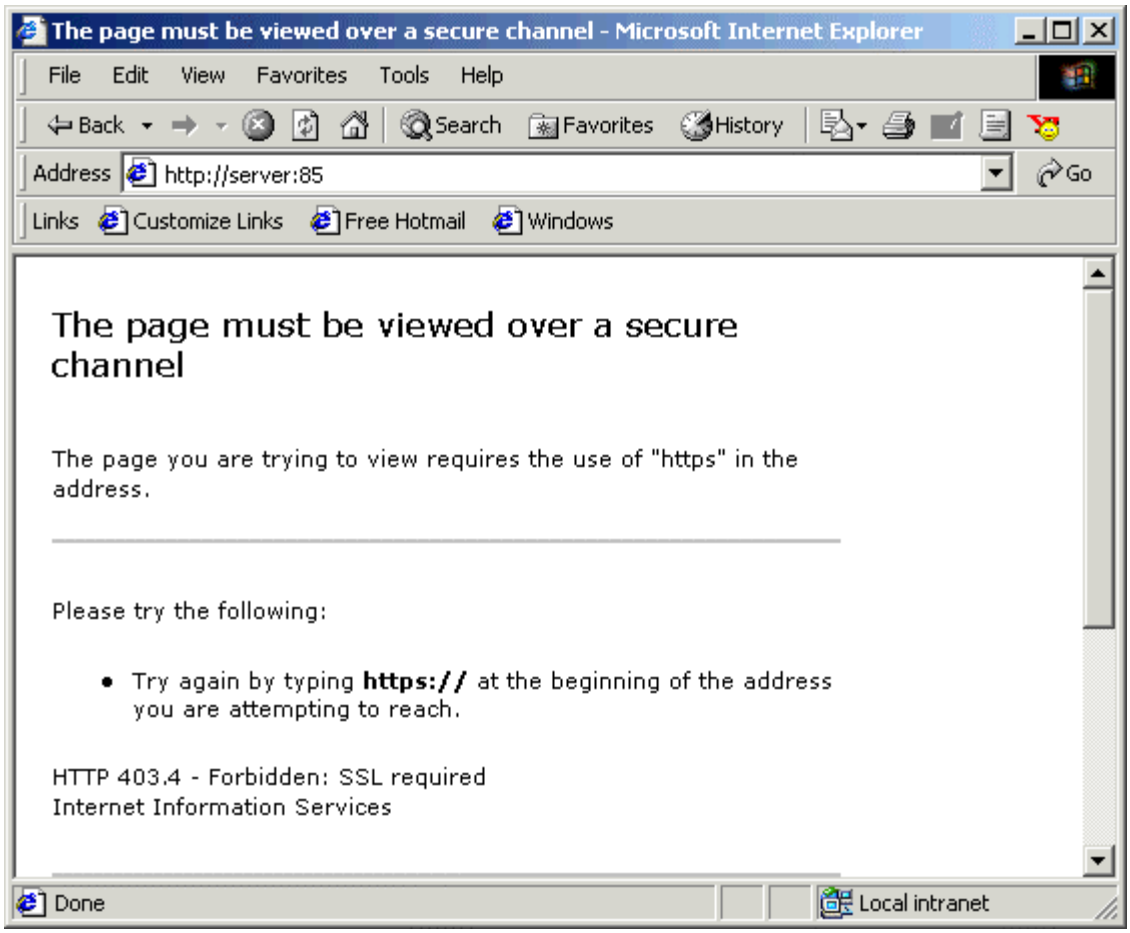


1. Select **Require Secure Channel (SSL)**.

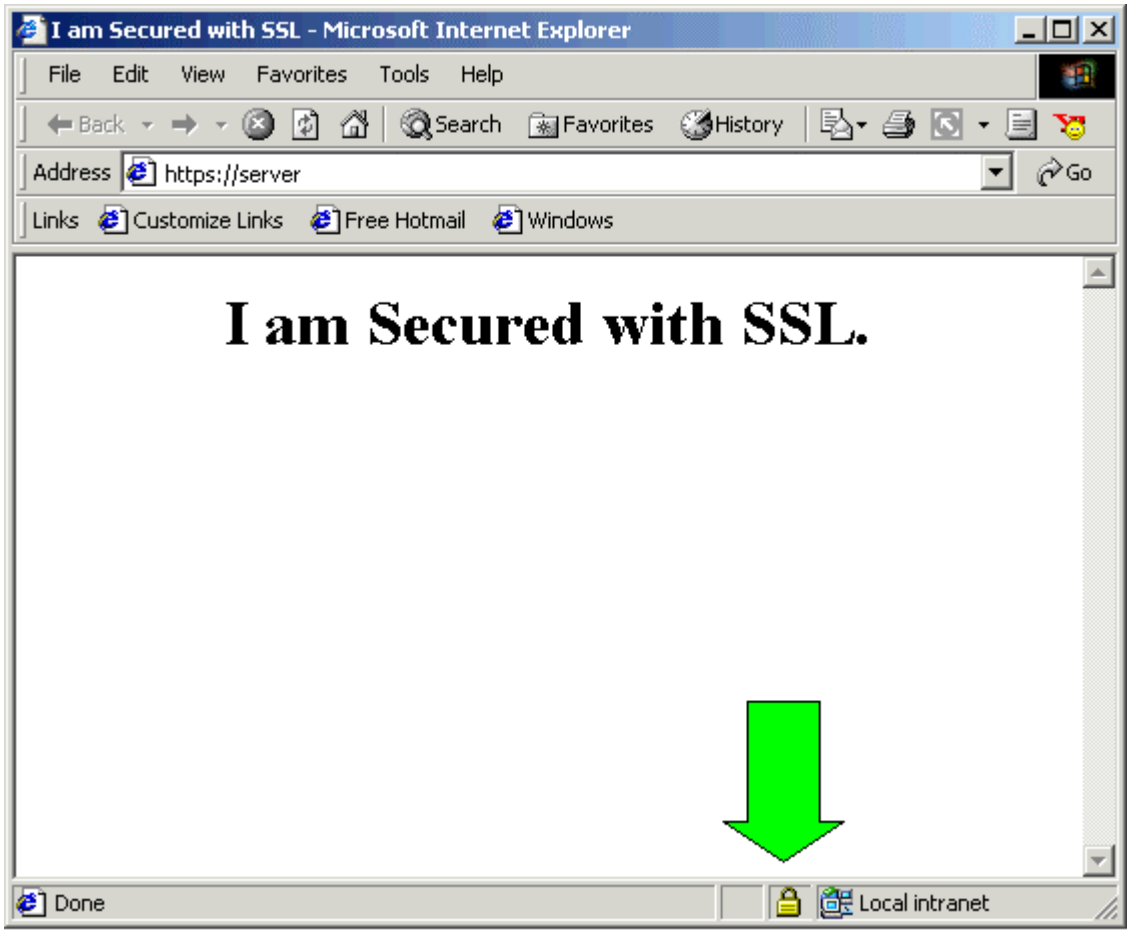
   NOTE: If you specify 128-bit encryption, clients who use 40-bit or 56-bit strength browser will not be able to communicate with your site unless they upgrade their encryption strength.



2. Open your browser and try to connect to your Web server by using the standard http:// protocol. If SSL is being enforced, you receive the following error message:



3. Now access your server with the https://Server URL. Your secure site with SSL enabled will be shown.



SSL Secured (128 Bit)

Important Note:

Before using your Trial SSL Server ID, install the Test CA Root in each browser you plan to use as part of your test of SSL. To download the Test CA Root, Click on the link (Like this http://www.verisign.com/support/install/index.html#trial) provided you in your e-mail and follow the instructions there.

If you like this article, then please give your comments in the forum and cast your vote for this topic.