ORACLE®

PRIMAVERA

Primavera Portfolio Management 8.0
Enabling SSL

Copyright © 1999-2010, Oracle and/or its affiliates.

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 is a registered trademark 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.

How to install and activate SSL for Primavera® Portfolio Management

Last saved on 1/17/10 2:24 PM

Primavera® Portfolio Management fully supports the Secure Socket Layer (SSL), which allows for secure communications between web browser and server, using Secure HTTP (HTTPS).

Some functionality, such as password content checking rules, is available in Primavera® Portfolio Management only when SSL is active.

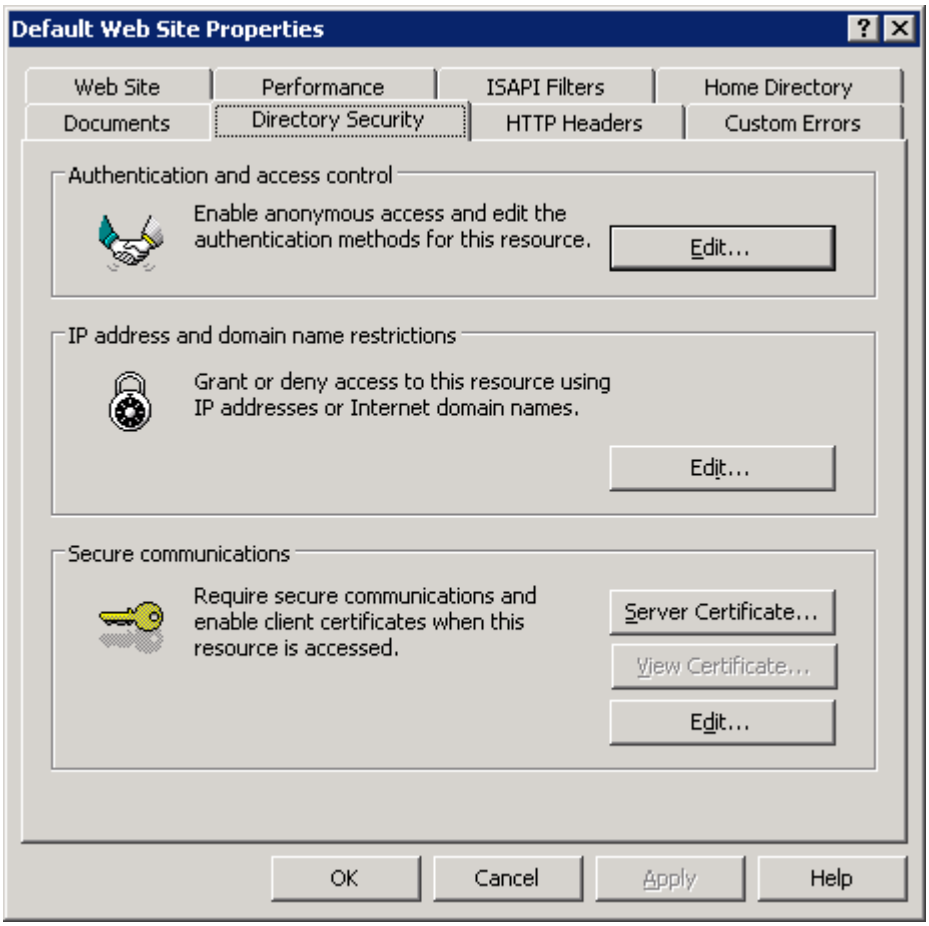
This document describes the procedure to follow in order to activate SSL on your server. To activate SSL, you have to go through several steps:

1) Request a certificate from a Certificate Authority
2) Receive and install the certificate on your IIS server.
3) Activate HTTPS for the Primavera® Portfolio Management virtual directory
4) Testing SSL and establishing a trust relationship between the CA and the browser

1. Request a Certificate

To request a certificate, follow these steps:

Click Start/Programs/Administrative Tools/Internet Information Services (IIS) Manager
Click on the plus sign next to the computer name
Right-click on Default Web Site and select Properties
Click on the Directory Security tab
You will get a screen like this:

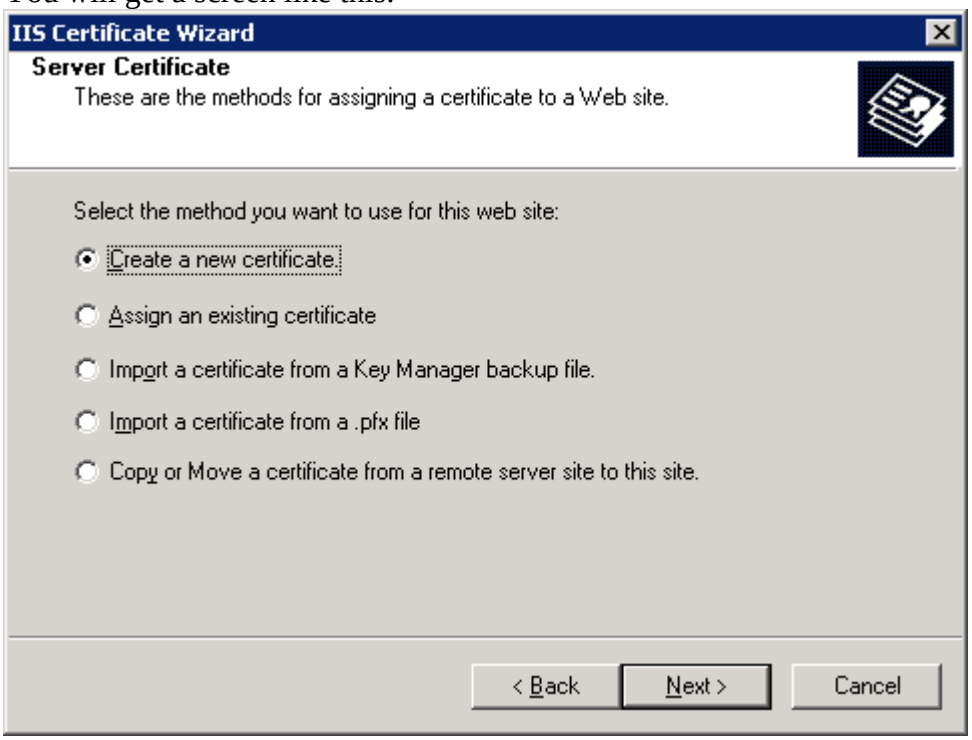


Click on “Server Certificate…”

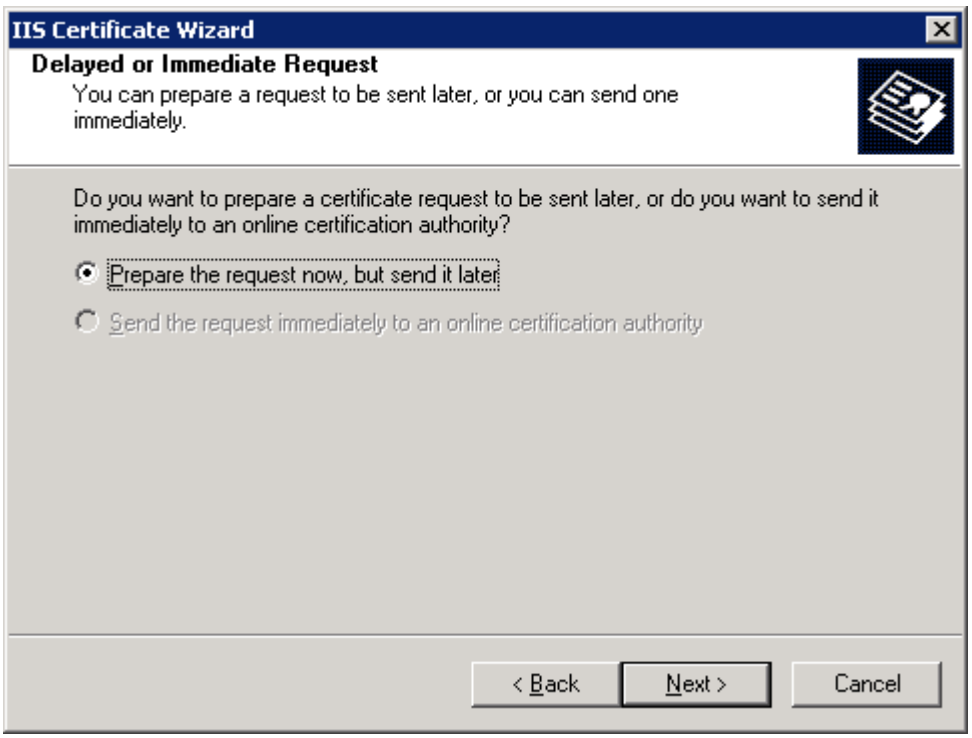
You will enter a Wizard, like this:

Click Next.

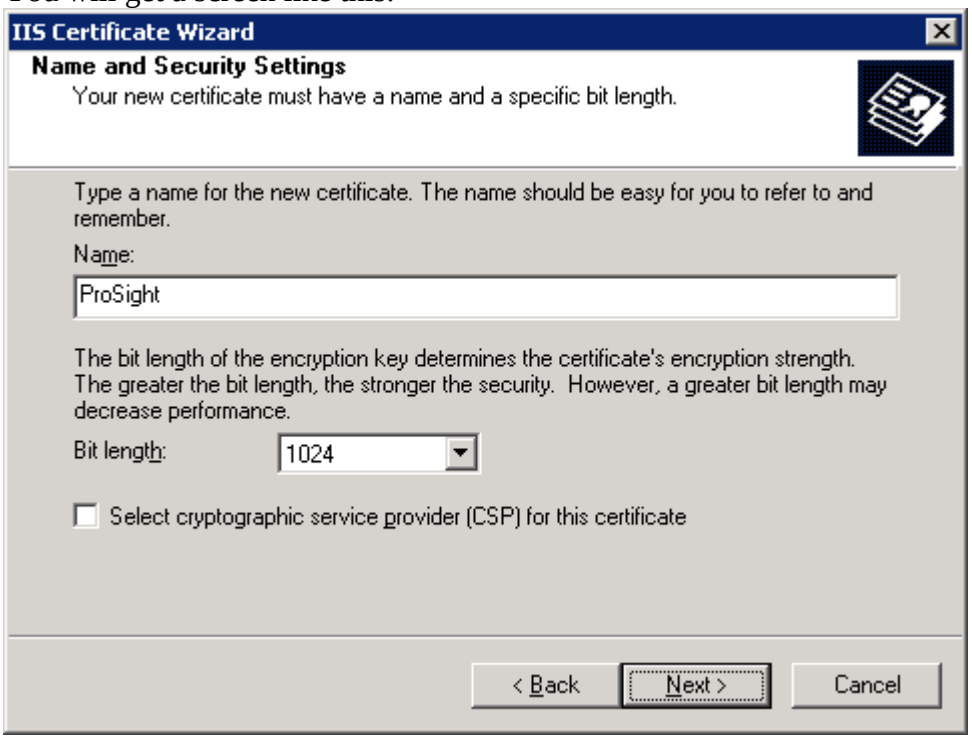
You will get a screen like this:



Select “Create a new certificate” and click Next.
You will get a screen like this:

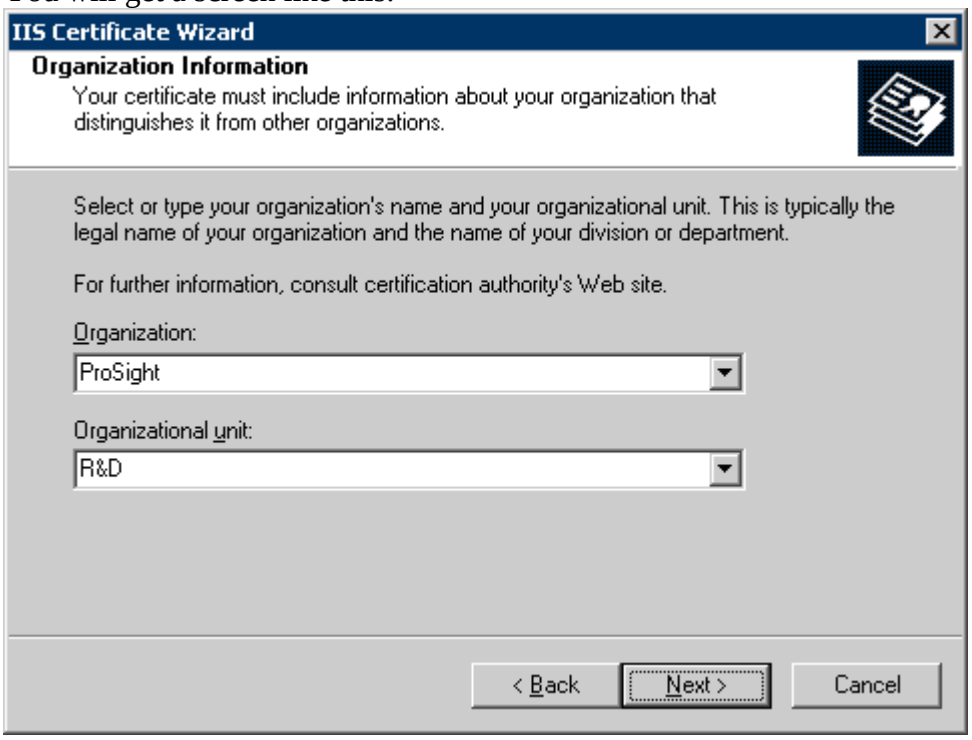


Select “Prepare the request now, but send it later” and click Next.
You will get a screen like this:



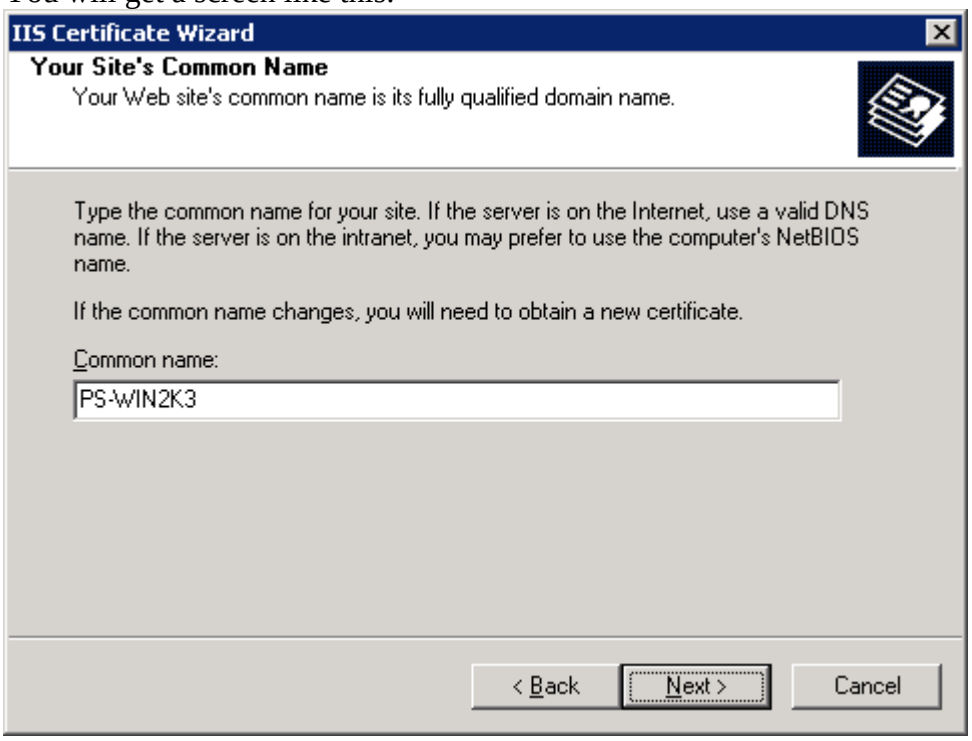
Under “Type a name for the new certificate”, type “ProSight”. Under “Bit length”, select the desired bit length for your certificate. Please note that some Certificate Authorities require a certain minimum bit length. Please check with your Certificate Authority as to their requirements. When done, click Next.

You will get a screen like this:

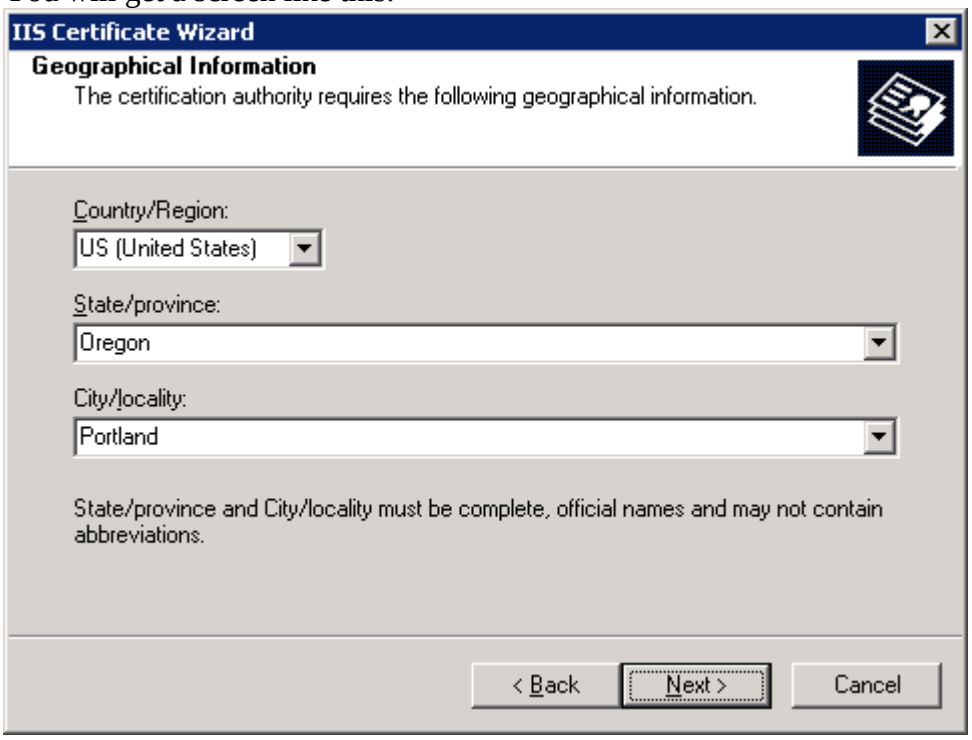


Under “Organization”, type the name of your organization (i.e. “ProSight”), and under “Organizational Unit”, type the name of your organizational unit (i.e. “R&D”), then click Next.

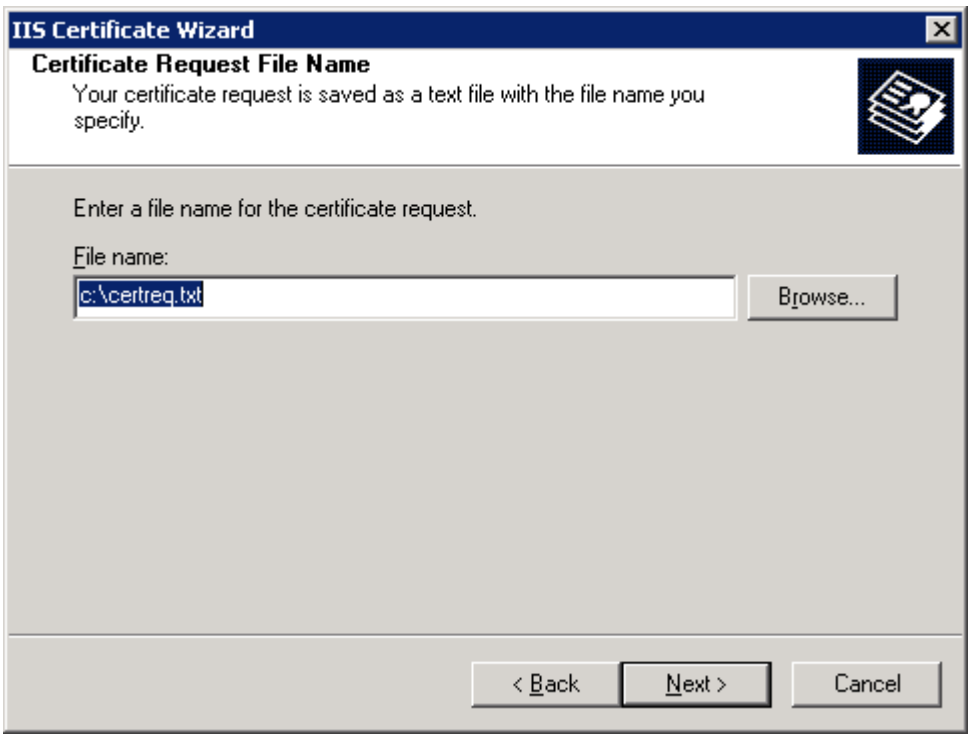
You will get a screen like this:



Under “Common name”, type the name of your server. Make sure it is spelled correctly, including case, then click Next.
You will get a screen like this:

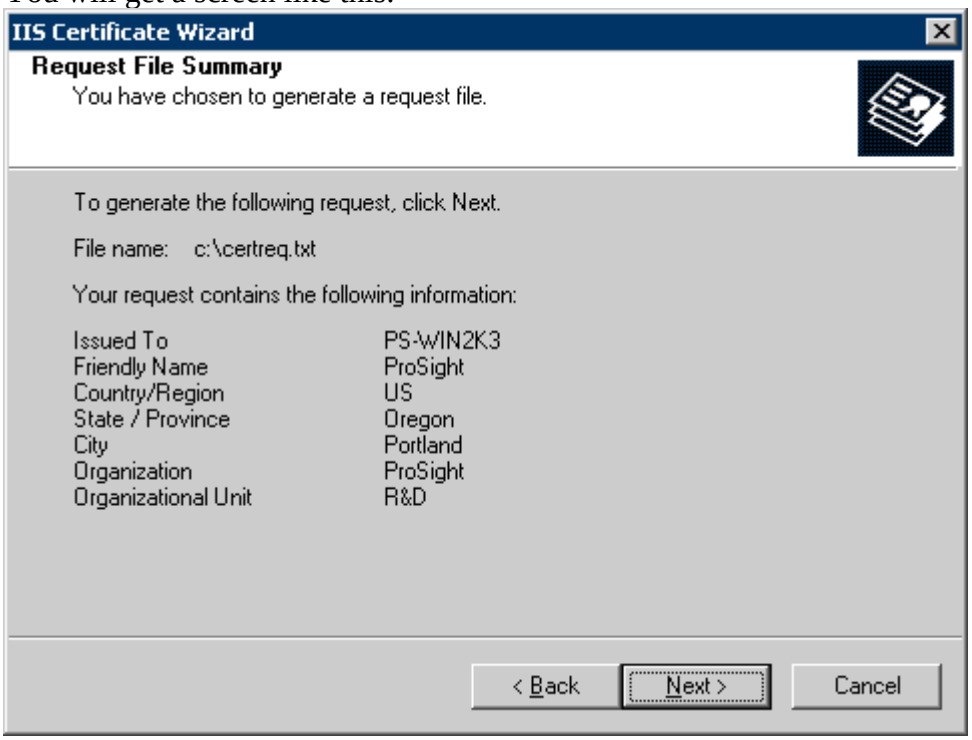


Under “Country/Region”, select the appropriate location. Fill in both “State/province” as well as “City/locality”, then click Next.
You will get a screen like this:



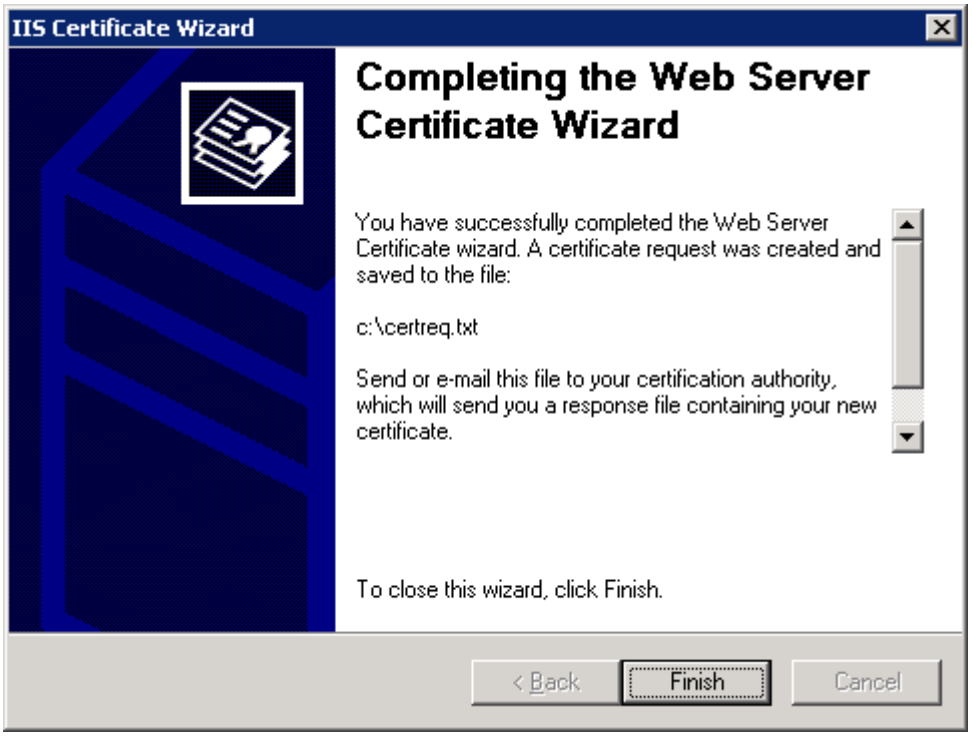
Fill in a file name. This is the name of the file which will contain your certificate request. You should select a file name which doesn't exist yet, and remember the location this file will be placed in. Click Next.

You will get a screen like this:



Check the information, then click Next.

You will get a screen like this:



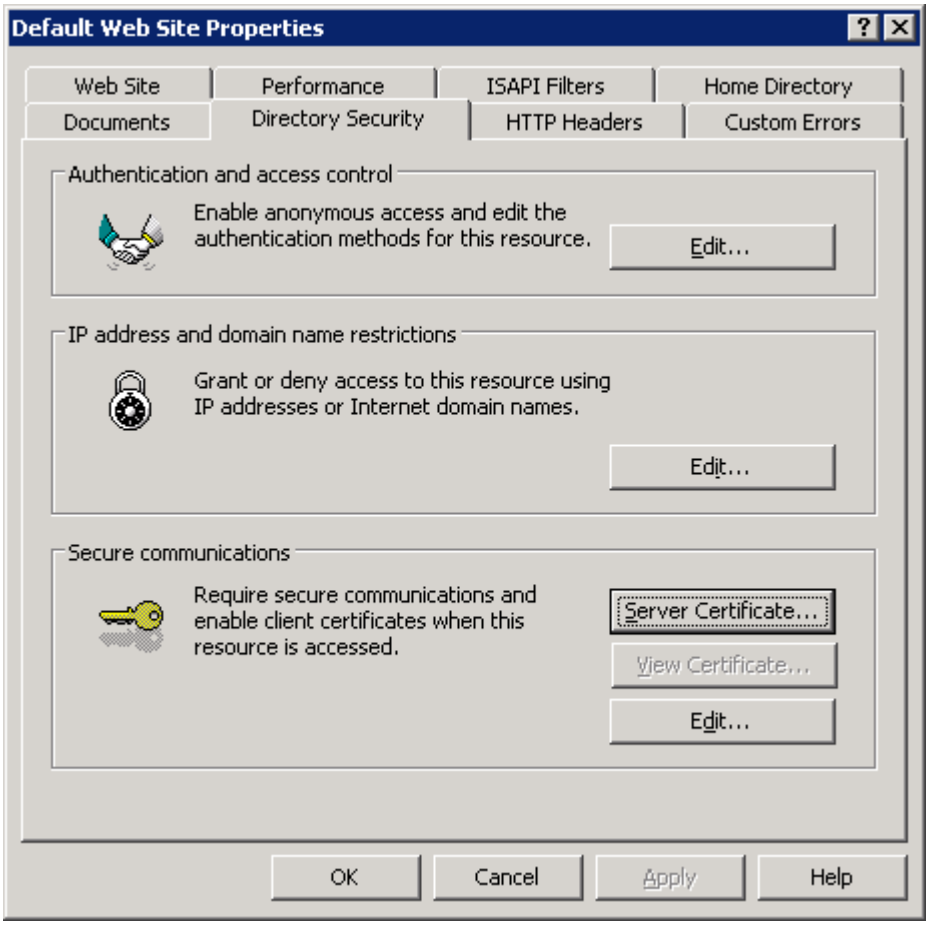
Click Finish to close the wizard
Send the file generated by this wizard to your Certificate Authority.

2. Receive and install the certificate on your IIS server

After a while, you will receive an email from your Certificate Authority, containing the new certificate. Save this file in a known location on your disk.

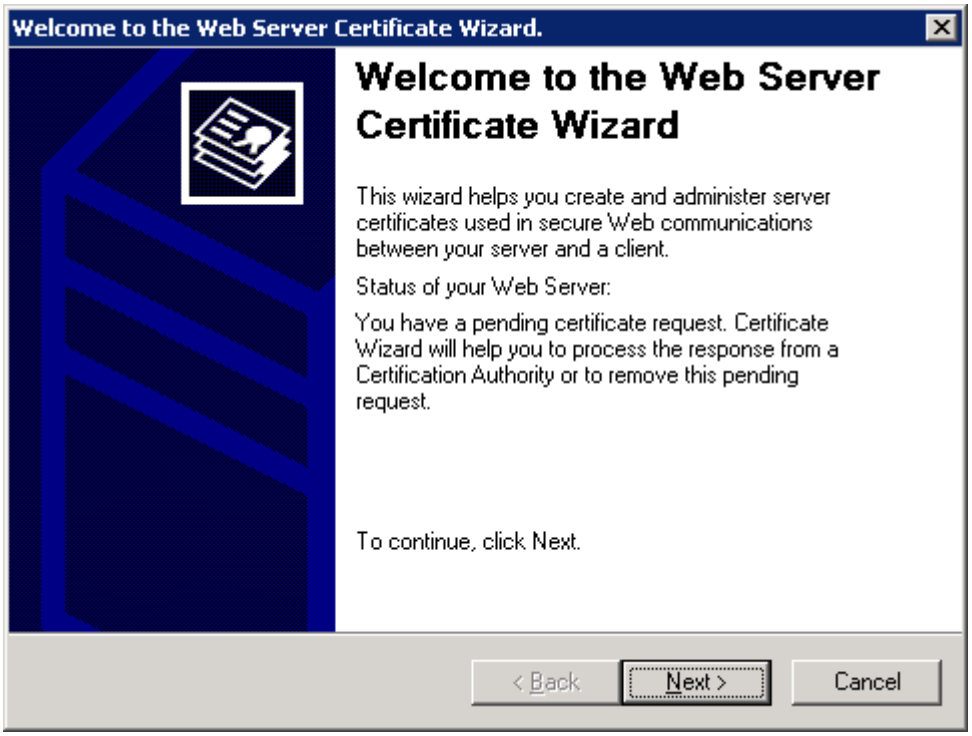
To install the certificate, follow these steps:

Click Start/Programs/Administrative Tools/Internet Services Manager
Click on the plus sign next to the computer name
Right-click on Default Web Site and select Properties
Click on the Directory Security tab
You will get a screen like this:



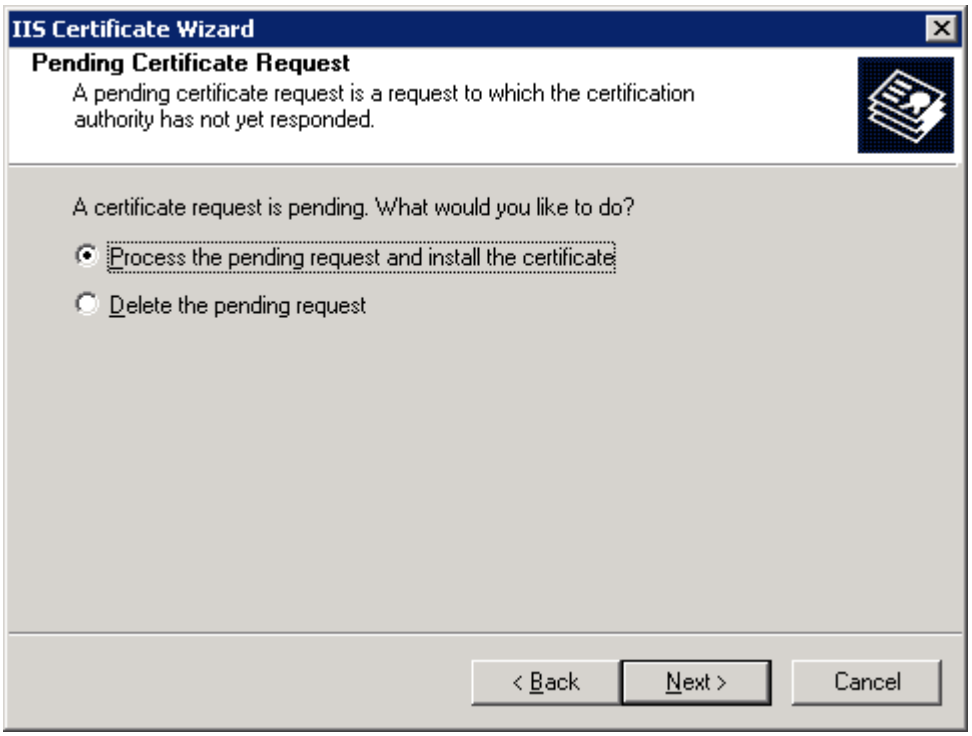
Click on “Server Certificate…”.

You will enter a Wizard, like this:



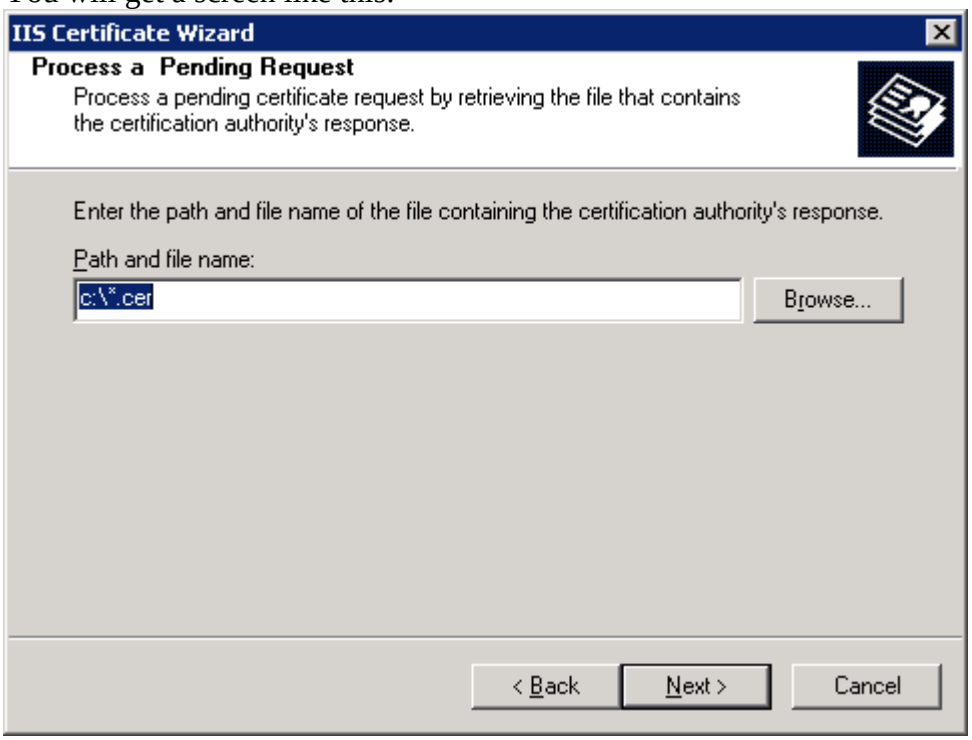
Click Next.

You will get a screen like this:



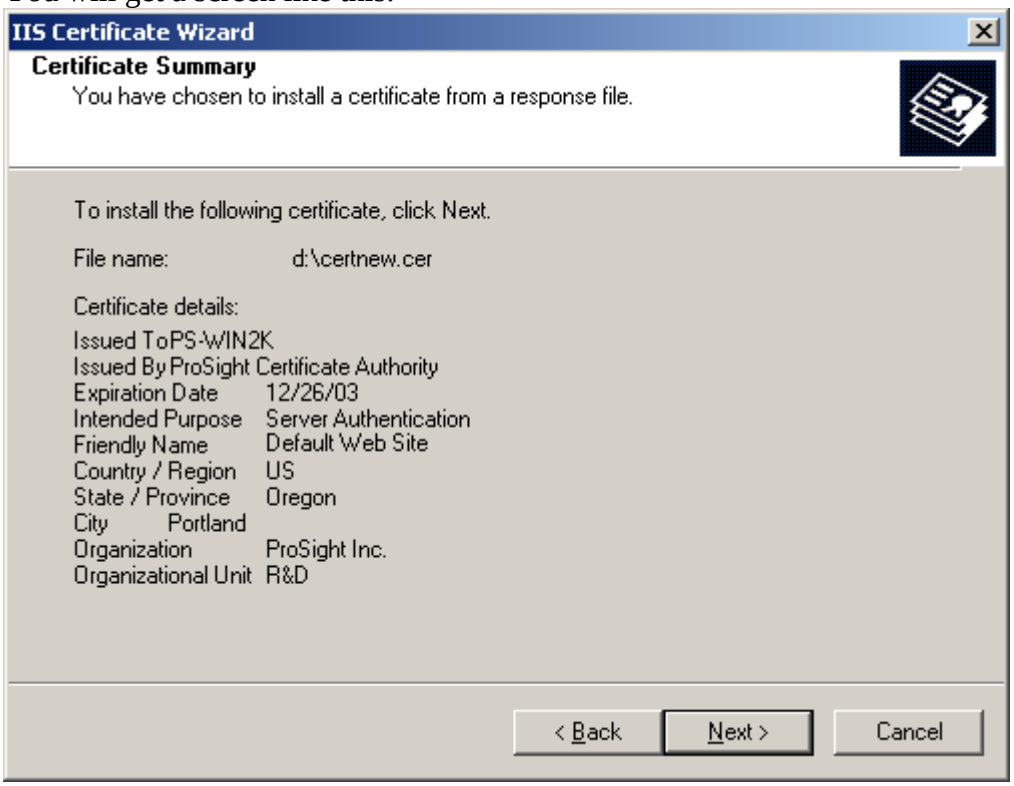
Select “Process the pending request and install the certificate”, then click Next.

You will get a screen like this:

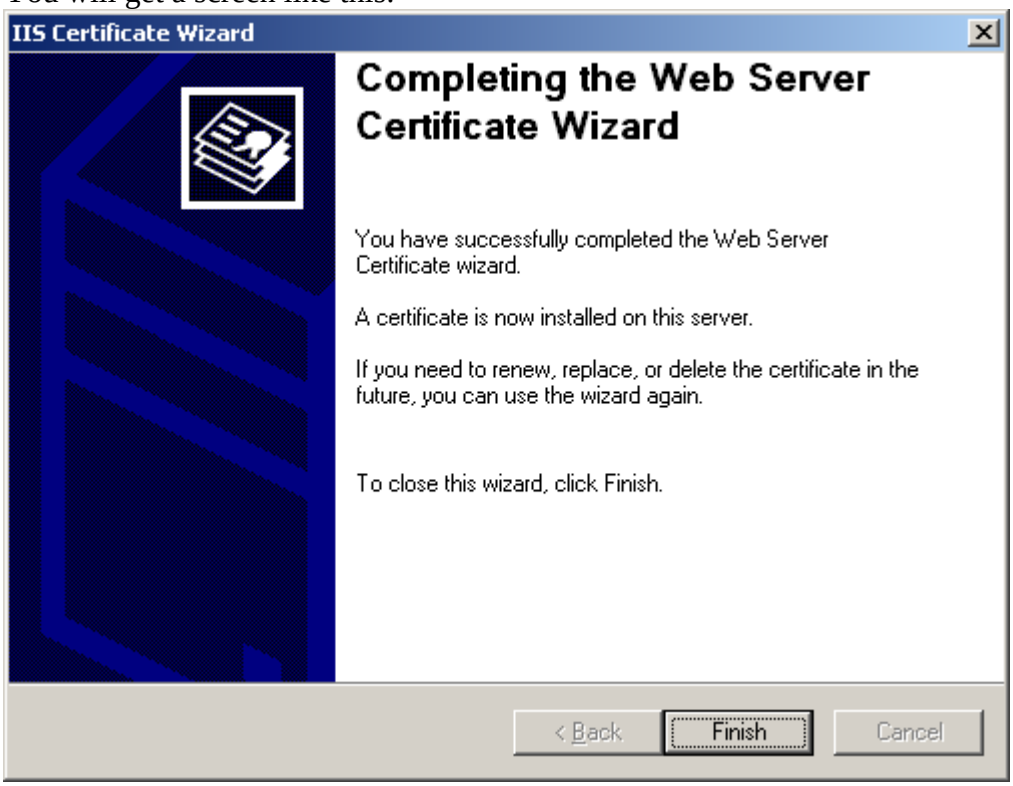


Enter the name and location of the certificate file, or click Browse and select the certificate file. Then click Next.

You will get a screen like this:



Click Next.
You will get a screen like this:



Click Finish to close the wizard.

3. Activate HTTPS for Primavera® Portfolio Management

In order to use SSL, you must activate it.

Note: in a distributed installation of Primavera® Portfolio Management ("Scale Out"), the below described settings must be made on all Primavera® Portfolio Management application servers.

- If you have not yet installed Primavera® Portfolio Management , you can do so now. During the installation you can select the desired SSL mode (see below). When done with the install, skip to chapter 4 in this document.

- If you already installed Primavera® Portfolio Management prior to requesting and installing a certificate, you can activate SSL by running the psEnableSSL.bat command script from the location in which you installed Primavera® Portfolio Management (i.e. run "C:\Program Files\Oracle\Primavera Portfolio Management\Portfolios\bin\psEnableSSL.bat").

The psEnableSSL.bat command script accepts one parameter, which indicates the requested SSL mode. Activating psEnableSSL.bat without specifying any parameter will indicate the current SSL mode. Note that running psEnableSSL.bat will restart Primavera® Portfolio Management.

The four SSL modes which Primavera® Portfolio Management supports are:

none	-	in this mode, SSL is not active.
password	-	in this mode, SSL is activated only for pages which require the user to enter sensitive information such as passwords.
all	-	in this mode, SSL is active for the entire application.
clientless_vpn	-	special mode which supports SSL offloading using proxies. Do not activate unless instructed by Customer Support.

Examples:

To activate SSL for the entire application, run the following command:

```
psEnableSSL /all
```

To activate SSL only for pages which request sensitive information, run the following command:

```
psEnableSSL /password
```

To deactivate SSL entirely, run the following command:

```
psEnableSSL /none
```

To check the current SSL mode of Primavera® Portfolio Management, run the following
command:

```
psEnableSSL
```

4. Testing SSL and establishing a trust relationship between the CA and the browser

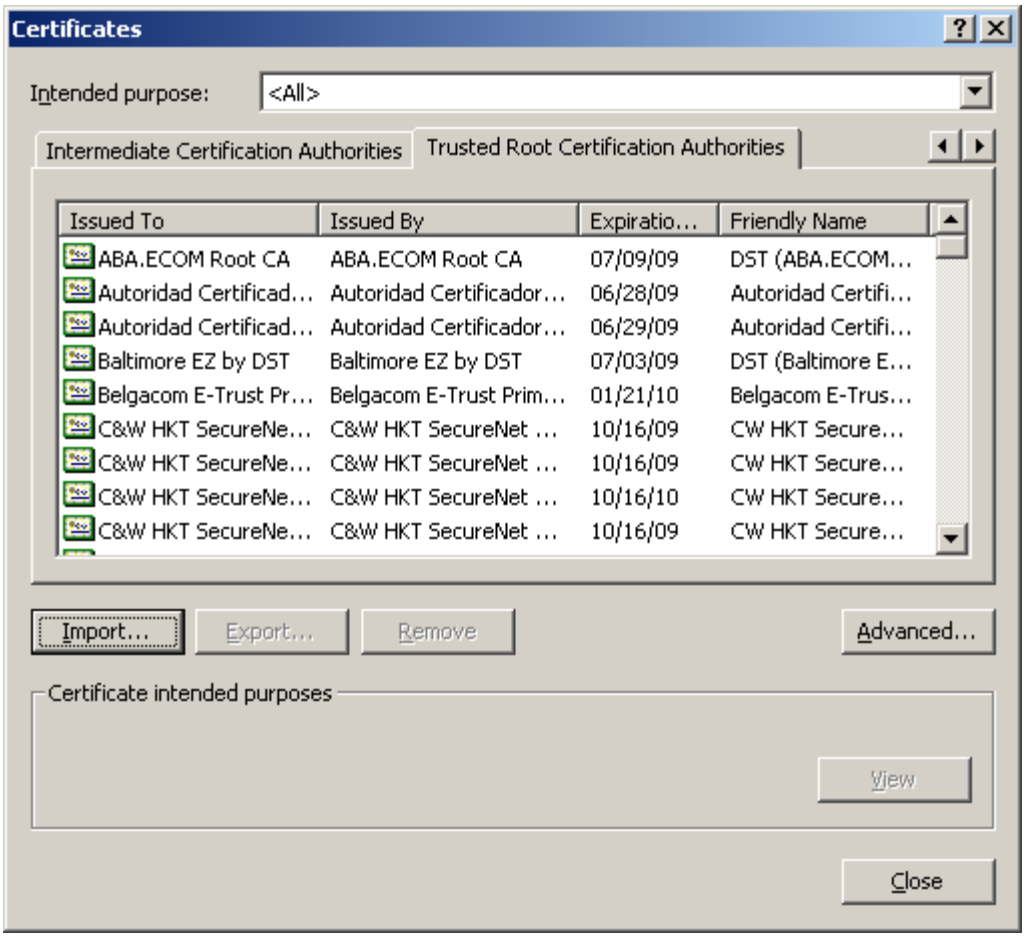
If you activated SSL for the entire Primavera® Portfolio Management application ("All" mode as described above in chapter 3), you must now access Primavera® Portfolio Management using a secure URL starting with "https://", such as "https://myservername/prosight". You will not be able to access the application using a non-secure URL such as "http://myservername/prosight", and if you attempt to do so, you will receive a failure message.

If you activated SSL either for the entire application ("All" mode as described above in chapter 3), or only for pages which request sensitive information ("Password" mode as described above in chapter 3), some or all pages will be accessed using secure URL's. When first accessing (pages in) Primavera® Portfolio Management using secure URL's, you may receive one or two "Security Alert" messages from your browser.

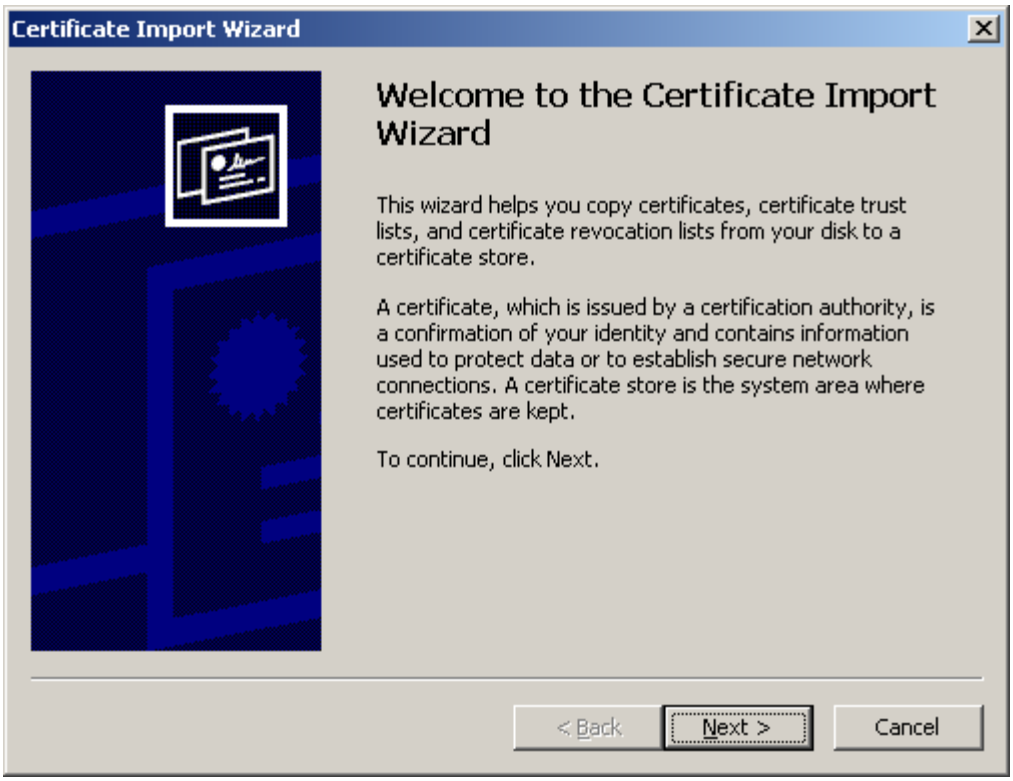
The first message will appear only if your web browser is not set up to trust certificates from the Certificate Authority from which you received your server certificate.

To set up browsers to trust certificates from the Certificate Authority from which you received your server certificate, please proceed as follows (you must have received a file called "certnew.p7b" from the Certificate Authority together with your server certificate, for these steps to work):

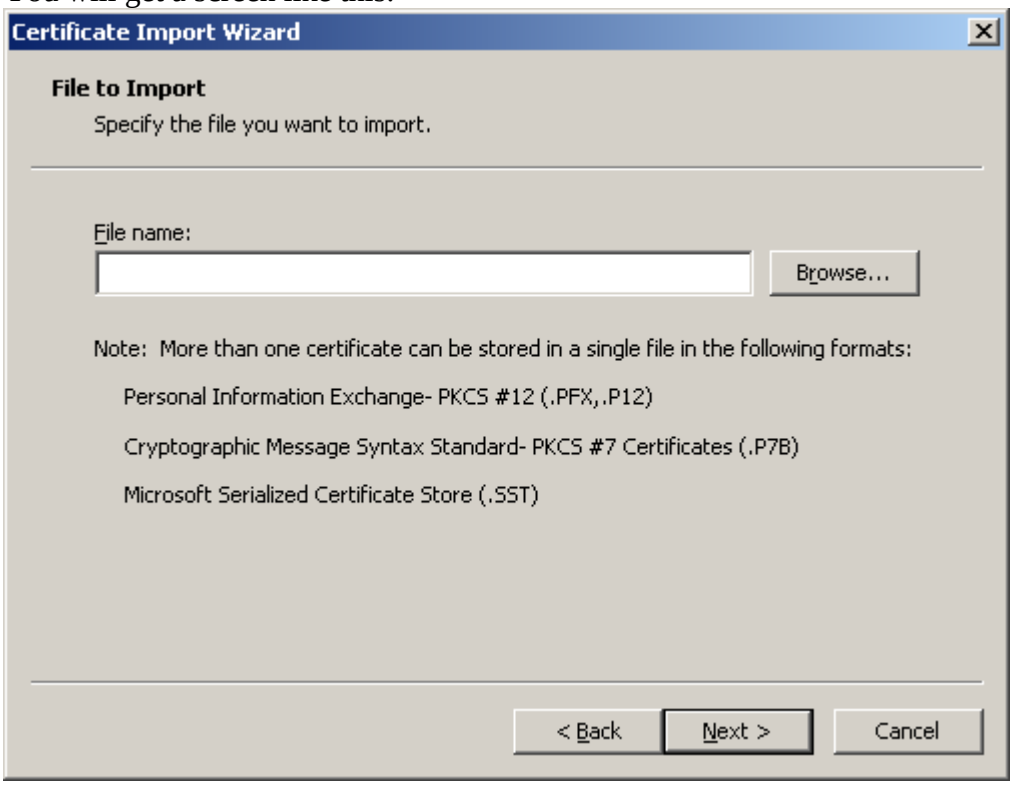
Start your Internet Explorer.
From the menu, select Tools/Internet Options…
Select the Content tab.
Click the Certificates… button
Select the Trusted Root Certification Authorities tab.
You will get a screen like this:



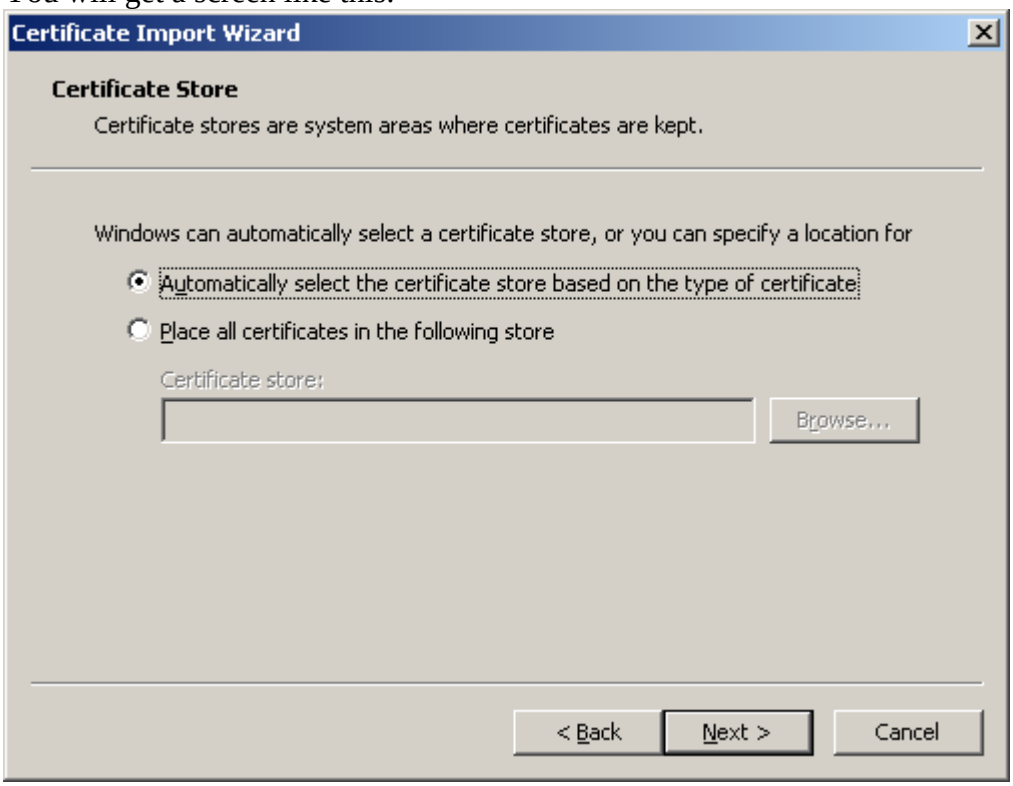
Click the Import… button.
You will get a screen like this:



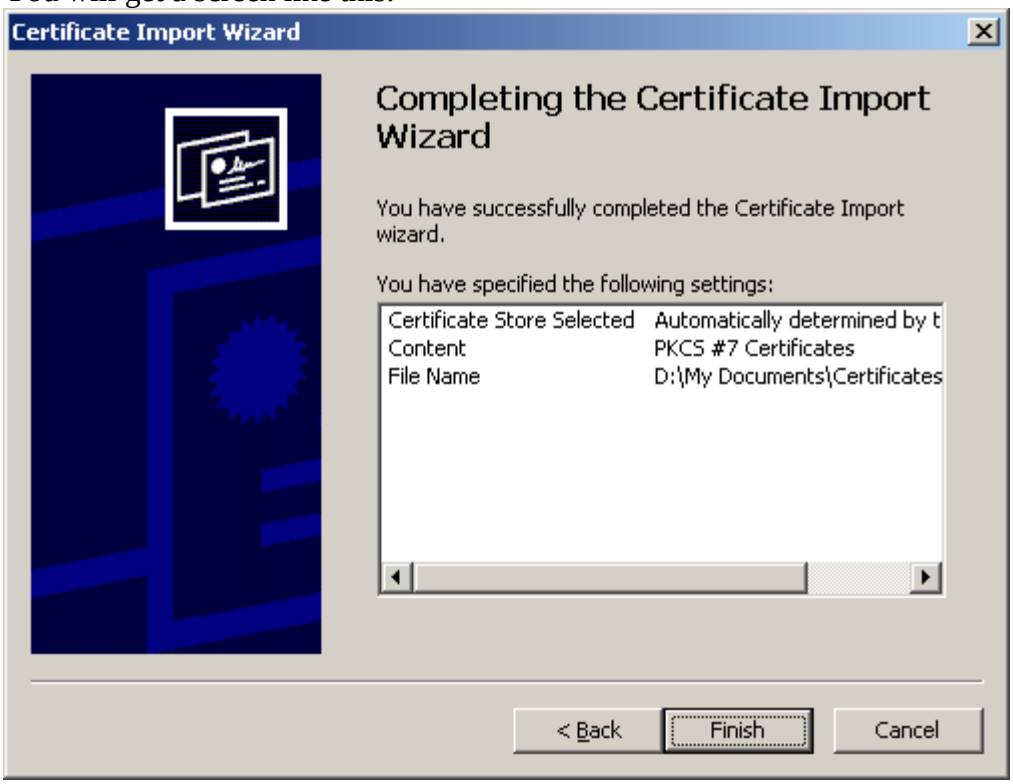
Click Next.
You will get a screen like this:



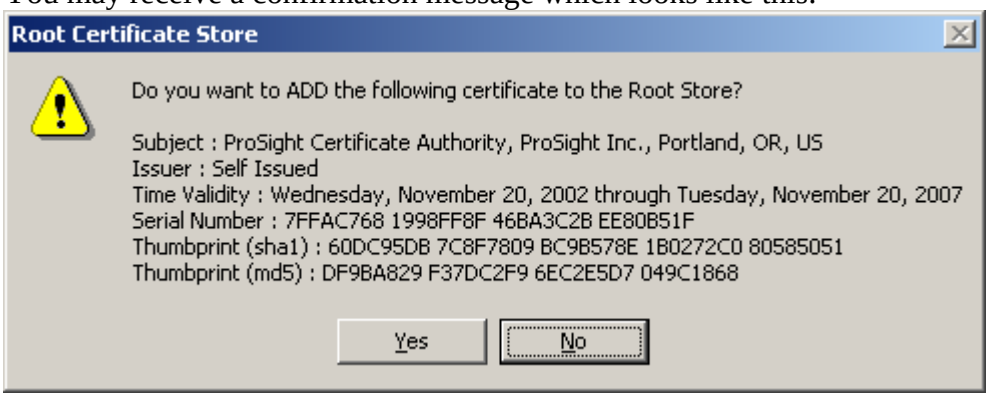
Click the Browse… button, and locate the file “certnew.p7b” which you received from the Certificate Authority together with your own certificate. Click Open, then click Next. You will get a screen like this:



Click Next.
You will get a screen like this:

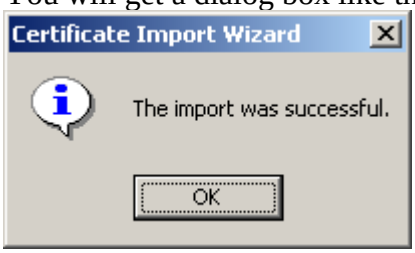


Click Finish.
You may receive a confirmation message which looks like this:



If you received the above confirmation message, click “Yes”.

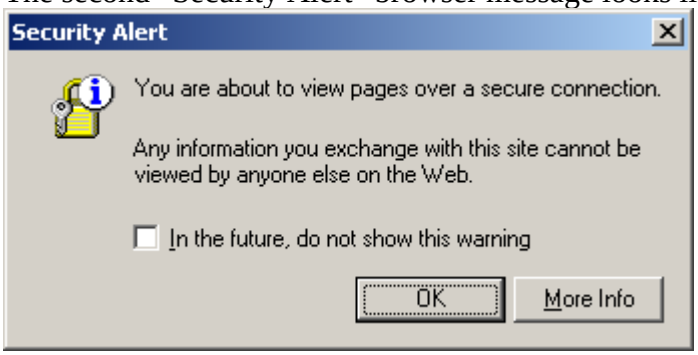
You will get a dialog box like this:



Click OK.
Click Close.
Click OK.

You must repeat this procedure on every browser which accesses Primavera® Portfolio Management. To avoid having to do this, we recommend getting a server certificate from one of the major Certificate Authorities which the browser is set up to trust by default.

The second “Security Alert” browser message looks like this:



This second message appears every time the web browser switches between non-secure and secure mode, or vice versa. This message can be turned off by selecting “In the future, do not show this warning”.