Setting Up SSL on IIS6 for MEGA Advisor

Revised: July 5, 2012

Created: February 1, 2008

Author: Melinda BODROGI

CONTENTS

PRINCIPLE

By default, web browsing is performed through the use of the HTTP protocol, i.e. a connection between the client computer (using a web browser) and the web server (using IIS, Apache or any other sort of web server program). HTTP relies on TCP (Transmission Control Protocol) and uses port 80 on the listening server.

The main security issue with HTTP is the fact that all traffic between the client and the server is in the form of clear text, which means that anyone could potentially "listen" and grab valuable information from the net.

To secure the transmission of information between your web server running IIS 6.0 on Windows Server 2003 and your browser clients, you can encrypt the information being transmitted by using SSL (Secure Sockets Layer).

In order to successfully use SSL, you need to obtain a Server Certificate. This article only describes the case of obtaining a certificate from a local CA (Certificate Authority) or importing an already existing certificate. However, it is possible (and in many cases preferred) to use a Server Certificate issued by a trusted 3rd party CA, such as Verisign.

This document describes a concrete example of setup on a server with the following configuration:

- OS: Windows 2003 Sever SP2 Standard Edition
- IIS6
- Internet Explorer 6.0, SP2

Note:

You can deploy secured and unsecured Web sites on the same server however, the example in this document deals with a given web site (the MEGA Advisor web site) which does not remain accessible via HTTP but only via HTTPS.

REQUIREMENTS

This article assumes that you already have MEGA Advisor working on your IIS 6 Web server. The MEGA Advisor login page should be accessible via the http://localhost:8080/advisor URL.

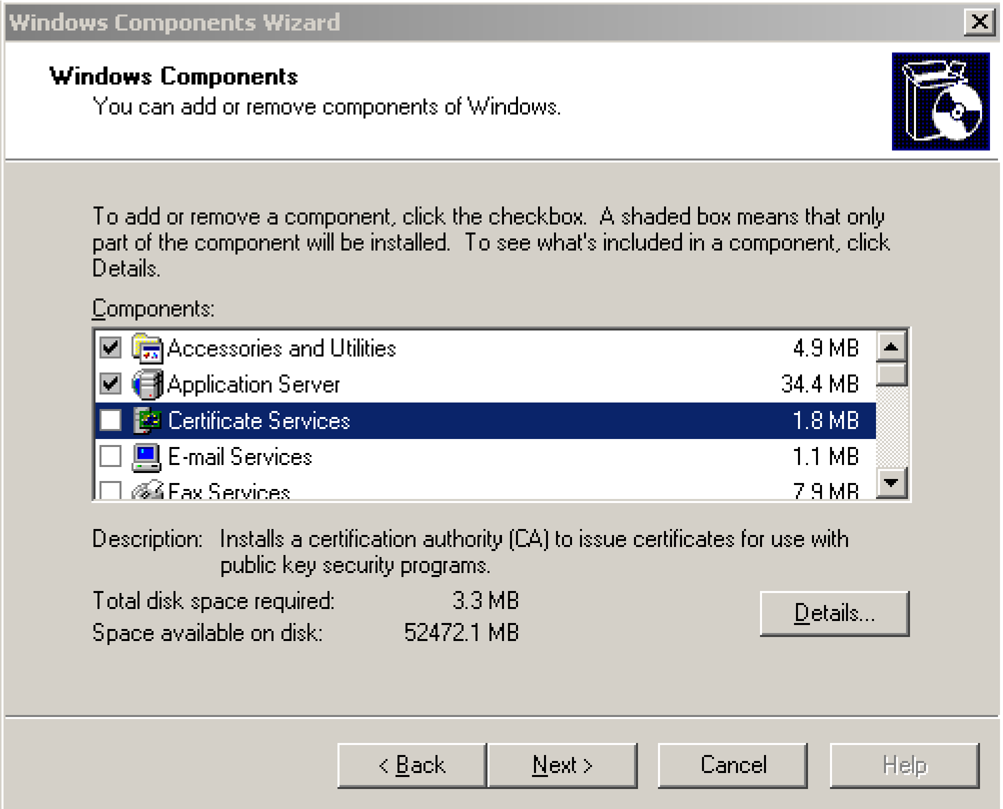
For further information on how to set up MEGA Advisor, please see the "MEGA Advisor Step by Step Setup on IIS6 (Windows 2003 Server)" document.

INSTALL THE CERTIFICATION AUTHORITY SERVICE

If the Certification Authority Service is already installed on your server, please skip this step.

To install the CA service:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. In **Add or Remove Programs**, click **Add/Remove Windows Components**.
3. In the list of components, check **Certificate Services**.



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

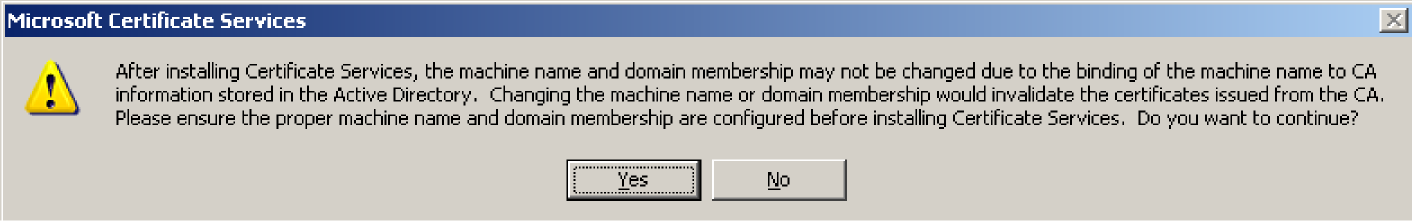
Components:

☑	Accessories and Utilities	4.9 MB
☑	Application Server	34.4 MB
□	Certificate Services	1.8 MB
□	E-mail Services	1.1 MB
□	Fax Services	7.9 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 3.3 MB
Space available on disk: 52472.1 MB

A warning message appears concerning domain membership and computer renaming constraints.



Microsoft Certificate Services

After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?

4. Click **Yes** to continue.

5. On the CA **Type** page that appears, click **Enterprise root CA**, then click **Next**.

6. On the CA **Identifying Information** page, in the **Common name for this CA** box, type the name of the server, and then click **Next**.

7. On the **Certificate Database Settings** page, accept the defaults in the **Certificate database box** and the **Certificate database log** box, and then click **Next**.

You will get a prompt to stop Internet Information Services.

8. Click **Yes**.

9. Enable **Active Server Pages (ASPs)** by clicking **Yes**.

10. When the installation process is completed click **Finish**.

CREATE A CERTIFICATE REQUEST

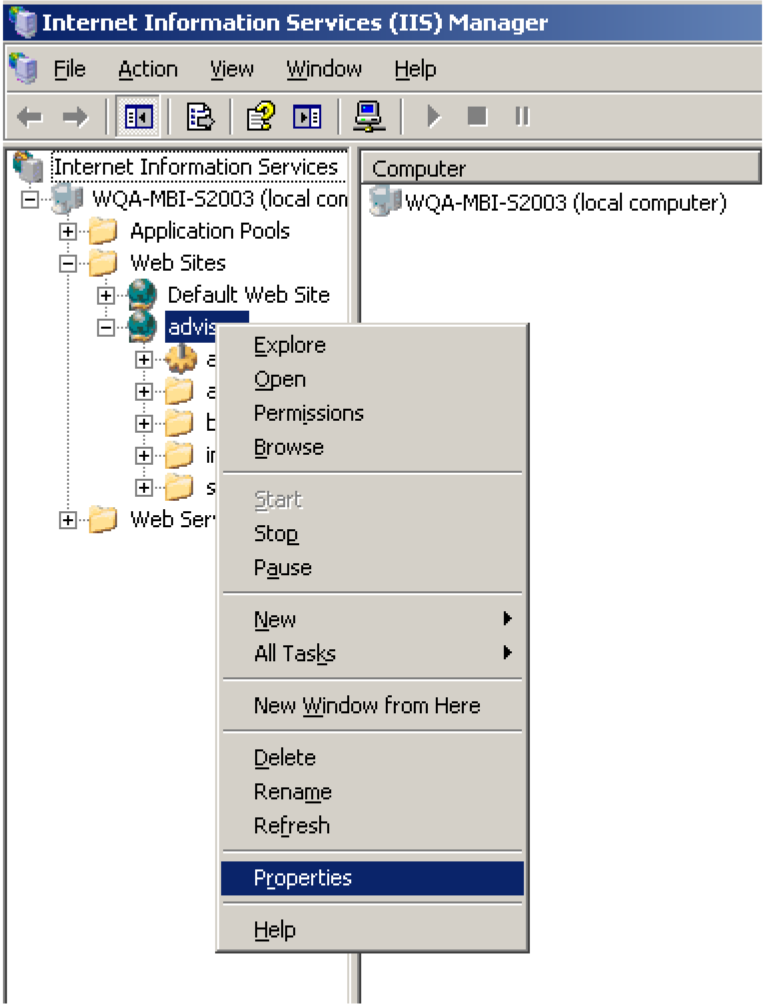
To enable SSL in IIS, you must first obtain a certificate that is used to encrypt and decrypt information transferred over the network. IIS includes its own certificate request tool that you can use to send a certificate request to a certification authority. This tool simplifies the process of obtaining a certificate.

In order to make a certificate request, follow the steps below:

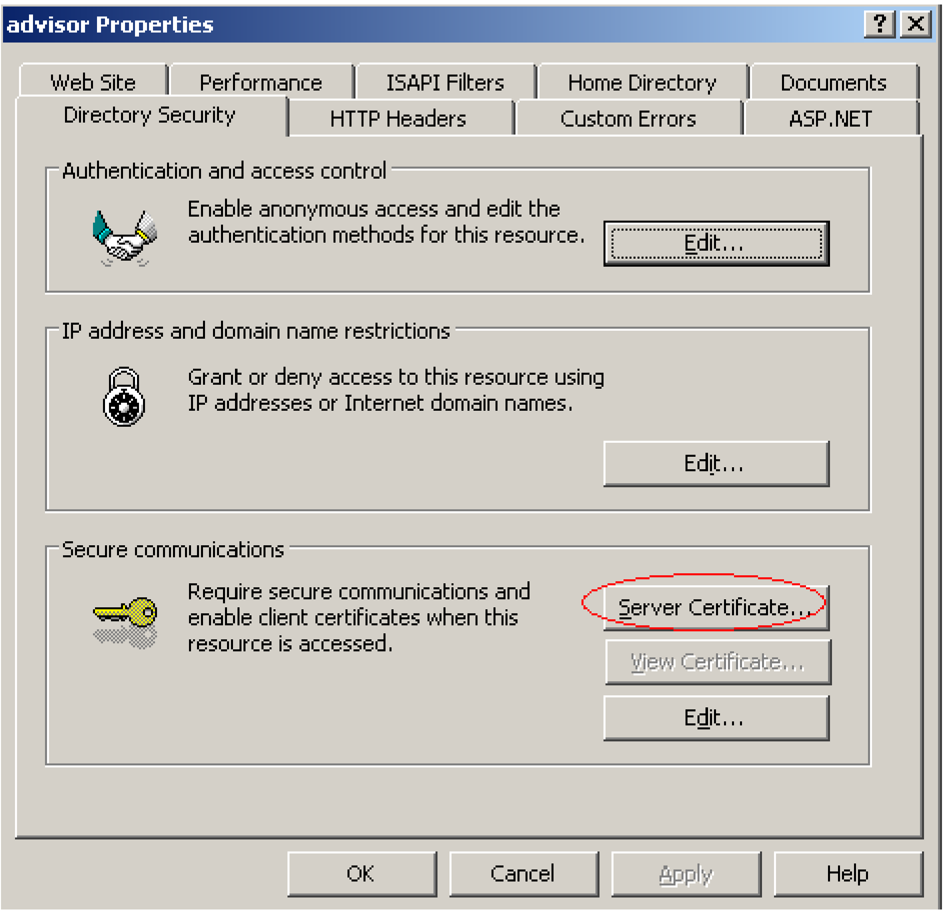
1. Start the **Internet Service Manager (ISM)**, which loads the Internet Information Server snap-in for the Microsoft Management Console (MMC) via **Start > Programs > Administrative Tools > Internet Service Manager** or **Internet Information Services (IIS) Manager**.

2. Double-click the server name in order to display all the Web sites, and expand the **Web Sites** folder.

3. Right-click the Web site (advisor) on which you want to install the certificate, and then click **Properties**.



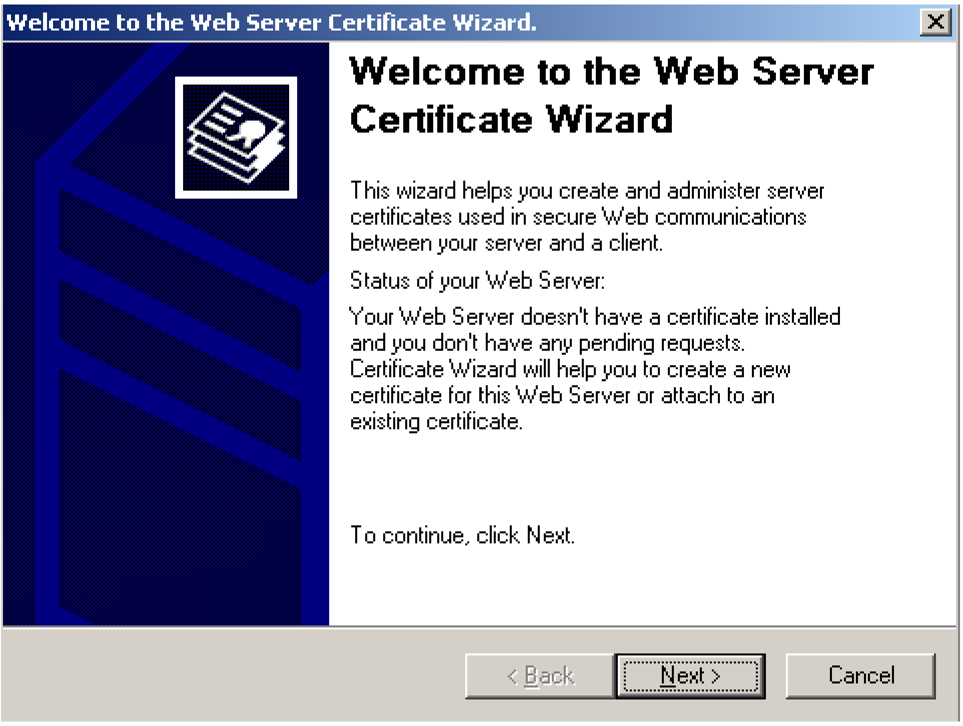
4. Click the **Directory Security** tab, and then under **Secure Communications**, click **Server Certificate** to start the Web Server Certificate Wizard.



Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or Internet domain names.

Require secure communications and enable client certificates when this resource is accessed.



Welcome to the Web Server Certificate Wizard.

Welcome to the Web Server Certificate Wizard

This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

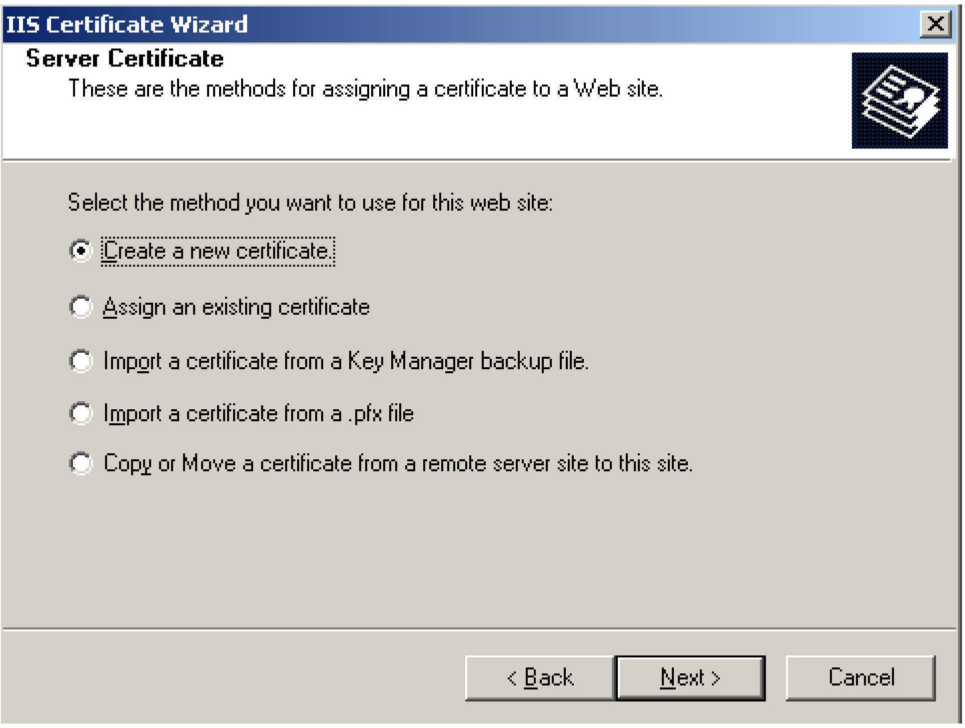
Status of your Web Server:

Your Web Server doesn't have a certificate installed and you don't have any pending requests. Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.

To continue, click Next.

5. Click **Next.**

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



IIS Certificate Wizard

Server Certificate

These are the methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

● Create a new certificate.

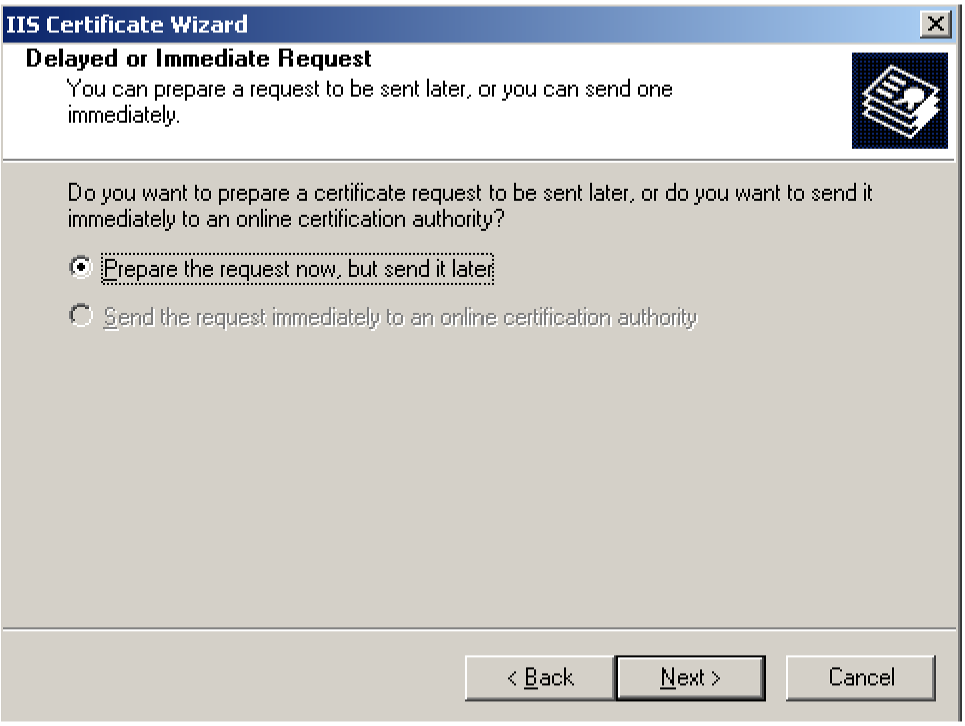
○ Assign an existing certificate

○ Import a certificate from a Key Manager backup file.

○ Import a certificate from a .pfx file

○ Copy or Move a certificate from a remote server site to this site.

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



Delayed or Immediate Request

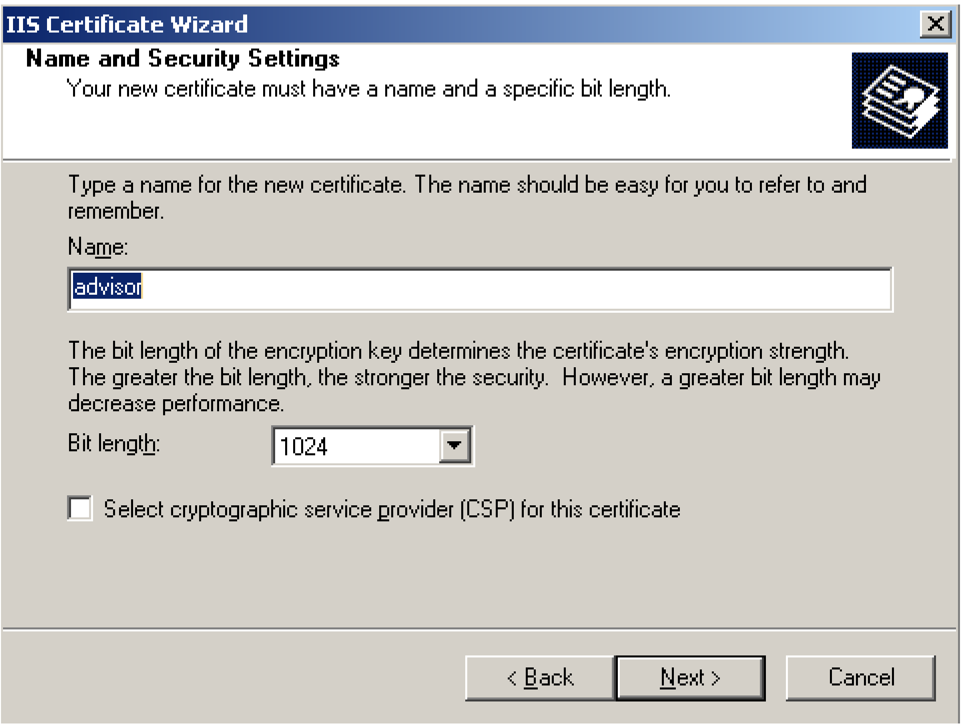
You can prepare a request to be sent later, or you can send one immediately.

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

8. Type a name for the certificate (advisor). You may want to match the certificate name to the name of the Web site. Now, select a bit length (the higher the bit length, the stronger the certificate encryption) and click **Next**.



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.

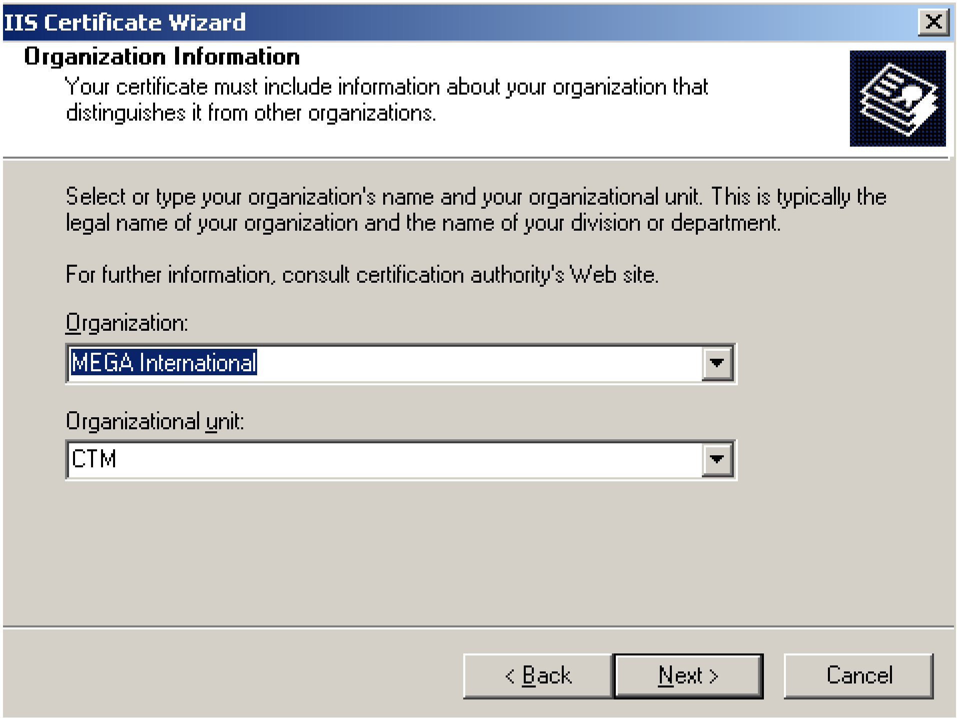
Name: advisor

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

□ Select cryptographic service provider (CSP) for this certificate

9. Type the name of your organization and the organizational unit and click **Next**.



IIS Certificate Wizard

Organization Information

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

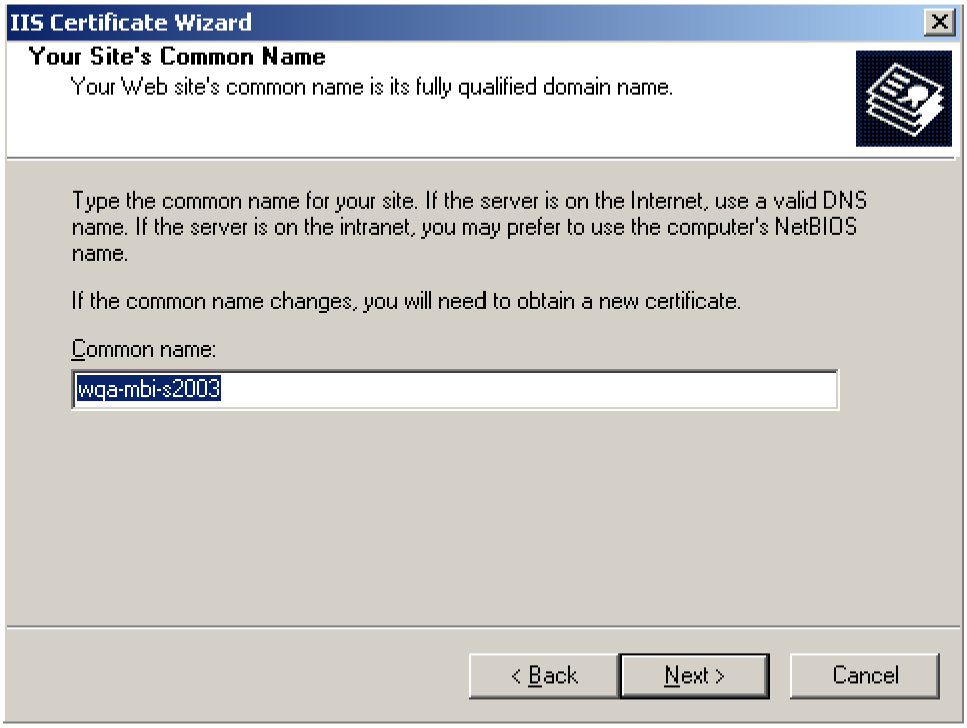
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

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

Organization: MEGA International

Organizational unit: CTM

10. Type either the fully qualified domain name (FQDN) or the server name as the common name. If you are creating a certificate that will be used over the Internet, it is preferable to use a FQDN. Click **Next**.



IIS Certificate Wizard

Your Site's Common Name

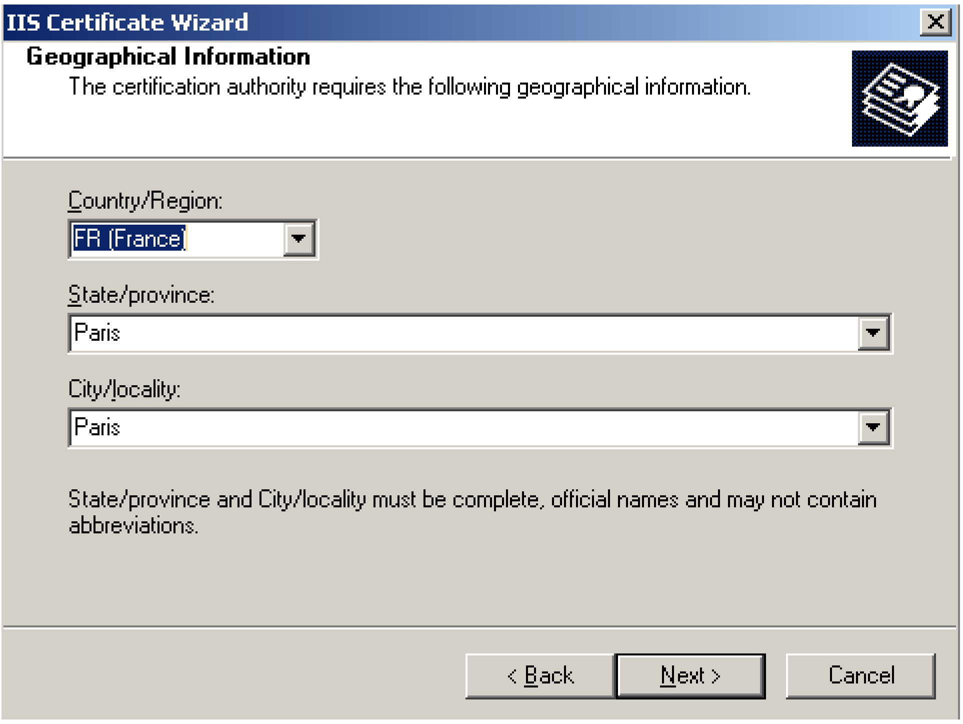
Your Web site's common name is its fully qualified domain name.

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: wga-mbi-s2003

11. Enter your location information, and then click **Next**.



IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

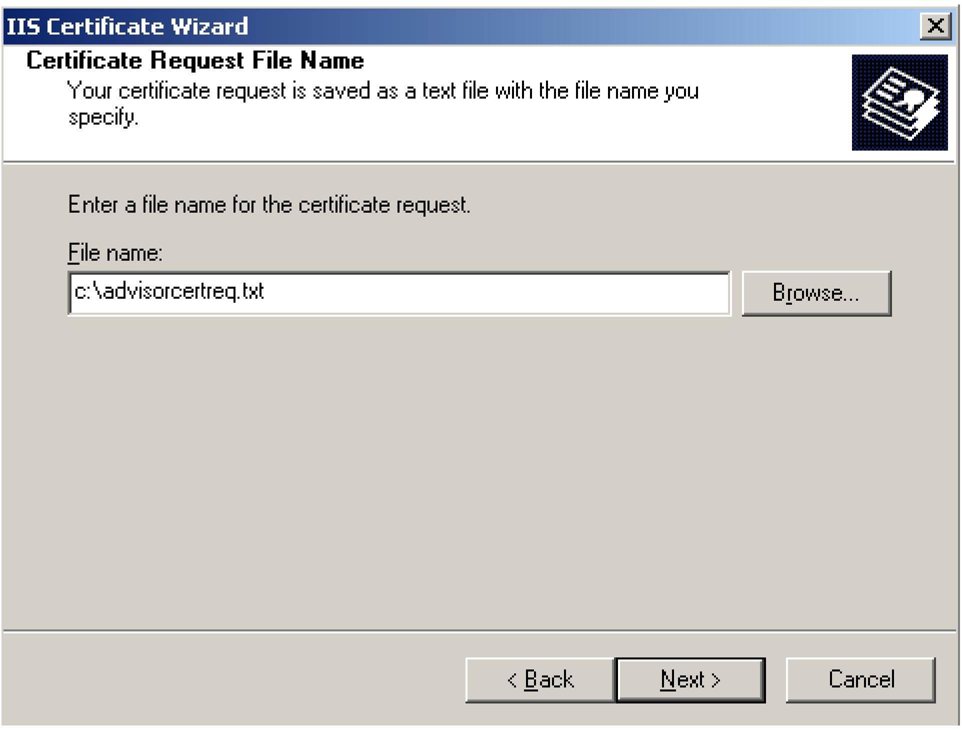
Country/Region: FR (France)

State/province: Paris

City/locality: Paris

State/province and City/locality must be complete, official names and may not contain abbreviations.

12. Type the path and name of the file to which the certificate information will be saved, and click **Next** to continue.



IIS Certificate Wizard

Certificate Request File Name

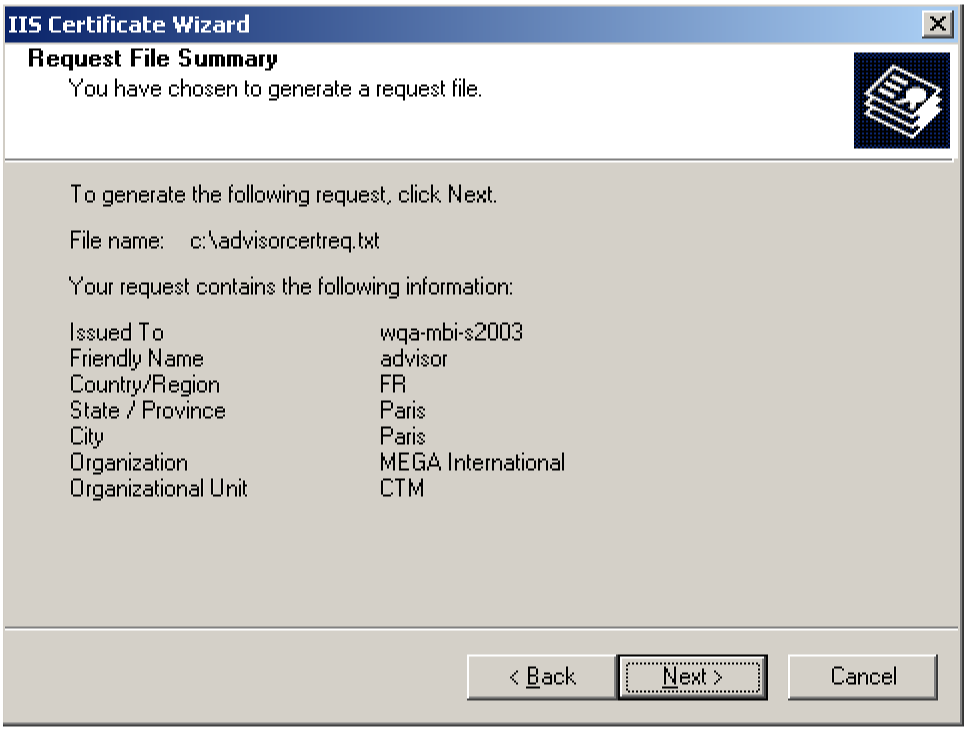
Your certificate request is saved as a text file with the file name you specify.

Enter a file name for the certificate request.

File name: c:\advisorcertreq.txt

Note: If you type anything other than the default location and file name, be sure to note the name and location you choose, because you will have to access this file in later steps.

13. Verify the information you have typed then click **Next** to complete the process and create the certificate request.



Request File Summary

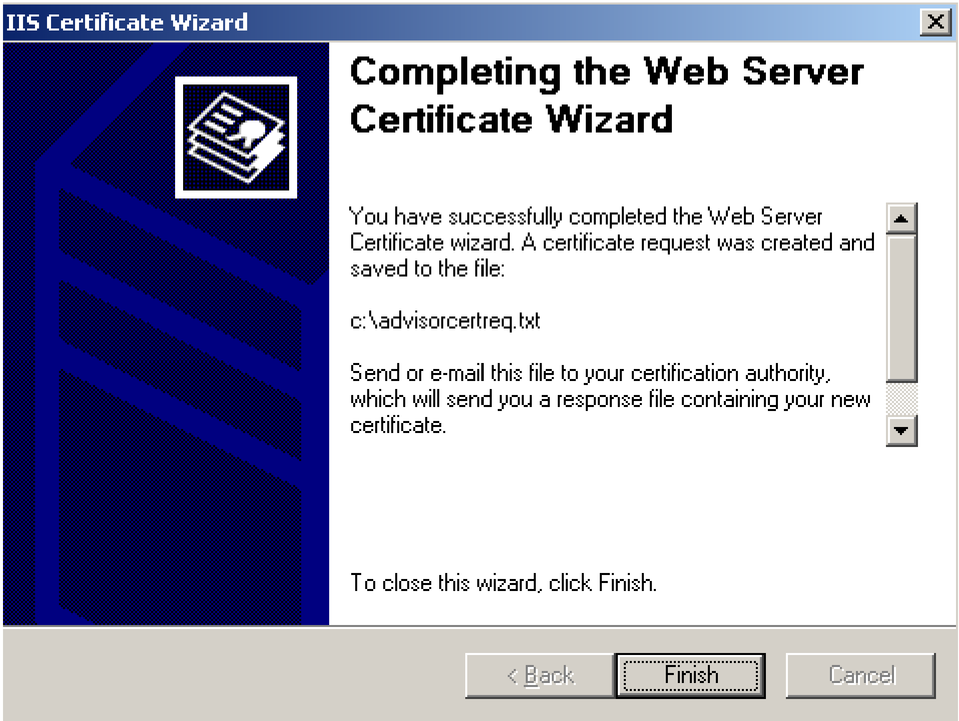
You have chosen to generate a request file.

To generate the following request, click Next.

File name: c:\advisorcertreq.txt

Your request contains the following information:

Issued To	wqa-mbi-s2003
Friendly Name	advisor
Country/Region	FR
State / Province	Paris
City	Paris
Organization	MEGA International
Organizational Unit	CTM



Completing the Web Server Certificate Wizard

You have successfully completed the Web Server Certificate wizard. A certificate request was created and saved to the file:

c:\advisorcertreq.txt

Send or e-mail this file to your certification authority, which will send you a response file containing your new certificate.

To close this wizard, click Finish.

SUBMIT THE CERTIFICATE REQUEST

The certificate request you just created needs to be submitted to a Certificate Authority (CA). This may be your own server with Certificate Server 2.0 installed on it or an online CA such as VeriSign. Contact the certificate provider of your choice and determine the best level of certificate for your needs.

There are different methods of submitting your request. You can:

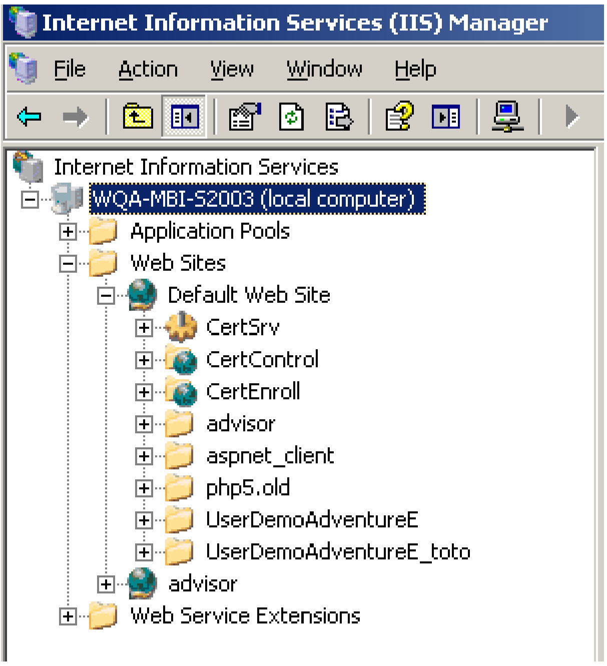
- Contact the Certificate Authority of your choice to request and receive your certificate.

- Create your own certificate with Certificate Server 2.0, but your clients must implicitly trust you as the Certificate Authority.

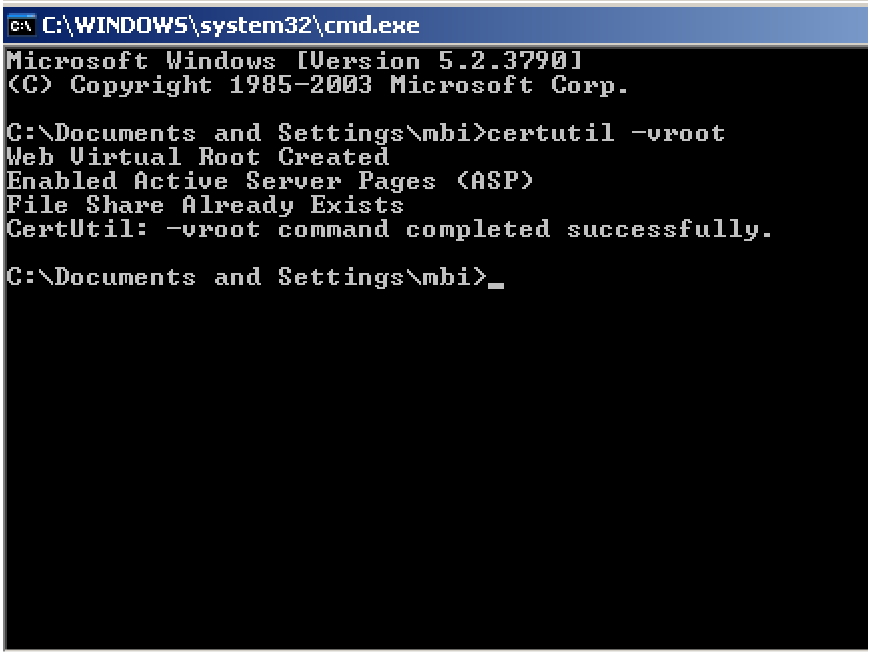
The steps indicated below are for submitting the certificate request if you are using Certificate Server 2.0 as the certificate provider.

Note: The IIS Certificate Wizard will only recognize the Default Web Server template. When you select an Online Enterprise CA, the Authority will not be listed unless the CA is using the Default Web Server template.

1. Open a browser and browse to http://YourWebServerName/CertSrv/.



Note: If CertSrv does not appear under "Default Web Site" please execute the "certutil –vroot" command.

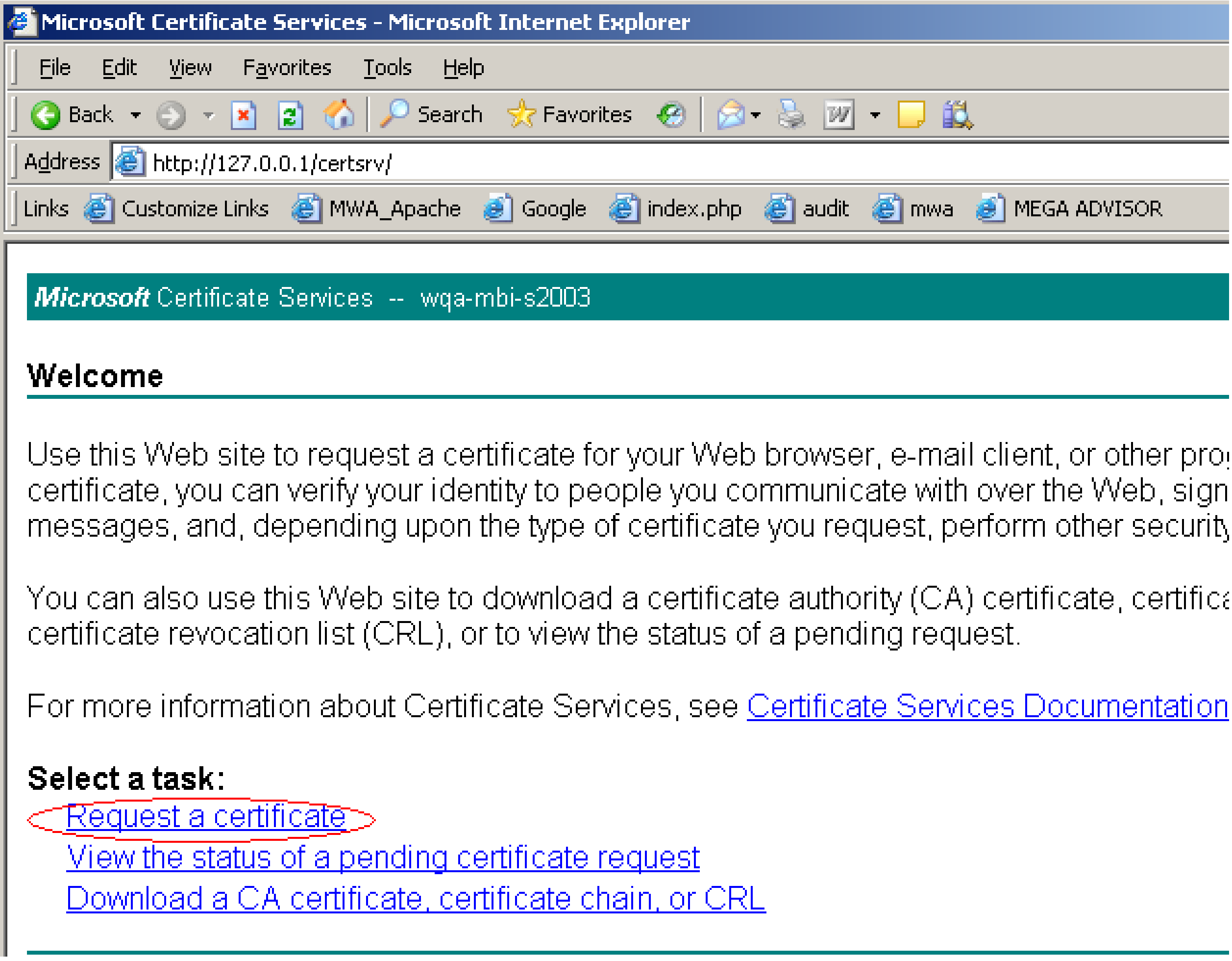


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\mbi>certutil -vroot
Web Virtual Root Created
Enabled Active Server Pages (ASP)
File Share Already Exists
CertUtil: -vroot command completed successfully.

C:\Documents and Settings\mbi>_
```

2. Click **Request a certificate.**


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/
Links Customize Links MWA_Apache Google index.php audit mwa MEGA ADVISOR

Microsoft Certificate Services -- wqa-mbi-s2003

Welcome

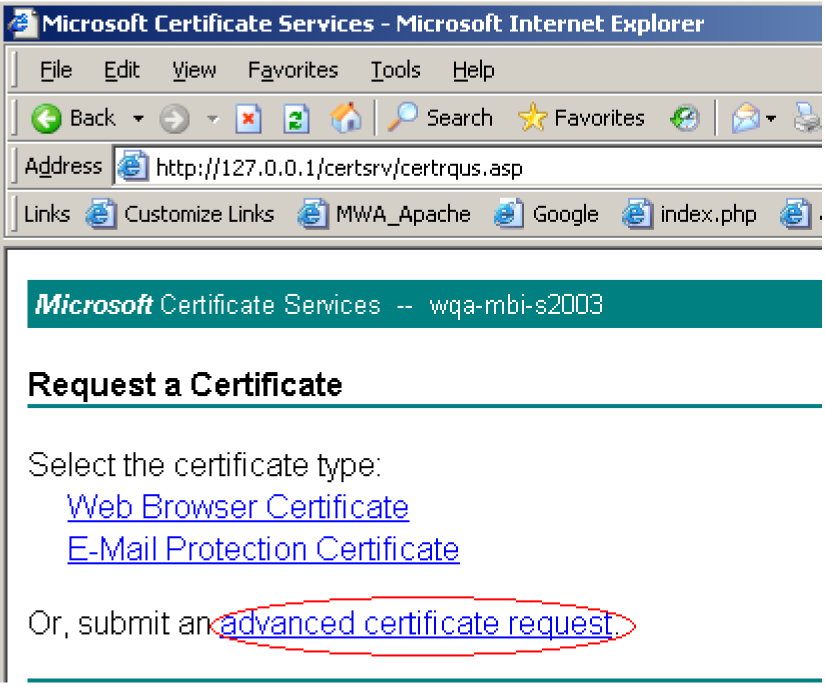
Use this Web site to request a certificate for your Web browser, e-mail client, or other pro certificate, you can verify your identity to people you communicate with over the Web, sign messages, and, depending upon the type of certificate you request, perform other security

You can also use this Web site to download a certificate authority (CA) certificate, certifica certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. Click **advanced certificate request.**


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certrqus.asp
Links Customize Links MWA_Apache Google index.php

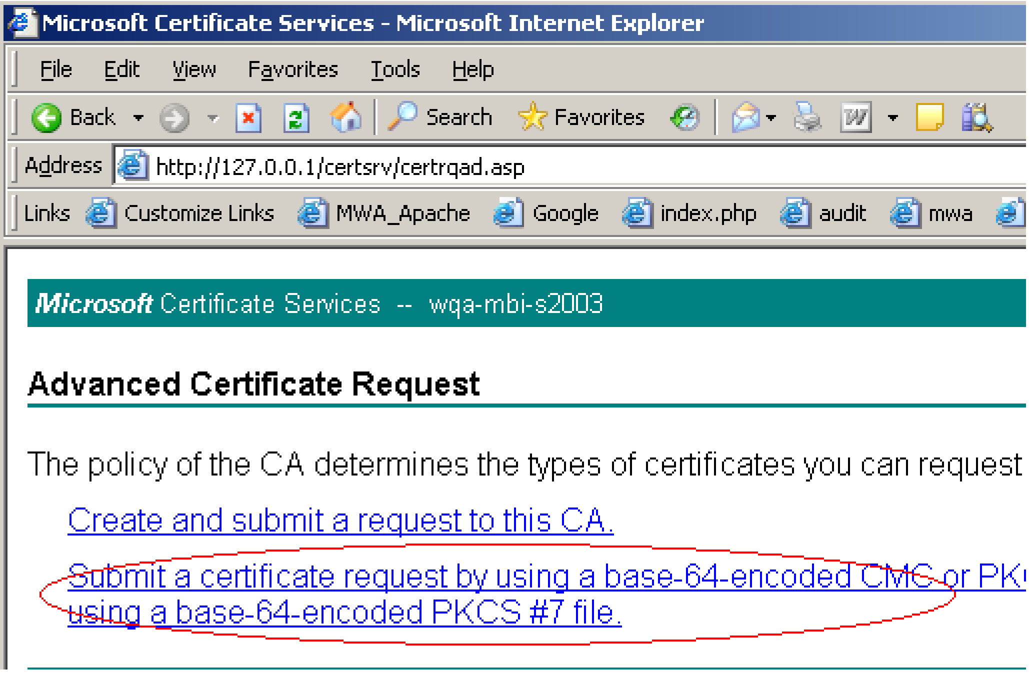
Microsoft Certificate Services -- wqa-mbi-s2003

Request a Certificate

Select the certificate type:
Web Browser Certificate
E-Mail Protection Certificate

Or, submit an advanced certificate request.

4. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file**, or submit a renewal request by using a base-64-encoded PKCS #7 file.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certrqad.asp
Links Customize Links MWA_Apache Google index.php audit mwa

Microsoft Certificate Services -- wqa-mbi-s2003

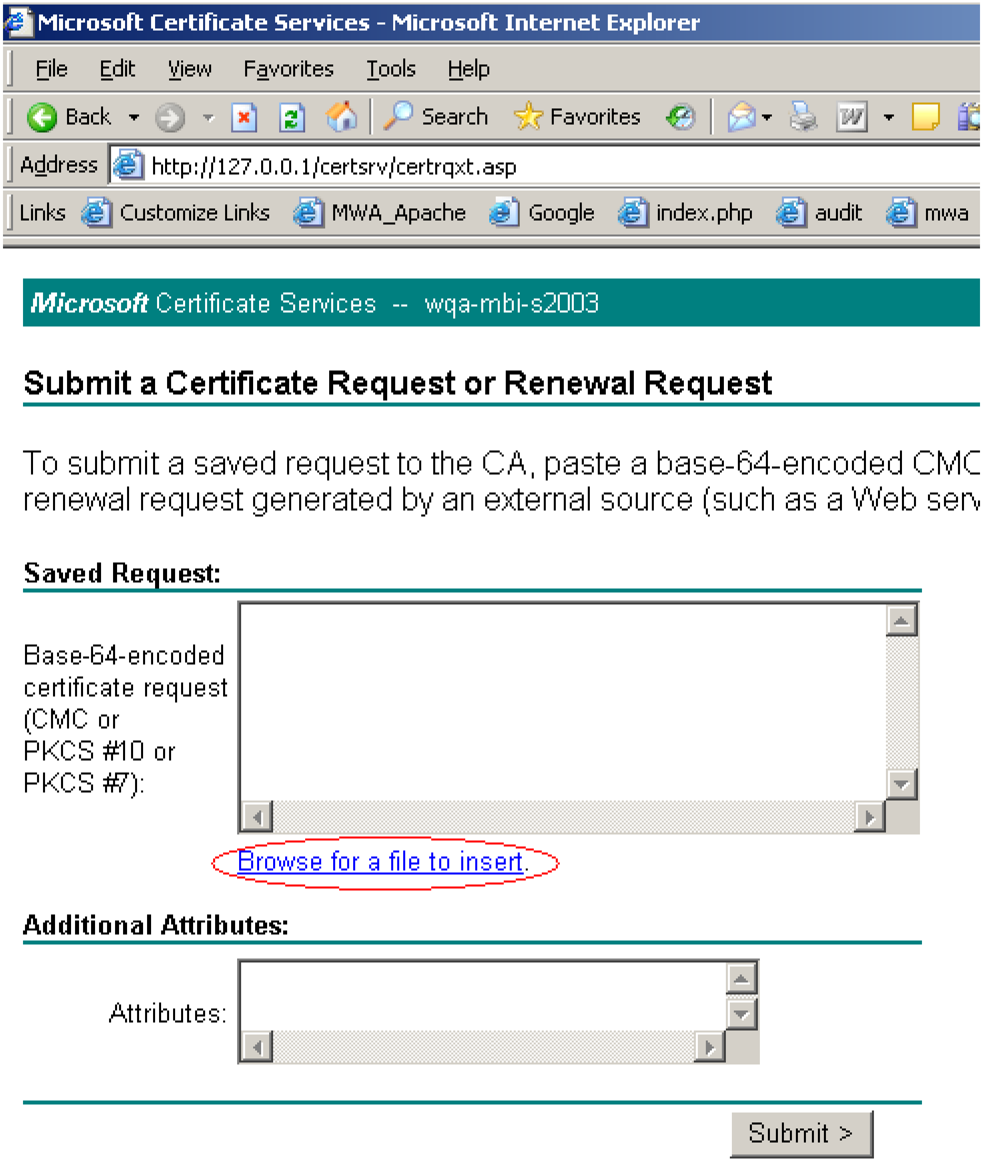
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PK
using a base-64-encoded PKCS #7 file.

5. Click **Browse for a file to insert**.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certrqxt.asp
Links Customize Links MWA_Apache Google index.php audit mwa

Microsoft Certificate Services -- wqa-mbi-s2003

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC
renewal request generated by an external source (such as a Web serv

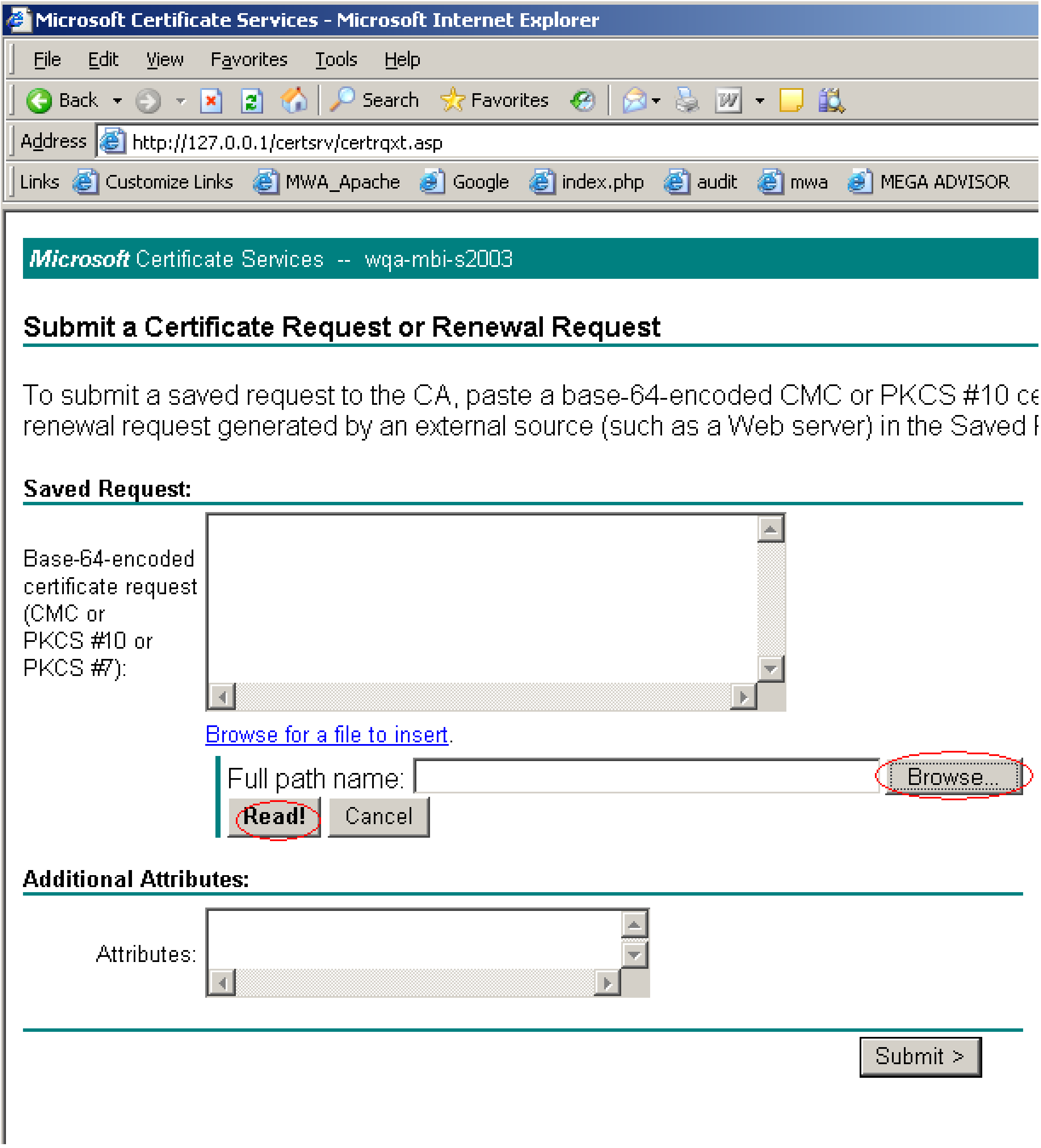
Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Browse for a file to insert.

Additional Attributes:

Attributes:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certrqxt.asp
Links Customize Links MWA_Apache Google index.php audit mwa MEGA ADVISOR

Microsoft Certificate Services -- wqa-mbi-s2003

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 ce
renewal request generated by an external source (such as a Web server) in the Saved F

Saved Request:

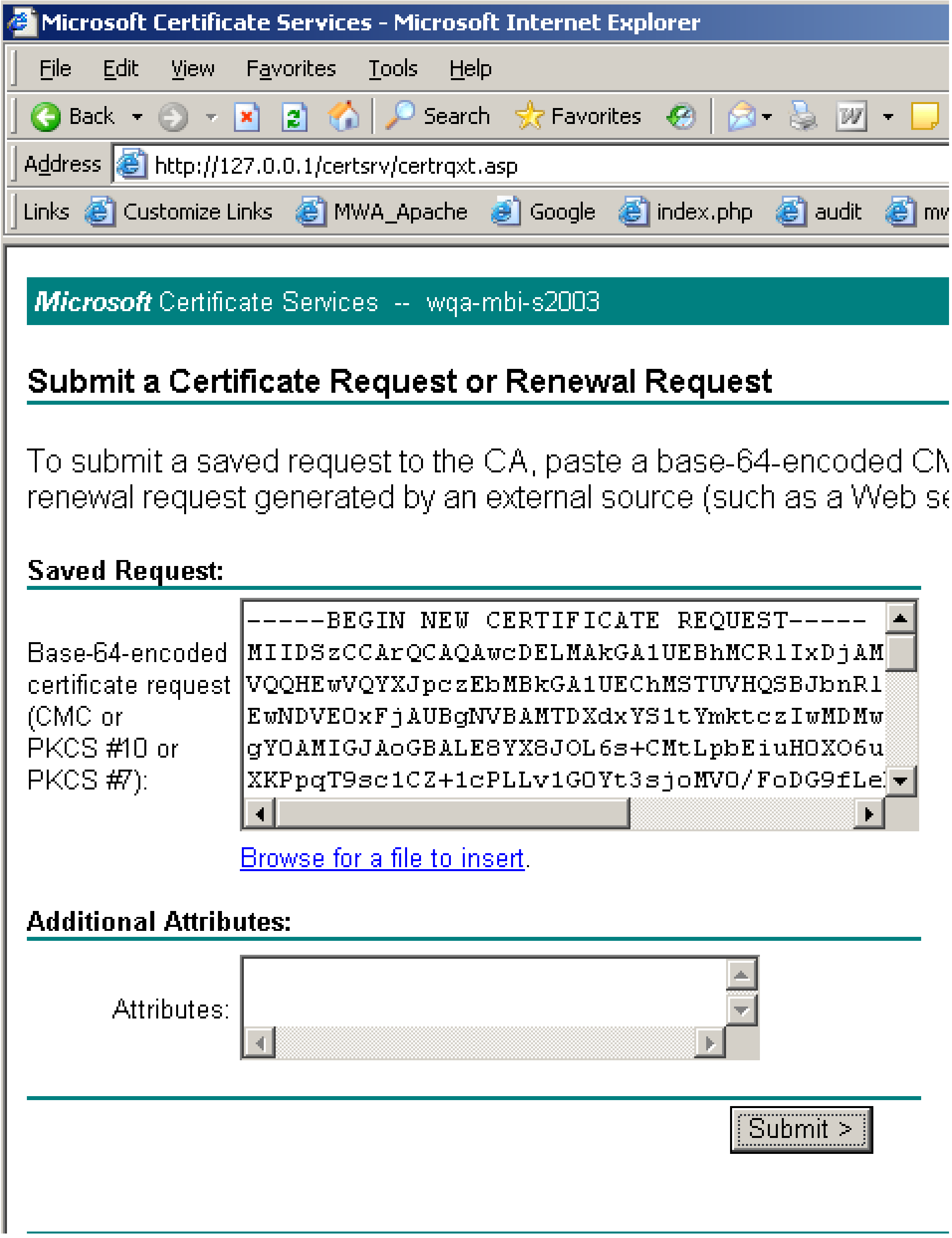
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Browse for a file to insert.

Full path name:

Additional Attributes:

Attributes:


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certrqxt.asp
Links Customize Links MWA_Apache Google index.php audit mv

Microsoft Certificate Services -- wqa-mbi-s2003

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CN
renewal request generated by an external source (such as a Web se

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSzCCArQCAQAwcDELMAkGA1UEBhMCRlIxDjAM
VQQHEwVQYXJpczEbMBkGA1UEChMSTUVHQSBJbnRl
EwNDVEOxFjAUBgNVBAMTDXdxYS1tYmktczIwMDMw
gYOAMIGJAoGBALE8YX8JOL6s+CMtLpbEiuHOXO6u
XKPpqT9sc1CZ+1cPLLv1GOYt3sjoMVO/FoDG9fLe
```

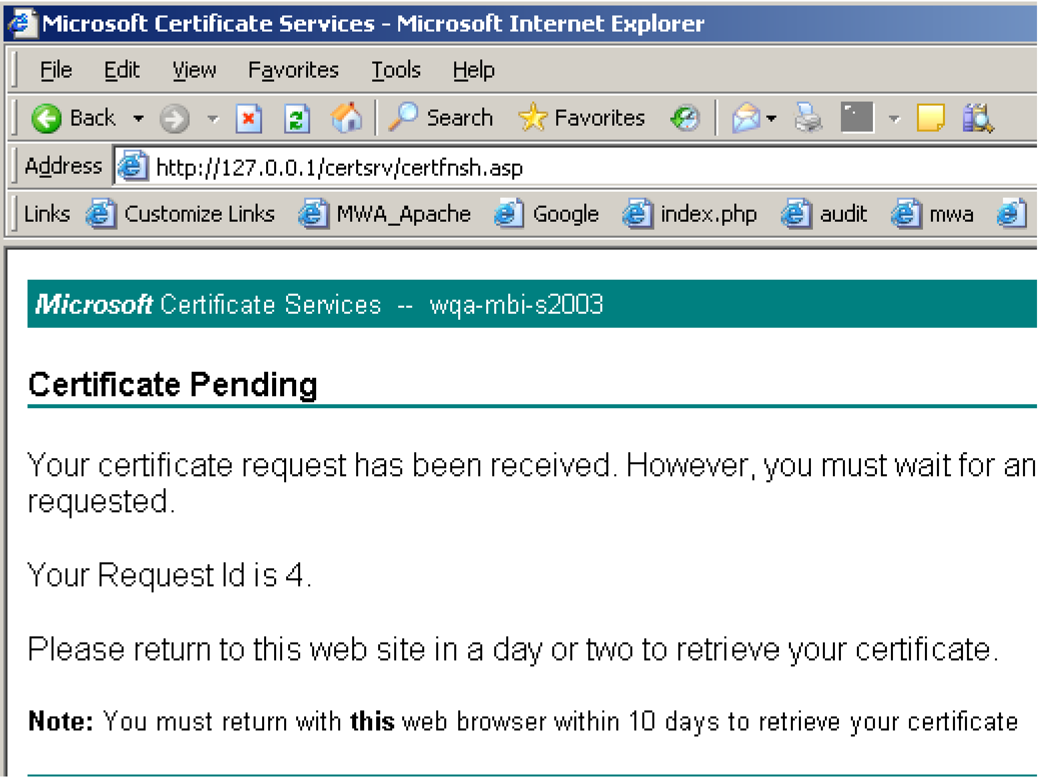
Browse for a file to insert.

Additional Attributes:

Attributes:

6. Click **Submit**.

If Certificate Server is set to “Always Issue the Certificate” (See Appendix A for more details), you can access and download the certificate immediately. If this is not the case, the next step consists of issuing the certificate.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certfnsh.asp
Links Customize Links MWA_Apache Google index.php audit mwa

Microsoft Certificate Services -- wqa-mbi-s2003

Certificate Pending

Your certificate request has been received. However, you must wait for an
requested.

Your Request Id is 4.

Please return to this web site in a day or two to retrieve your certificate.

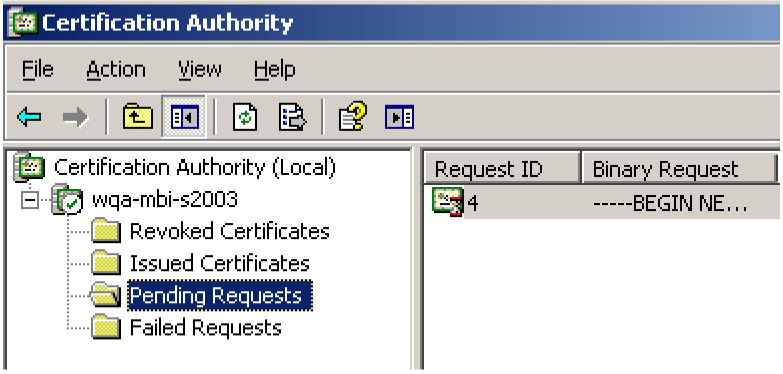
Note: You must return with **this** web browser within 10 days to retrieve your certificate

ISSUE AND DOWNLOAD THE CERTIFICATE

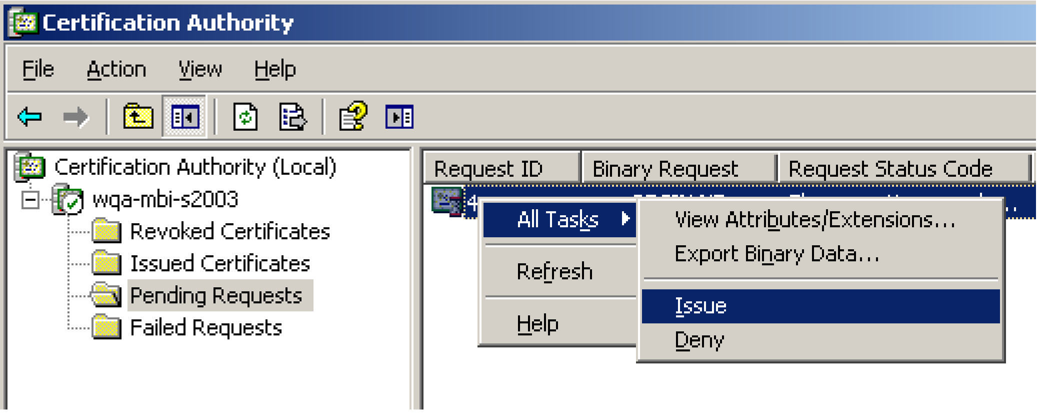
To issue a certificate in Certificate Server, follow the steps below:

1. Open the CA MMC snap-in. To do so, click **Start > Programs > Administrative Tools > Certificate Authority**.

2. Expand folder with the name of the server.



3. Right-click the pending certificate request you just submitted, select **All Tasks**, and then click **Issue**.

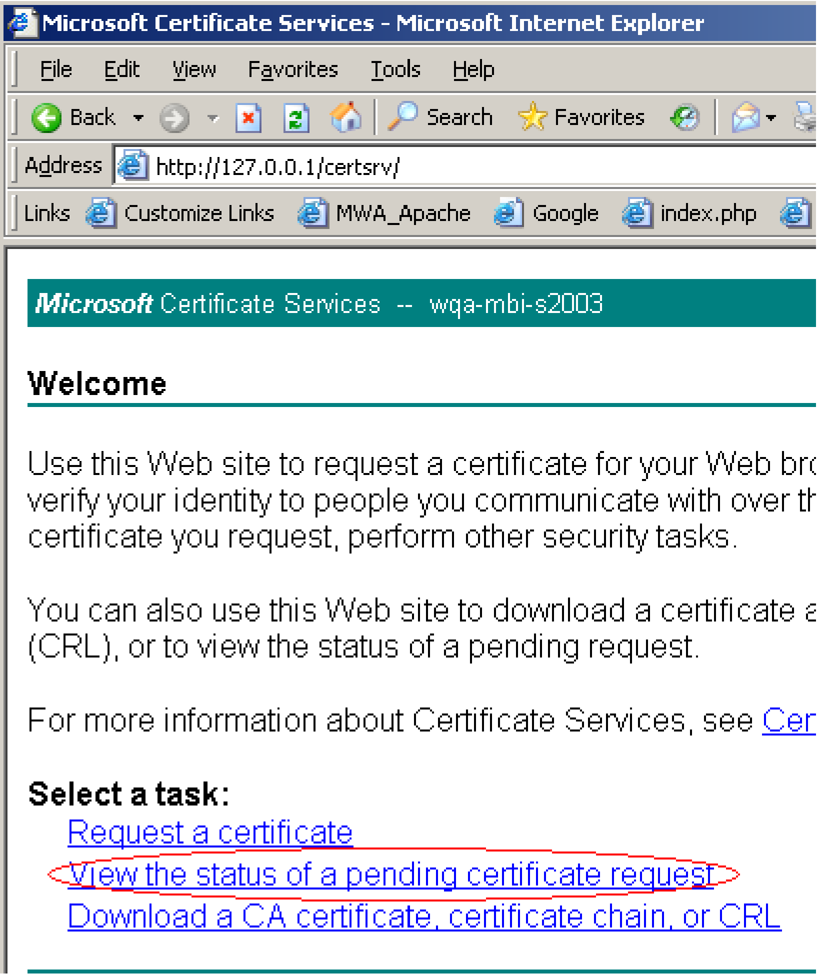


Note: after selecting Issue, the certificate is no longer displayed in this window or in the **Pending Requests** folder. It is now located in the **Issued Certificate** folder.

After having issued (and authorized) the certificate, you can return to the Certificate Server Web interface to select and download the certificate. To do so:

1. Browse to http://YourWebServerName/CertSrv/.

2. On the default page, click **View the status of a pending certificate request**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/
Links Customize Links MWA_Apache Google index.php

Microsoft Certificate Services -- wqa-mbi-s2003

Welcome

Use this Web site to request a certificate for your Web br
verify your identity to people you communicate with over tl
certificate you request, perform other security tasks.

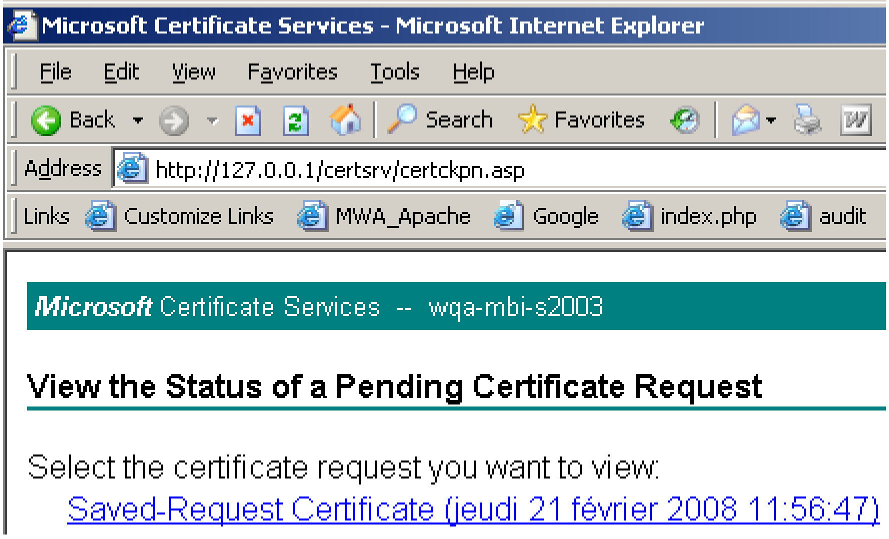
You can also use this Web site to download a certificate a
(CRL), or to view the status of a pending request.

For more information about Certificate Services, see Cer

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. Select your pending certificate, then click **Next** to go to the download page.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certckpn.asp
Links Customize Links MWA_Apache Google index.php audit

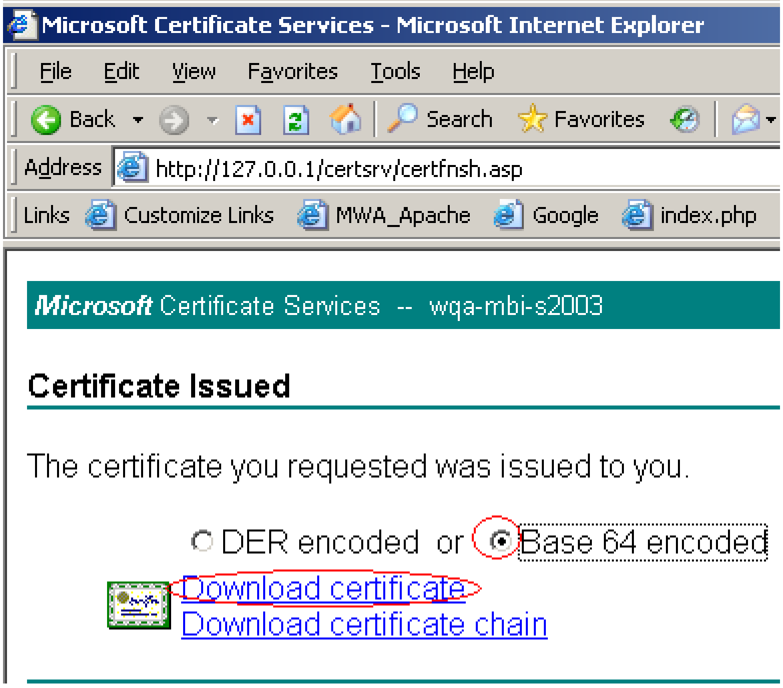
Microsoft Certificate Services -- wqa-mbi-s2003

View the Status of a Pending Certificate Request

Select the certificate request you want to view:

Saved-Request Certificate (jeudi 21 février 2008 11:56:47)

4. On the download page, click **Download certificate** (DO NOT click Download certificate chain).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/certsrv/certfnsh.asp
Links Customize Links MWA_Apache Google index.php

Microsoft Certificate Services -- wqa-mbi-s2003

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate

Download certificate chain

5. When prompted, select **Save this file to disk** and save the certificate to a location you will remember.

INSTALL THE CERTIFICATE

To install the certificate:

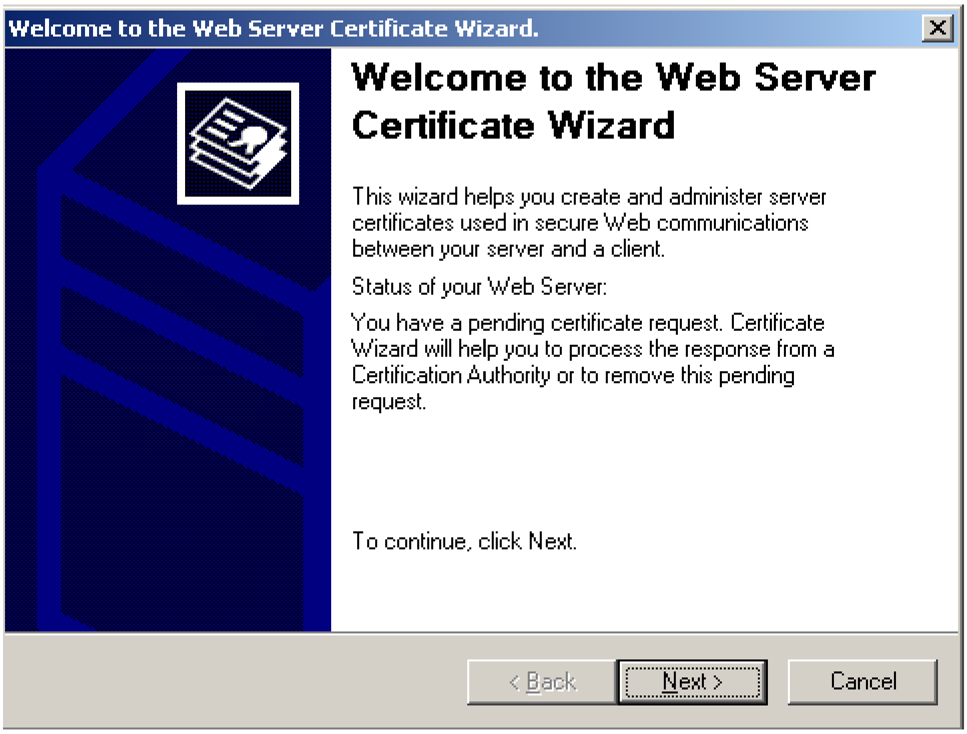
1. Open the **Internet Services Manager** and expand the server name so that you can view the Web sites.

2. Right-click the Web site for which you created the certificate request and click **Properties**.

3. Click the **Directory Security** tab and under **Secure Communications**, click **Server Certificate**.

This starts the **Certificate Installation Wizard**.

4. Click **Next** to continue.



Welcome to the Web Server Certificate Wizard.

Welcome to the Web Server Certificate Wizard

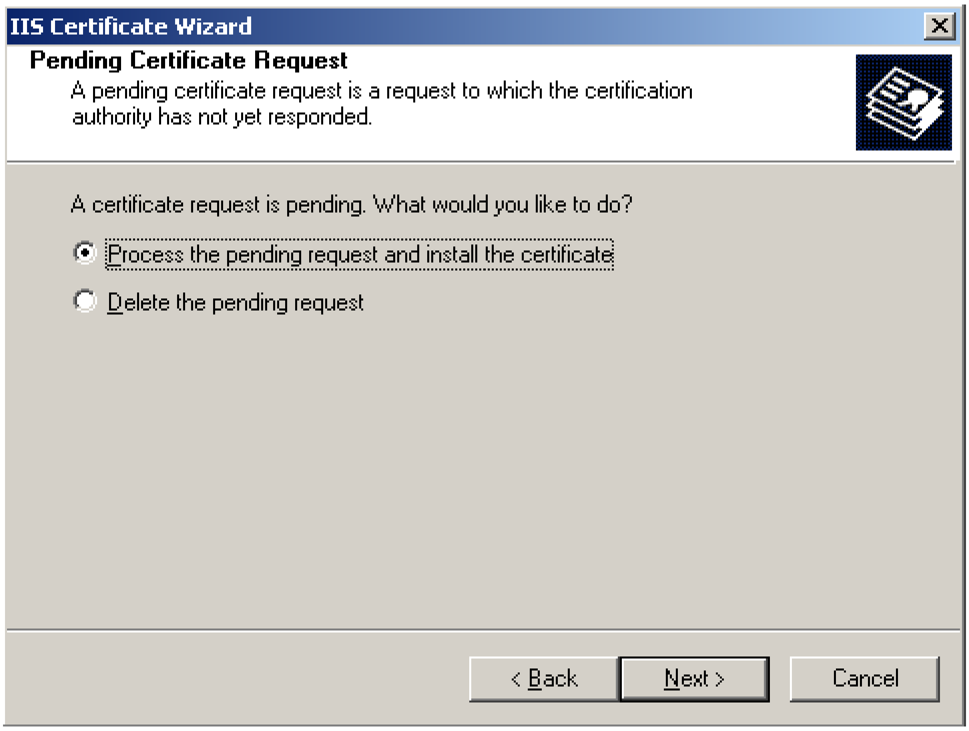
This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

Status of your Web Server:

You have a pending certificate request. Certificate Wizard will help you to process the response from a Certification Authority or to remove this pending request.

To continue, click Next.

5. Select **Process the pending request and install the certificate** and click **Next**.



IIS Certificate Wizard

Pending Certificate Request

A pending certificate request is a request to which the certification authority has not yet responded.

A certificate request is pending. What would you like to do?

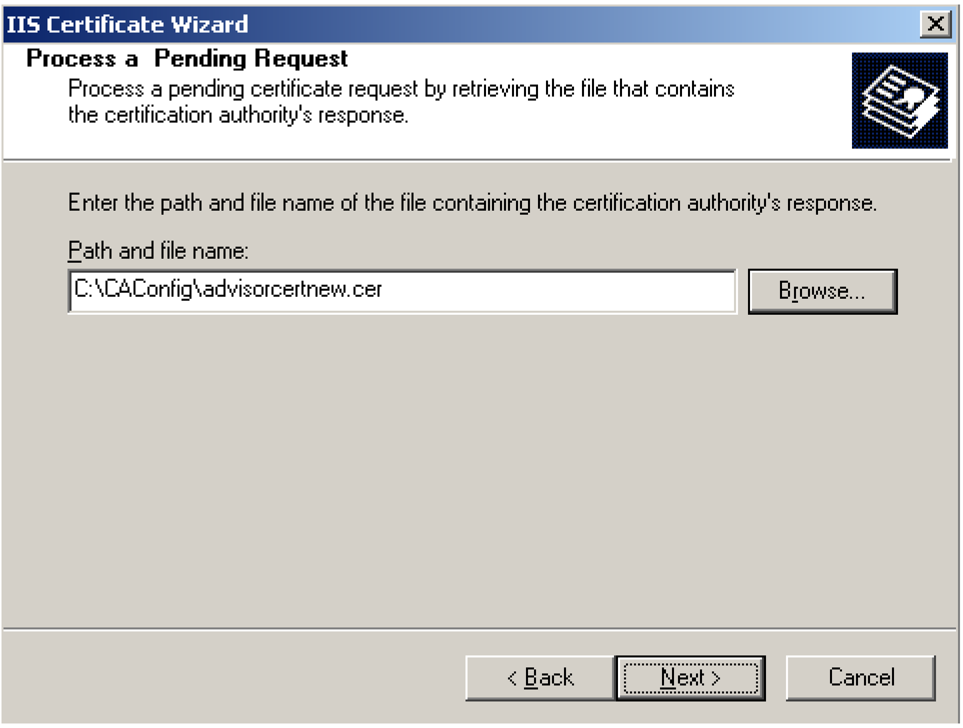
● Process the pending request and install the certificate

○ Delete the pending request

6. Type the location of the certificate you downloaded in the "Issue and download a certificate" section, then click **Next**.

The Wizard displays the Certificate Summary.

7. Verify that the information is correct, then click **Next** to continue.



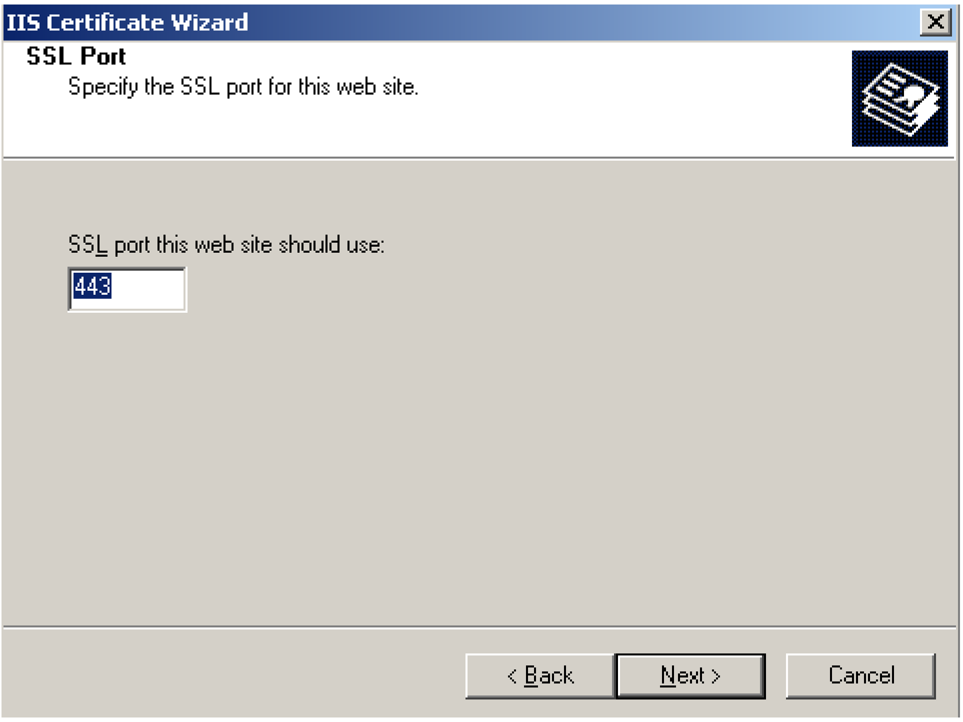
IIS Certificate Wizard

Process a Pending Request

Process a pending certificate request by retrieving the file that contains the certification authority's response.

Enter the path and file name of the file containing the certification authority's response.

Path and file name: C:\CAConfig\advisorcertnew.cer

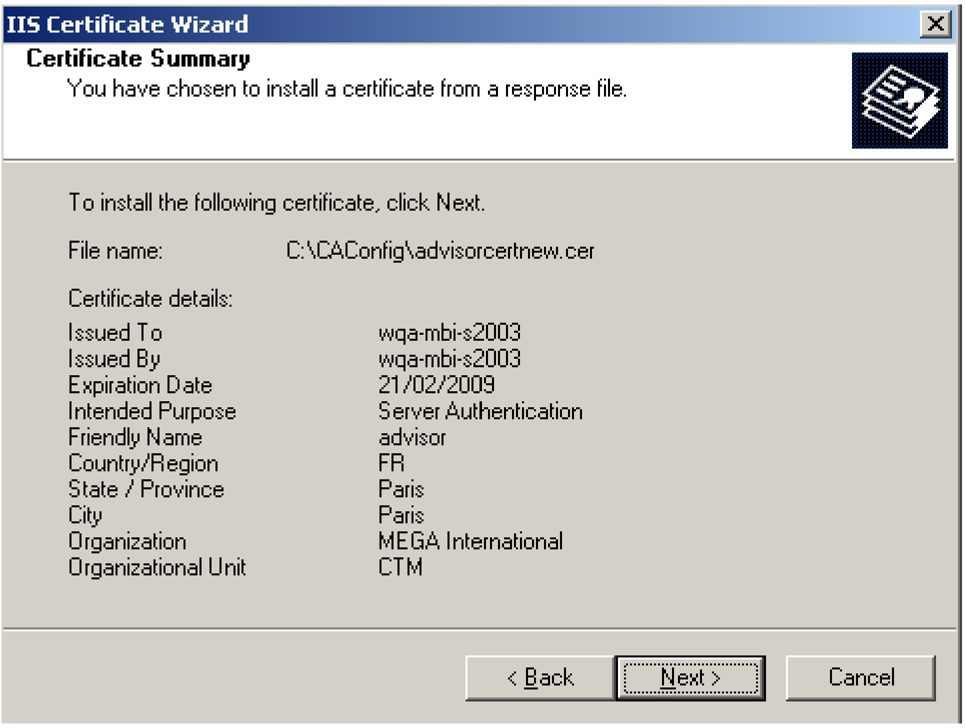


SSL Port

Specify the SSL port for this web site.

SSL port this web site should use:

443



Certificate Summary

You have chosen to install a certificate from a response file.

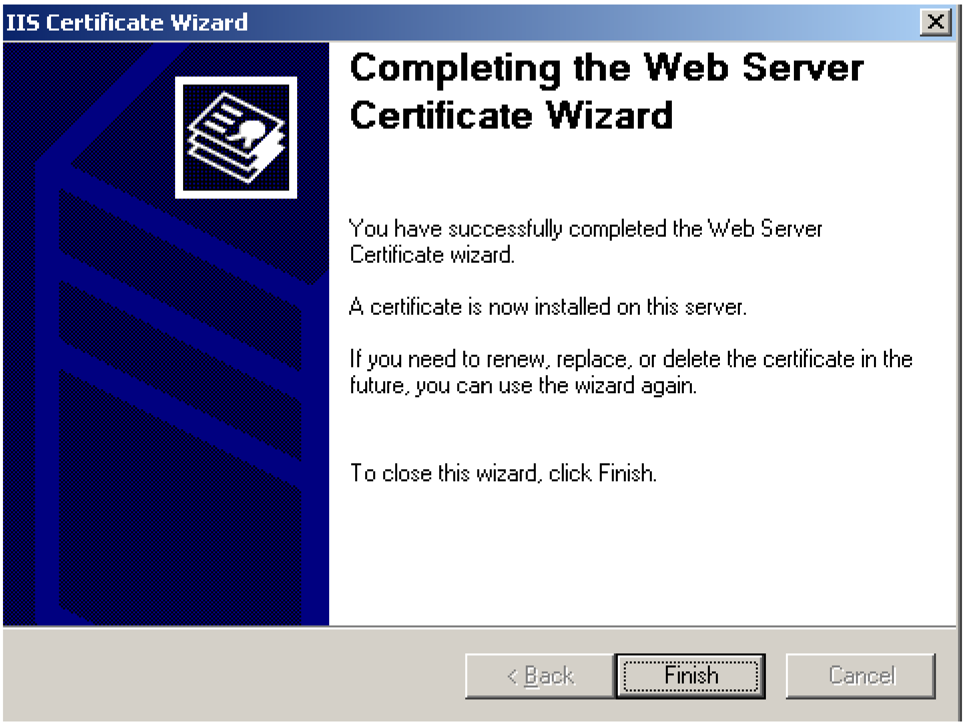
To install the following certificate, click Next.

File name: C:\CAConfig\advisorcertnew.cer

Certificate details:

Issued To	wqa-mbi-s2003
Issued By	wqa-mbi-s2003
Expiration Date	21/02/2009
Intended Purpose	Server Authentication
Friendly Name	advisor
Country/Region	FR
State / Province	Paris
City	Paris
Organization	MEGA International
Organizational Unit	CTM

8. Click **Finish** to complete the process.



Completing the Web Server Certificate Wizard

You have successfully completed the Web Server Certificate wizard.

A certificate is now installed on this server.

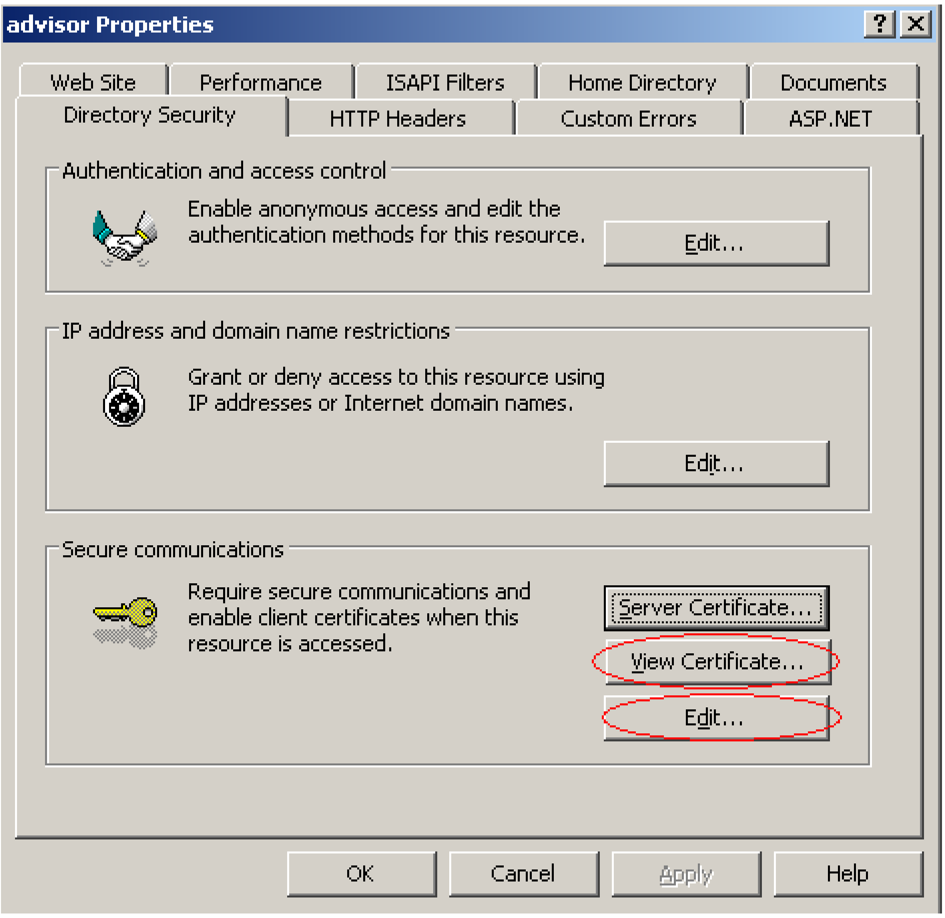
If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.

To close this wizard, click Finish.

Configure and Test the Certificate

To configure and test the certificate, follow the steps below.

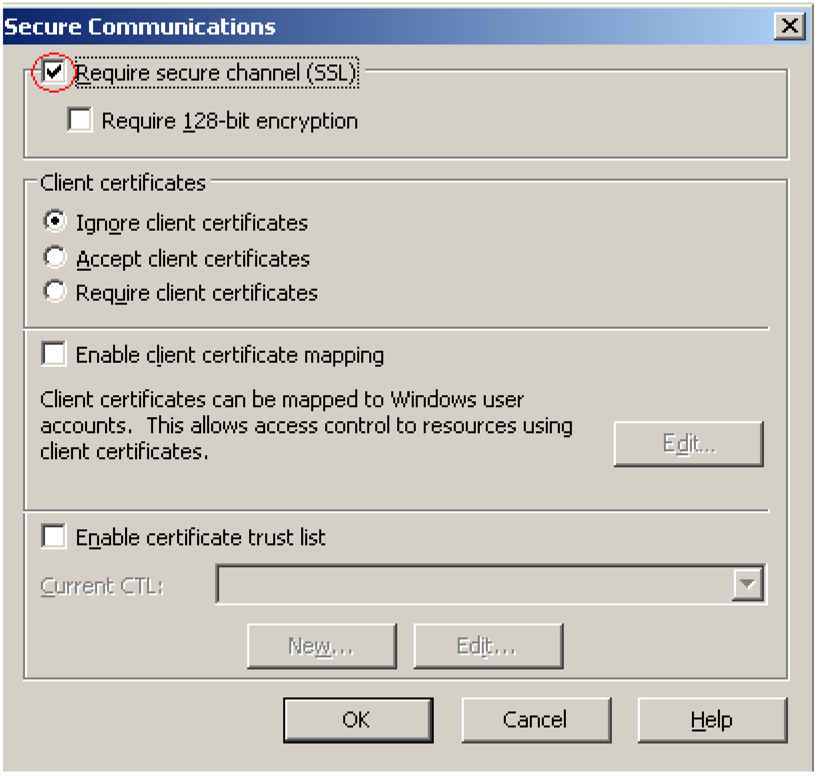
In the Directory Security tab and under Secure communications, there are now three available options.


advisor Properties
Web Site
Performance
ISAPI Filters
Home Directory
Documents
Directory Security
HTTP Headers
Custom Errors
ASP.NET
Authentication and access control
Enable anonymous access and edit the authentication methods for this resource.
Edit...
IP address and domain name restrictions
Grant or deny access to this resource using IP addresses or Internet domain names.
Edit...
Secure communications
Require secure communications and enable client certificates when this resource is accessed.
Server Certificate...
View Certificate...
Edit...
OK
Cancel
Apply
Help

To set the Web site to require secure connections:

1. Click **Edit**.

The Secure Communications dialog box appears.



Secure Communications

☑ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

□ Enable certificate trust list

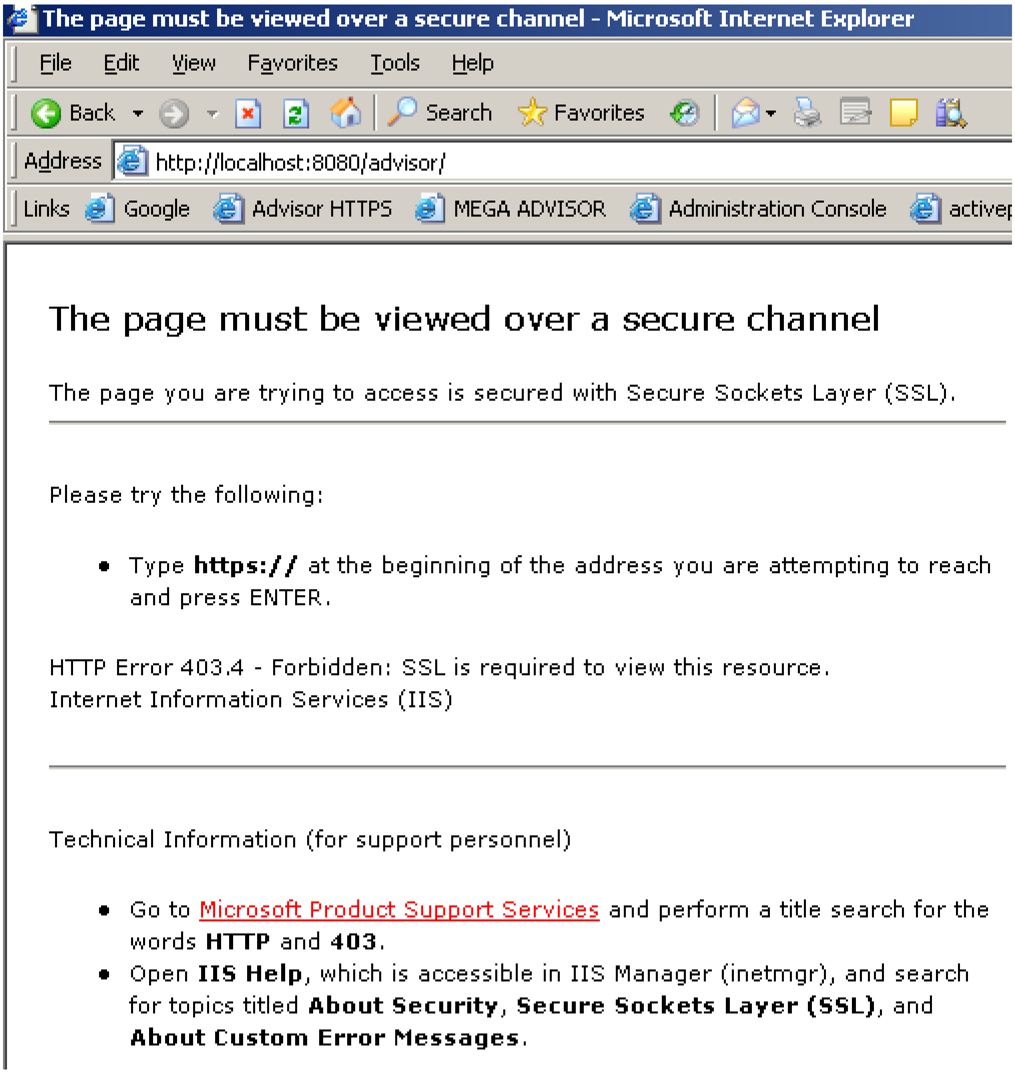
Current CTL:

2. Select **Require secure channel (SSL)** and click **OK**.

3. Click **Apply** and then **OK** to close the property window.

4. Browse to the site and verify that it works. To do so, follow these steps:

   a. Access the site through HTTP by typing http://localhost:8080/advisor in the browser. You receive an error message that resembles the following:


The page must be viewed over a secure channel - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8080/advisor/
Links Google Advisor HTTPS MEGA ADVISOR Administration Console activep

The page must be viewed over a secure channel

The page you are trying to access is secured with Secure Sockets Layer (SSL).

Please try the following:

- Type **https://** at the beginning of the address you are attempting to reach and press ENTER.

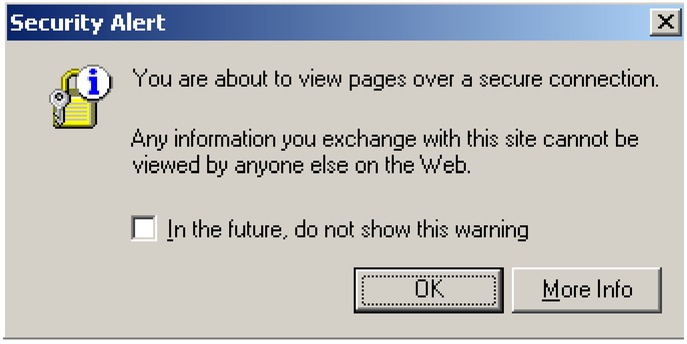
HTTP Error 403.4 - Forbidden: SSL is required to view this resource.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **About Security**, **Secure Sockets Layer (SSL)**, and **About Custom Error Messages**.

b. Try to browse to the same Web page using a secured connection (HTTPS) by typing https://CommonNameYouEnteredForTheCertificate/advisor/ (https://wqa-mbi-s2003/advisor) in the browser.

A security alert may appear if the "Warn if changing between secure and not secure mode" security option of your browser is active.

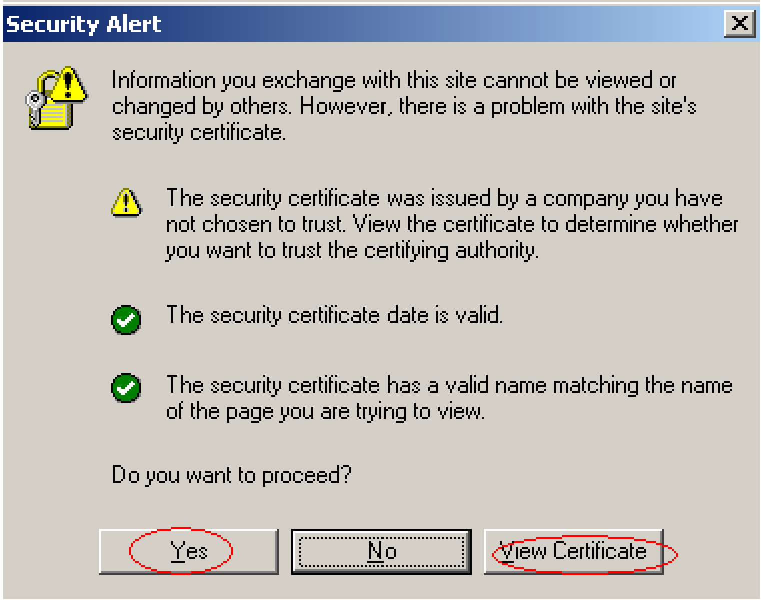


You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the Web.

☐ In the future, do not show this warning

You may also receive a security alert which states that the certificate is not from a trusted root CA.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

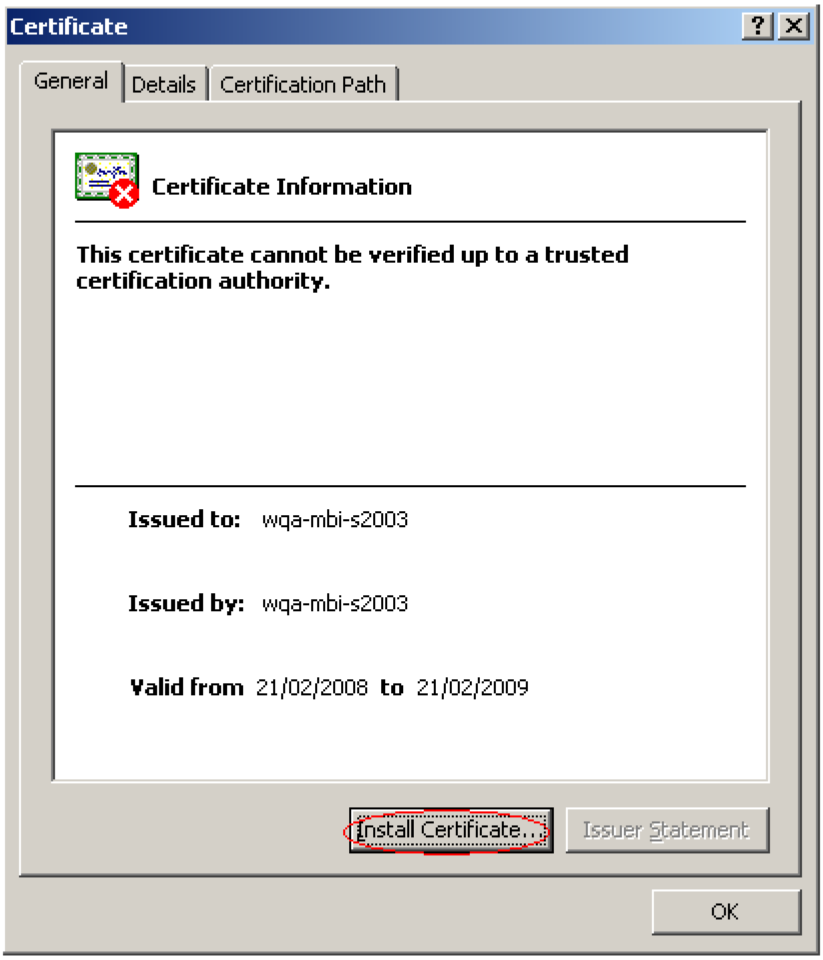
Do you want to proceed?

You can click **Yes** to continue to the Web page or install the certificate in order to not show this warning in the future.

Note: You can also add the certificate to the trusted certificate list later on (See Appendix B for more details).

If you choose the second option, please follow these steps:

- Click **View Certificate**.



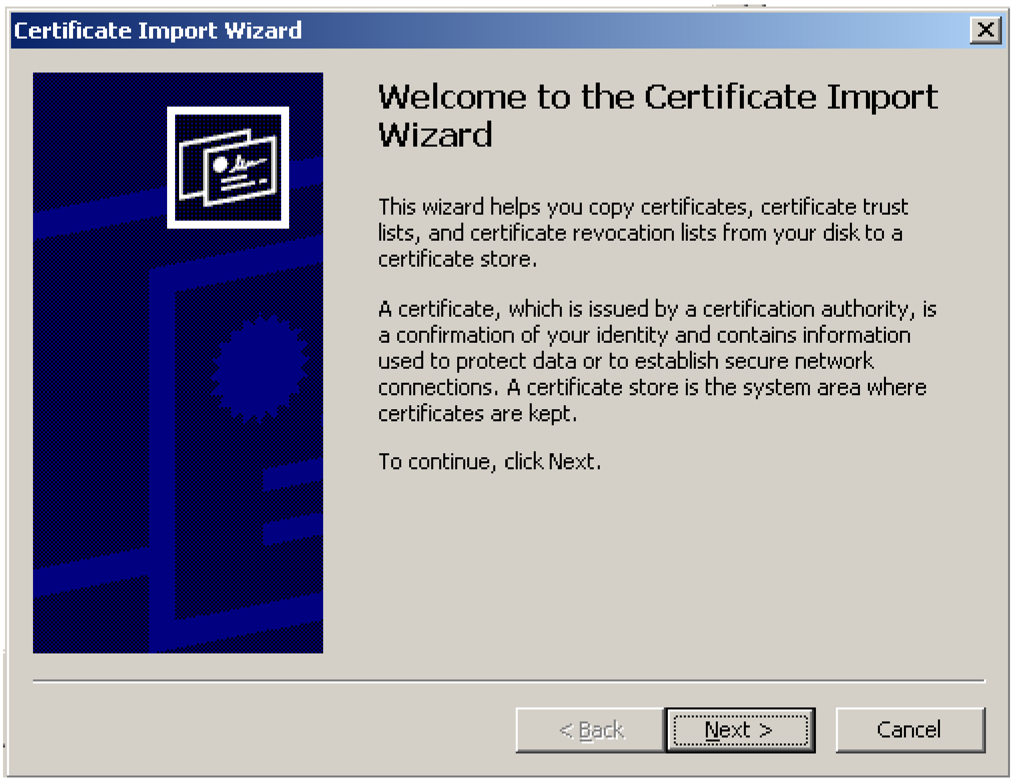
This certificate cannot be verified up to a trusted certification authority.

Issued to: wqa-mbi-s2003

Issued by: wqa-mbi-s2003

Valid from 21/02/2008 to 21/02/2009

- Click **Install Certificate** in order to launch the “Certificate Import Wizard”.



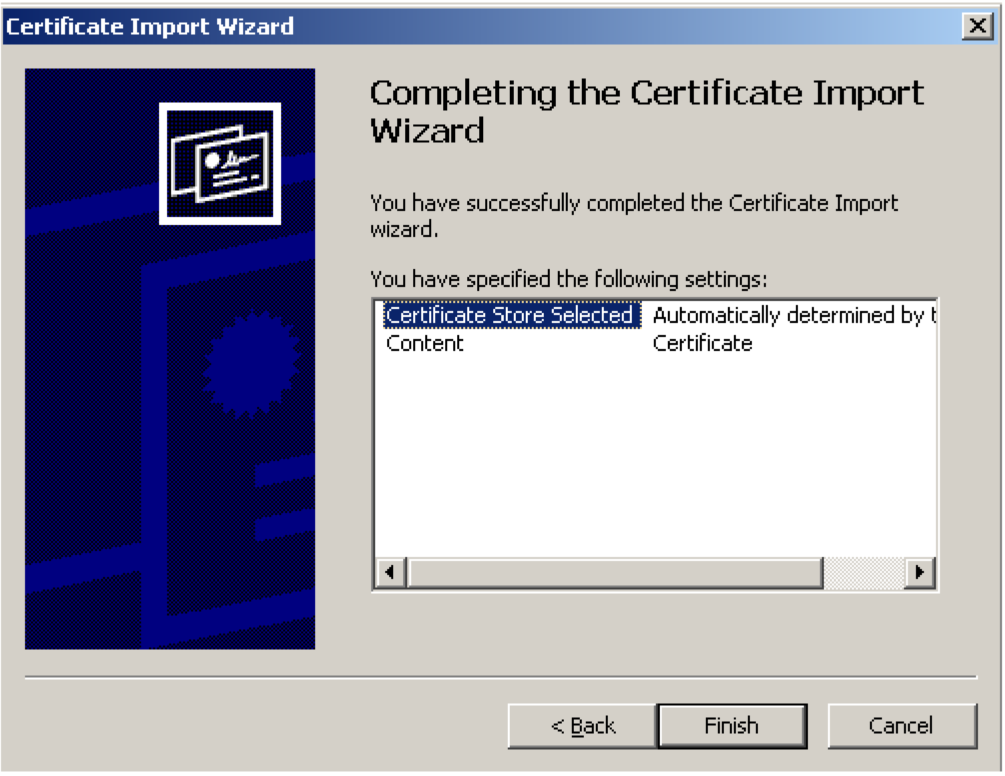
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

- Click **Next**.

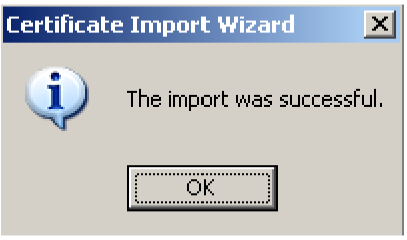


Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

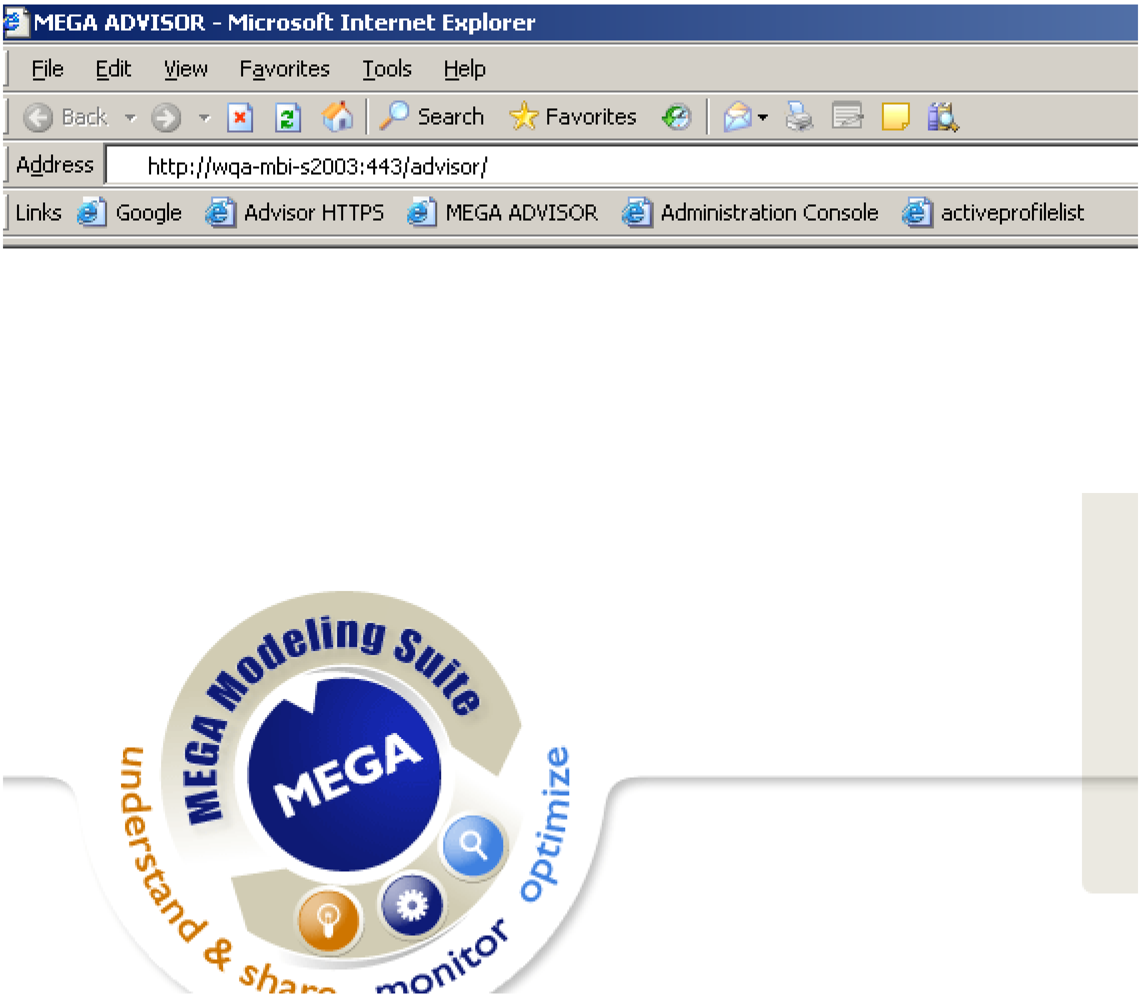
Certificate Store Selected	Automatically determined by t
Content	Certificate



Certificate Import Wizard

The import was successful.

If the page below appears, you have successfully installed your certificate.



MEGA ADVISOR - Microsoft Internet Explorer

Address http://wqa-mbi-s2003:443/advisor/

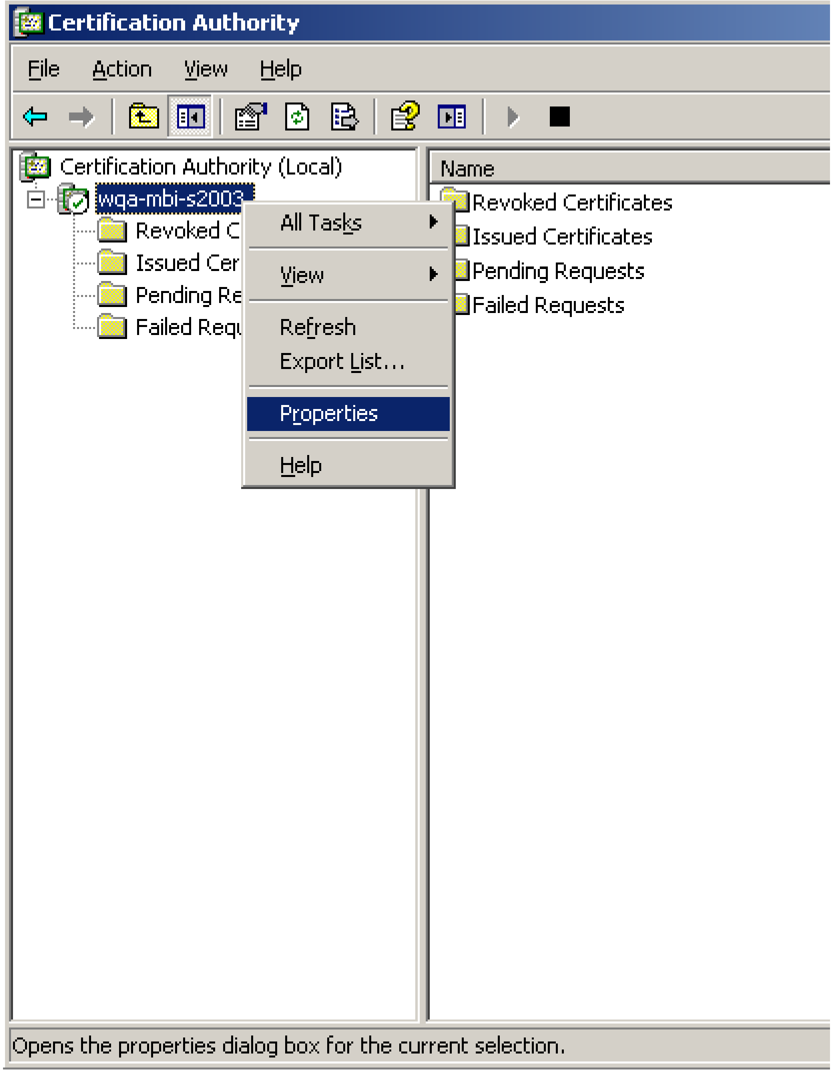
APPENDIX A: MODIFY THE CERTIFICATE ISSUING STRATEGY

To set the default action upon receipt of a certificate request, please follow the steps below:

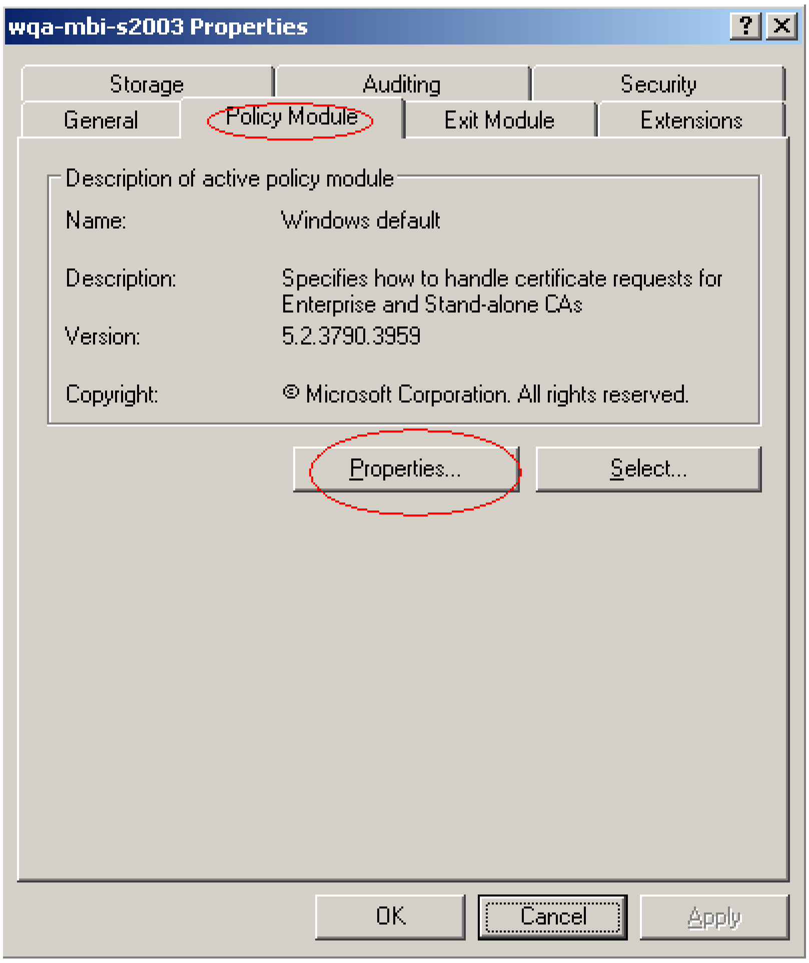
1. Log on to the system as a Certification Authority Administrator.

2. Open the CA MMC snap-in. To do so, click **Start > Programs > Administrative Tools > Certificate Authority**.

3. In the console tree, click the name of the certification authority (CA).



4. Click **Properties > Policy Module tab > Properties**.



Description of active policy module

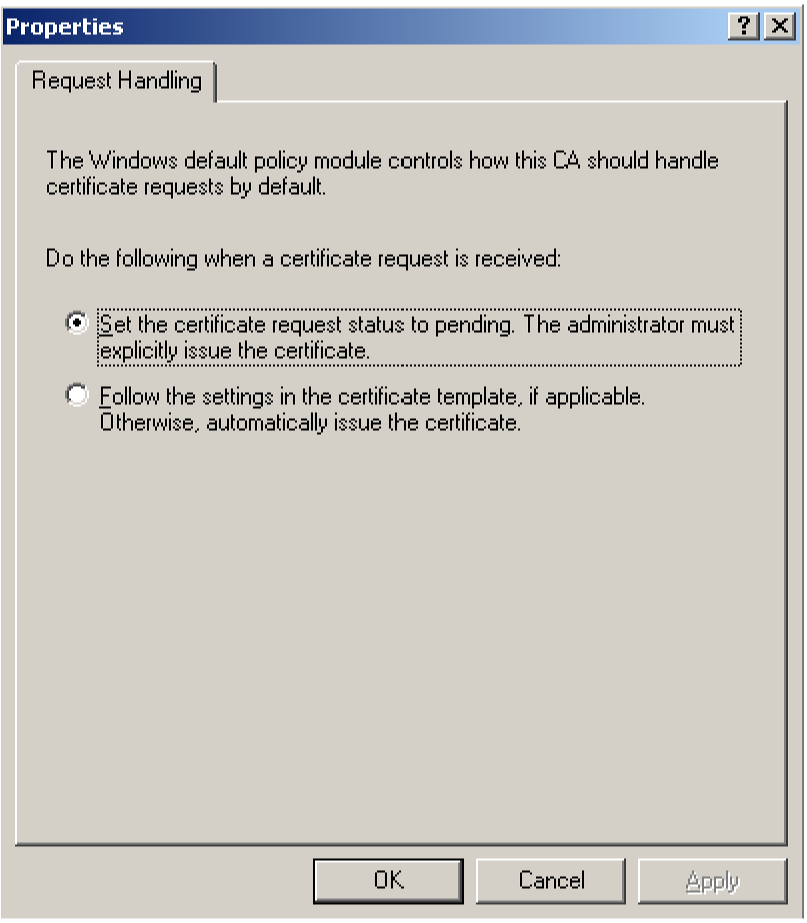
Name: Windows default

Description: Specifies how to handle certificate requests for Enterprise and Stand-alone CAs

Version: 5.2.3790.3959

Copyright: © Microsoft Corporation. All rights reserved.

5. Click the option you prefer.



Properties

Request Handling

The Windows default policy module controls how this CA should handle certificate requests by default.

Do the following when a certificate request is received:

● Set the certificate request status to pending. The administrator must explicitly issue the certificate.

○ Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.

6. Stop and restart the Certificate Services service.

Caution

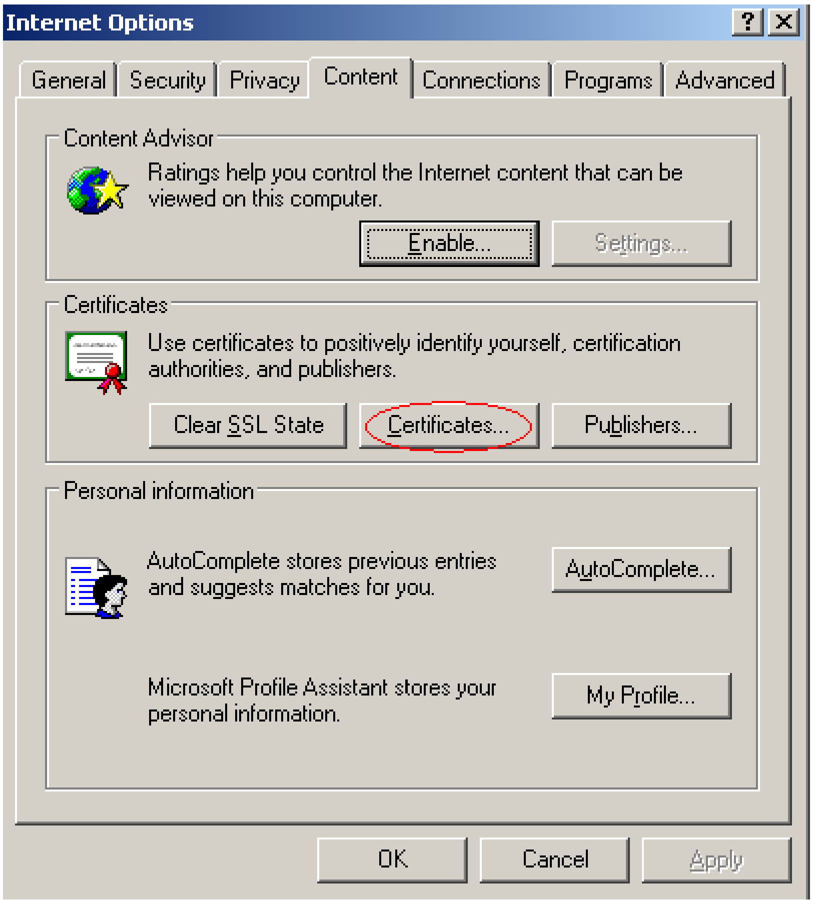
In most cases, for security reasons, it is strongly recommended that all incoming certificate requests to a stand-alone CA be marked as "pending". Unlike enterprise certification authorities, stand-alone CAs do not use the Active Directory directory service, even if it is available, to verify that an individual or computer is authorized to be issued a certificate from the CA automatically. For stand-alone CAs, the CA administrator is responsible for verifying the identity of the certificate requestor.

Note

If you change the setting from "Set the certificate request status to pending" to "Follow the settings in the certificate template…", this will only apply to certificate requests submitted to the CA after the default action has been changed. If there are pending requests held by the CA, these requests will remain as pending until the CA administrator issues the certificates or denies the requests.

APPENDIX B: INSTALL A CERTIFICATE

The "Certificate Import Wizard" is available via the Internet options.

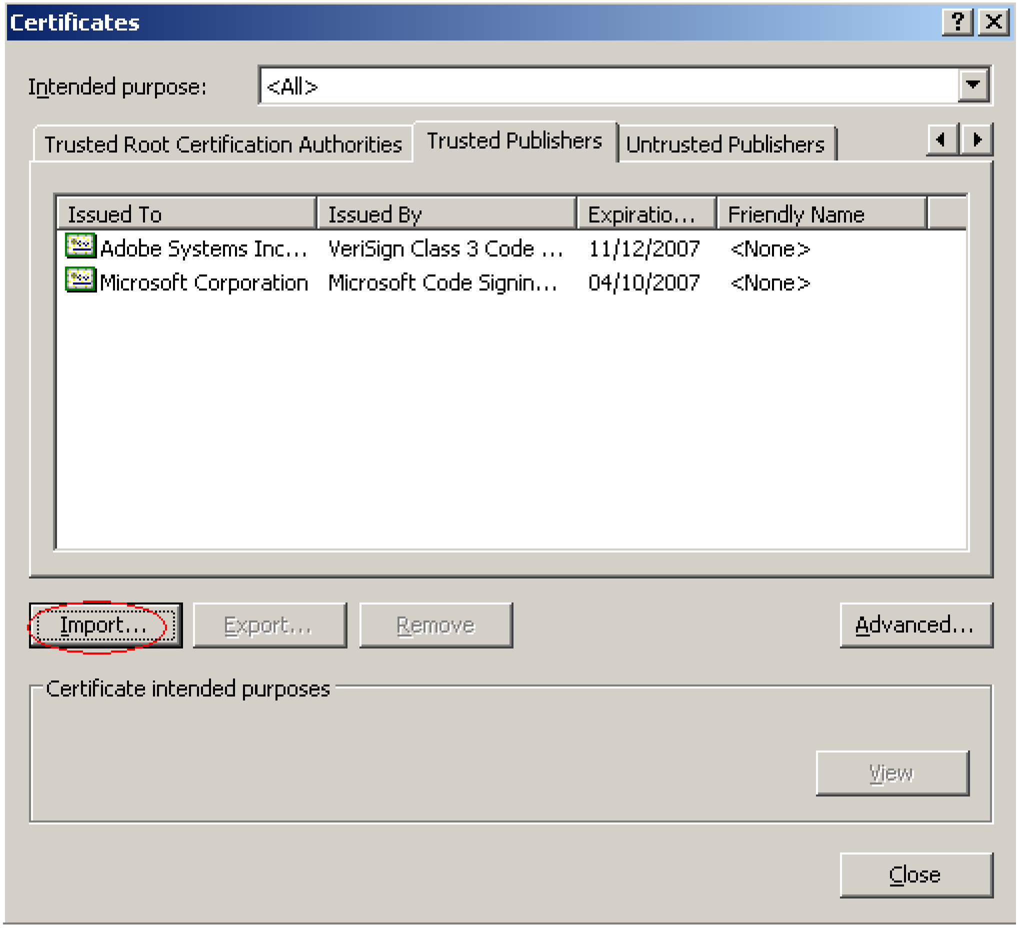


Ratings help you control the Internet content that can be viewed on this computer.

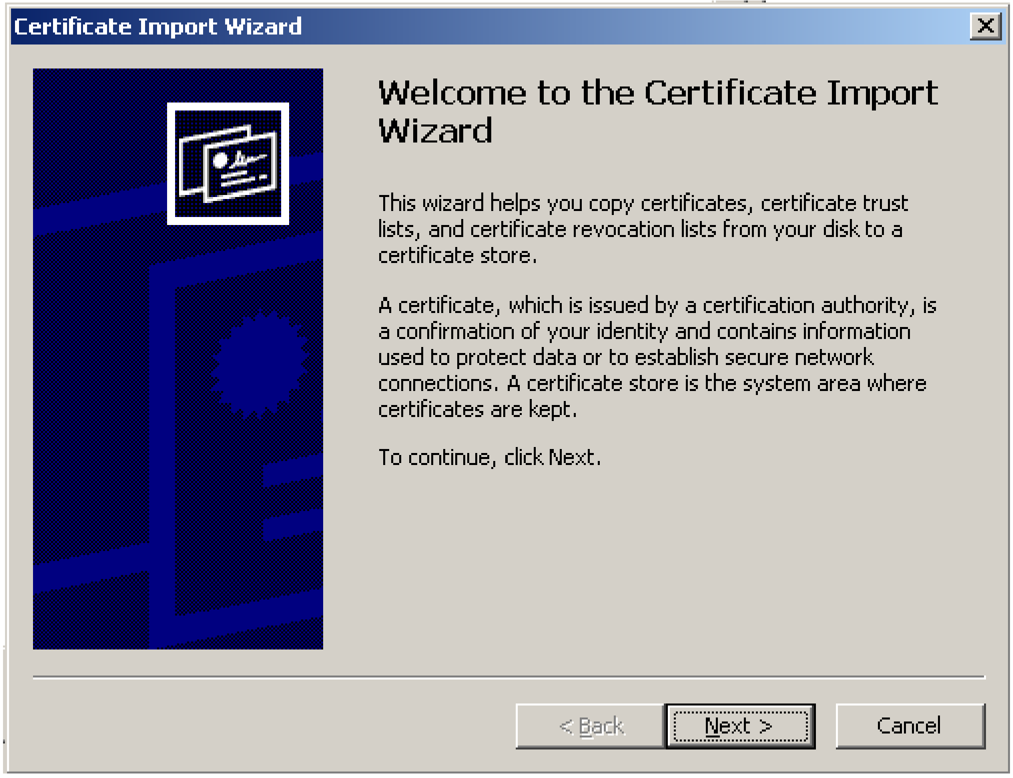
Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.



Issued To	Issued By	Expiratio...	Friendly Name
Adobe Systems Inc...	VeriSign Class 3 Code ...	11/12/2007	<None>
Microsoft Corporation	Microsoft Code Signin...	04/10/2007	<None>



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Please follow the steps described in the "Install the certificate" chapter.