

**Oracle® Enterprise Single Sign-on
Provisioning Gateway**

Certificate Setup Guide

Release 11.1.1.1.0

E15694-01

March 2010

Copyright ©2005–2010 Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents

Abbreviations and Terminology.....	4
About ESSO-PG Certificate Setup Guide.....	5
Installing the Microsoft Certificate Authority.....	6
Enabling SSL for Your Web Site.....	9
Submitting a Certificate Request to a CA Manually.....	15

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Terminology	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Agent
FTU	First Time Use Wizard
ESSO-AM	Oracle Enterprise Single Sign-on Authentication Manager
ESSO-ODE	Oracle Enterprise Single Sign-on On Demand Edition
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-KM	Oracle Enterprise Single Sign-on Kiosk Manager
ESSO-LM	Oracle Enterprise Single Sign-on
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset

About ESSO-PG Certificate Setup Guide

In order to use ESSO-PG, you must obtain an X.509 Certificate for SSL and Certificate Chain from a trusted certificate authority.

Certificates can be obtained from any trusted certificate authority. This purpose of this guide is to demonstrate how certificates can be obtained through Microsoft® Certificate Services.

These instructions will guide you through installation of a standalone CA, which can be used to issue certificates to anyone, even non-Windows entities.

Certificates can be installed on Windows 2000 and Windows 2003. The instructions and screen shots in this guide are primarily for Windows 2000. The instructions in this guide can easily be followed using either operating system.



The following articles from the Microsoft Web site can be referred to for information on installing certificates and setting up SSL:

"Install an Enterprise Root Certificate Authority (Windows 2003)",
<http://technet2.microsoft.com/windowsserver/en/library/4ffc15cf-f42f-43db-8eb9-fcd8c3102d621033.msp>

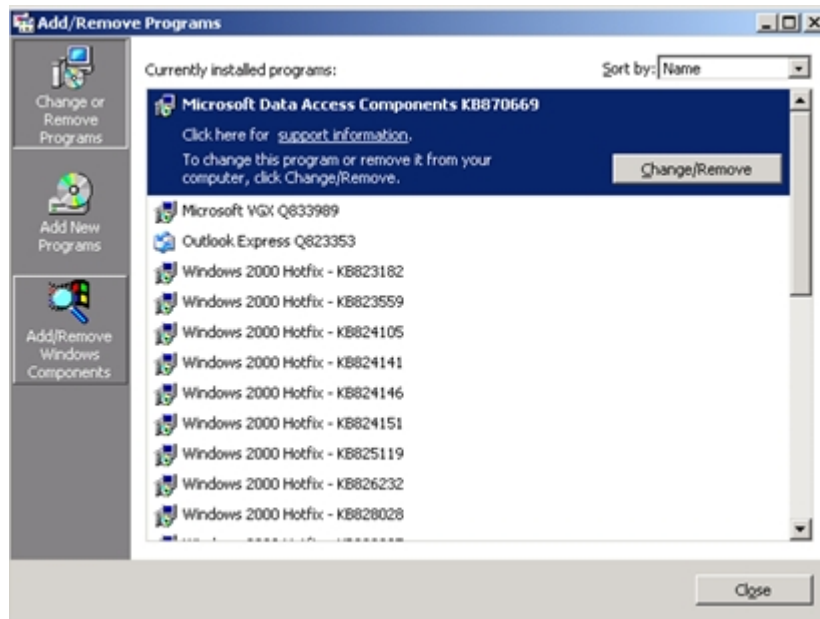
"How to Set Up SSL on a WebServer",
<http://technet2.microsoft.com/windowsserver/en/library/4ffc15cf-f42f-43db-8eb9-fcd8c3102d621033.msp>

The following pages contain the procedures involved in certificate setup:

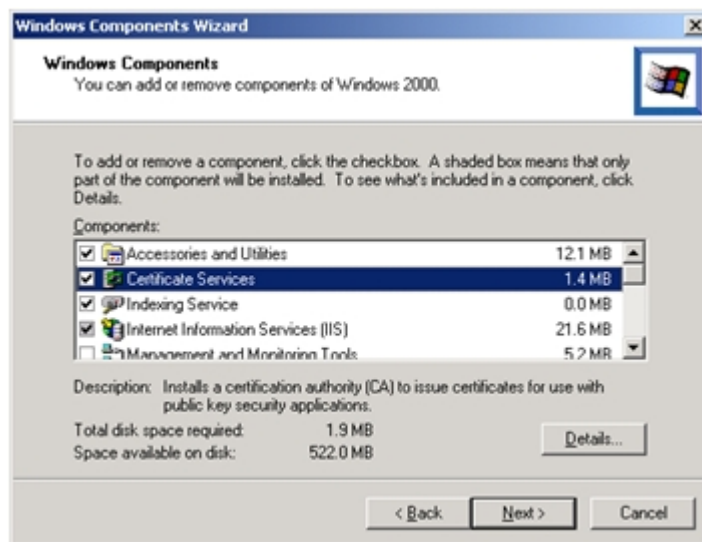
- [Installing the Microsoft Certificate Authority](#)
- [Enabling SSL for Your Web Site](#)
- [Submitting a Certificate Request to a CA Manually](#)

Installing the Microsoft Certificate Authority

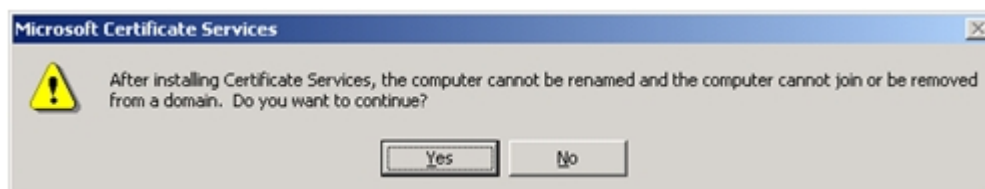
1. Click **Start > Settings > Control Panel > Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.



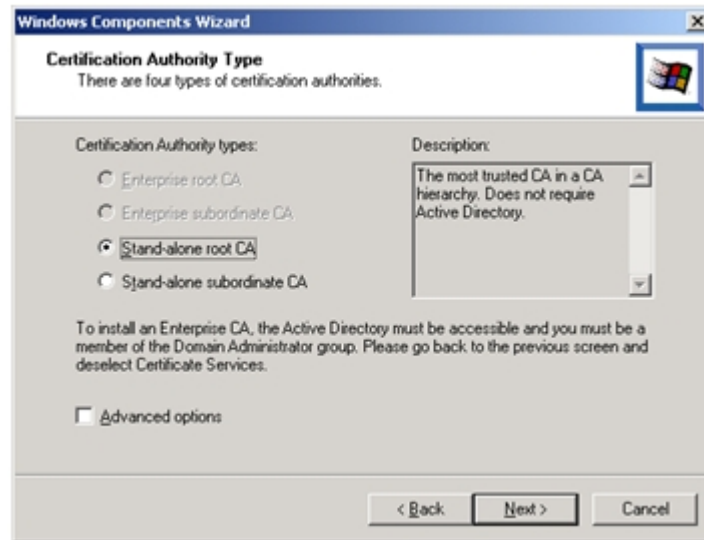
3. Check **Certificate Services** and click **Next**.



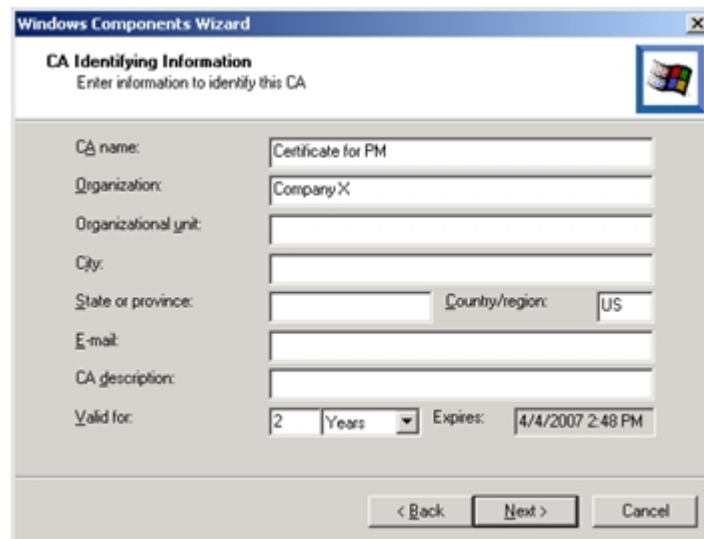
4. When you are asked if you want to continue, click **Yes**.



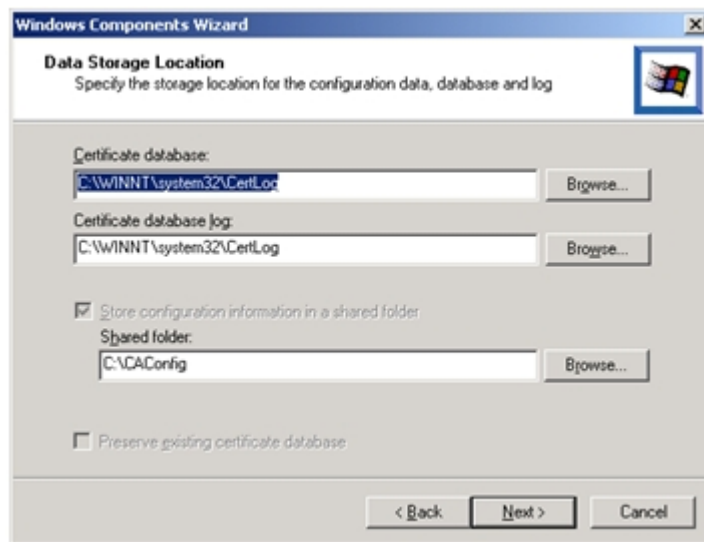
5. Select **Stand-alone root CA**.



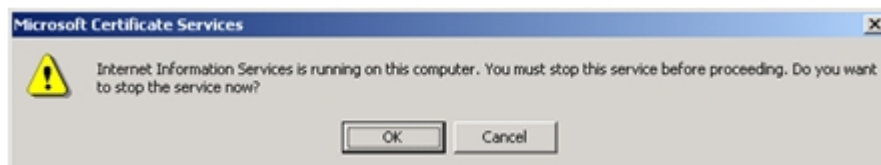
6. Enter CA Identifying Information. Enter the length of time that this certificate should be valid. Click **Next**.



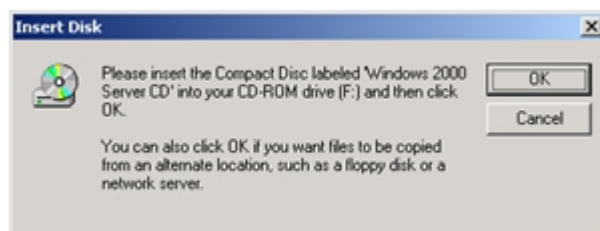
7. Specify the storage location for the configuration data. Click **Next**.



8. You might be prompted to stop IIS. If so, click **OK**.



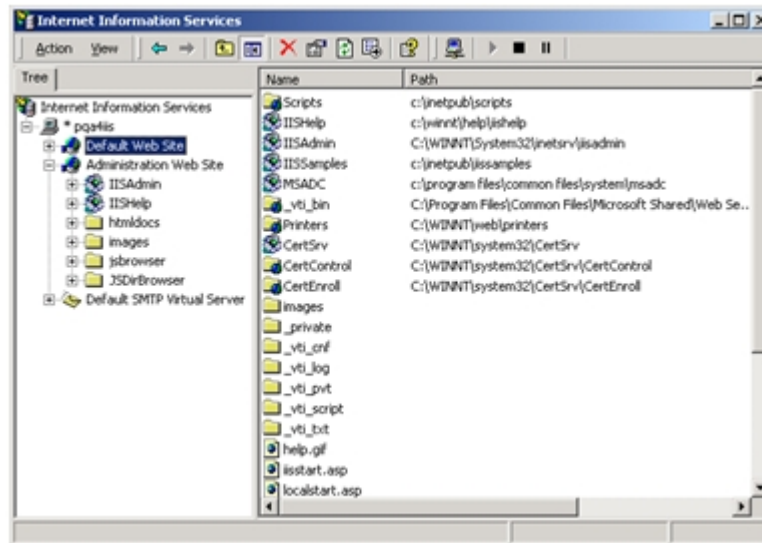
9. You might be prompted to insert the Windows CD. If so, insert it and click **OK**.



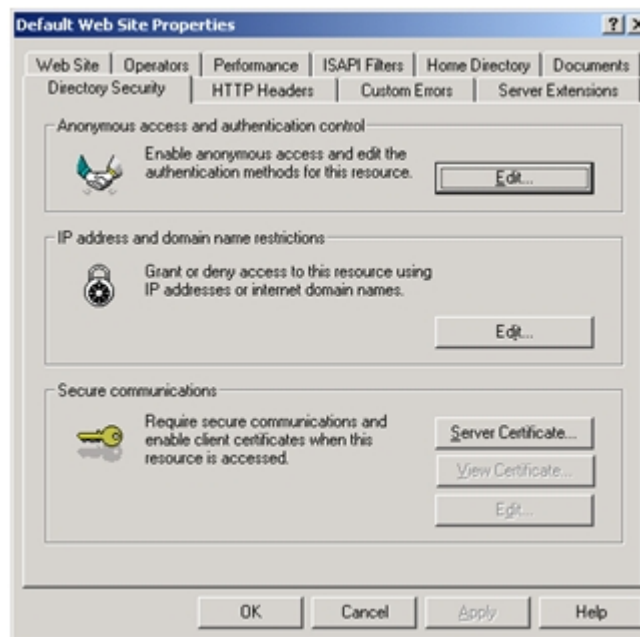
10. At this point, you might be prompted to enable ASP pages. You must select **Yes**.
11. Click **Finish**.

Enabling SSL for Your Web Site

1. Open Microsoft IIS and expand the Default Web Site. You will perform the following steps for each ESSO-PG Web site.
2. Right-click the Web site (for example, Default Web Site). Click **Properties**.



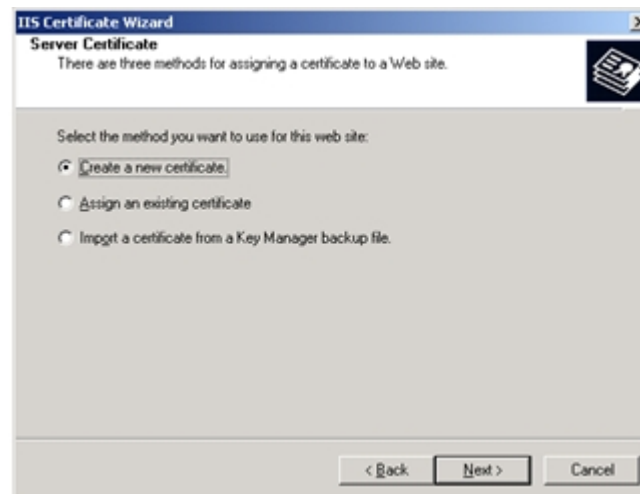
3. Select the **Directory Security** tab. Under **Secure communications**, click **Server Certificate**.



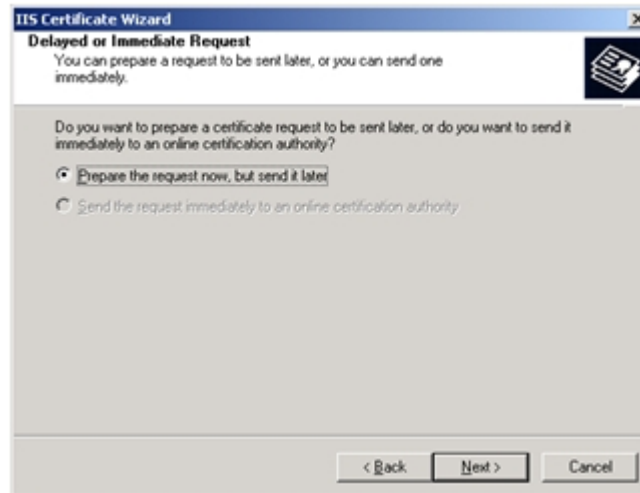
4. The Web Server Certificate Wizard appears. You will use the wizard to generate a request for a certificate. Click **Next**.



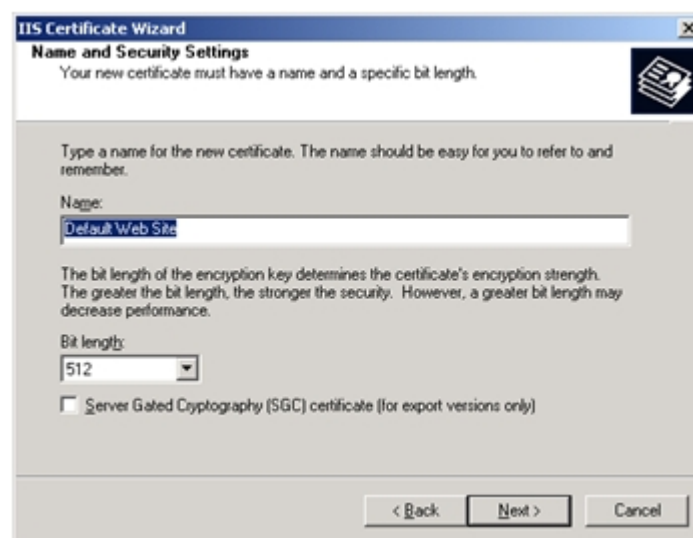
5. Select **Create a new certificate** and click **Next**.



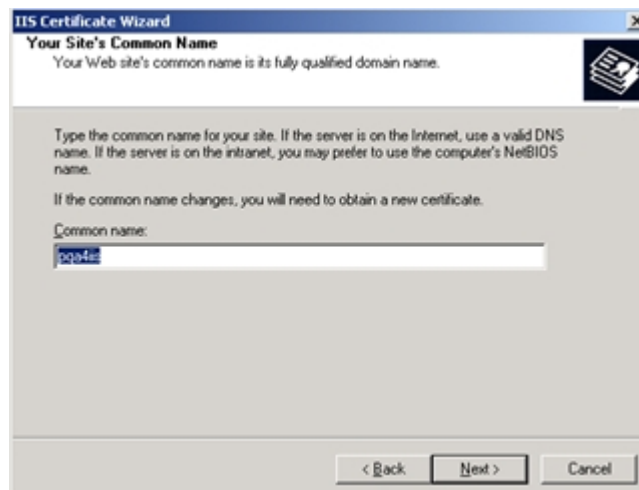
6. Select **Prepare the request now, but send it later** and click **Next**. If you have an Enterprise-level CA and the machine is part of the domain, a request can be directly prepared. The **Send the request immediately to an online certification authority** will be available. If you select this option, you do not need to follow the steps in [Submitting a Certificate Request to a CA Manually](#).



7. Enter a name for the new certificate. Ensure that the name is easy to refer to and to remember. Choose the bit length. The higher the bit length, the stronger the encryption, but the slower the performance. Choose a bit length that will balance strength and performance for your needs. For a root CA, you should use a key length of at least 2048 bits. This option is not available if you use existing keys. Click **Next**.

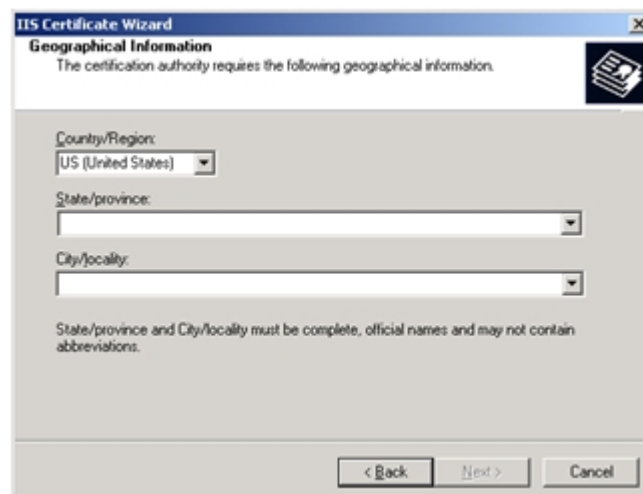


8. Enter your site's common name. This name must match the machine name or site URL. Click **Next**.



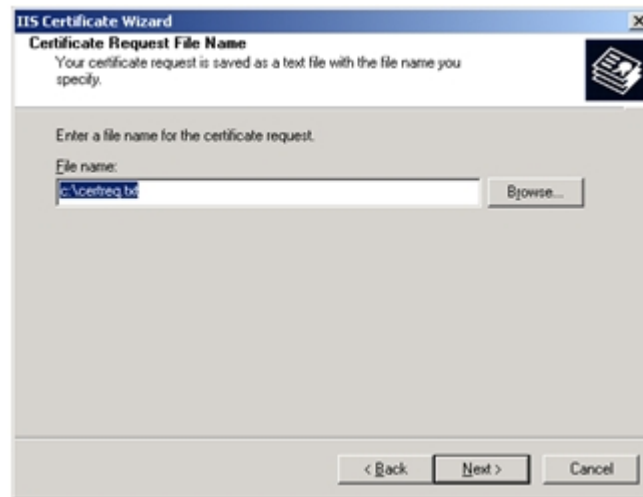
The screenshot shows the 'IIS Certificate Wizard' window with the title 'Your Site's Common Name'. The text inside says: 'Your Web site's common name is its fully qualified domain name.' Below this, it instructs the user to 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.' It also notes: 'If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' with the value 'ppp42' entered. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Enter your geographical information and click **Next**.

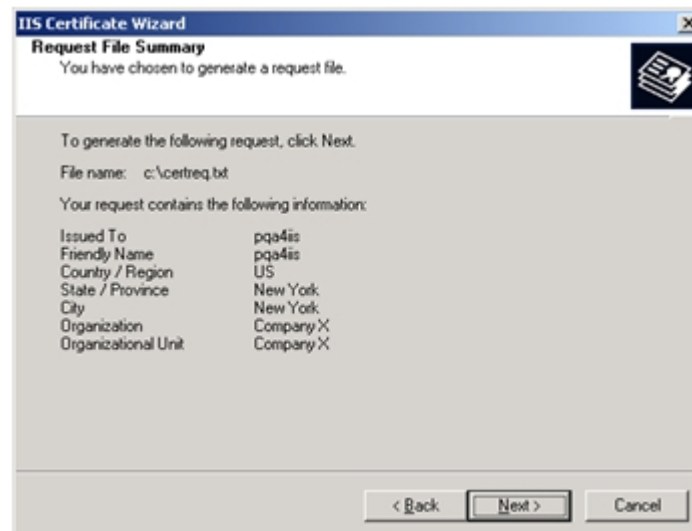


The screenshot shows the 'IIS Certificate Wizard' window with the title 'Geographical Information'. The text inside says: 'The certification authority requires the following geographical information.' Below this, there are three dropdown menus: 'Country/Region:' with 'US (United States)' selected, 'State/province:', and 'City/locality:'. A note at the bottom 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'.

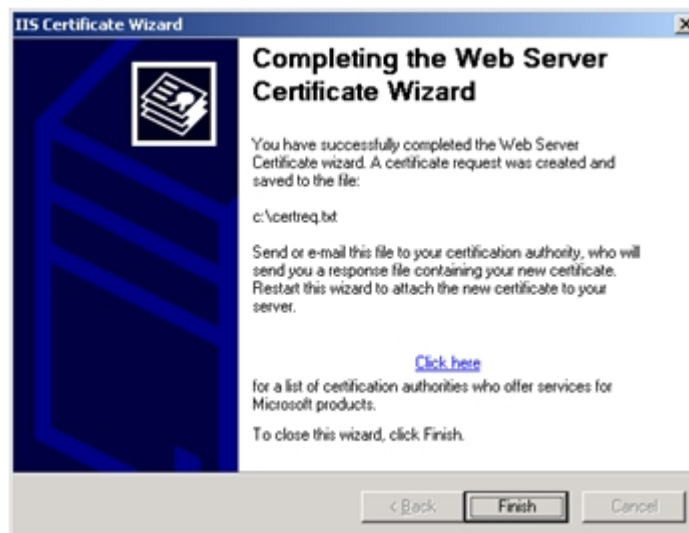
10. Enter a file name for the certificate request. Click **Browse** to locate it. Remember the location of this file as you will open it after completing the request.



11. Review the summary of your request. Click **Next**.

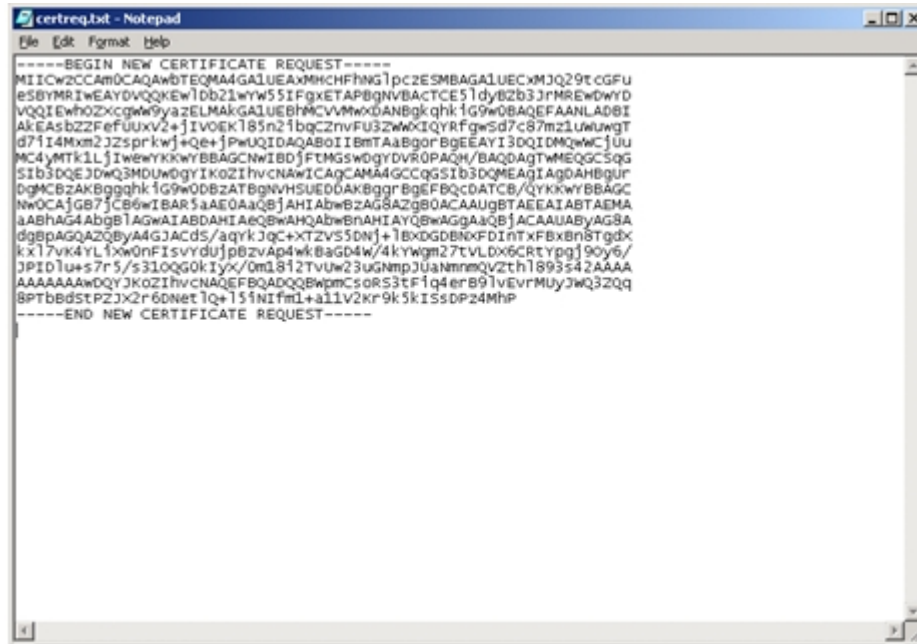


12. Click **Finish**.

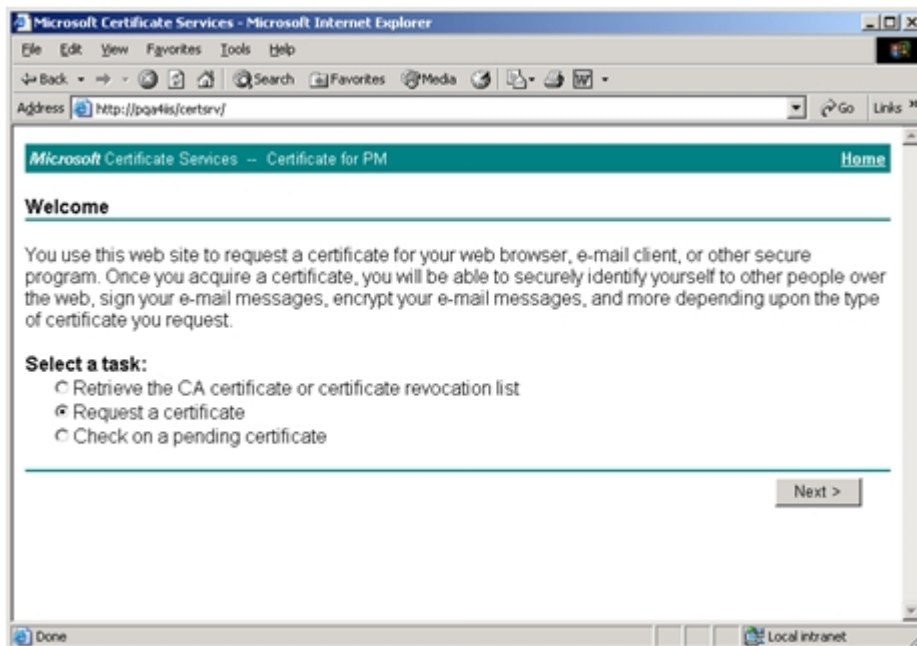


Submitting a Certificate Request to a CA Manually

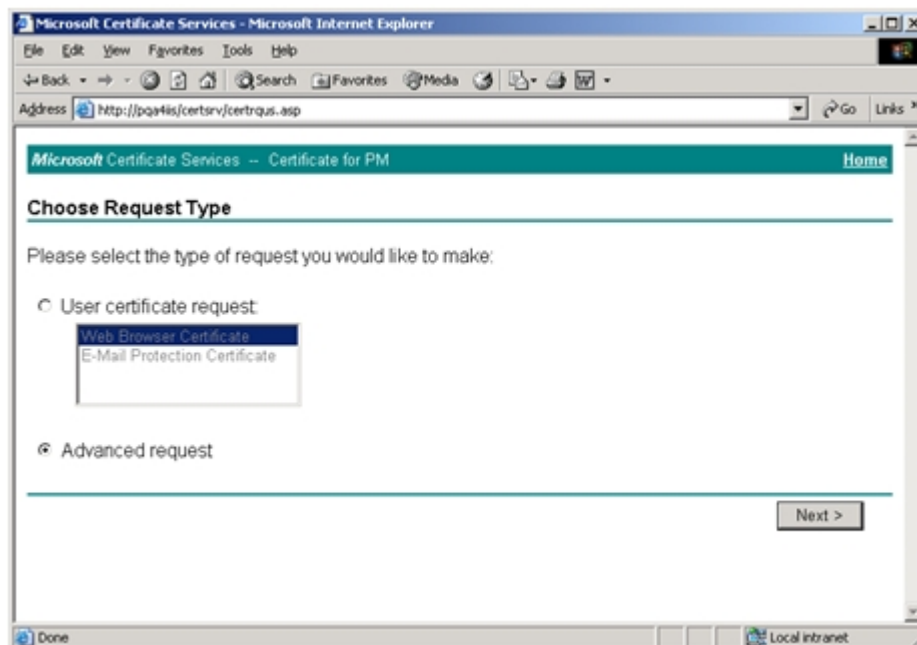
1. Locate the certificate request document (refer to Step 11 for the location). Open the text file and copy all of the contents to a clipboard. You will paste the contents into a request in Step 5.



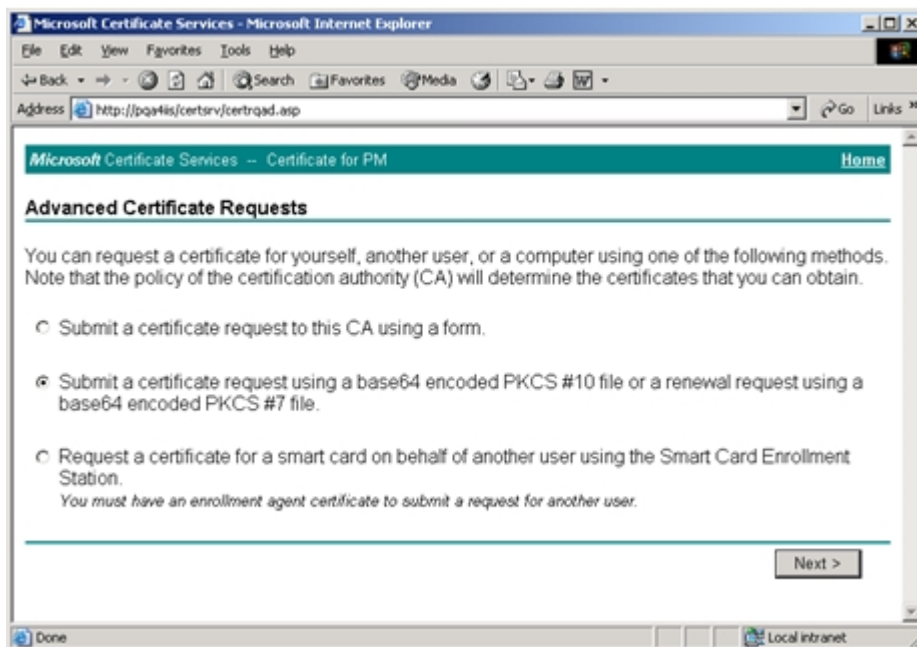
2. Open Microsoft Certificate Services. The URL is <http://yourmachinename/certsrv/>. Select **Request a Certificate** and click **Next**.



3. Select **Advanced Request** and click **Next**.



4. Select **Submit a certificate request using a base64 encoded... file** and click **Next**.



5. In the **Saved Request** text box, paste the contents of the certificate request file copied in Step 1 (or you can browse to locate the file and insert it). Click **Submit**.

Microsoft Certificate Services - Certificate for PM [Home](#)

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

[Browse](#) for a file to insert.

Additional Attributes:

Attributes:

Done Local intranet

Microsoft Certificate Services - Certificate for PM [Home](#)

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
dgBpAGQA2QByA4GJACdS/aqTkJqC+XTZV85DNj+1  
kx17vK4YL1Xv0nFIsVYdUjpBzvAp4wkBAGD4W/4k  
JPID1u+s7r5/s31OQ00kIyX/Om1812TvUw23uGNm  
AAAAAAvDQYJKoZIhvcNAQEFBQADQCBUpmCsoRS3  
8PTbBdStPZJX2r6DNNet1Q+15iNIfm1+a11V2Kr9k  
-----END NEW CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

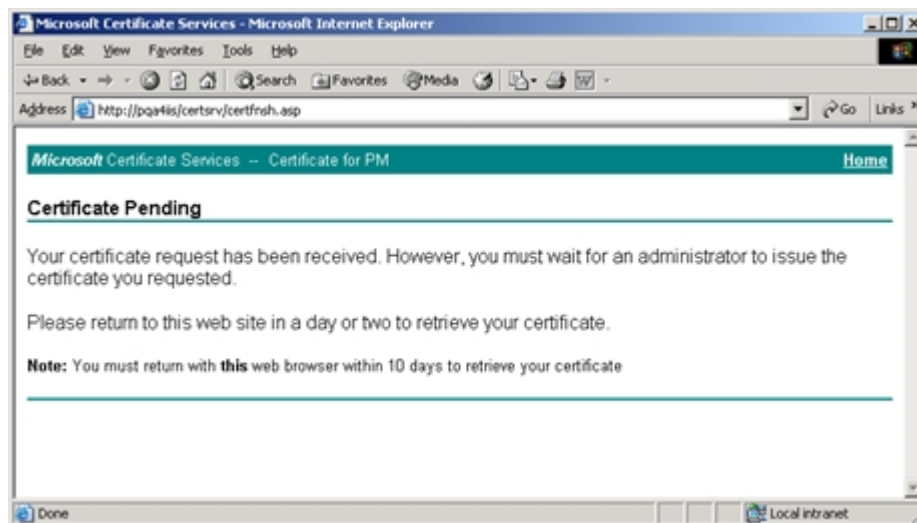
Additional Attributes:

Attributes:

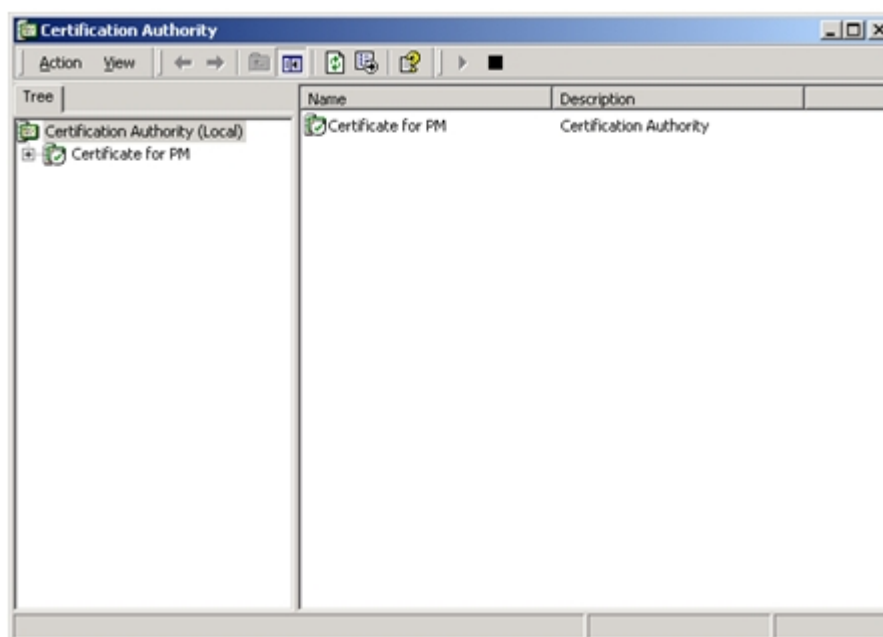
[Submit >](#)

Done Local intranet

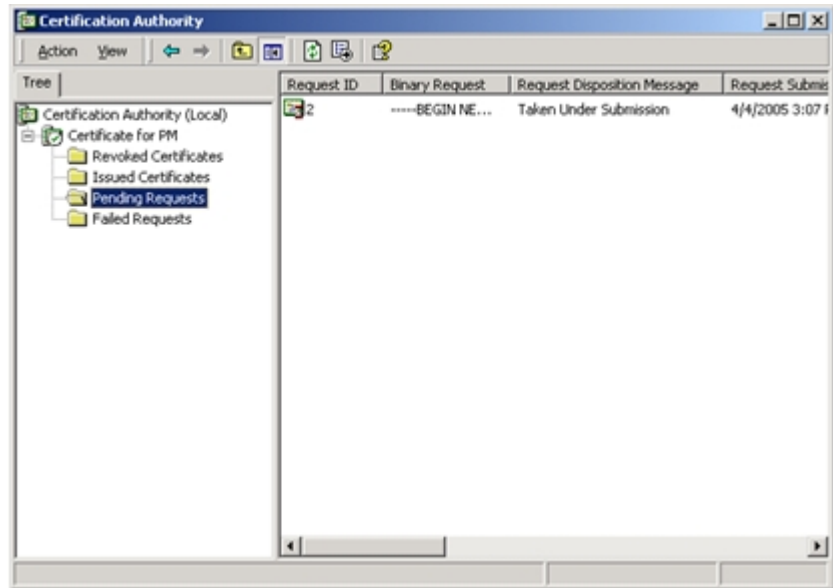
Your certificate request has been received and is pending.



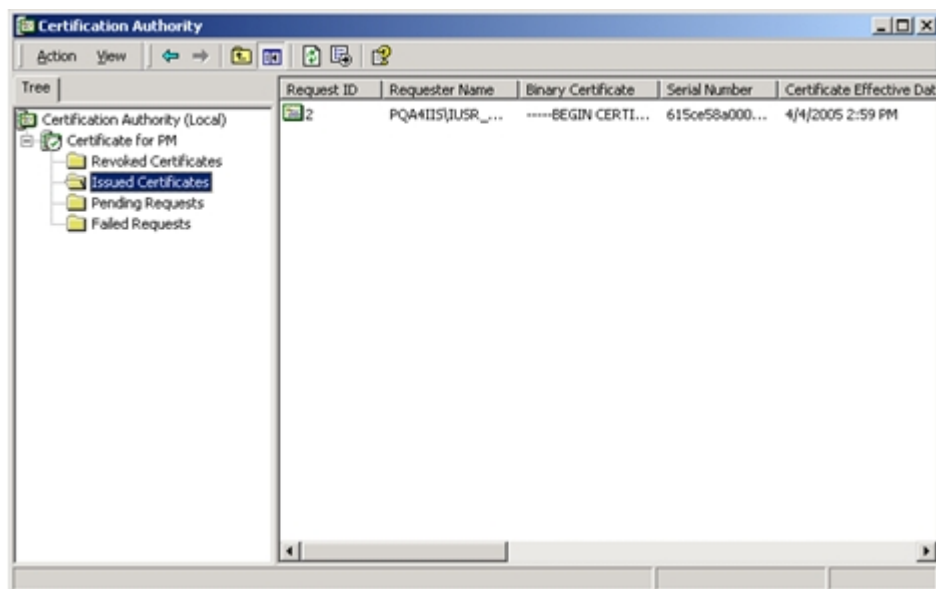
6. Open the Certificate Authority tool by clicking **Start > Programs > Administrative Tools > Certificate Authority**. Expand the certificate authority.



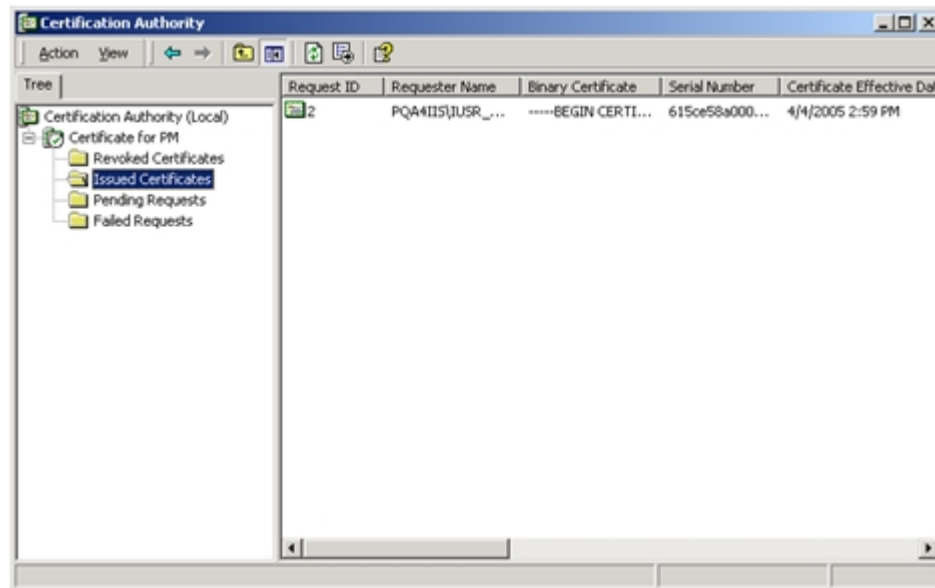
7. Click on the **Pending Requests** folder. Click the certificate request in the right pane, and click **All Tasks > Issue**.



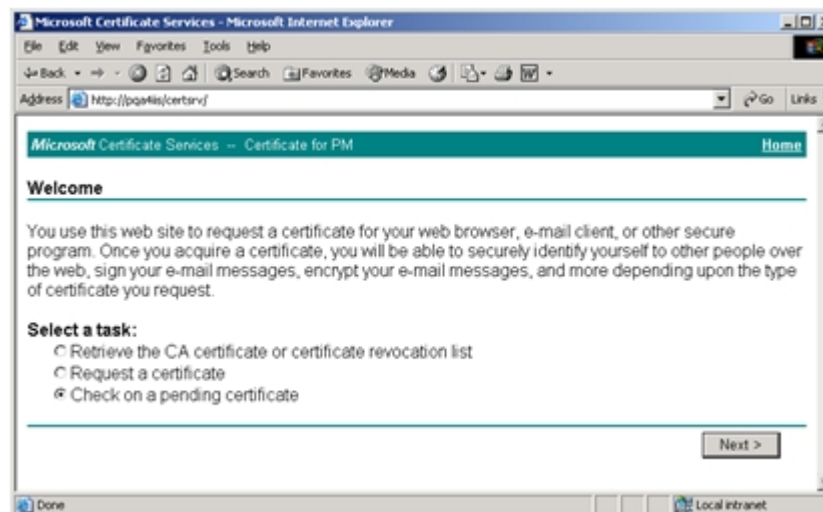
The **Pending Requests** folder is now empty.



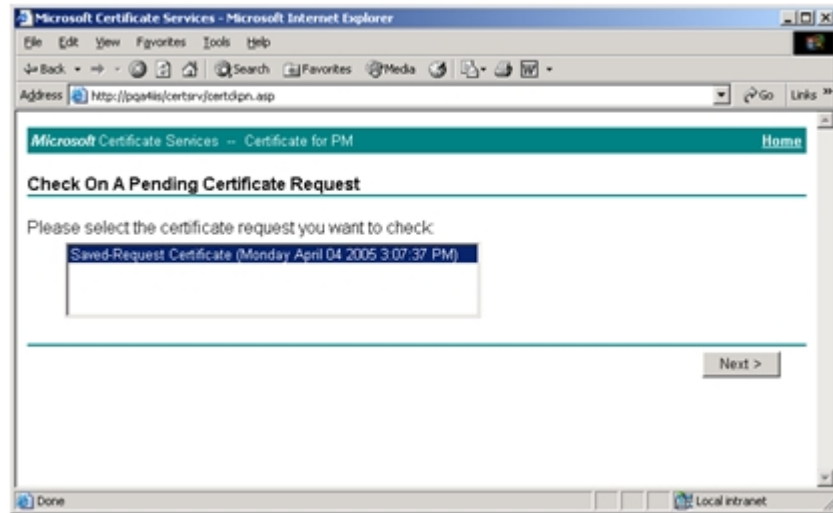
The certificate moves to the **Issued Certificates** folder.



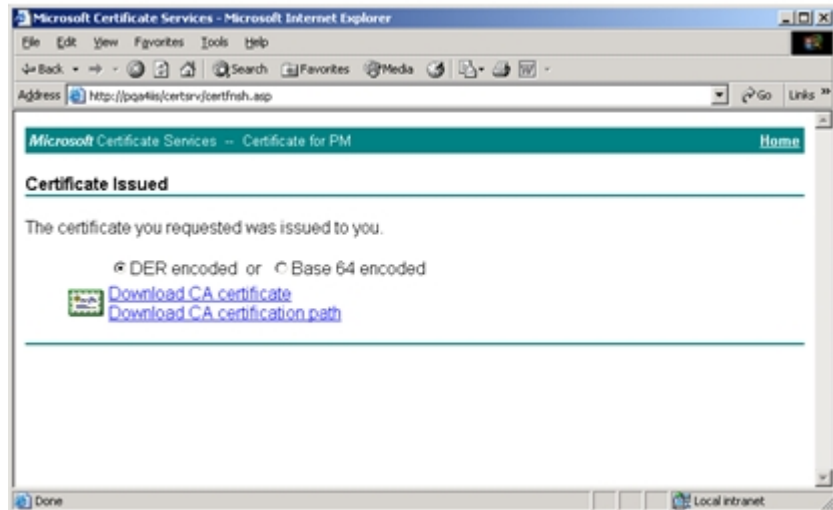
8. Open Microsoft Certificate Services. The URL is <http://yourmachinename/certsrv/>. Select **Check on a pending certificate** and click **Next**.



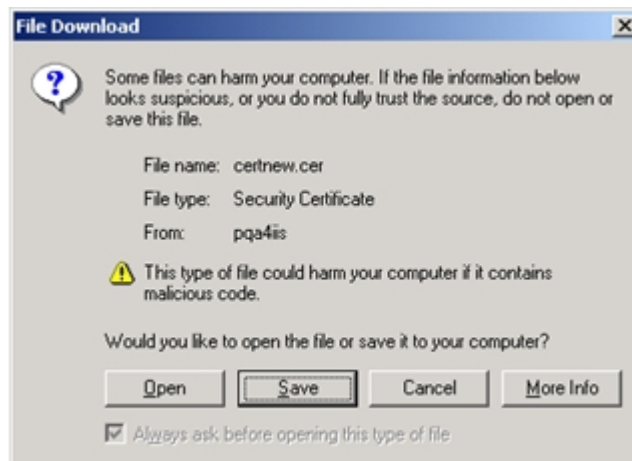
9. Select the certificate that was just created and click **Next**.



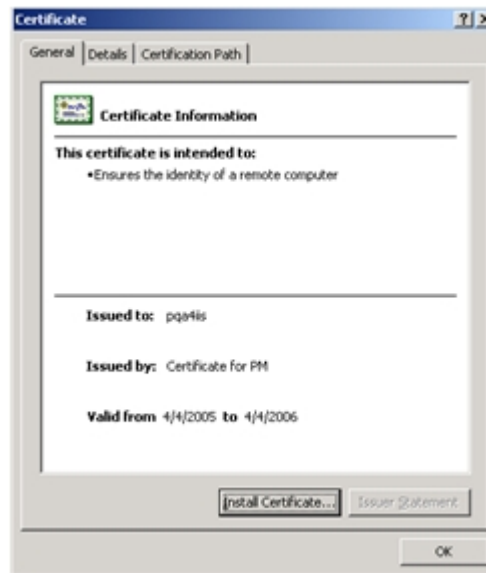
10. Click **Download CA certificate**. You can select either DER or Base 64 encoded.



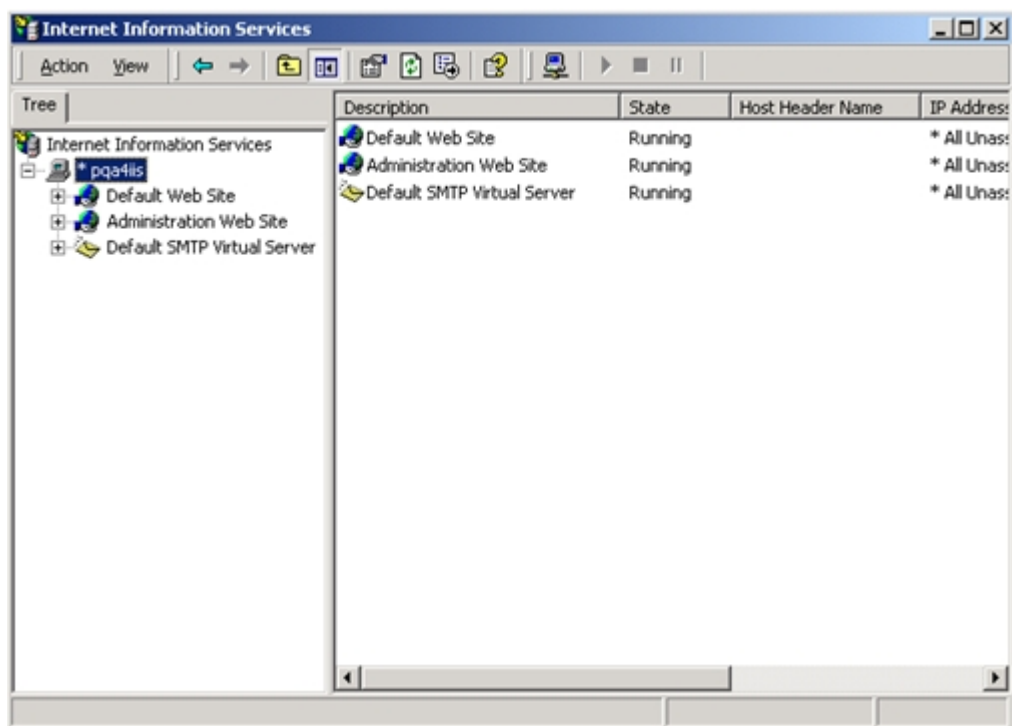
11. Save the file to a location on your computer. Download the certificate.



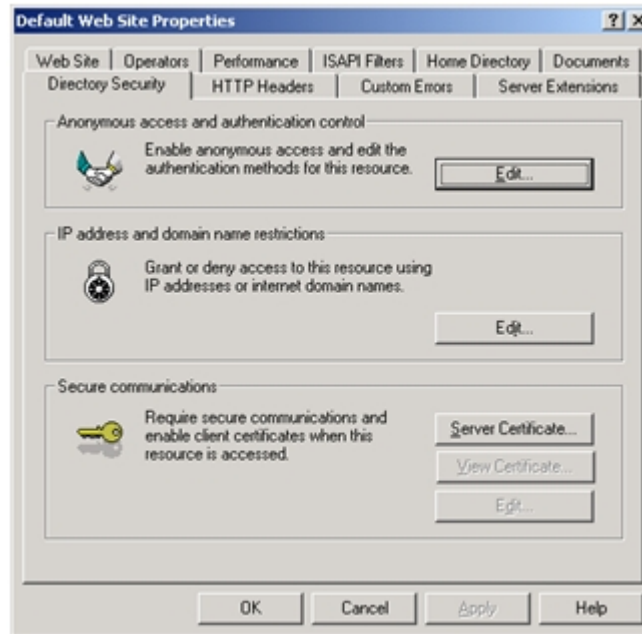
12. Locate the certificate that was just downloaded and double-click it to open it.



13. This certificate must now be installed into IIS. Open IIS and locate the Web site where ESSO-PG is installed. Right-click the Web site and click **Properties**.



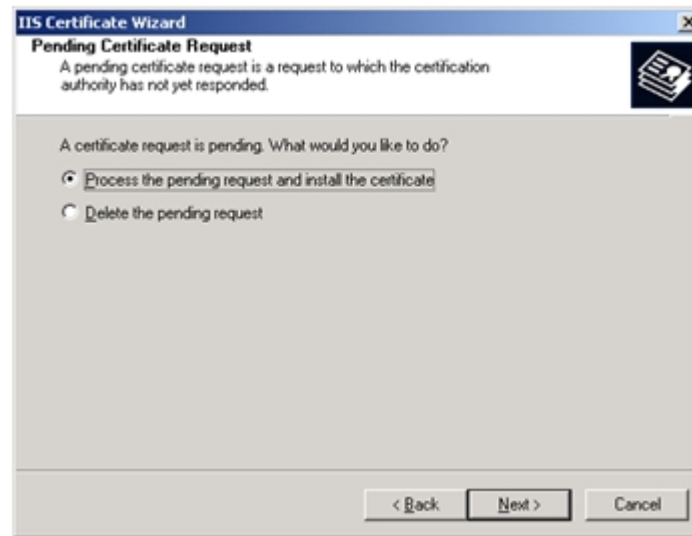
14. Select the **Directory Security** tab and click **Server Certificate**.



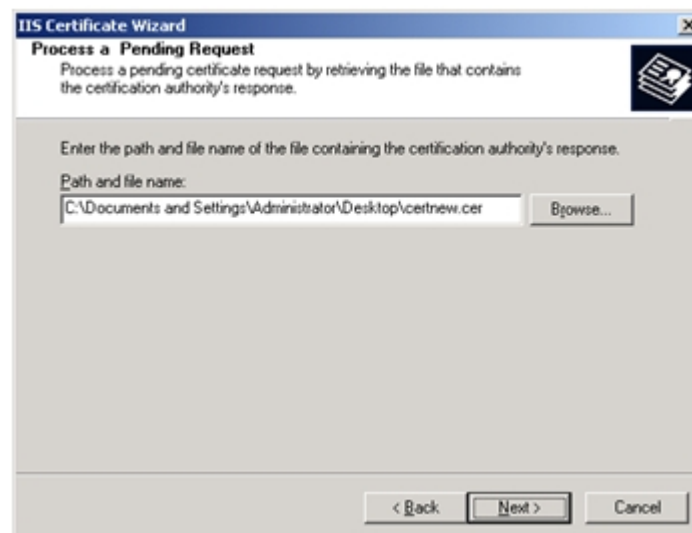
15. On the Web Server Certificate Wizard panel, click **Next**.



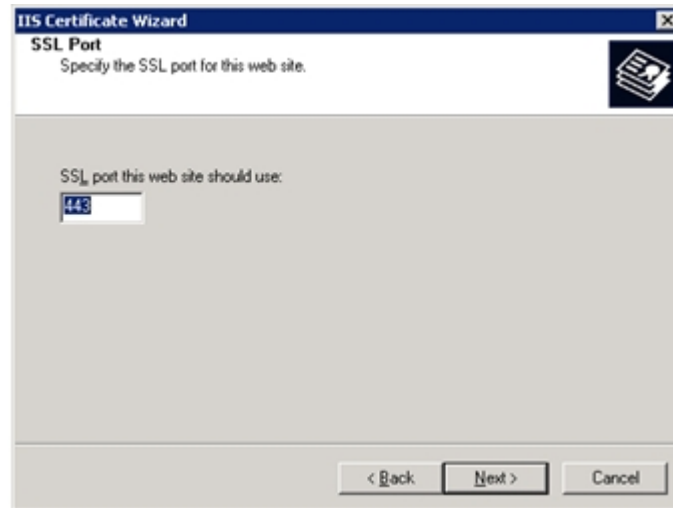
16. Click Process the pending request and install the certificate. Click **Next**.



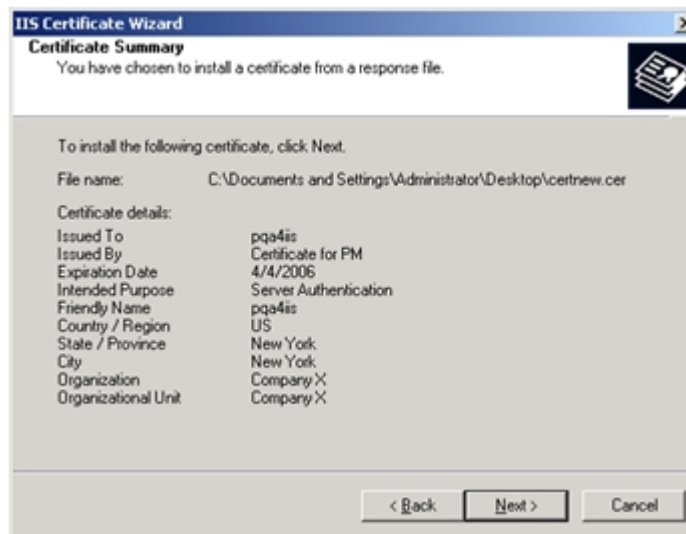
17. Browse to the location of the saved certificate file. Click **Next**.



18. The Wizard asks for the SSL port to use with this Web site. The default SSL Port is 443. Click **Next**.



19. Review the summary of your request. If there are any problems, you might have to issue a new certificate. If everything is correct, click **Next** to install the certificate.



20. When the IIS Certificate Wizard is done, click **Finish**.