# Oracle® Enterprise Single Sign-on Password Reset

How-To: Configuring SSL Support for the ESSO-PR Web Interface

Release 11.1.1.5.0

**20995-01**

March 2011

ORACLE

Oracle Enterprise Single Sign-on Password Reset How-To: Configuring SSL Support for the ESSO-PR Web Interface

Release 11.1.1.5.0

20995-01

# Table of Contents


Table of Contents ..... 3

Introduction ..... 4

About This Guide ..... 4

Prerequisites ..... 4

Terms and Abbreviations ..... 4

Accessing ESSO-PR Documentation ..... 4

Part 1: Creating and Installing an SSL Certificate ..... 5

Overview ..... 5

Step 1: Installing Microsoft Certificate Services ..... 6

Step 2: Generating a Certificate Request for the IIS Site Serving the ESSO-PR Web Interface ..... 11

Step 3: Submitting the Certificate Request to the Certificate Authority ..... 19

Step 4: Issuing the Certificate ..... 23

Step 5: Installing the Certificate ..... 25

Part 2: Configuring the ESSO-PR Web Interface for SSL Connections ..... 31

Overview ..... 31

Step 1: Modifying the ESSO-PR Server Configuration Files ..... 31

Step 2: Granting ESSO-PR Server Access to the `WebServices` Directory ..... 35

Step 3: Restricting Web Interface Connections to SSL Only ..... 37

Part 3: Testing the New Configuration ..... 40

# Introduction

## About This Guide

This document describes how to create and install an X.509 SSL certificate using Microsoft Certificate Services (MCS) to enable SSL security for ESSO-PR. The instructions in this guide apply to Windows 2000 and Windows Server 2003 families of operating systems. The guide also describes how to configure Microsoft Internet Information Services (IIS) to enable SSL (and disallow non-SSL) connections to the ESSO-PR Web interface.

## Prerequisites

Readers of this guide should be familiar with the administration and maintenance of the Windows family of operating systems, and particularly, configuring Microsoft Internet Information Services (IIS). Readers should also understand cryptography concepts such as certificates, certificate authorities, and the Secure Sockets Layer (SSL) technology.

## Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

| Term or Acronym | Description |
|---|---|
| ESSO-PR | Oracle Enterprise Single Sign-on Password Reset |
| CA | Certificate Authority |
| MCS | Microsoft Certificate Services |
| Server | ESSO-PR Server |
| Client | ESSO-PR client-side software |
| Console | ESSO-PR Administrative Console |

## Accessing ESSO-PR Documentation

We continually strive to keep ESSO-PR documentation accurate and up to date. For the latest version of this and other ESSO-PR documents, visit http://download.oracle.com/docs/cd/E21040_01/index.htm.

# Part 1: Creating and Installing an SSL Certificate

## Overview

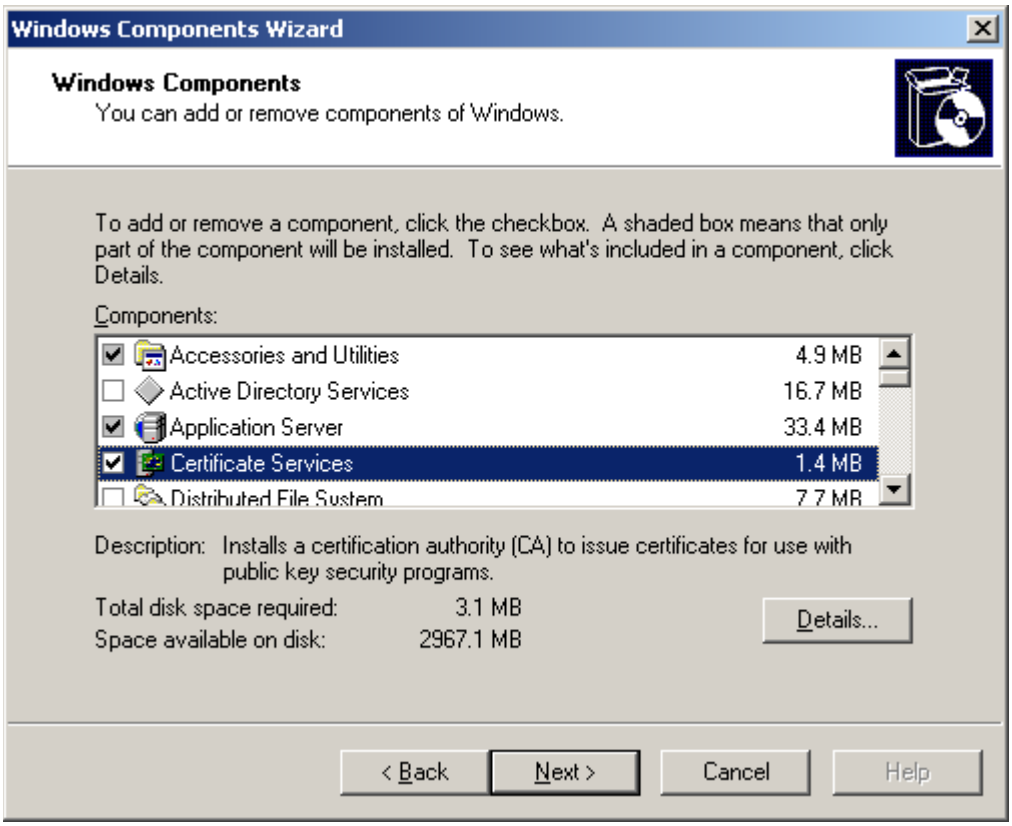
To enable SSL support for ESSO-PR, you must create and install an X.509 SSL certificate for the IIS Web site serving the ESSO-PR Web interface. The certificate is issued by a Certificate Authority (CA), which can be a commercial entity or a software application on the target local machine. This guide describes how to create a certificate through the latter option using Microsoft Certificate Services (MCS), a component of the Windows 2000 and 2003 families of operating systems.

The steps are:

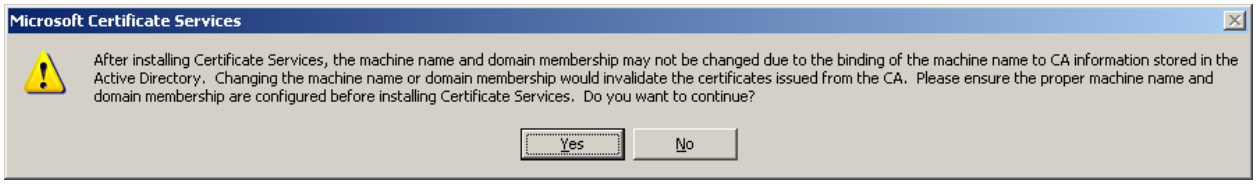
1. Installing Microsoft Certificate Services
2. Generating a certificate request for the ESSO-PR Web interface IIS site
3. Submitting the request to the CA for processing
4. Issuing the certificate
5. Installing the certificate for the ESSO-PR Web interface IIS site

## Step 1: Installing Microsoft Certificate Services

1. Open the "Add/Remove Programs" applet:
   a. Click **Start → Settings → Control Panel**.
   b. In the Control Panel, double-click the **Add/Remove Programs** icon.
2. In the "Add/Remove Programs" applet, click **Add/Remove Windows Components**.
3. In the **Components** list, select **Certificate Services**.

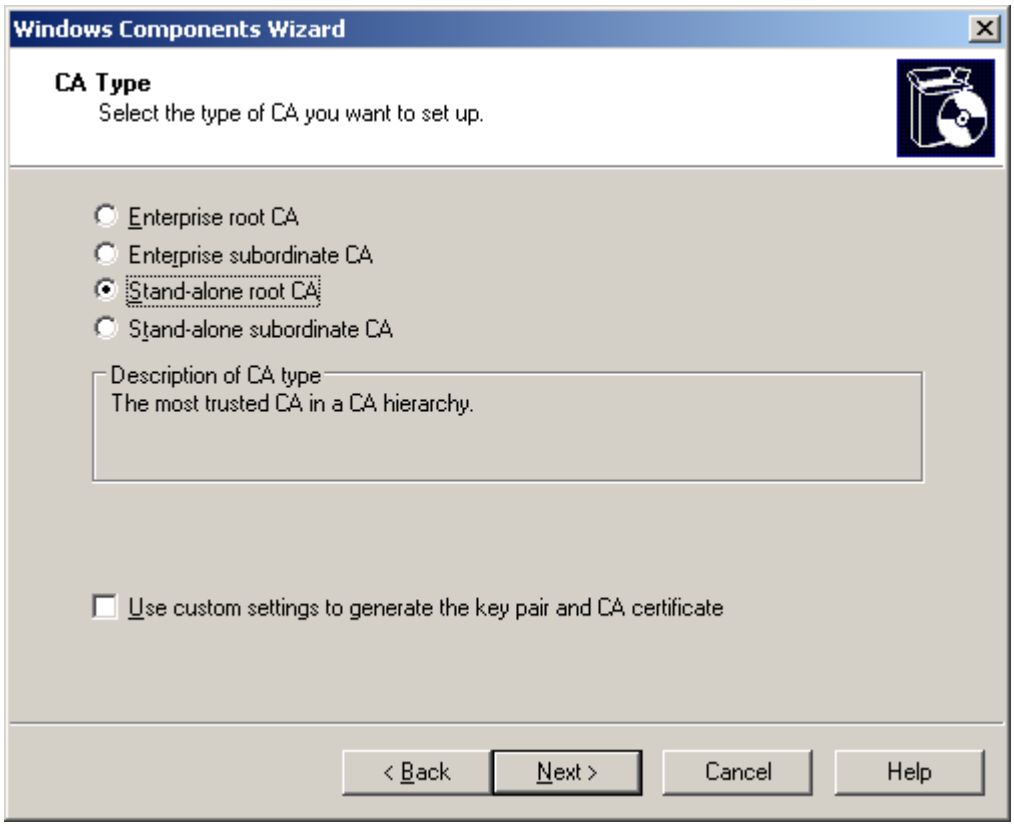



4. When the following warning appears, read it carefully, then click **Yes** to proceed.

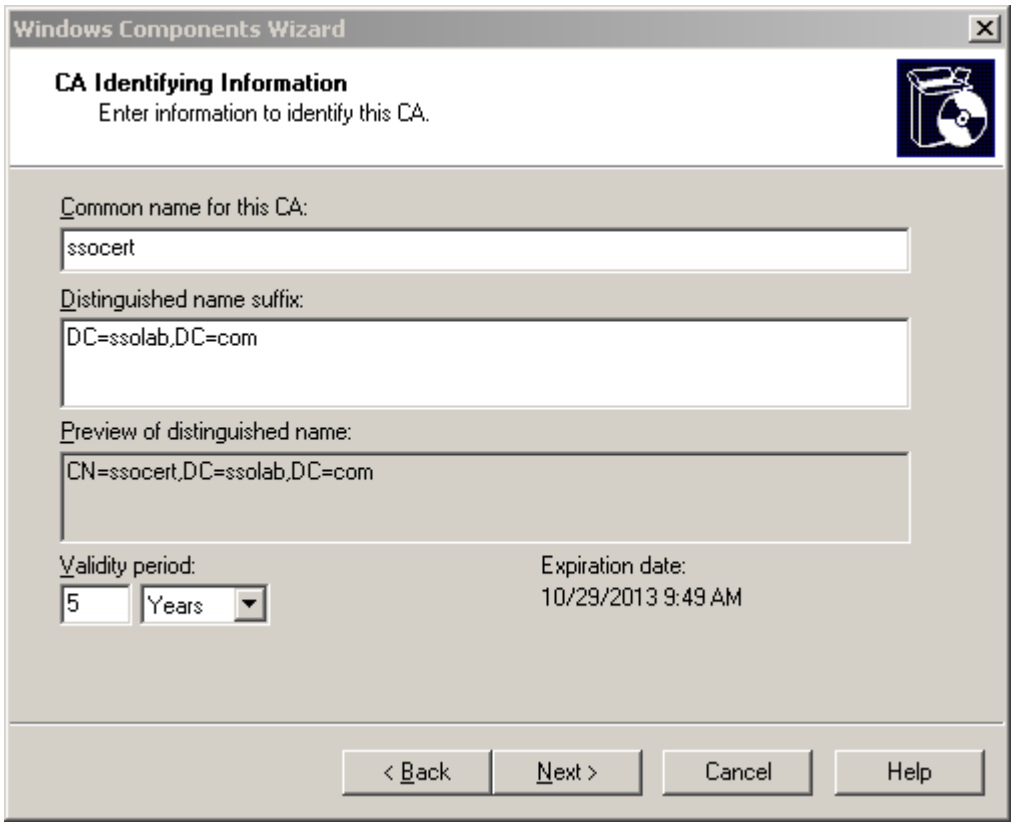



5. Click **Next**.

6. In the “CA Type” dialog, select **Stand-alone root CA** and click **Next**.

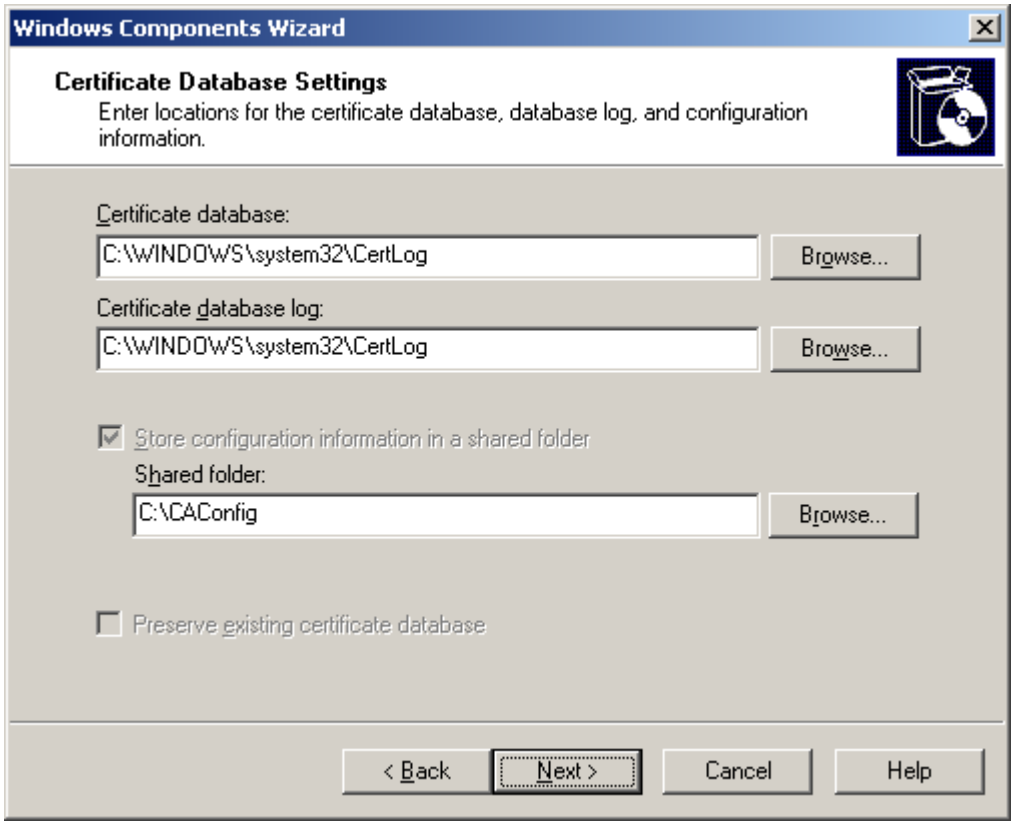


7. In the “CA Identifying Information” dialog, fill in the appropriate fields and click **Next**.

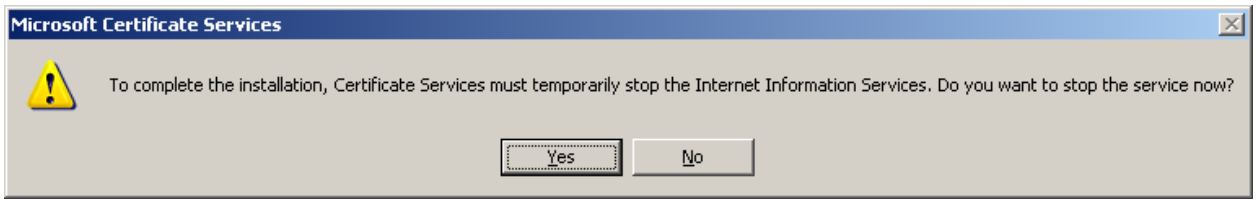



8. Wait for the cryptographic key to be generated, then proceed to the next step.

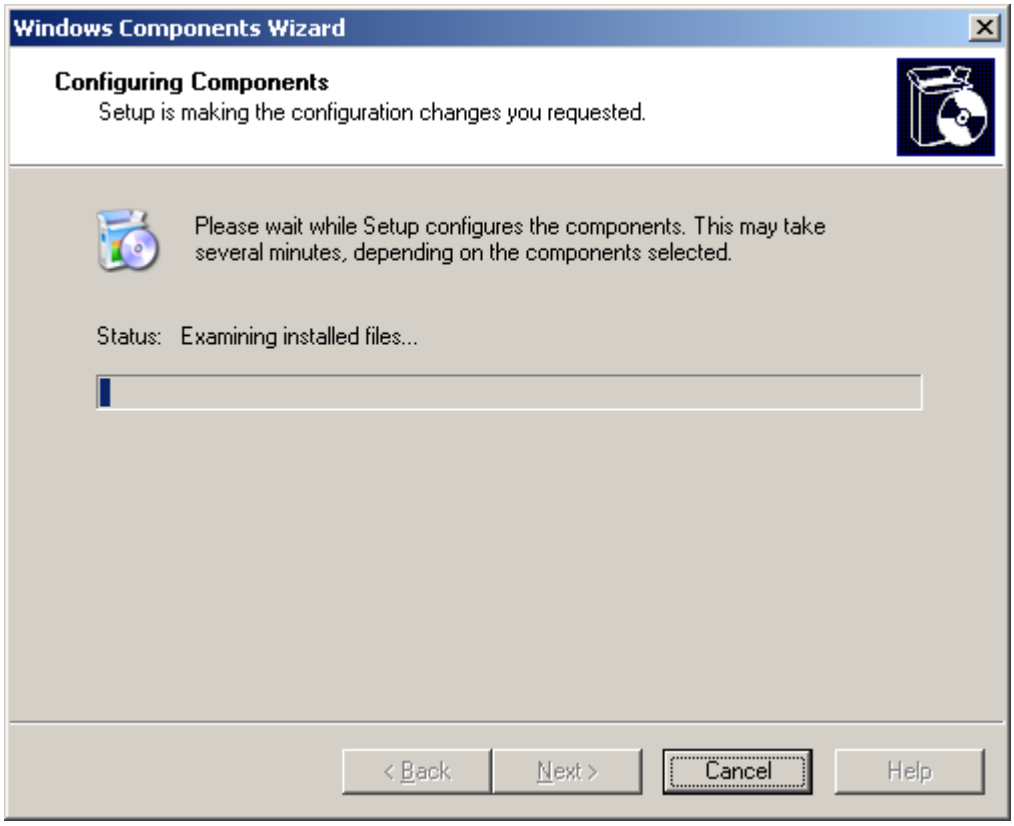
9. In the “Certificate Database Settings” dialog, enter the desired paths. If unsure, leave the fields at their default values. When you’re finished, click **Next**.



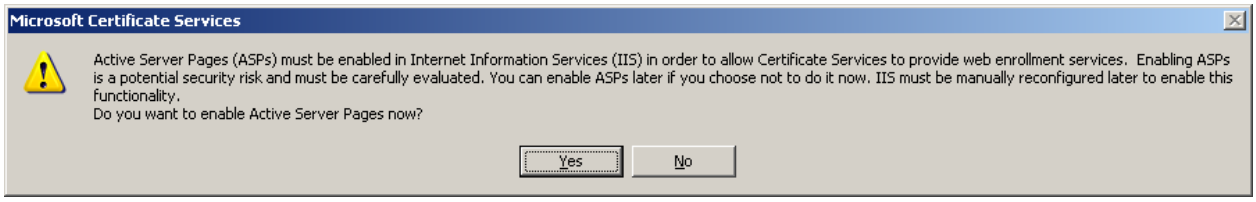

10. When prompted to temporarily stop IIS, click **Yes**.



11. Wait for the installation to complete. If you are prompted for your Windows CD-ROM, insert it, and follow the displayed instructions.




12. When prompted to enable Active Server Pages, click **Yes**.




13. When the "Windows Components Wizard" completes, click **Finish**.

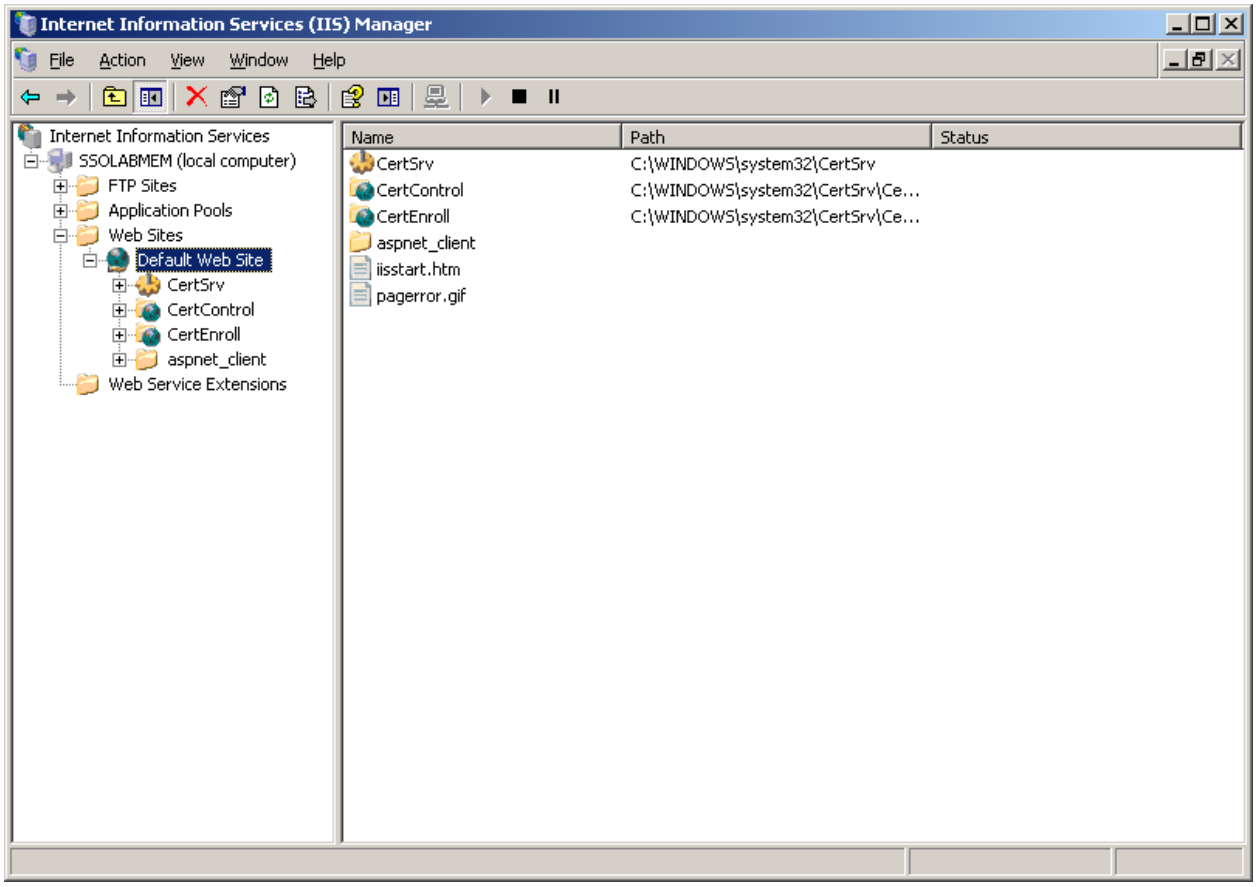
Microsoft Certificate Services is now installed.
Proceed to the next section to generate a certificate request.

## Step 2: Generating a Certificate Request for the IIS Site Serving the ESSO-PR Web Interface

Once you have access to a trusted Certificate Authority, you must generate a certificate request for the IIS site serving the ESSO-PR Web interface. You will submit this request to the CA for processing as described later in this guide.

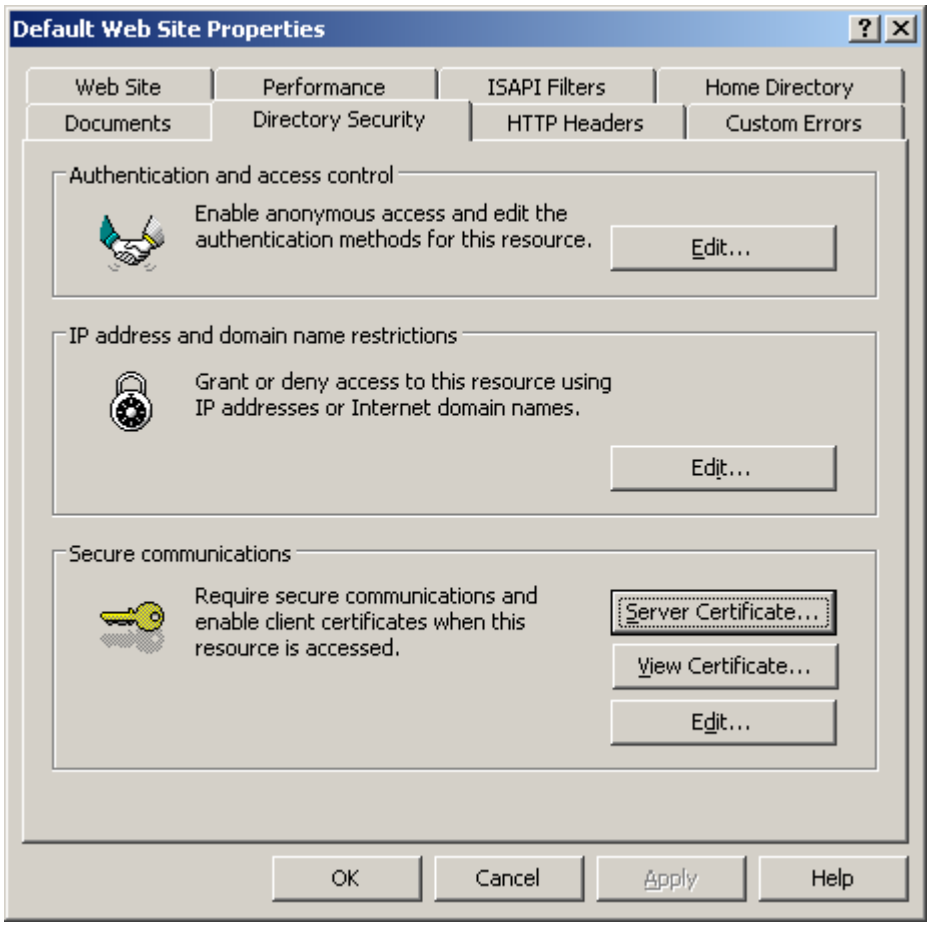
**Note:** You must perform this procedure for every ESSO-PR Web interface site served by IIS within the domain.

1. Launch the IIS Manager. Click **Start** → **Programs** → **Administrative Tools** → **Internet Information Services (IIS) Manager**.
2. In the tree in the left-hand pane, expand **Web Sites** and right-click the IIS site serving the SSPR Web interface. Typically, this will be **Default Web Site**. Select **Properties** from the context menu.

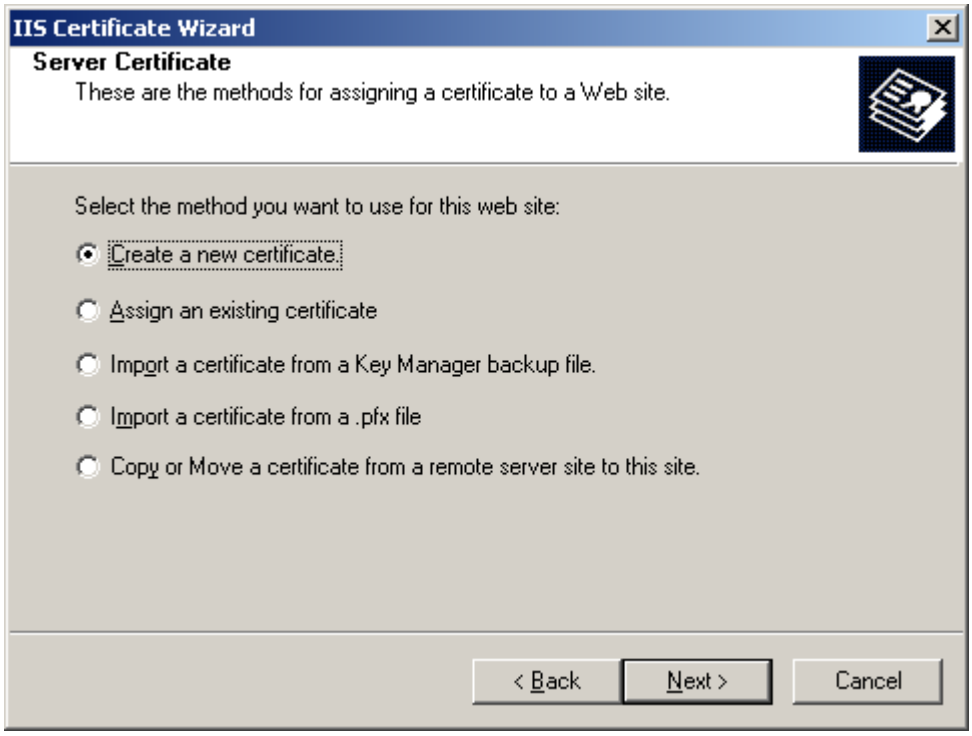



3. In the dialog that appears, select the **Directory Security** tab.

4. In the **Secure communications** section, click **Server Certificate**.

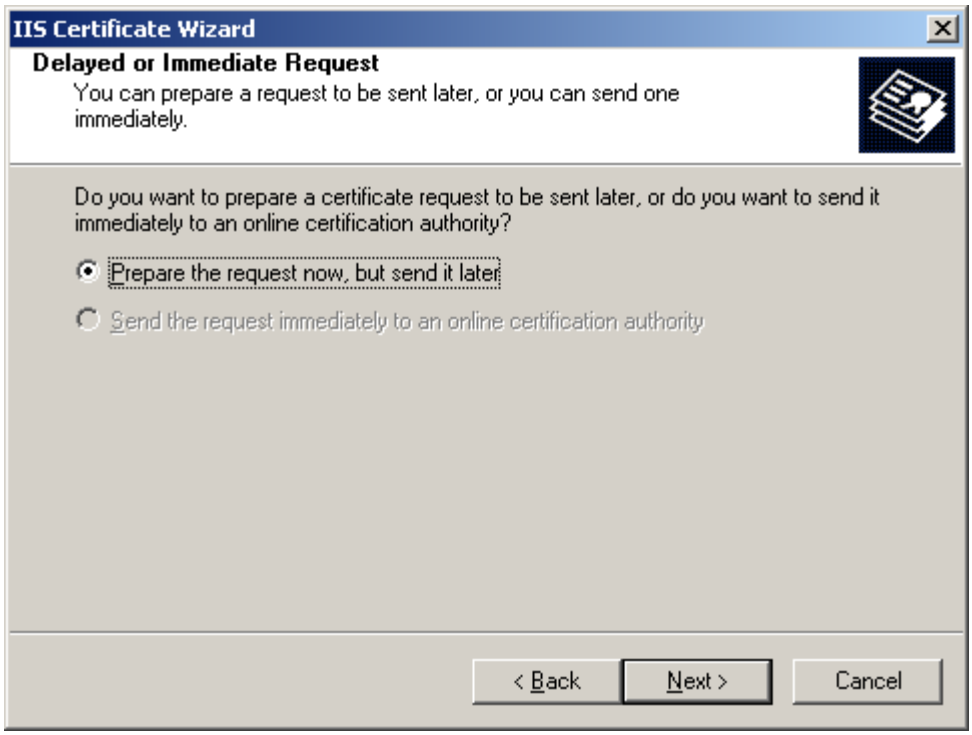


5. When the “Web Server Certificate Wizard” dialog appears, click **Next**.
6. In the “Server Certificate” dialog, select **Create a new certificate** and click **Next**.

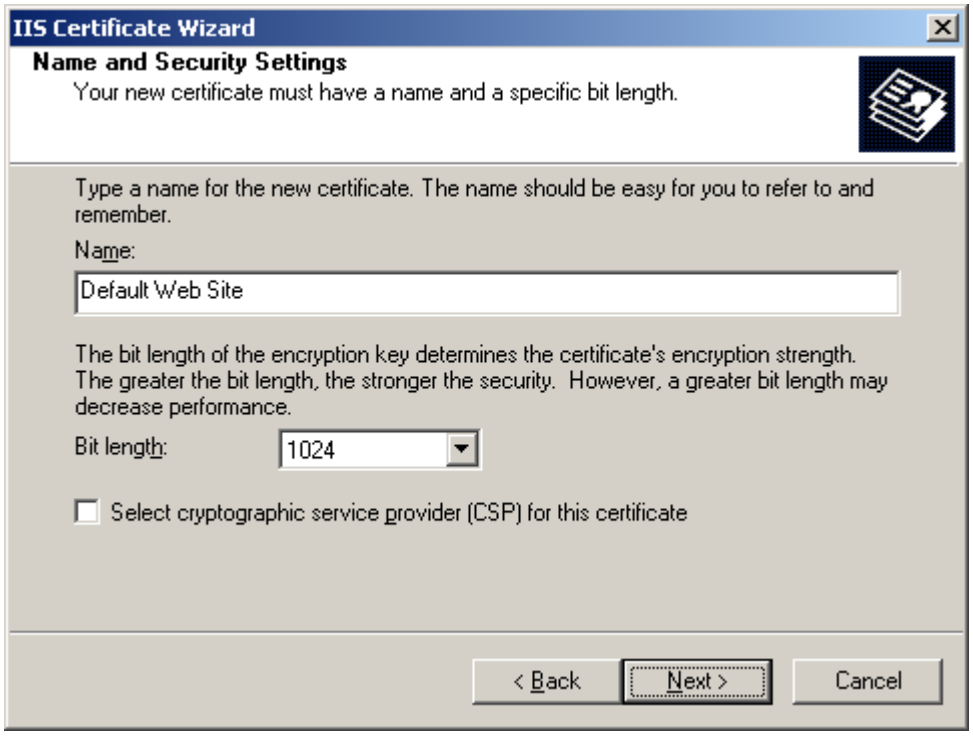


7. In the “Delayed or Immediate Request” dialog, select **Prepare the request now, but send it later** and click **Next**.

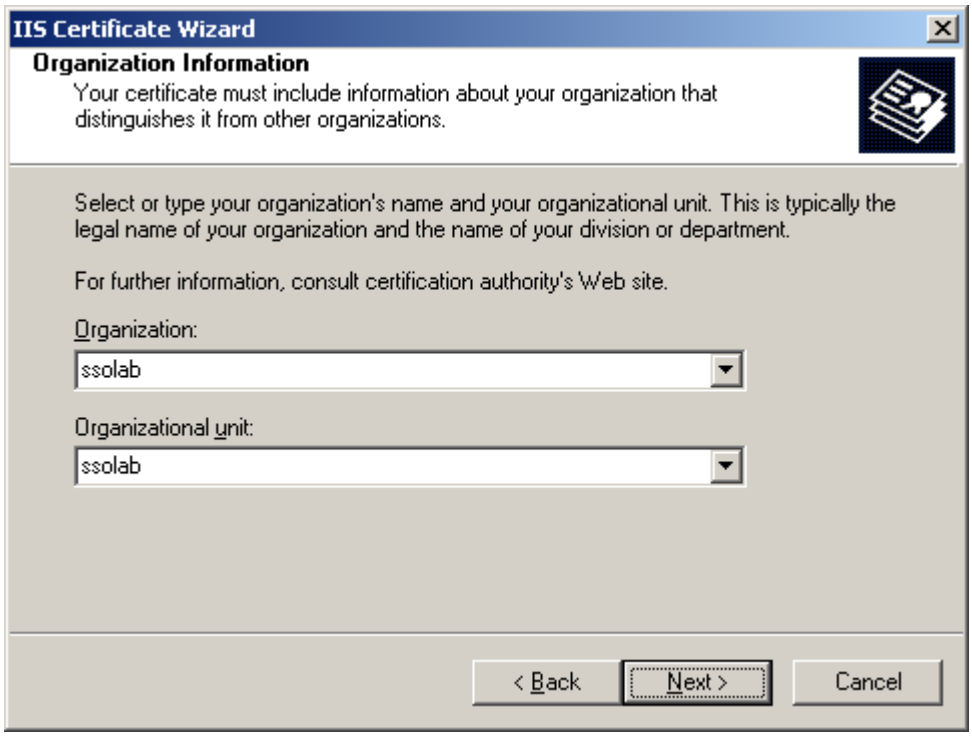
> **Note:** The **Send the request immediately to an online certification authority** option is not available unless an Enterprise-level CA exists on the domain of the target machine. In such cases you may select the option to generate and submit the certificate request immediately. If you do so, skip the steps in the next section and continue directly to Step 4: Issuing the Certificate once you complete this procedure.



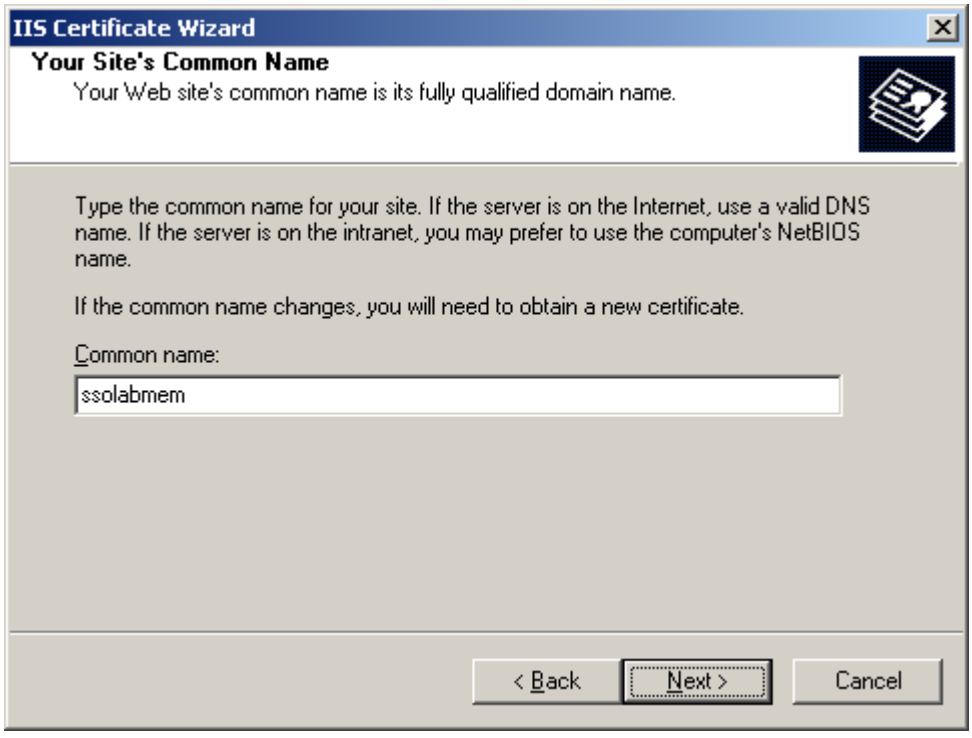
8. In the “Name and Security Settings” dialog, name your certificate and set its bit length. Keep the following in mind:
   - Choose a descriptive name that is easy to refer to and to remember.
   - For a root CA, we recommend a bit length of at least 2048 bits.
   - The longer the bit length, the stronger the encryption; however, stronger encryption requires more server resources. In the end, the bit length you choose will depend on the needs of your organization.
   - If you are using existing keys, the certificate’s bit length cannot be changed.



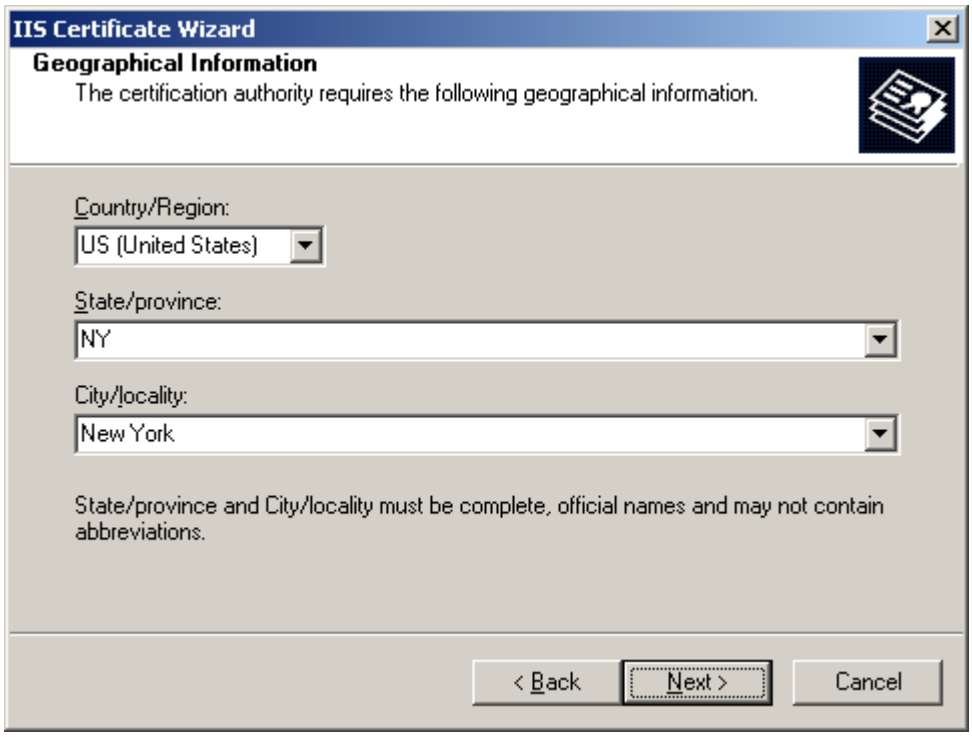
9. In the “Organization Information” dialog, select or enter the desired values, then click **Next**.



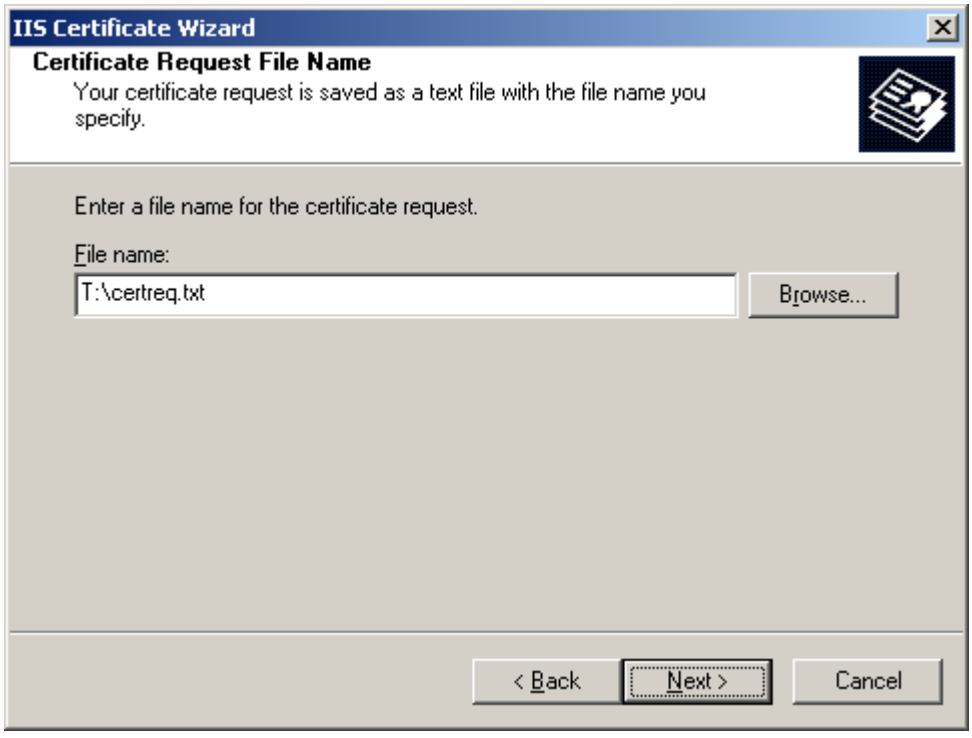

10. Enter the *exact* name of the target machine, or the *exact* URL of the IIS site serving the ESSO-PR Web interface, whichever applies to your configuration. Click **Next**.



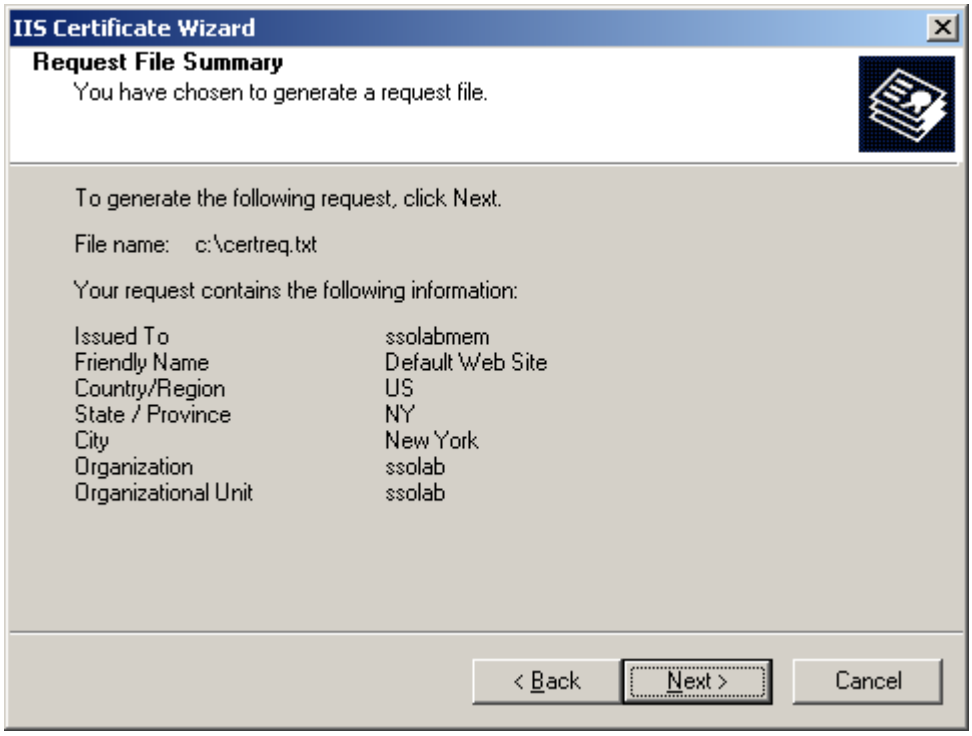
11. In the “Geographical Information” dialog, fill in the fields as appropriate, then click **Next**.




12. In the “Certificate Request File Name” dialog, enter the name of the file to which your request will be saved, then click **Next**.



13. In the summary dialog, review your choices and click **Back** if you need to make changes. If all the information is correct, click **Next**.



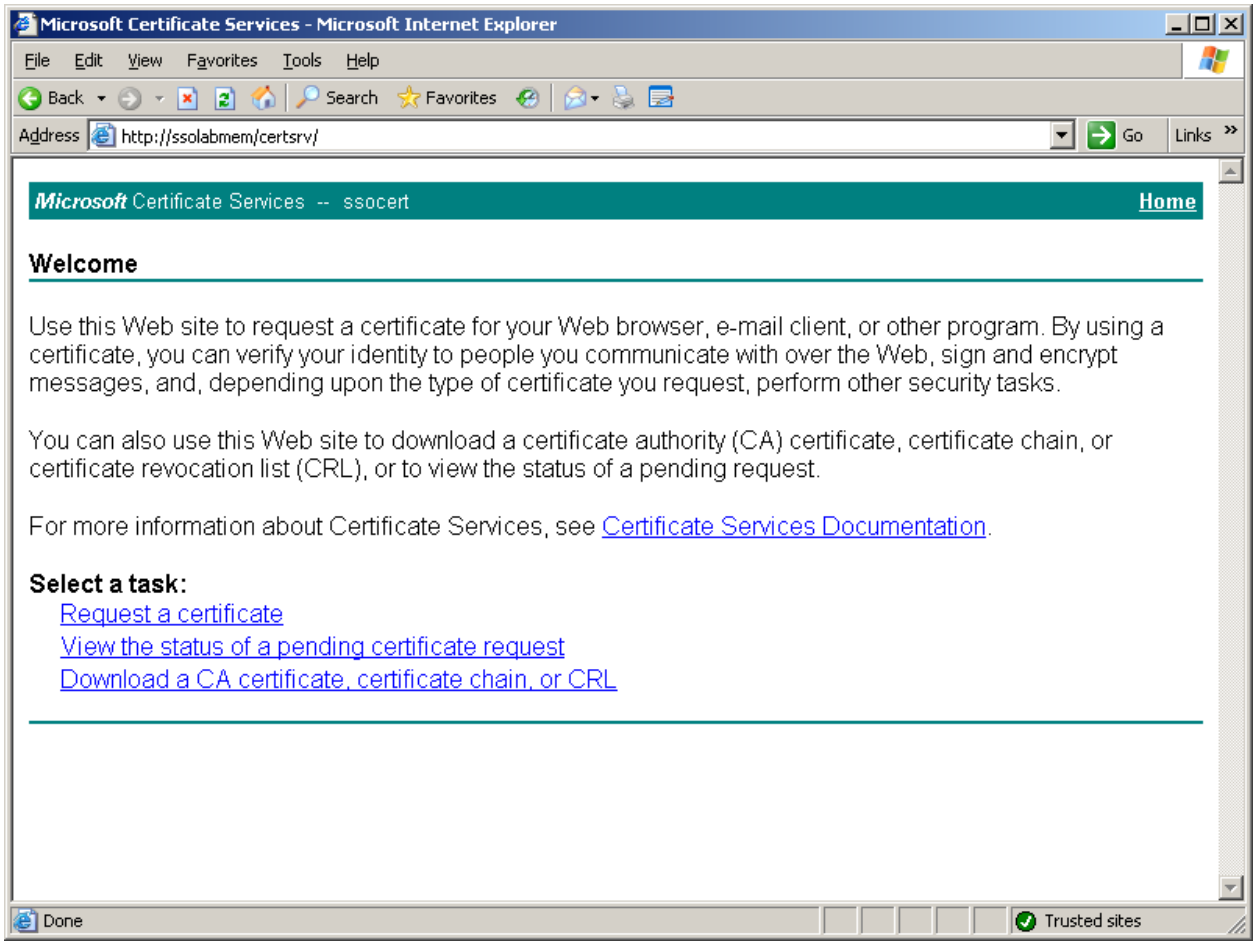

14. When the wizard completes, click **Finish**.

Your certificate request has been saved to a file and, if applicable, submitted to your enterprise CA. Your next step is one of the following:

- If you chose to submit the request manually, proceed to Step 3: Submitting the Certificate Request to the Certificate Authority.
- If you chose to submit the request automatically, proceed to Step 4: Issuing the Certificate.

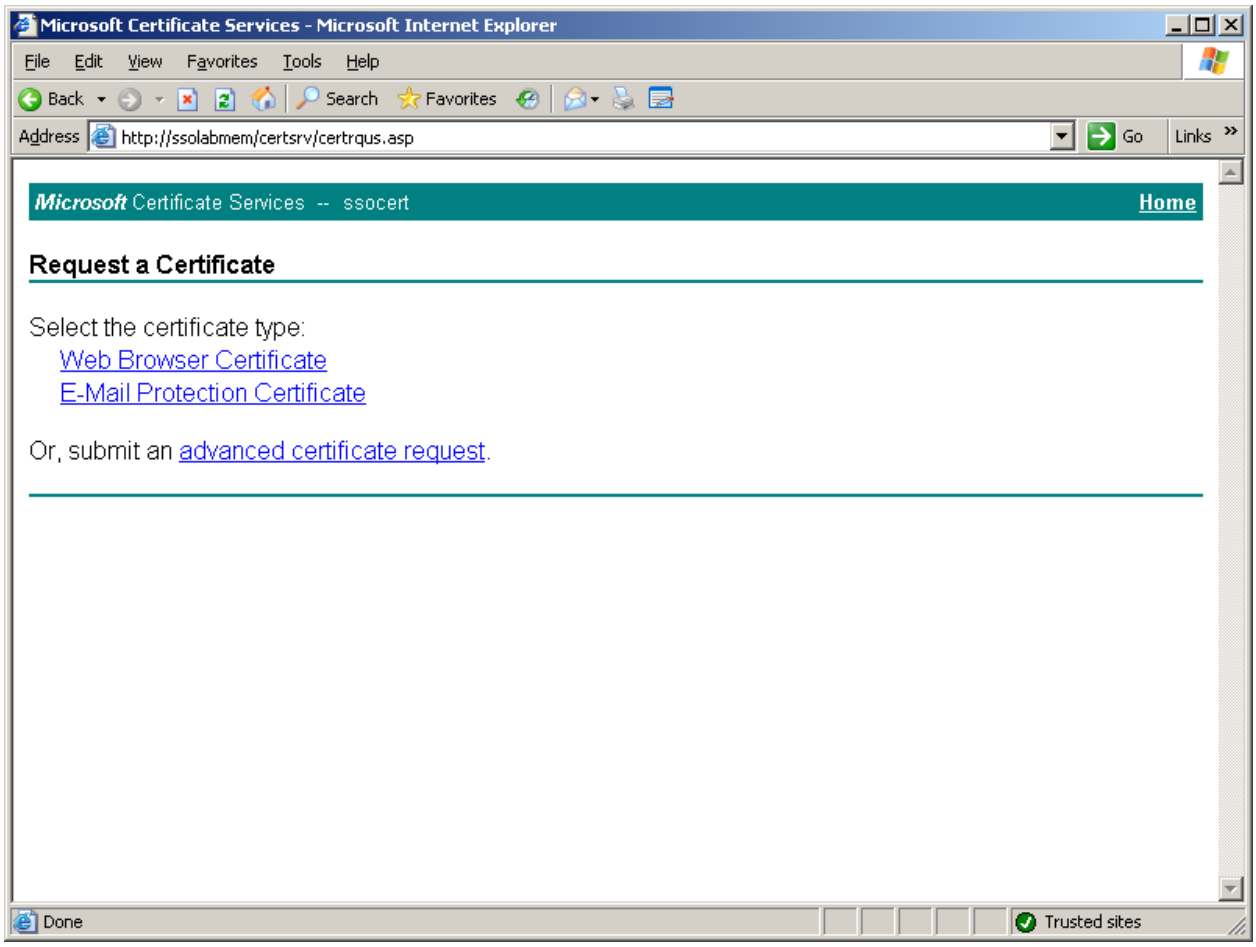
## Step 3: Submitting the Certificate Request to the Certificate Authority

1. Go to http://<machine_name>/certsrv/ to access the Microsoft Certificate Services Web interface.

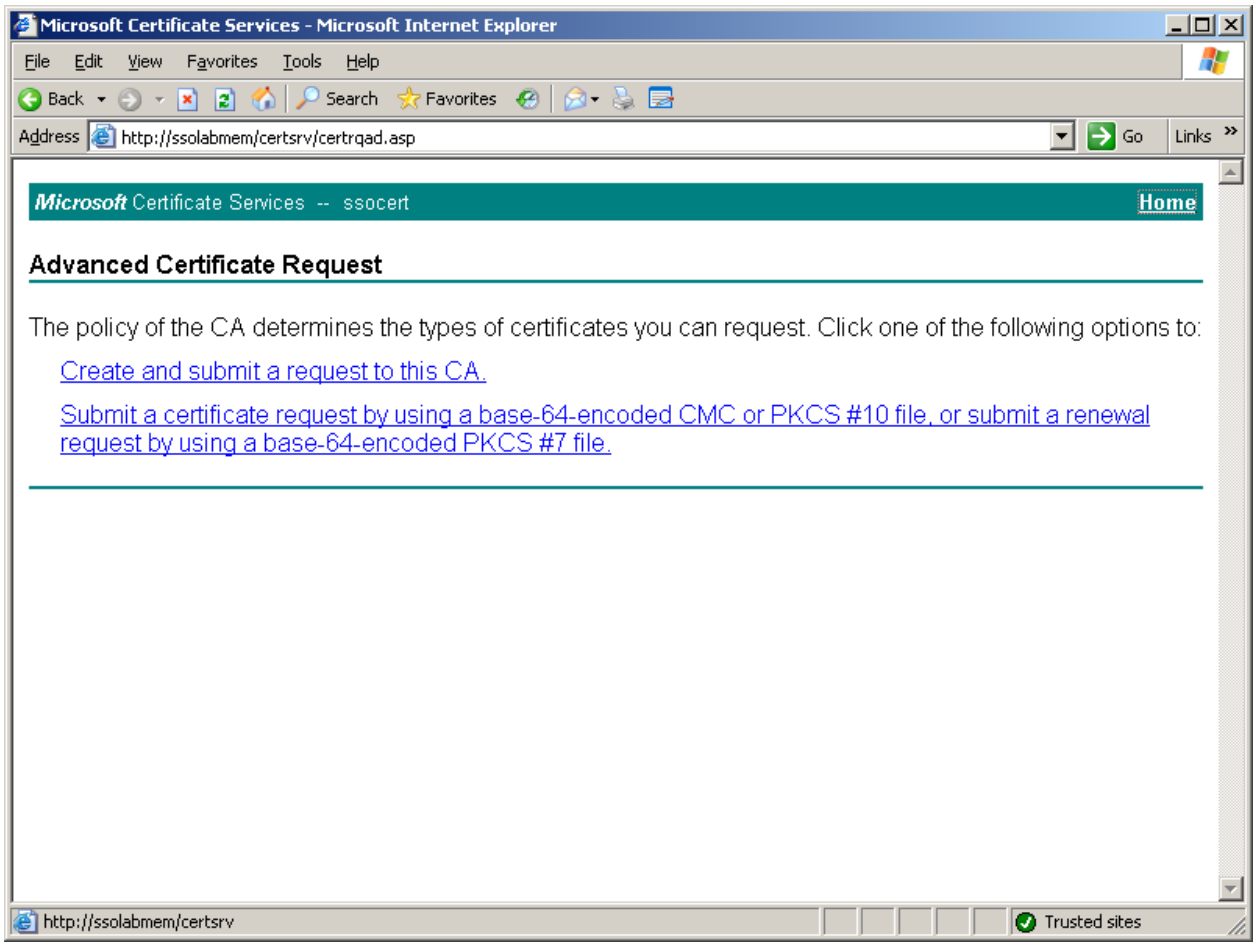



2. Click **Request a certificate**.

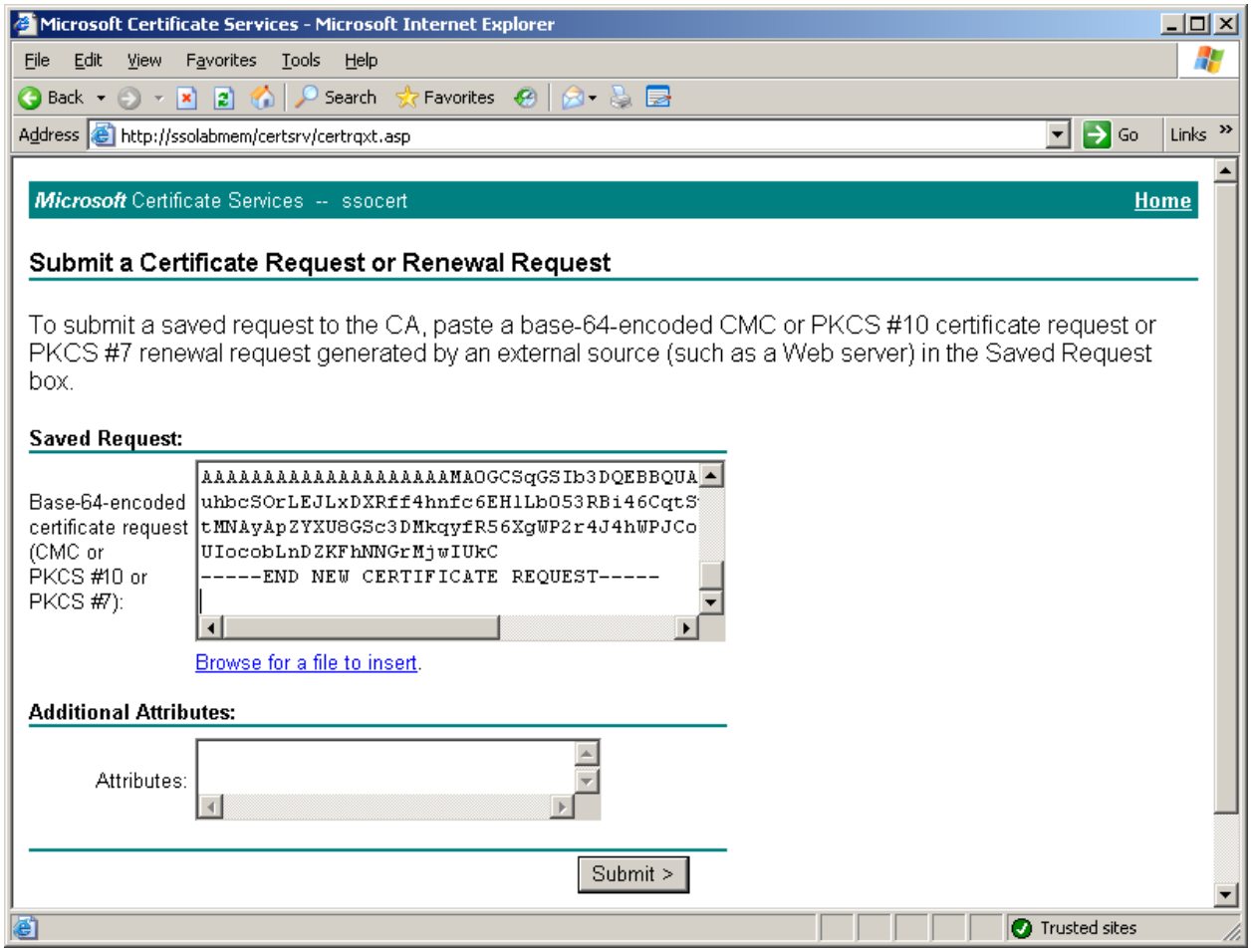
3. On the next page, click **advanced certificate request**.



4. On the next page, click **Submit a certificate request by using a […] file**.



5. Submit the certificate as follows:
   a. Locate the certificate request file you generated earlier in this guide and open it in a text editor.
   b. Copy the entire contents of the file and paste them into the **Saved Request** field on the page that appears.
   c. Click **Submit**.

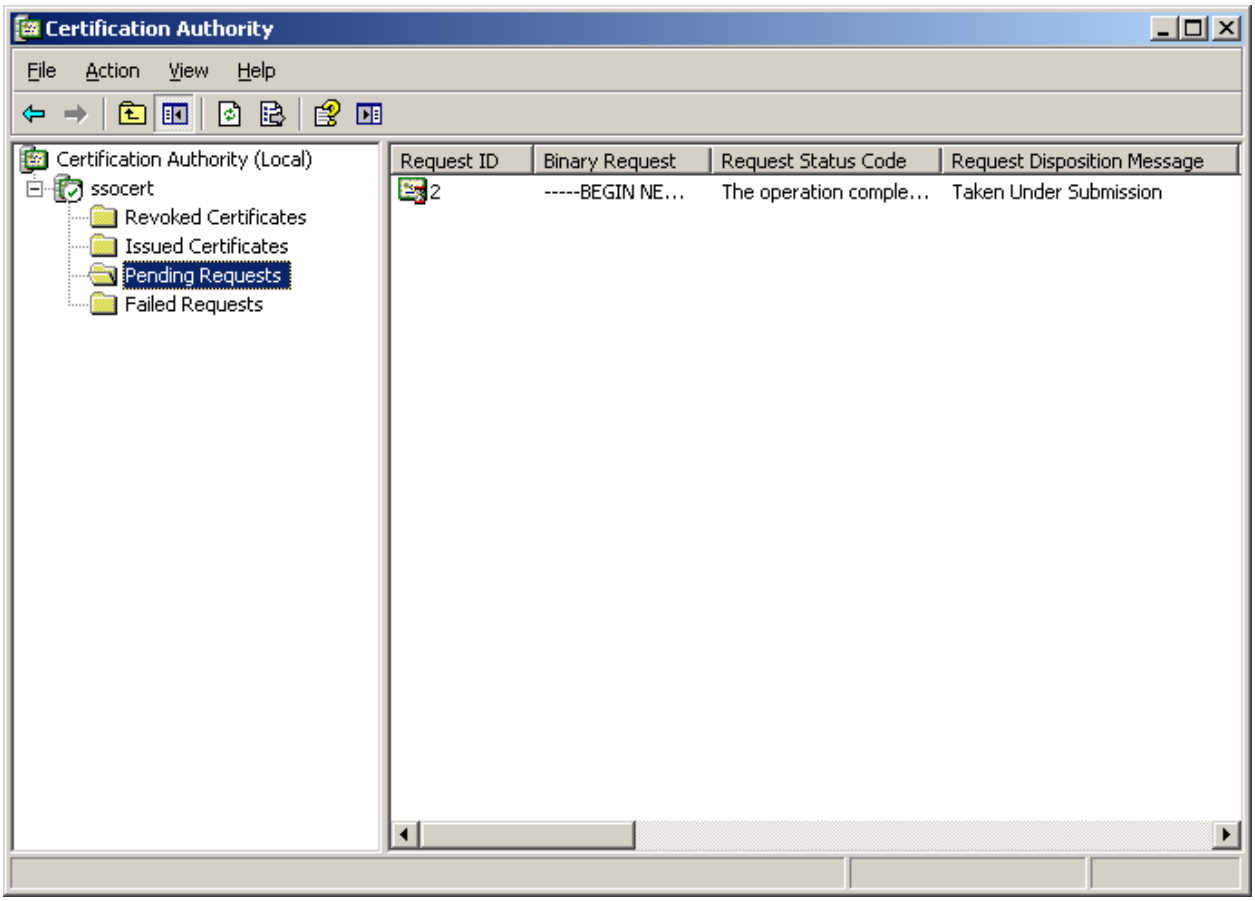



Your certificate request is now pending approval. Proceed to the next section to approve it and issue the certificate.

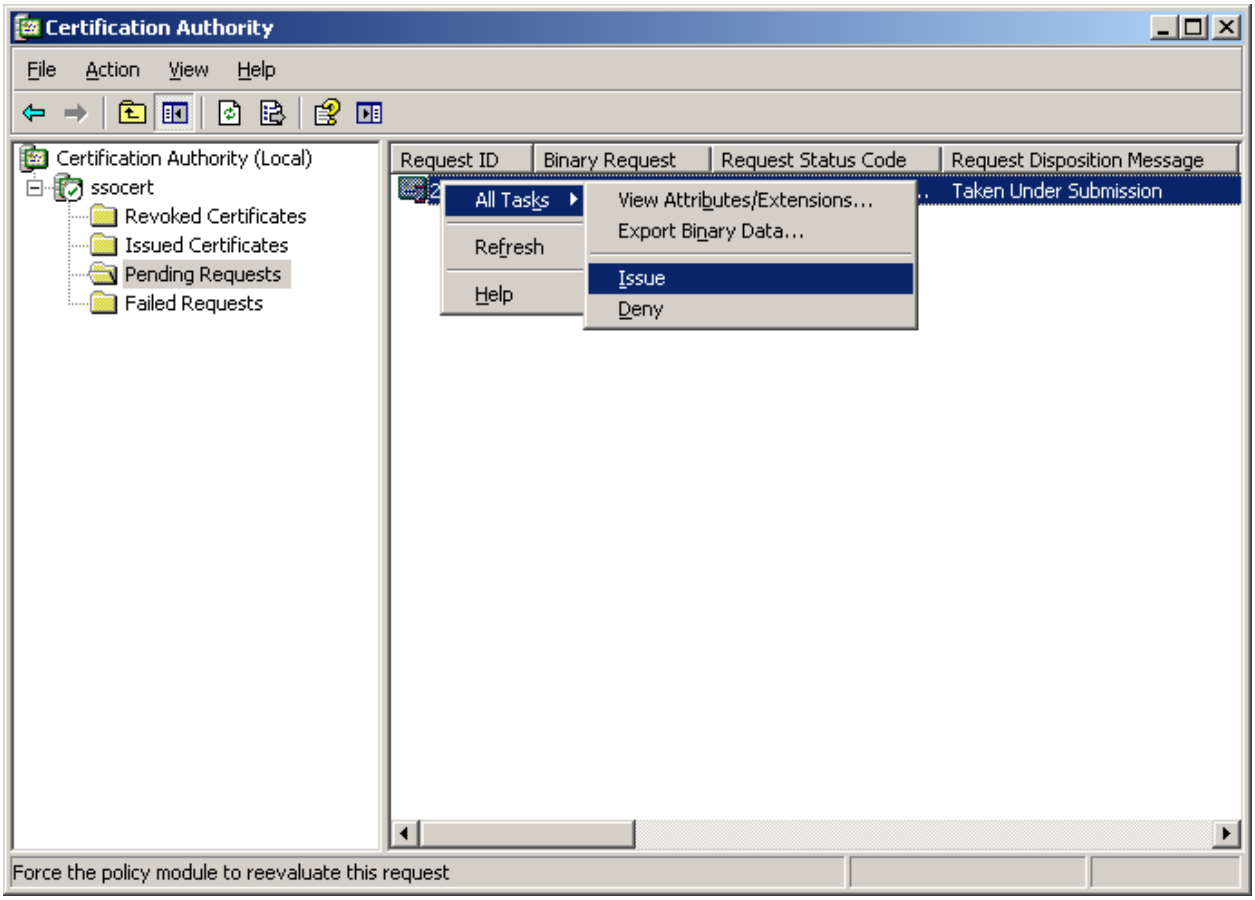
## Step 4: Issuing the Certificate

Issue the certificate as follows:

1. Launch the Certification Authority tool. Click **Start → Programs → Administrative Tools → Certification Authority**.
2. In the left-hand pane, expand the root tree node and click **Pending Requests**. The request you submitted earlier is listed in the list of pending requests.



3. Right-click the pending request and select **All Tasks → Issue** from the context menu.
   The certificate is issued and the request disappears from the list.

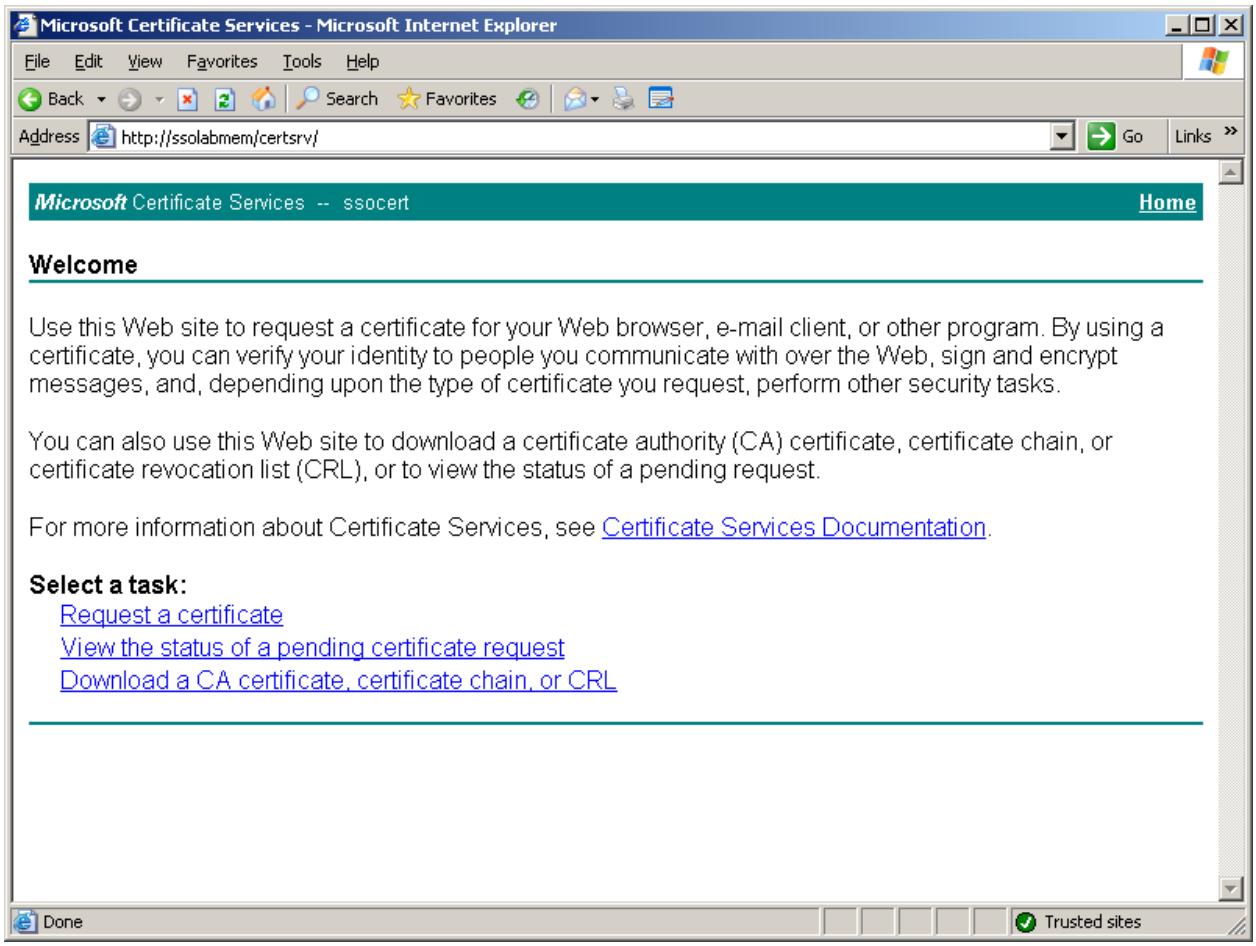



4. Verify that the certificate has been successfully issued. Click **Issued Certificates** in the left-hand pane and verify that your certificate appears in the list.

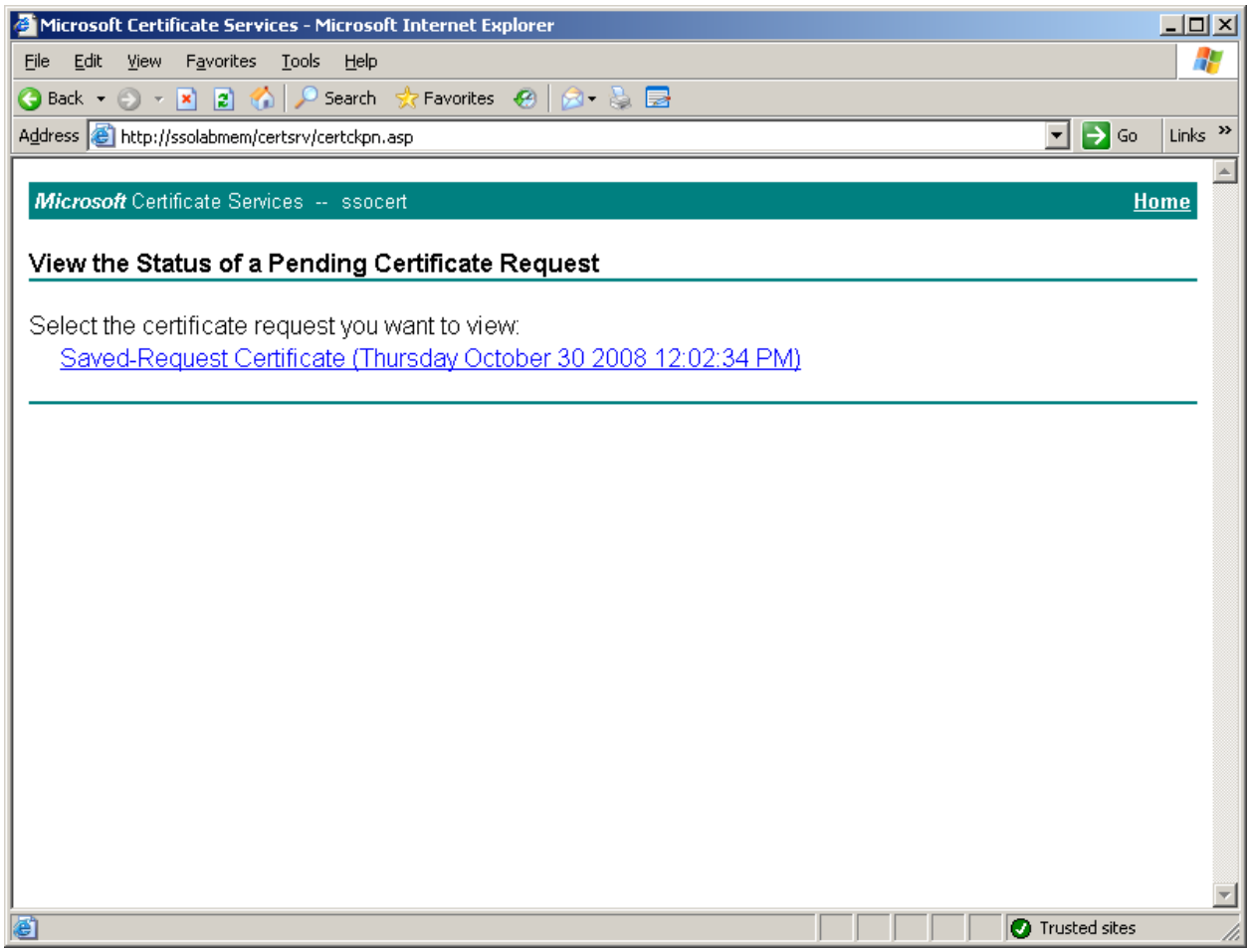
## Step 5: Installing the Certificate

Once the certificate has been issued, it must be installed for the ESSO-PR Web interface IIS site. This procedure assumes that the ESSO-PR Web interface is served by the default web site in IIS.

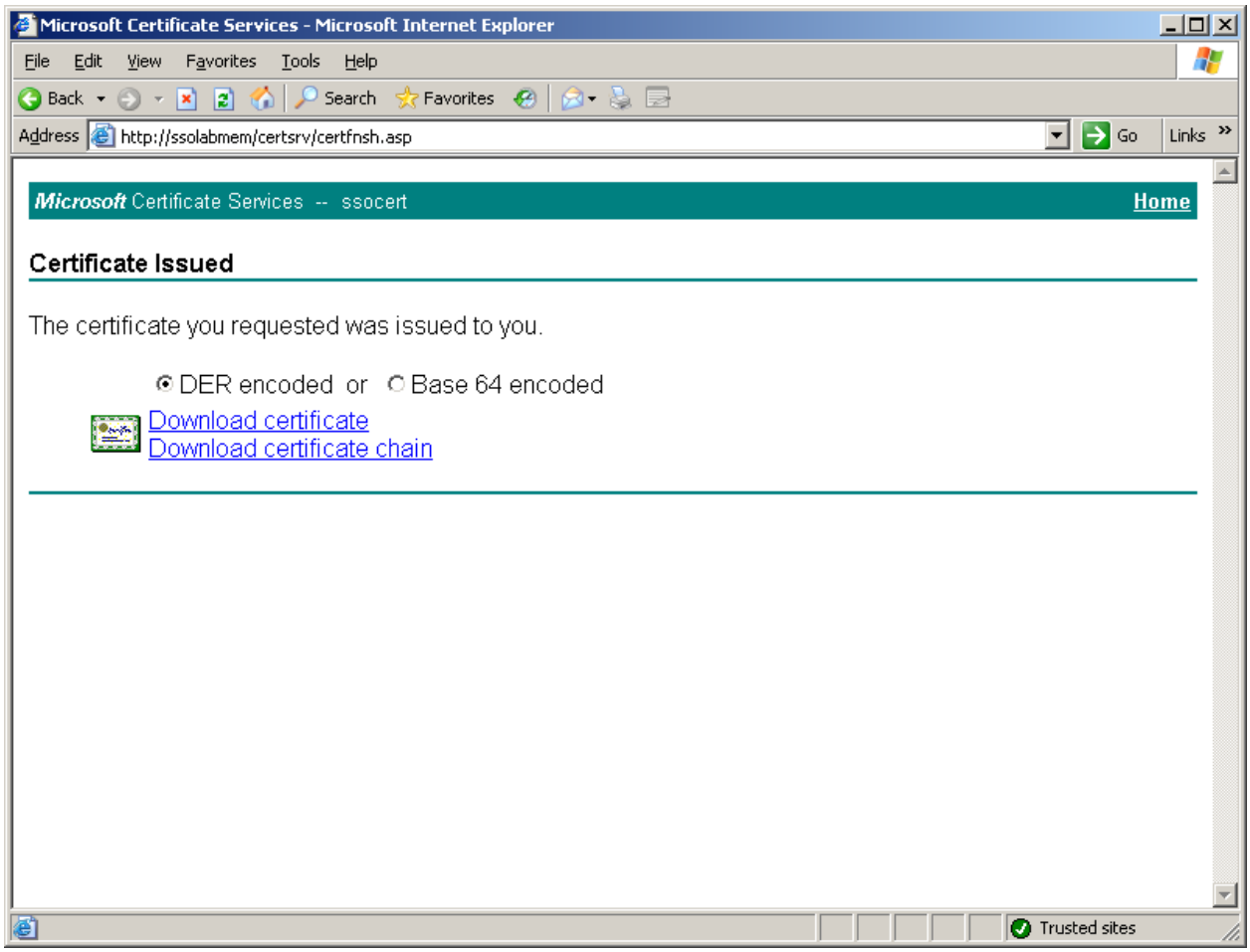
1. Return to the Microsoft Certificate Services Web interface and click **Home** in the upper right corner.
2. On the MCS home page, click **View the status of a pending certificate request**.



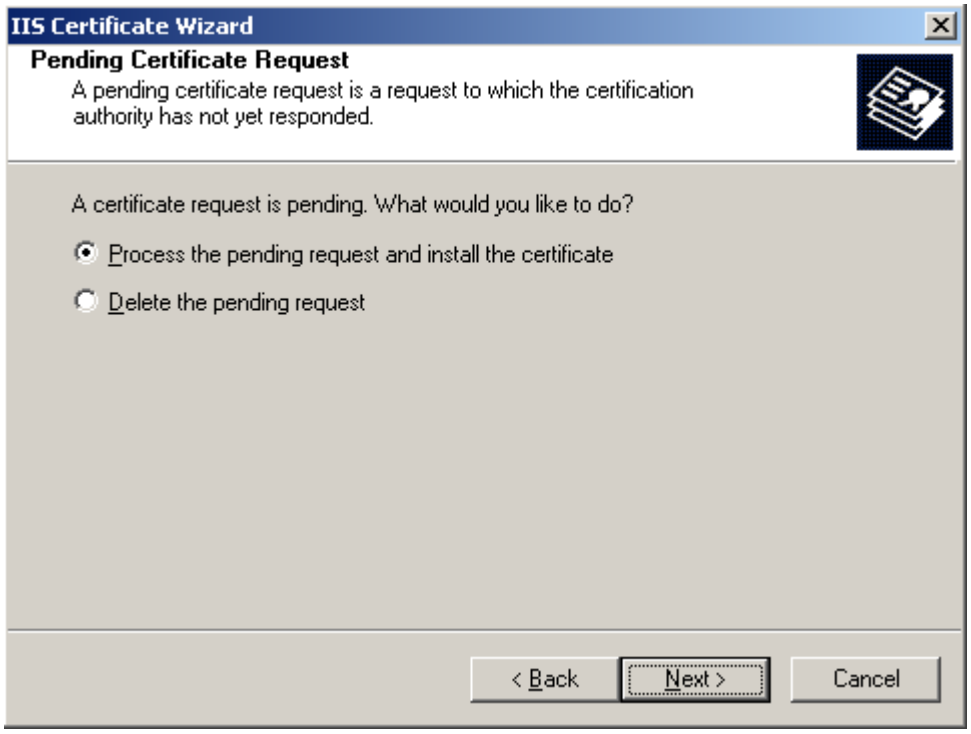
3. On the next page, click the certificate request you created earlier in this section.



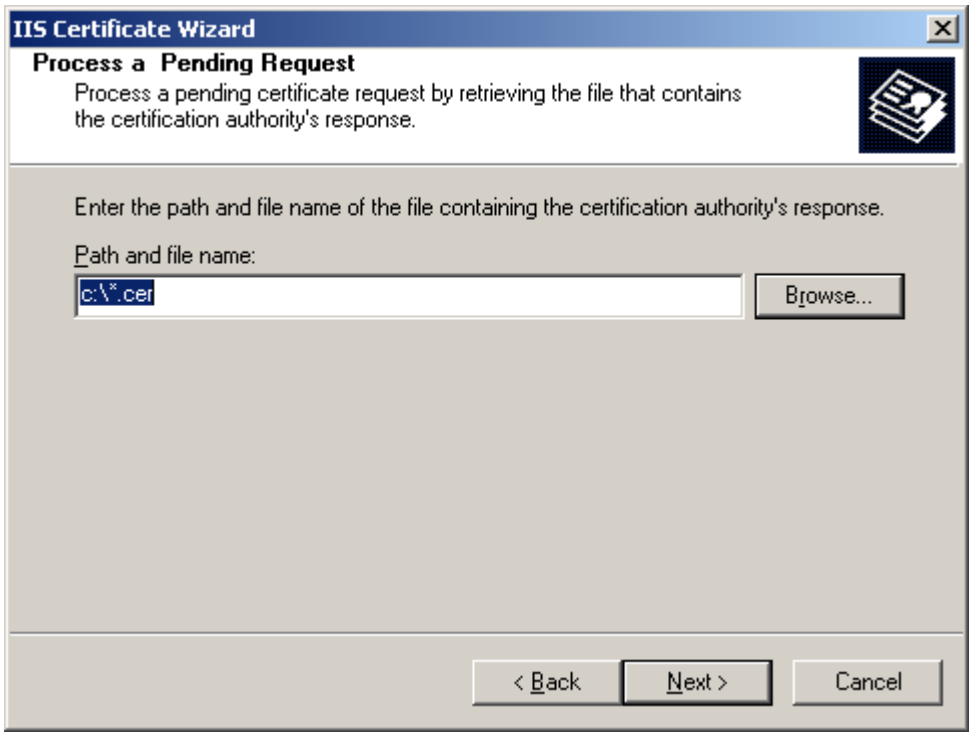
4. On the next page, click **Download certificate**.



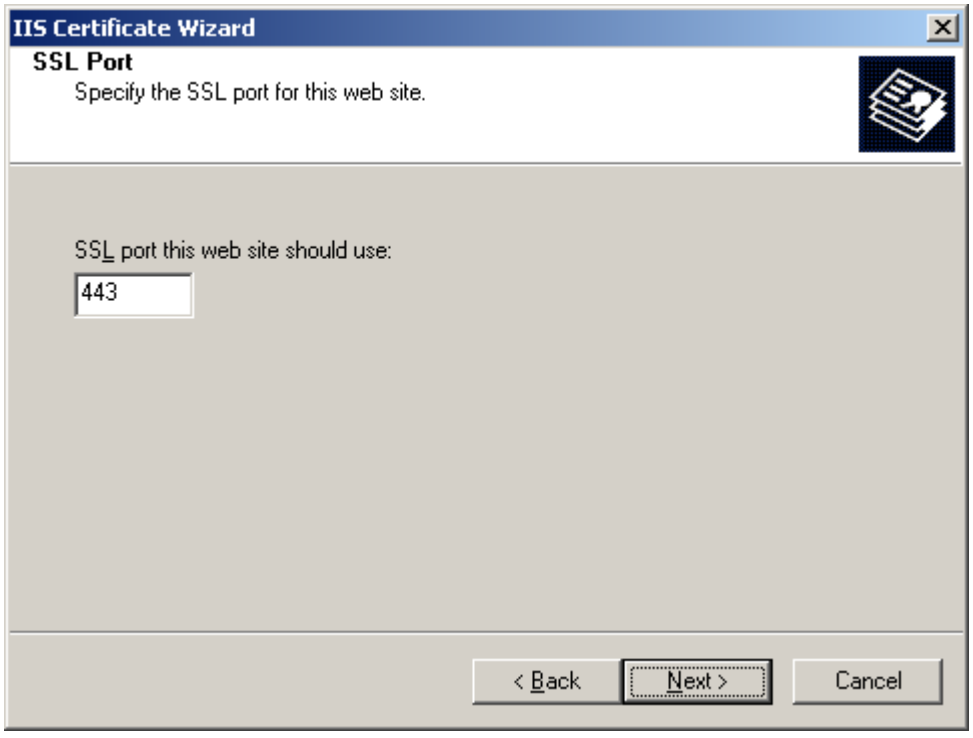
5. When prompted whether to open or save the certificate file, click **Save**.
6. In the dialog that appears, navigate to the target location for the file and click **Save**.
7. Install the certificate:
   a. If it is not already running, launch the IIS Manager.
   b. In the left-hand pane, expand the root node, then expand **Web Sites**.
   c. Right-click **Default Web Site** and select **Properties** from the context menu.
   d. In the dialog that appears, select the **Directory Security** tab.
   e. In the "Secure communications" field, click **Server Certificate**.
   f. In the wizard that appears, click **Next**.
   g. In the "Pending Certificate Request" dialog, select **Process the pending request and install the certificate**, then click **Next**.



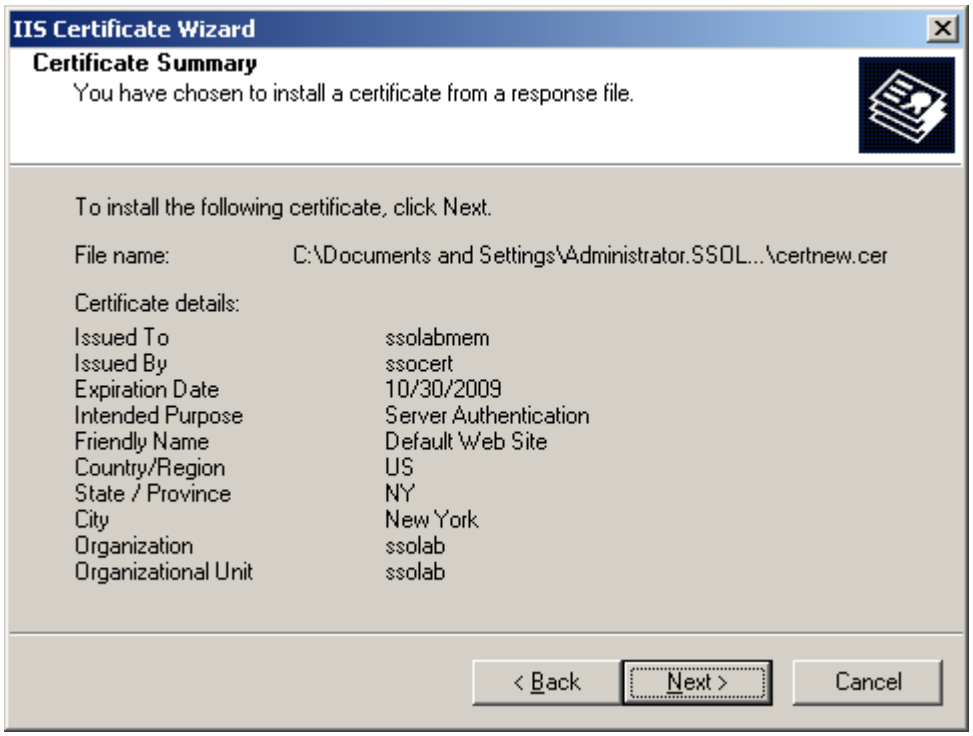
h. Enter the absolute path or navigate to the certificate file, then click **Next**.




i. Specify the SSL port for the ESSO-PR Web interface site and click **Next**.
The default value is 443.



j. Review the information displayed in the summary dialog.
If the information is correct, click **Next**.




k. In the dialog that appears, take note of the **Issued To** value (`ssolabmem` in our example). You will use this value to modify the ESSO-PR Server configuration files later in this document.

l. Click **Finish** to exit the wizard.

The certificate is now installed. Proceed to the next section to configure the ESSO-PR Web interface to accept SSL-only connections.

# Part 2: Configuring the ESSO-PR Web Interface for SSL Connections

This part describes the steps necessary to configure ESSO-PR to accept SSL-encrypted connections to its Web interface.

**Note:** If you have not already done so, install an SSL certificate by completing the steps earlier in this document.

## Overview

The steps required to enforce SSL-only connections to the ESSO-PR Web Interface are as follows:

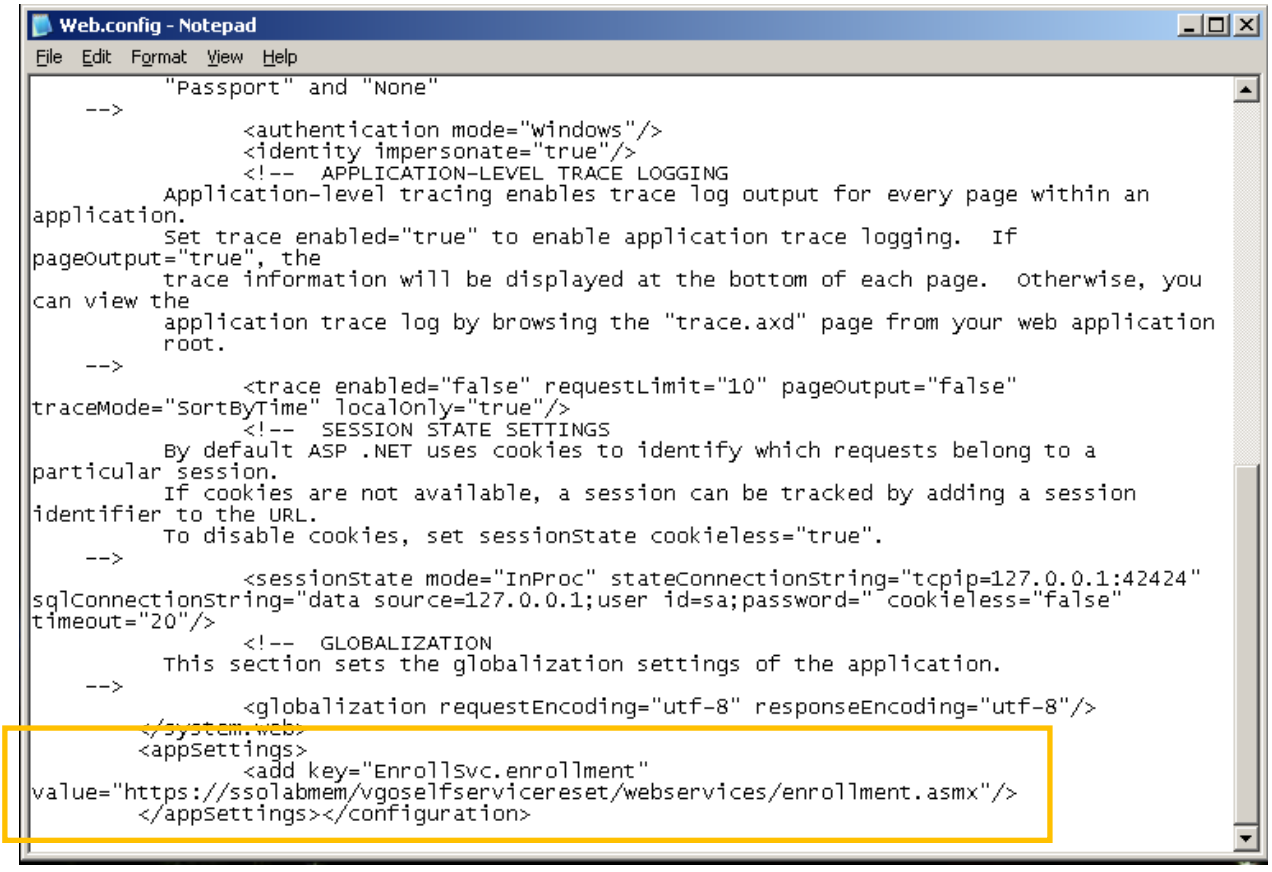
1. Modifying the ESSO-PR Server Configuration Files
2. Granting ESSO-PR Server Access to the WebServices Directory
3. Restricting Web Interface Connections to SSL Only

## Step 1: Modifying the ESSO-PR Server Configuration Files

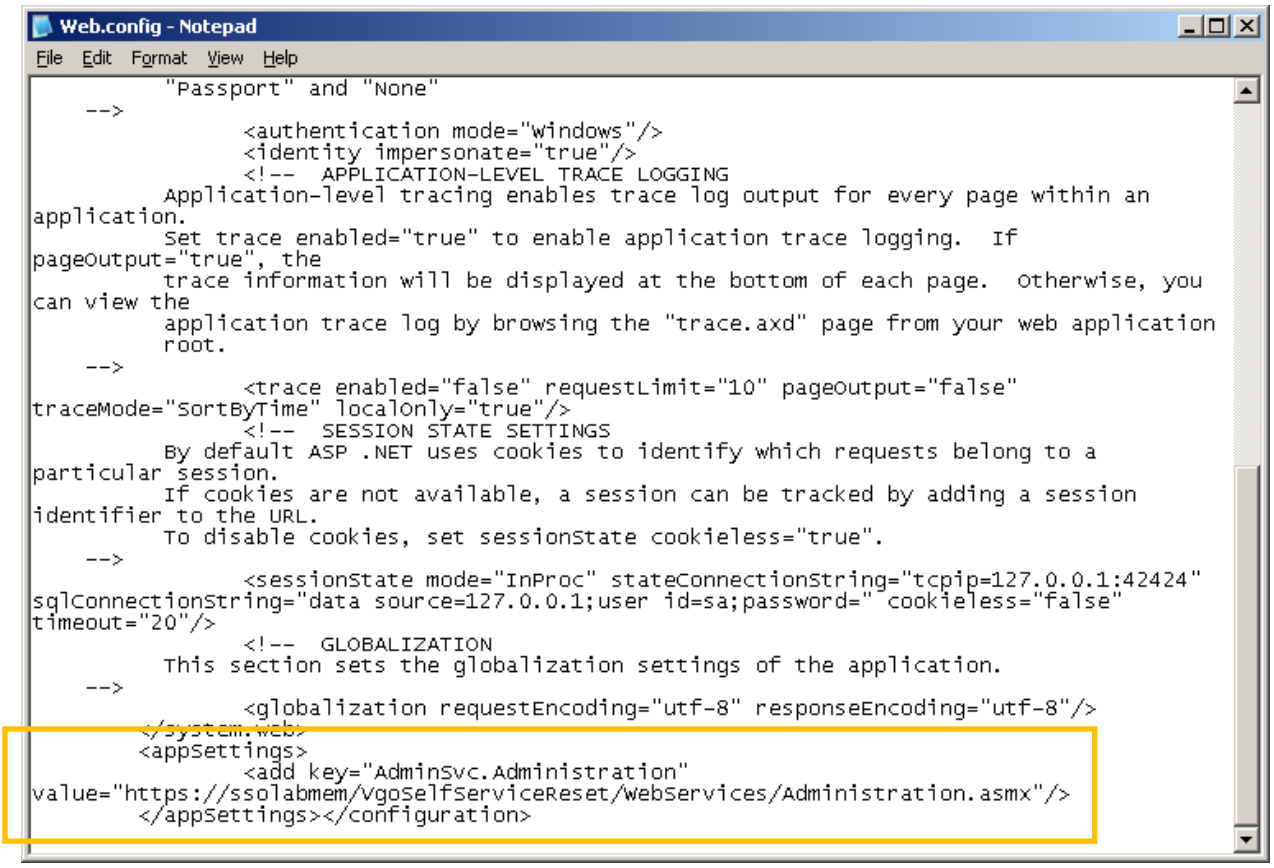
You must update the following configuration files to use the HTTP-over-SSL (HTTPS) protocol when calling the ESSO-PR Server Web interface pages:

- `C:\Program Files\Passlogix\v-GO SSPR\EnrollmentClient\web.config`
- `C:\Program Files\Passlogix\v-GO SSPR\ManagementClient\web.config`
- `C:\Program Files\Passlogix\v-GO SSPR\ResetClient\web.config`

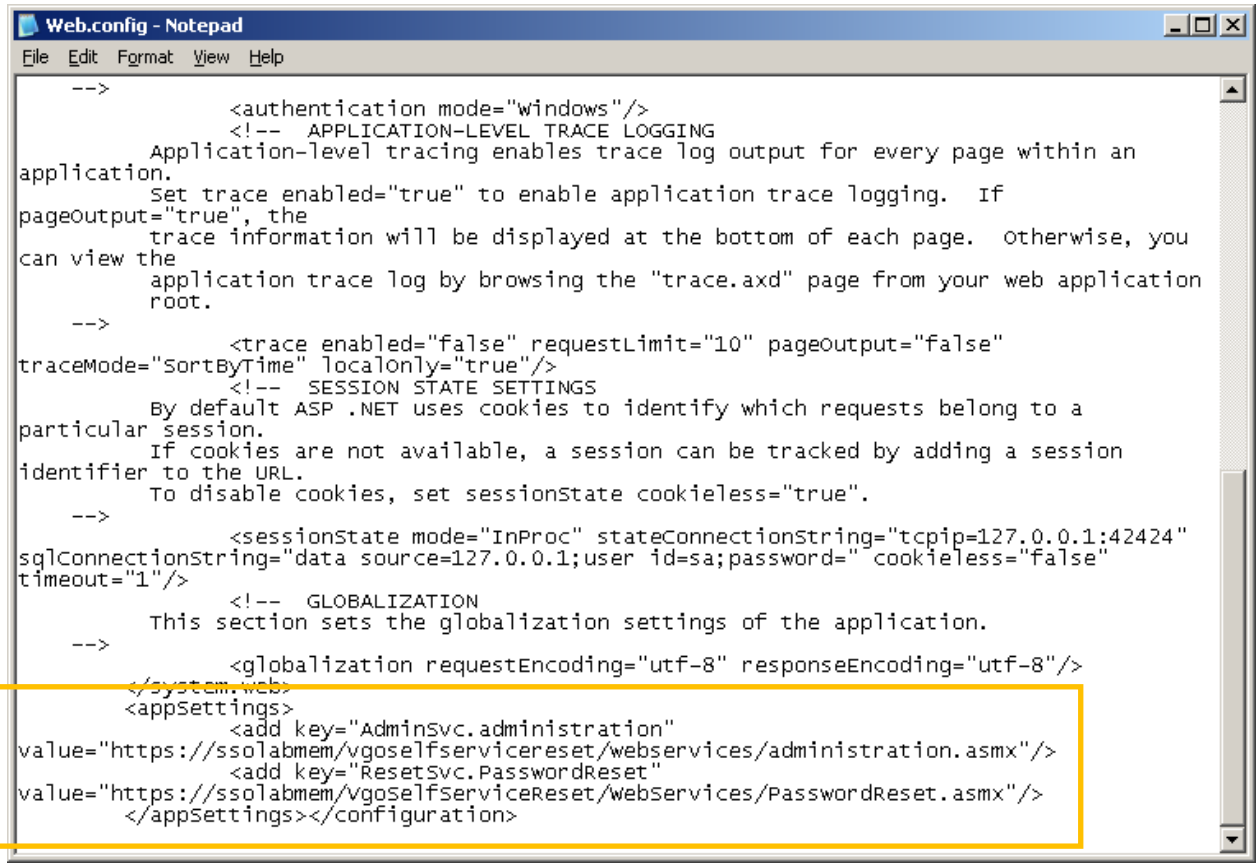
1. Modify the `\EnrollmentClient\web.config` file as follows:
    a. Locate the `<appSettings>` section.
    b. Modify the `EnrollSvc.enrollment` key value as follows:
        i. Change `http` to `https`.
        ii. Replace `localhost` with the **Issued To** value from your SSL certificate. You recorded this value in step 7k on page 31.
        iii. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon. For example: `http://sssolabmem.ssolab.com:1880`
    c. Save and close the file.



2. Modify the `\ManagementClient\web.config` file as follows:
    a. Locate the `<appSettings>` section.
    b. Modify the `AdminSvc.Administration` key value as follows:
        i. Change `http` to `https`.
        ii. Replace `localhost` with the **Issued To** value from your SSL certificate. You recorded this value in step 7k on page 31.
        iii. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon. For example: `http://sssolabmem.ssolab.com:1880`
    c. Save and close the file.



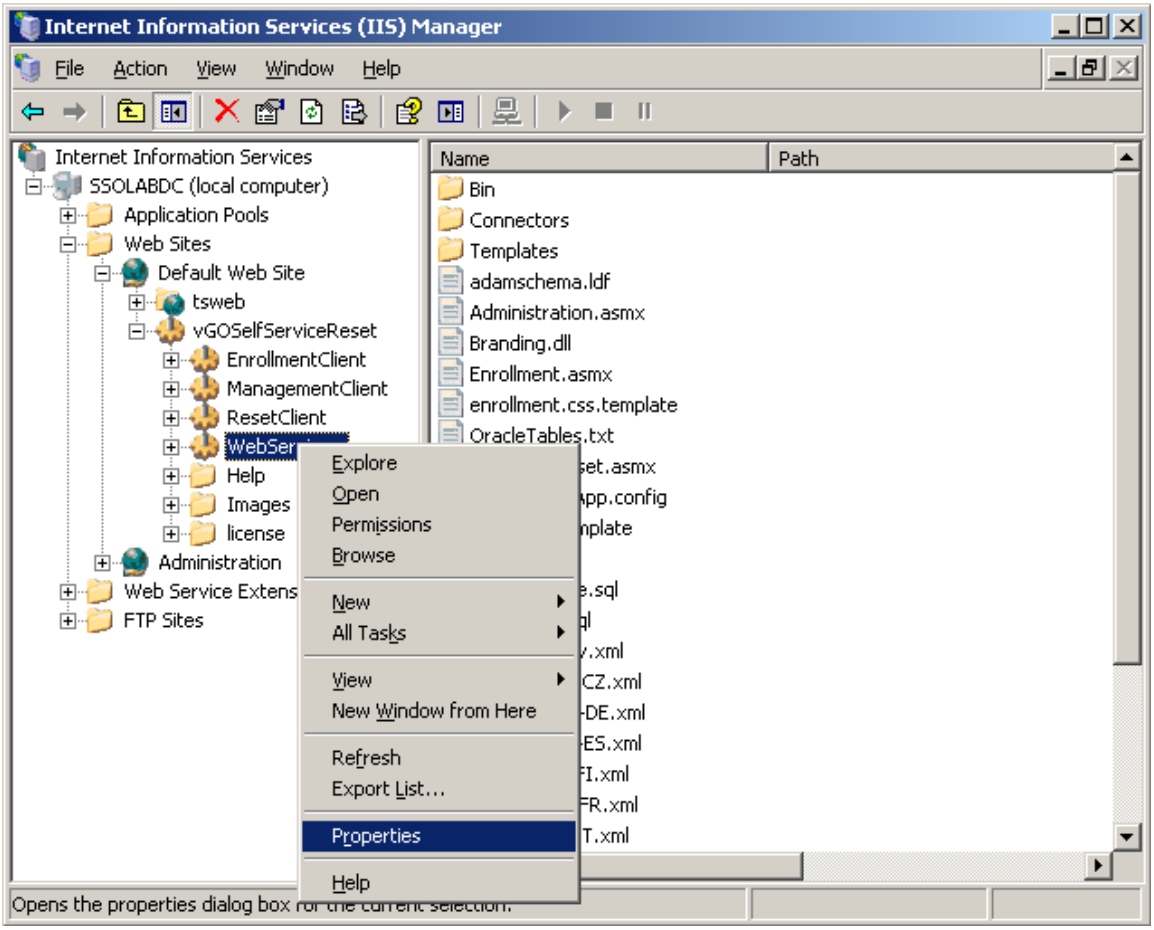
3. Modify the `\ResetClient\web.config` file as follows:
    a. Locate the `<appSettings>` section.
    b. Modify the `ResetSvc.PasswordReset` key value as follows:
        i. Change `http` to `https`.
        ii. Replace `localhost` with the **Issued To** value from your SSL certificate. You recorded this value in step 7k on page 31.
        iii. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon. For example: `http://sssolabmem.ssolab.com:1880`
    c. Modify the `AdminSvc.Administration` key value as follows:
        iv. Change `http` to `https`.
        v. Replace `localhost` with the **Issued To** value from your SSL certificate. You recorded this value in step 7k on page 31.
        vi. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon. For example: `http://sssolabmem.ssolab.com:1880`
    d. Save and close the file.



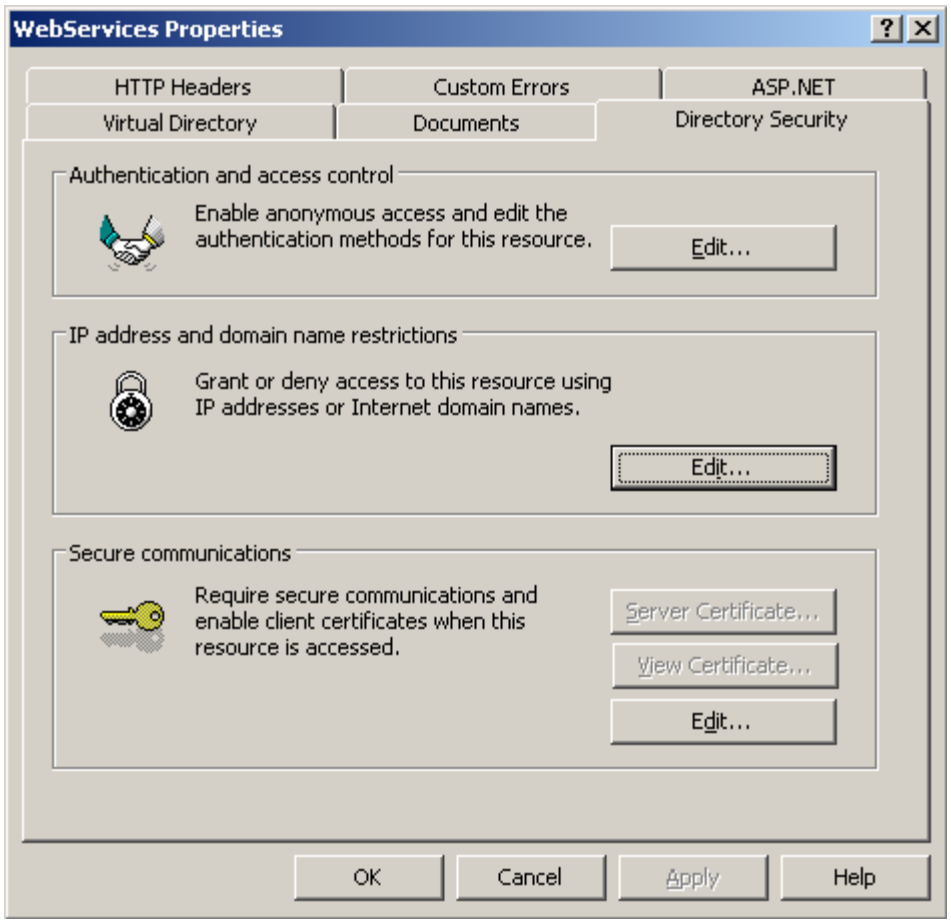
## Step 2: Granting ESSO-PR Server Access to the `WebServices` Directory

Complete the following steps to grant the ESSO-PR Server access to the **WebServices** virtual directory:

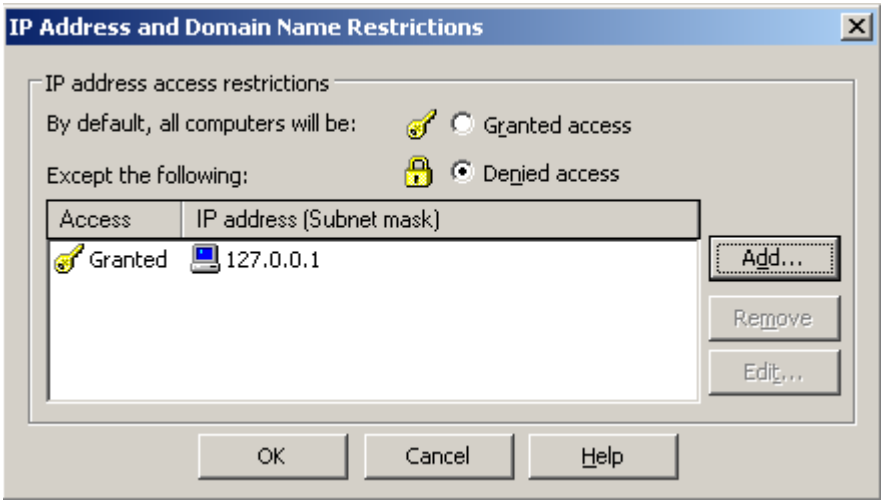
1. Launch the Internet Information Services (IIS) Manager console.
2. In the tree in the left-hand pane, navigate to and expand the **vGoSelfServiceReset** site node.
3. Right-click the **WebServices** node, located under the **vGOSelfServicePasswordReset**, and select **Properties** from the context menu that appears.



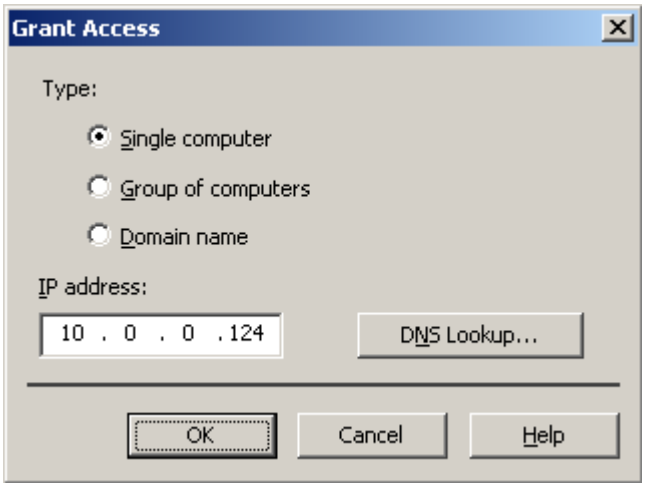
4. In the dialog that appears, select the **Directory Security** tab.
5. In the **Directory Security** tab, click **Edit** in the **IP address and domain name restrictions** section.




6. Grant the IP address of the ESSO-PR Server machine access to the **WebServices** directory:
    a. In the dialog that appears, select **Denied Access**. The dialog displays a list of IP addresses explicitly excluded from the global deny rule.
    b. Click **Add**.

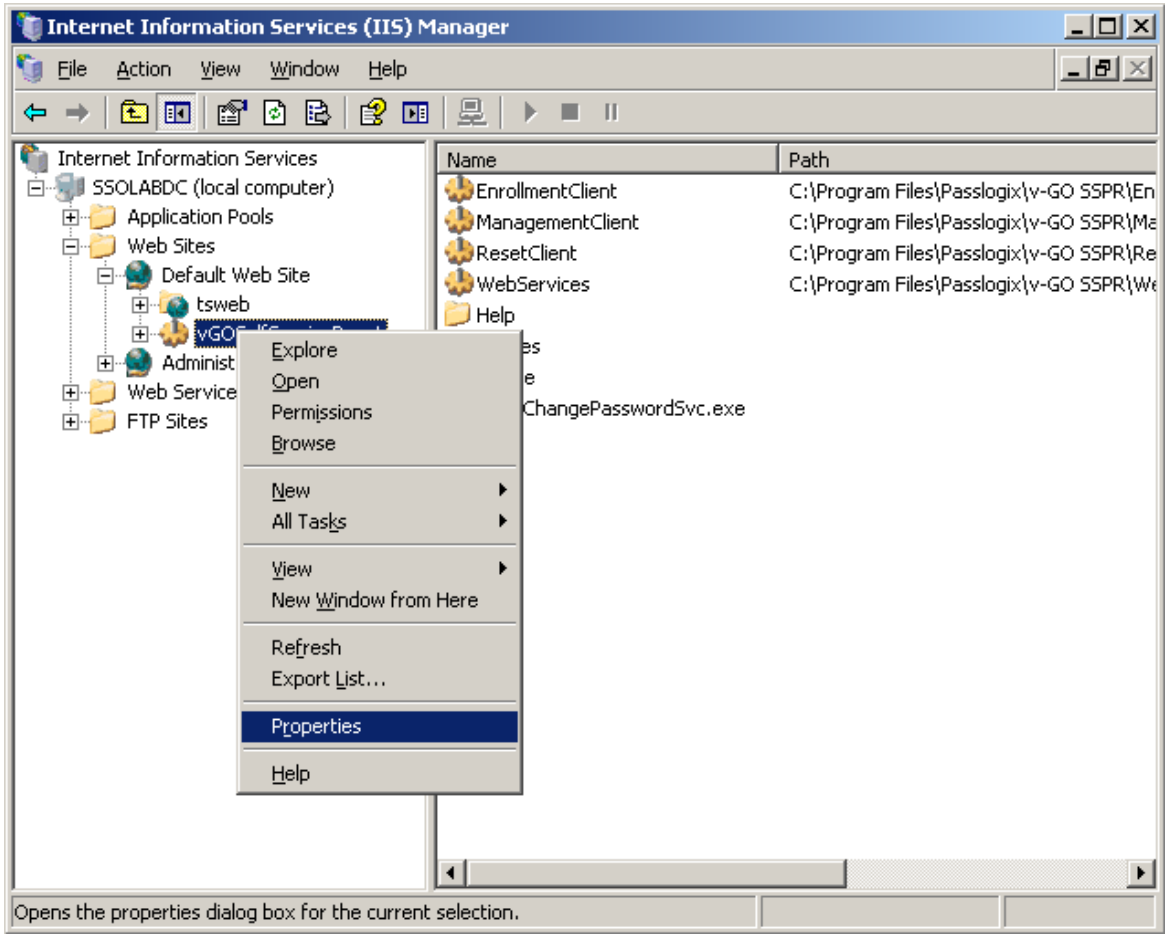


c. In the dialog that appears, select **Single Computer**, enter the target IP address, and click **OK**.

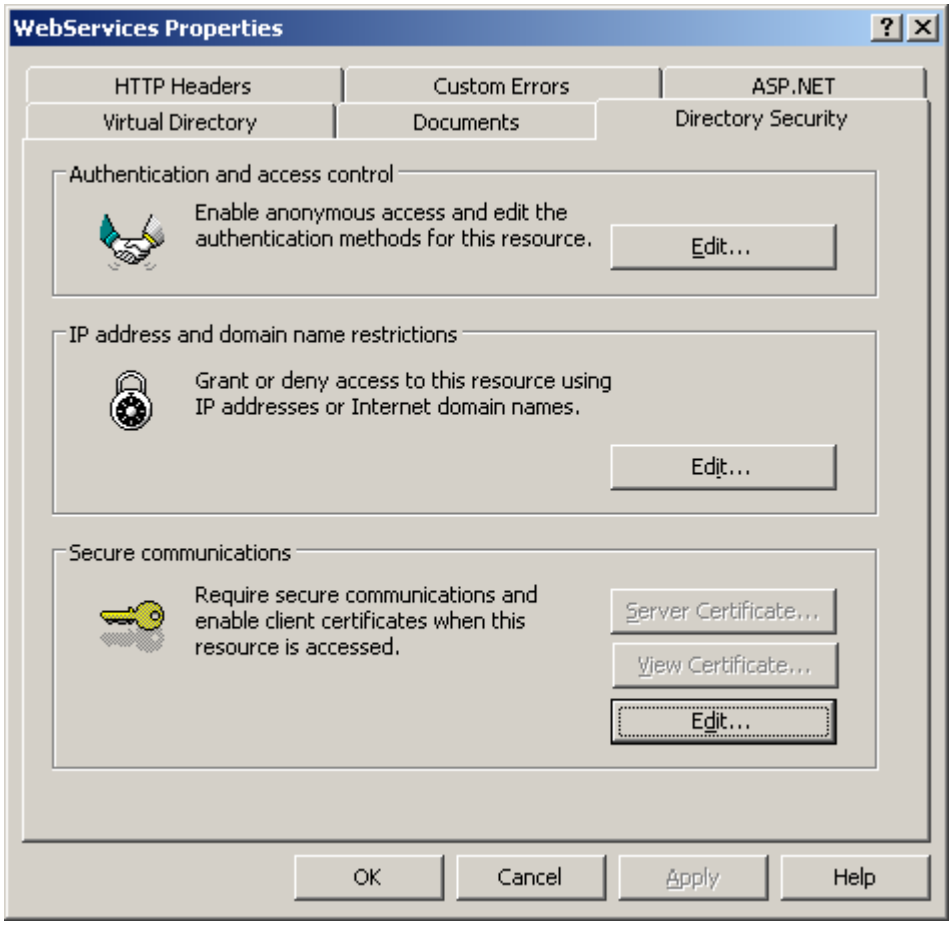



## Step 3: Restricting Web Interface Connections to SSL Only

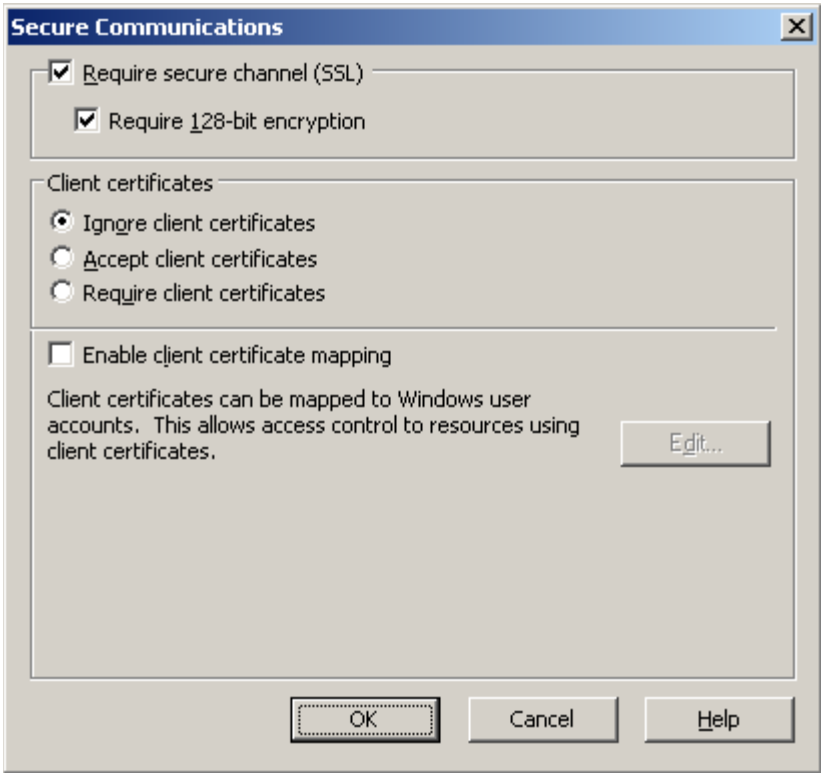
1. In the tree in the left hand pane in IIS Manager, right-click **vGOSelfServiceReset** and select **Properties** from the context menu.



2. In the dialog that appears, select the **Directory Security** tab.
3. In the **Directory Security** tab, click **Edit** in the **Secure communications** section.



4. In the dialog that appears, do the following:
    a. Select the **Require secure channel (SSL)** check box.
    b. (Optional) If your environment requires 128-bit encryption, select the **Require 128-bit encryption** check box.
    c. Click **OK**.




5. Click **OK** in the parent dialog to close it.
6. Restart Internet Information Services for the changes to take effect.

# Part 3: Testing the New Configuration

Using a Web browser, access each of the ESSO-PR Web interface services using the new SSL-enabled URLs (i.e., using the `https` protocol header in place of `http`). The URLs are as follows:

- **EnrollmentClient:**
  `https://<new_host_name>:<new_port>/vGOSelfServiceReset/WebServices/Enrollment.asmx`

- **ManagementClient:**
  `https://<new_host_name>:<new_port>/vGOSelfServiceReset/WebServices/Administration.asmx`

- **ResetClient:**
  `https://<new_host_name>:<new_port>/vGOSelfServiceReset/WebServices/PasswordReset.asmx`

If any of the URLs fail to load, check your configuration, such as virtual directory permissions and certificate options, then try again.