Oracle® Enterprise Single Sign-on Provisioning Gateway

Certificate Setup Guide

Release 10.1.4.1.0

E12609-01

November 2008

ORACLE®

Oracle Enterprise Single Sign-on Provisioning Gateway Certificate Setup Guide, Release 10.1.4.1.0

E12609-01

Table of Contents

About ESSO-PG Certificate Setup

This guide describes how to obtain certificates through Microsoft® Certificate Services and how to install a standalone certificate authority (CA), which can be used to issue certificates to anyone, even non-Windows® entities.

Audience

This guide is intended for experienced administrators responsible for obtaining certificates and for installing and managing a standalone certificate authority. Persons completing the procedures should also be familiar with their company's system standards.

Acronym or Abbreviation	Full Name
SSO Agent	ESSO-LM Agent
SSO Administrative Console	ESSO-LM Administrative Console
ESSO-LM	Oracle Enterprise Single Sign-On Logon Manager
ESSO-AM	Oracle Enterprise Single Sign-On Authentication Manager
ESSO-KM	Oracle Enterprise Single Sign-On Kiosk Manager
ESSO-PG	Oracle Enterprise Single Sign-On Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-On Password Reset
SSO	ESSO-LM
FTU	First Time Use
SSO Agent	ESSO-LM Agent

Using ESSO-PG Certificate Setup

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

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**.
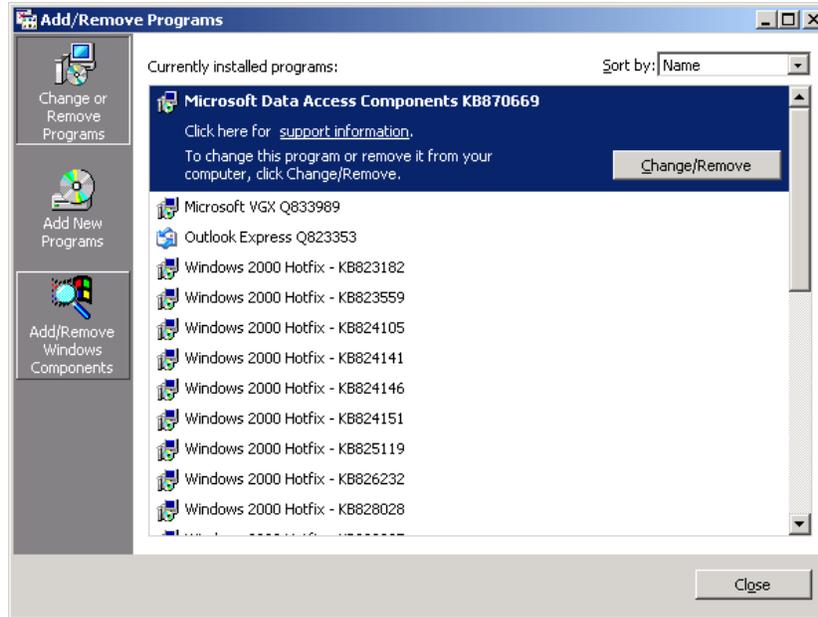
3. Check **Certificate Services** and click **Next**.
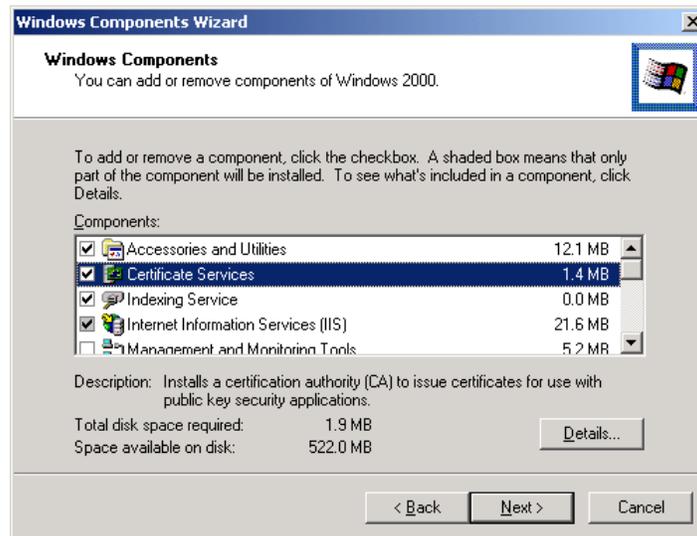
4. When you are asked if you want to continue, click **Yes**.
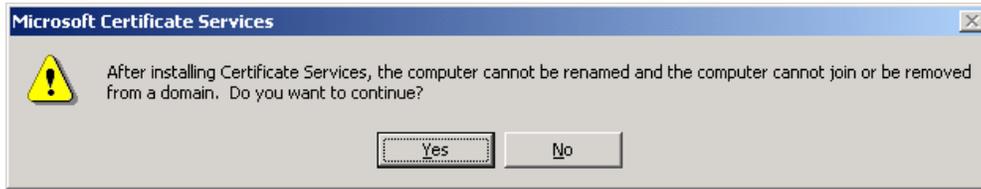
5. Select **Stand-alone root CA**.
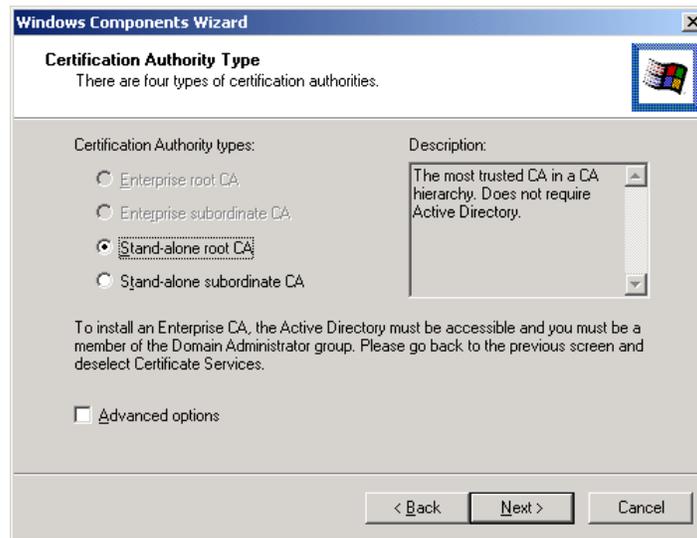
6. Enter CA Identifying Information. Enter the length of time that this certificate should be valid. Click **Next**.
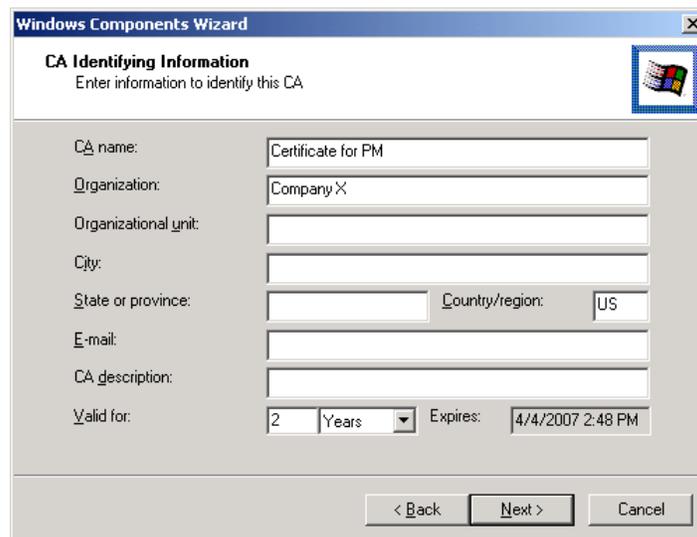
7. Specify the storage location for the configuration data. Click **Next**.
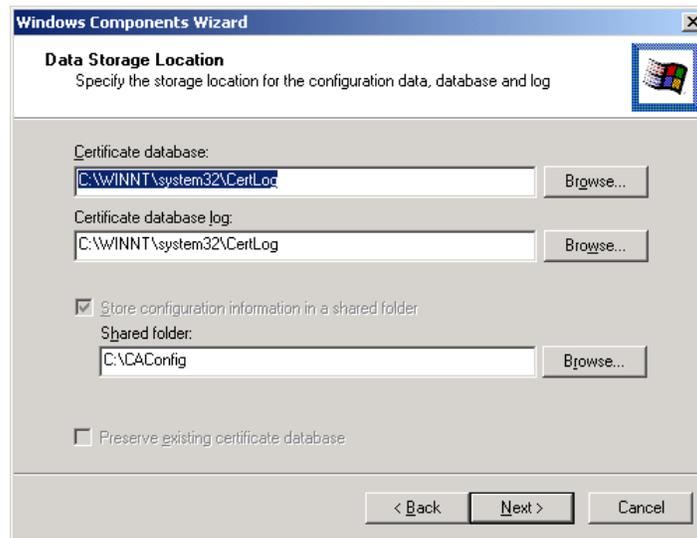
8. You might be prompted to stop IIS. If so, click **OK**.
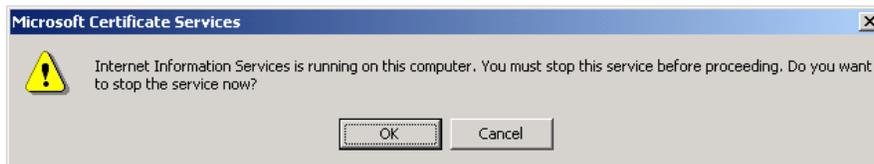
9. You might be prompted to insert the Windows CD. If so, insert it and click **OK**.
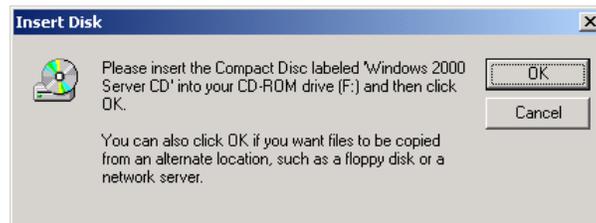
10. At this point, you might be prompted to enable ASP pages. You must select **Yes**.

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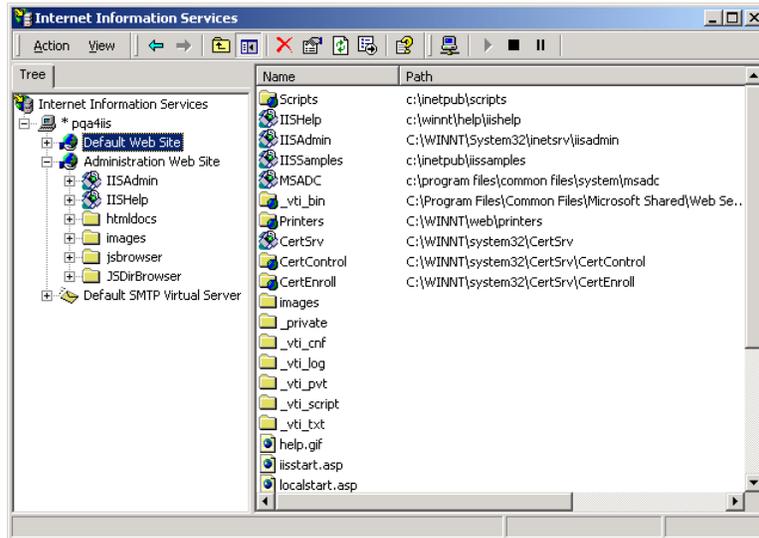
3. Select the **Directory Security** tab. Under **Secure communications**, click **Server Certificate**.

9
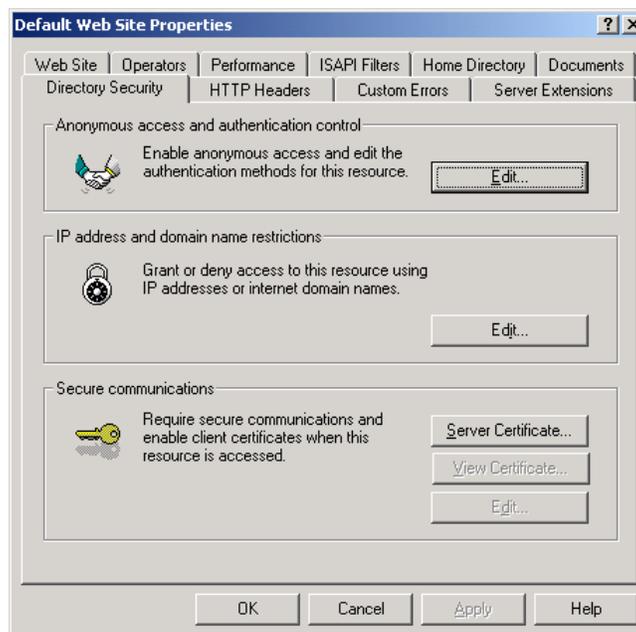
4. The Web Server Certificate Wizard appears. You will use the wizard to generate a request for a certificate. Click **Next**.

5. Select **Create a new certificate** and click **Next**.
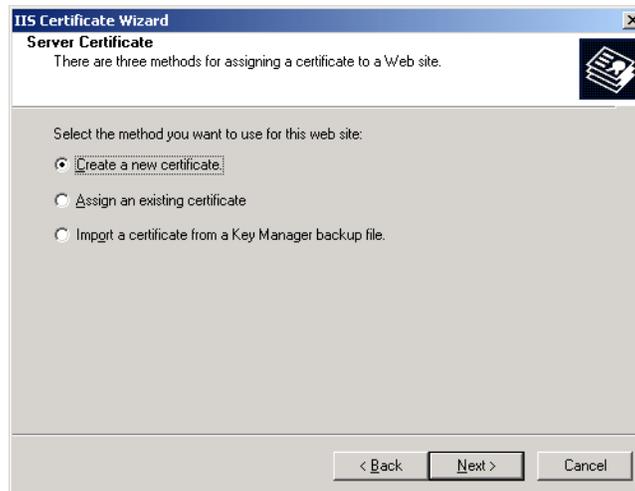
6. Select **Prepare the request now, but send it later** and click **Next**.
    If you have an Enterprise-level CA and the machine is part of the domain, a request can be directly prepared. The **Send the request immediately to an online certification authority** will be available. If you select this option, you do not need to follow the steps in Submitting a Certificate Request to a CA Manually.
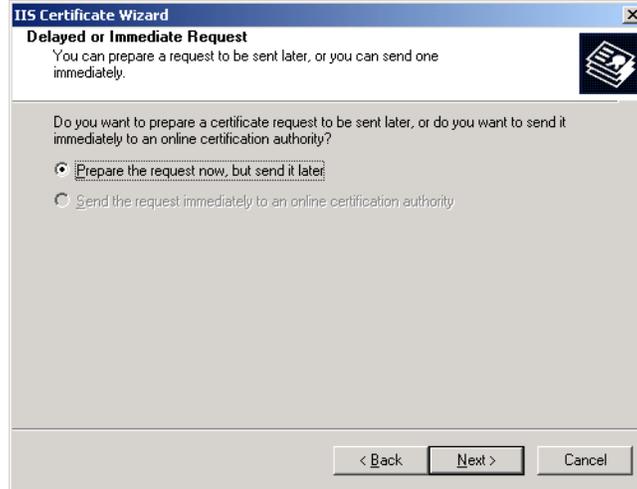
7. Enter a name for the new certificate. Ensure that the name is easy to refer to and to remember. Choose the bit length. The higher the bit length, the stronger the encryption, but the slower the performance. Choose a bit length that will balance strength and performance for your needs. For a root CA, you should use a key length of at least 2048 bits. This option is not available if you use existing keys. Click **Next**.

11

8. 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. Click **Next**.

9. Enter your site's common name. *This name must match the machine name or site URL.* Click N**ext**.

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

11. 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.
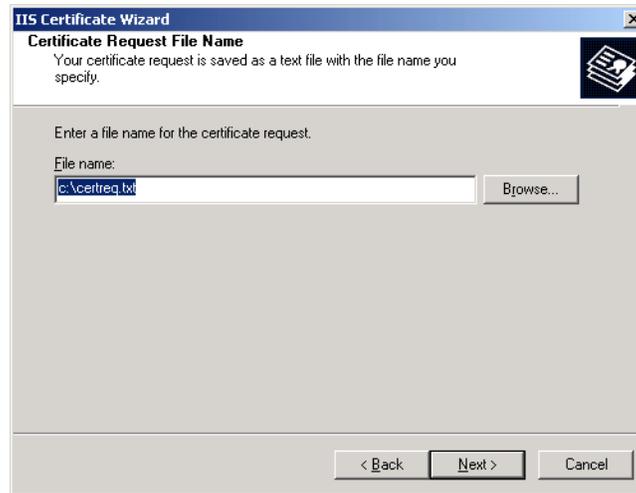
12. Review the summary of your request. Click **Next**.
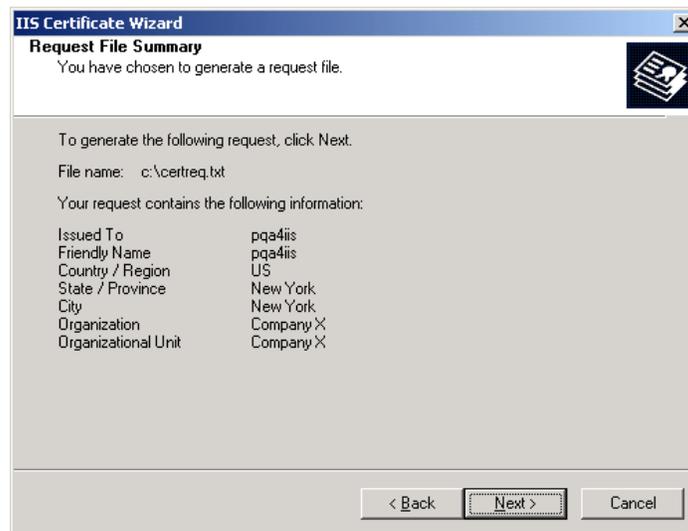
13. Click **Finish**.
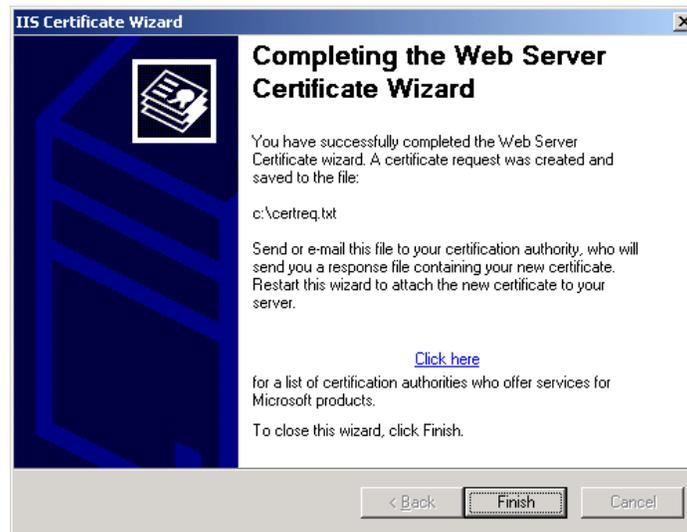
Submitting a Certificate Request to a CA Manually

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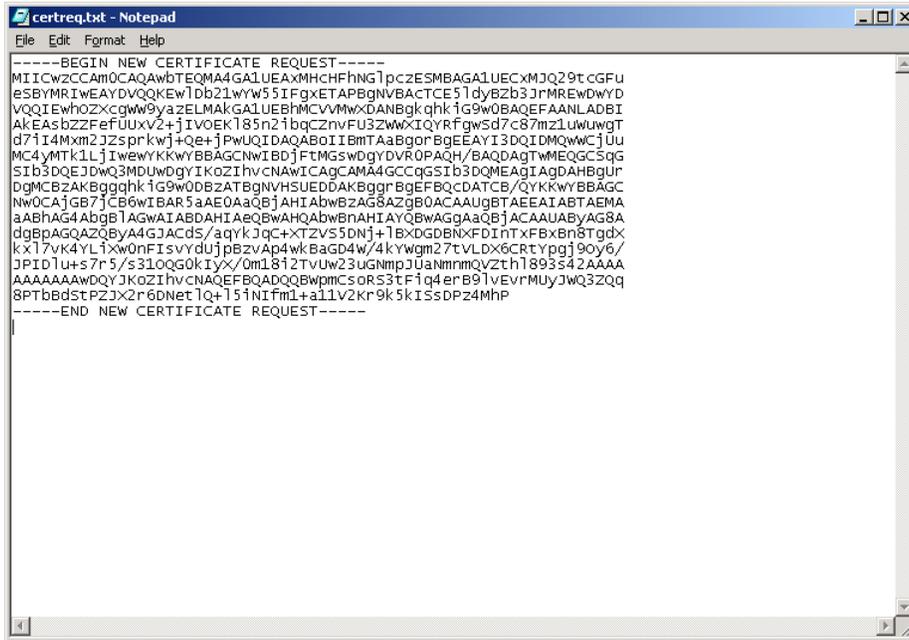
2. Open Microsoft Certificate Services. The URL is http://*yourmachinename*/certsrv/. Select **Request a Certificate** and click **Next**.

15
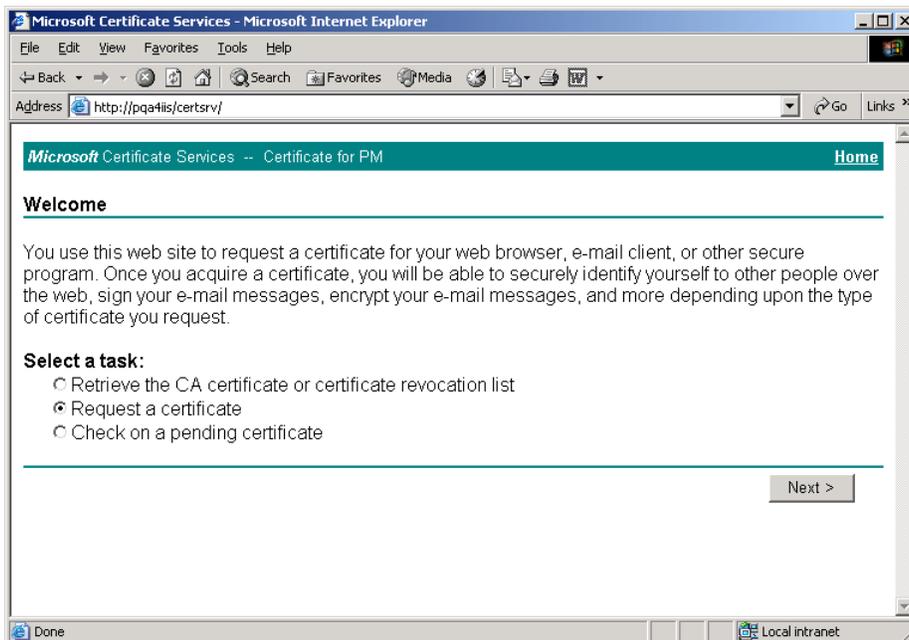
3. Select **Advanced Request** and click **Next.**
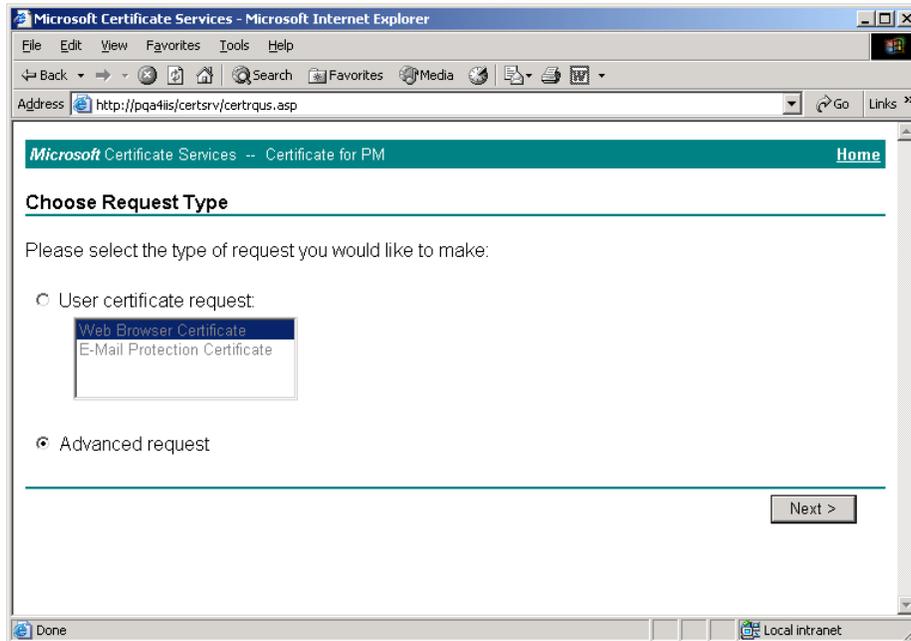
4. Select **Submit a certificate request using a base64 encoded... file** and click **Next**.
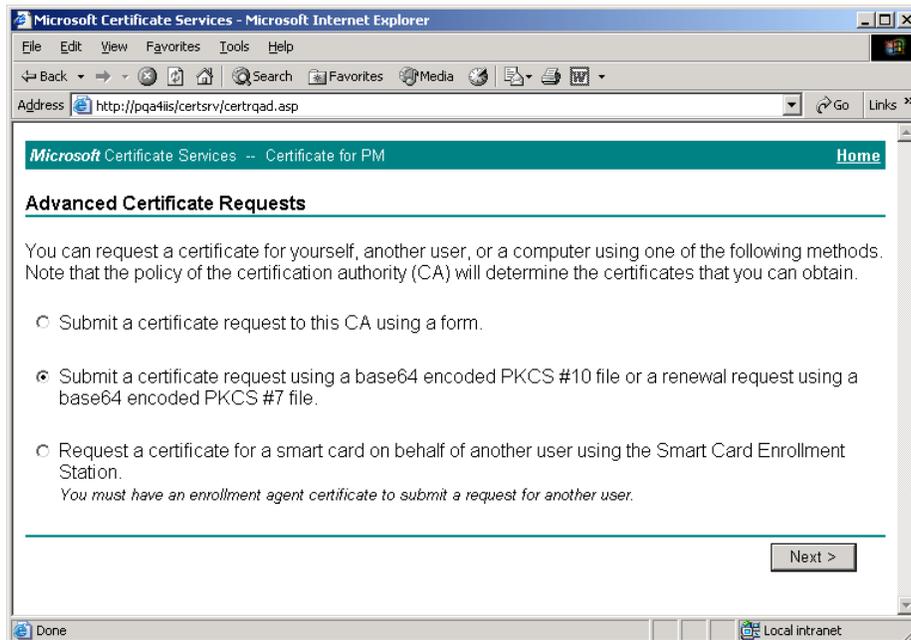
5. In the **Saved Request** text box, paste the contents of the certificate request file copied in Step 1 (or you can browse to locate the file and insert it). Click **Submit**.

6. Your certificate request has been received and is pending.
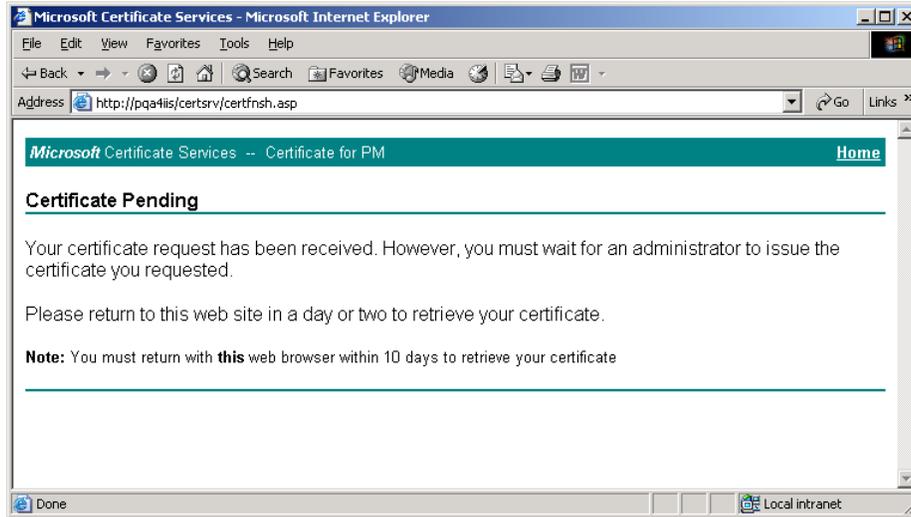
7. Open the Certificate Authority tool by clicking **Start** > **Programs** > **Administrative Tools** > **Certificate Authority**. Expand the certificate authority.
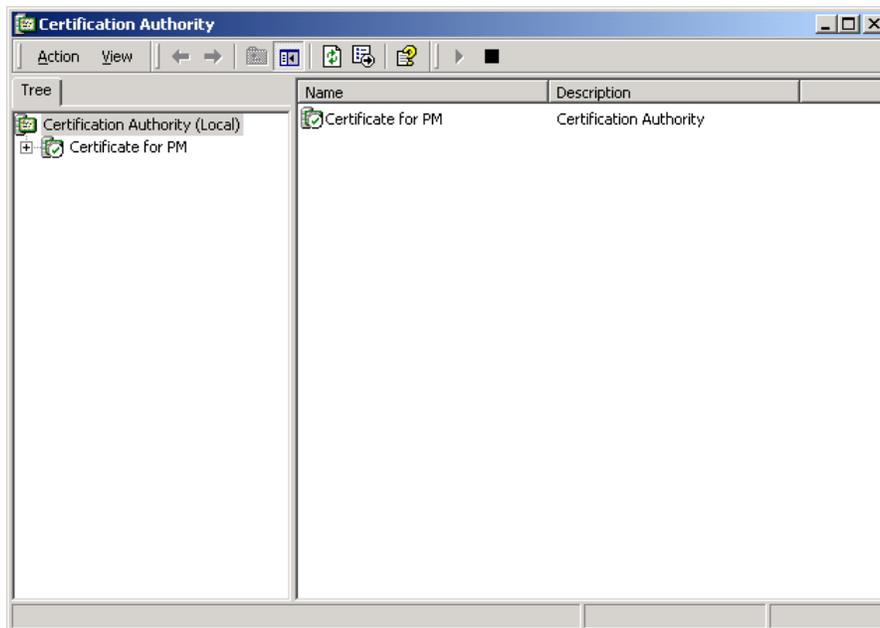
8. Click on the **Pending Requests** folder. Click the certificate request in the right pane, and click **All Tasks** > **Issue**.
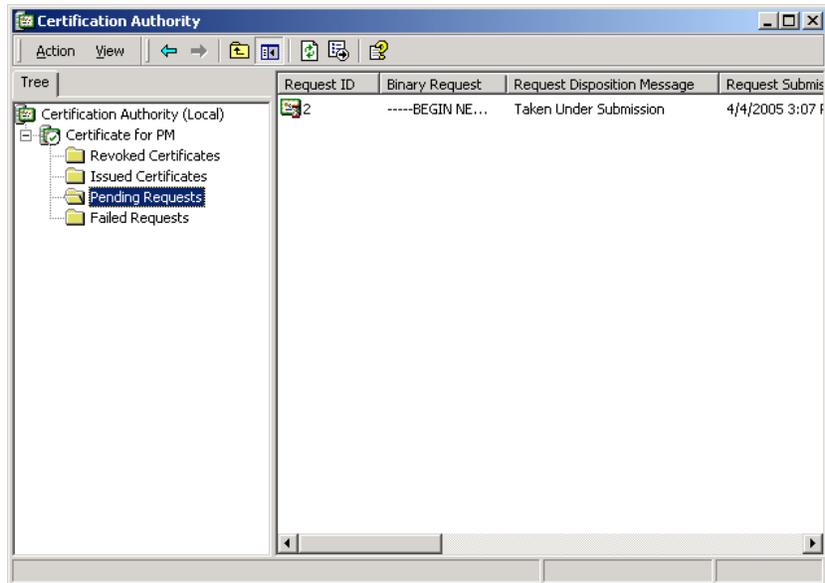
The Pending Requests folder is now empty.
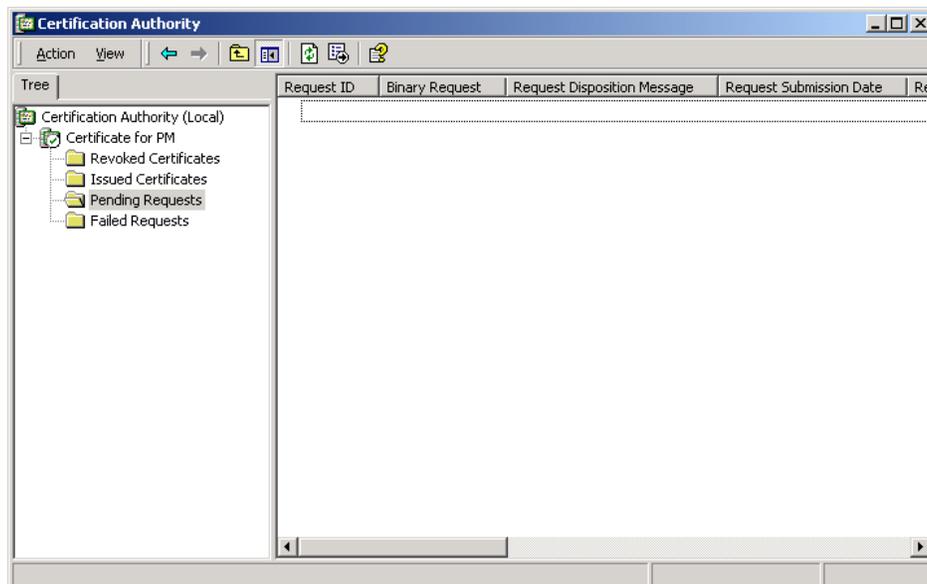
The certificate moves to the **Issued Certificates** folder.
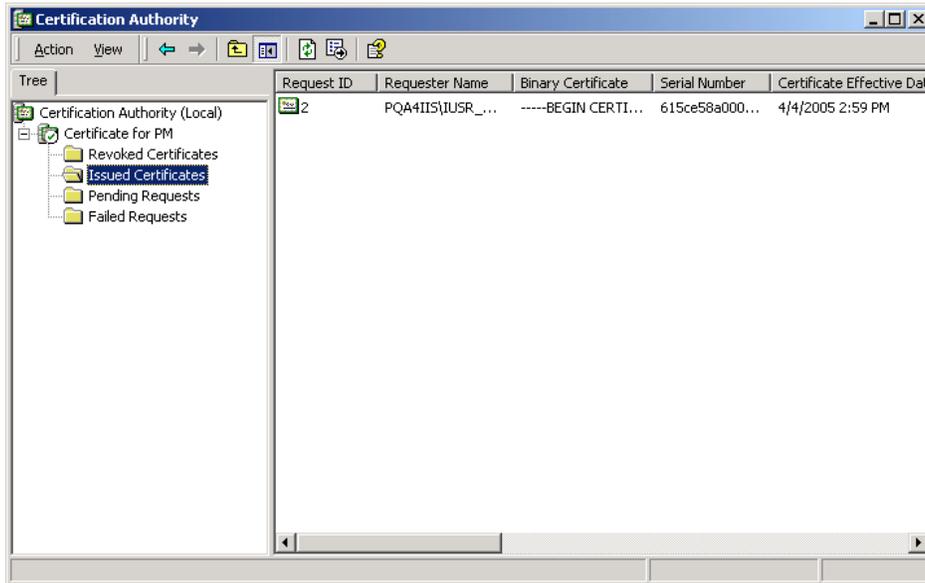
9. Open Microsoft Certificate Services. The URL is http://*yourmachinename*/certsrv/. Select **Check on a pending certificate** and click **Next**.
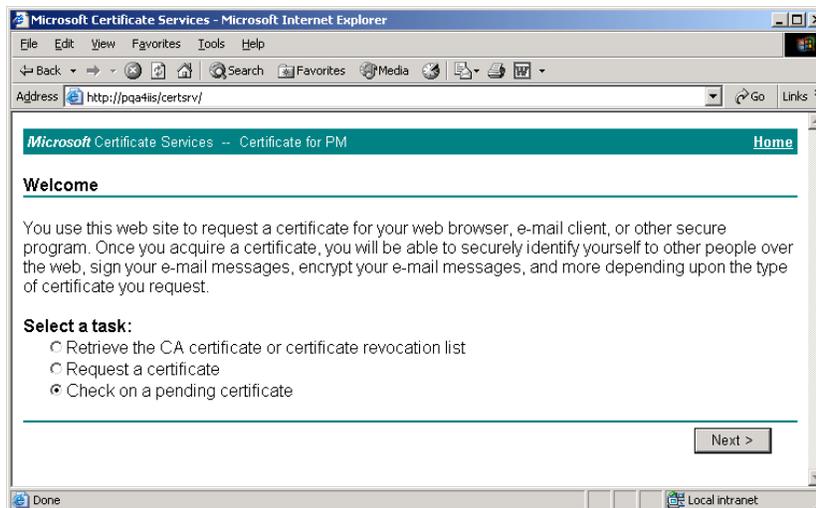
10. Select the certificate that was just created and click **Next**.
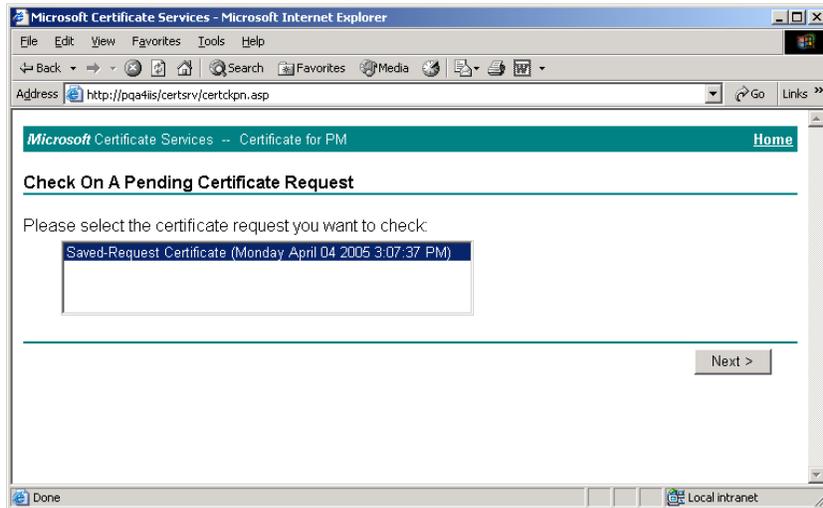
11. Click **Download CA certificate.** You can select either DER or Base 64 encoded.
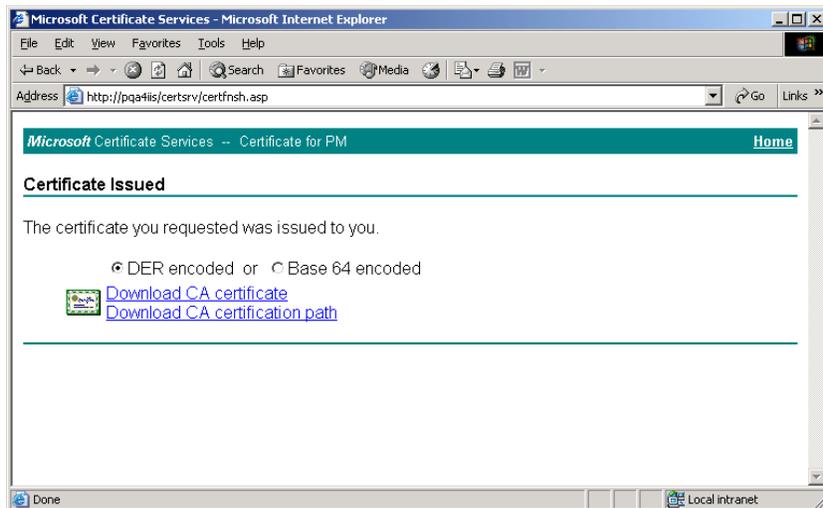
12. Save the file to a location on your computer. Download the certificate.
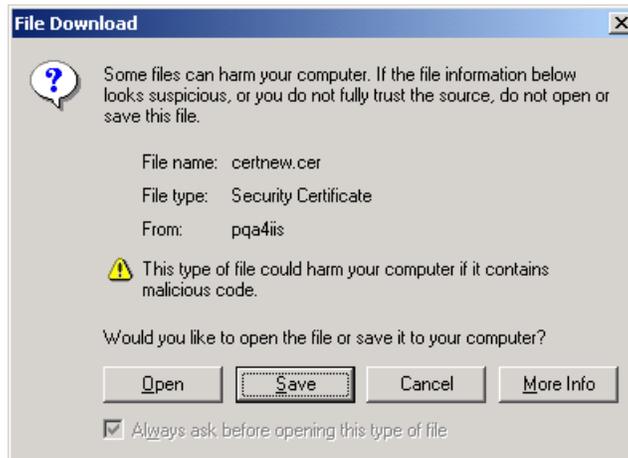
13. Locate the certificate that was just downloaded and double-click it to open it.

14. 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**.
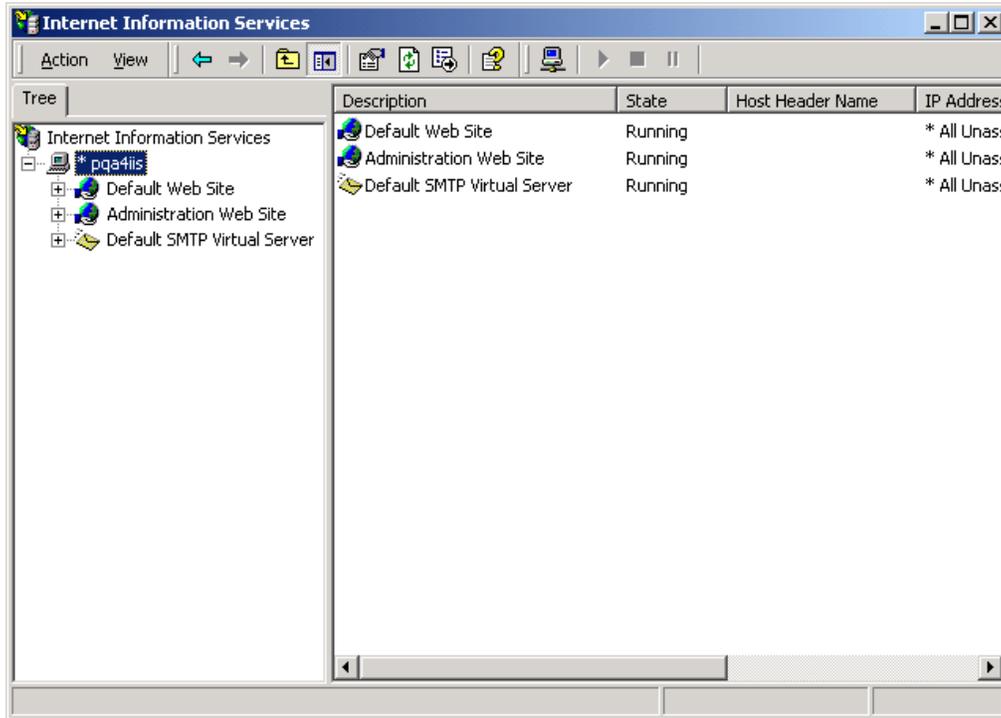
15. Select the **Directory Security** tab and click **Server Certificate.**
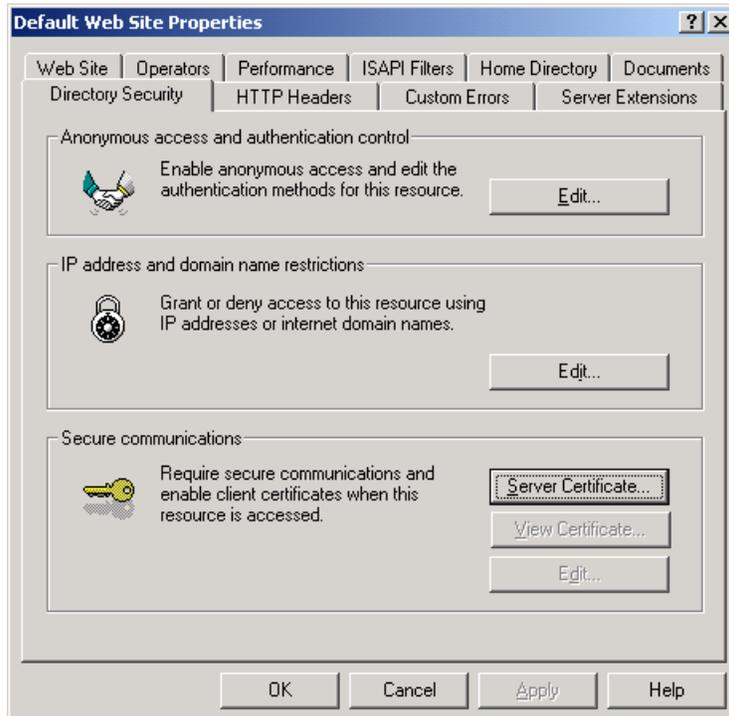
16. On the Web Server Certificate Wizard panel, click **Next**.
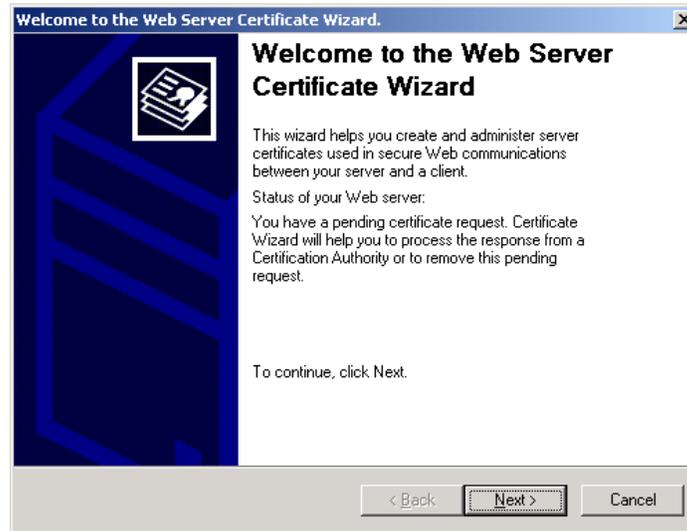
17. Click **Process the pending request and install the certificate**. Click **Next**.
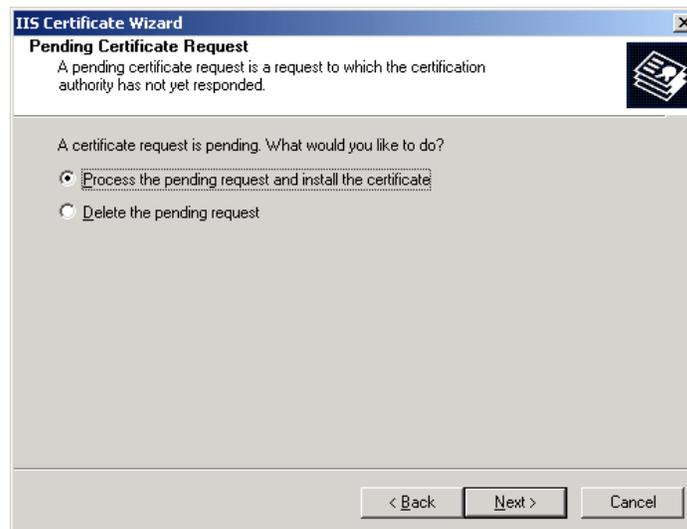
18. Browse to the location of the saved certificate file. Click **Next**.
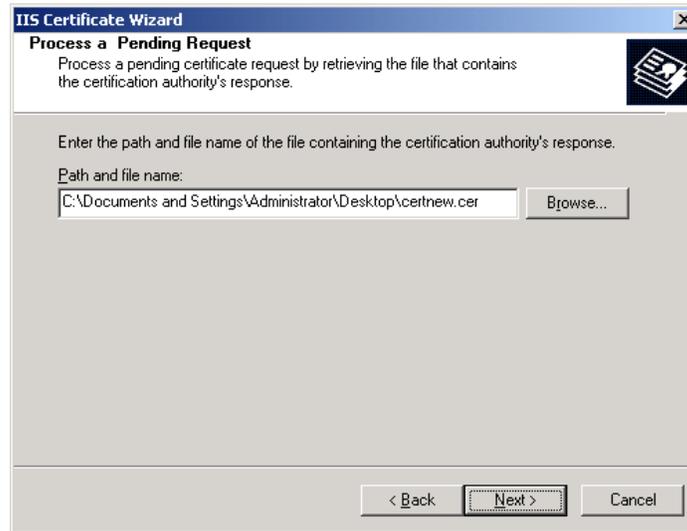
19. The Wizard asks for the SSL port to use with this Web site. The default SSL Port is 443. Click **Next**.
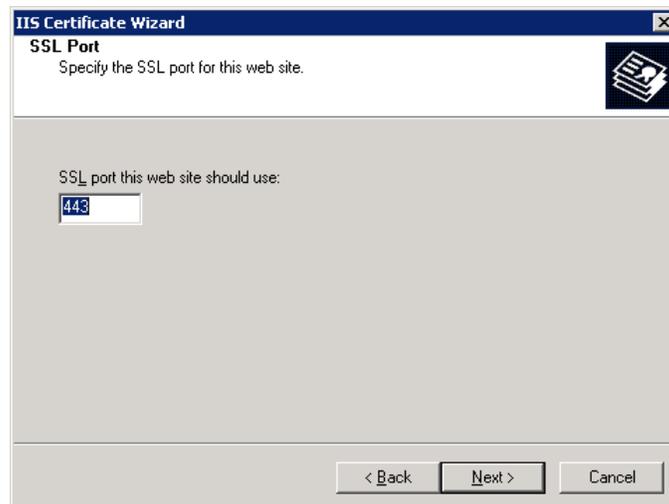
20. Review the summary of your request. If there are any problems, you might have to issue a new certificate. If everything is correct, click **Next** to install the certificate.
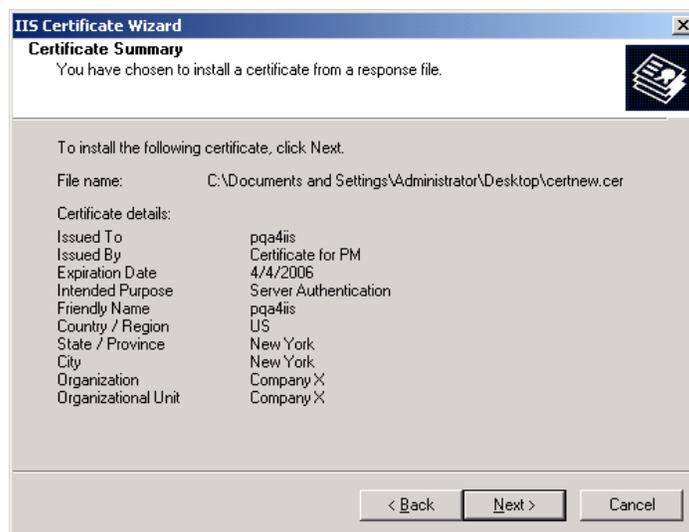
21. When the IIS Certificate Wizard is done, click **Finish**.