

Software Procedure

SWP-0011 tConsult Third Party SSL Certificate Procedures

Revision: 2

Effective Date: 8/5/2010

Alaska Native Tribal Health Consortium
Division of Health Information & Technology
4000 Ambassador Drive
Anchorage, AK 99508
Tel: (907) 729-2260
Fax: (907) 729-2269



Contents

Purpose	3
Audience	3
Scope	3
Acronyms and Abbreviations	3
Removing the Current AFHCAN tConsult Certificate	4
Requesting a Third Party SSL Certificate	7
Installing the Third Party SSL Certificate into the Certificate Personal Store	12
Installing the Third Party SSL Certificate into IIS	21

Purpose

The purpose of this document is to detail the steps necessary to request, obtain and install a third party SSL Certificate for use with the tConsult Server software.

Audience

This document is written for IT technicians and system administrators who are responsible for building, configuring, or maintaining an AFHCAN tConsult Server. It is assumed readers are familiar with intermediate-level computer terms and concepts.

Scope

tConsult Web Client uses SSL to communicate to the tConsult Server. Obtaining and installing a Third Party SSL Certificate is certifying the identity of the tConsult Server while providing strong encryption. **The Third Party SSL Certificate Vendor should be a Microsoft-recognized trusted root authority.**

There are different methods that can be used by Third Party SSL Vendors to request and receive SSL Certificates. Three are listed here.

- a. Create an email and submit the Certificate Request to the Third Party SSL Vendor who will be fulfilling this order. Upon receipt of a valid certificate from the Third Party SSL Vendor, place the certificate in the root of the C:\drive of the tConsult Server.
- b. Use an online order form with the Third Party SSL Vendor. Copy and paste the request into the form. Upon receipt of a valid certificate from the Third Party SSL Vendor, place the certificate in the root of the C:\drive of the tConsult Server.
- c. If the tConsult Server can connect to the World Wide Web – the Web Server Certificate Wizard can connect to the Third Party SSL Vendor to request and obtain a certificate.

This detailed steps outlined in this document utilizes the first method and walks the reader through how to request a third party certificate and installing it when received.

NOTE: During the procedure, this will disable the tConsult Web Client for the organization. It is strongly recommended that the Third Party SSL Vendor be pre-selected and standing by to receive the Certificate Signing Request and issue the SSL Certificate. Reading through the documentation and understanding the process before beginning will keep downtime to a minimum.

Acronyms and Abbreviations

Table 1

Acronyms and abbreviations

Acronym	Meaning
SSL	Secure Socket Layer
IIS	Internet Information Server
CSR	Certificate Signing Request
FQDN	Fully Qualified Domain Name
DN	Distinguished Name
MMC	Microsoft Management Console

Removing the Current AFHCAN tConsult Certificate

This section details the steps necessary to remove the current AFHCAN tConsult Certificate from within IIS only.

IMPORTANT: Do NOT remove the certificate from the Certificate Store, the tConsult Server Service uses this certificate!

1. Using IIS Manager on the tConsult Server, expand the Web Sites until tConsult website is located.

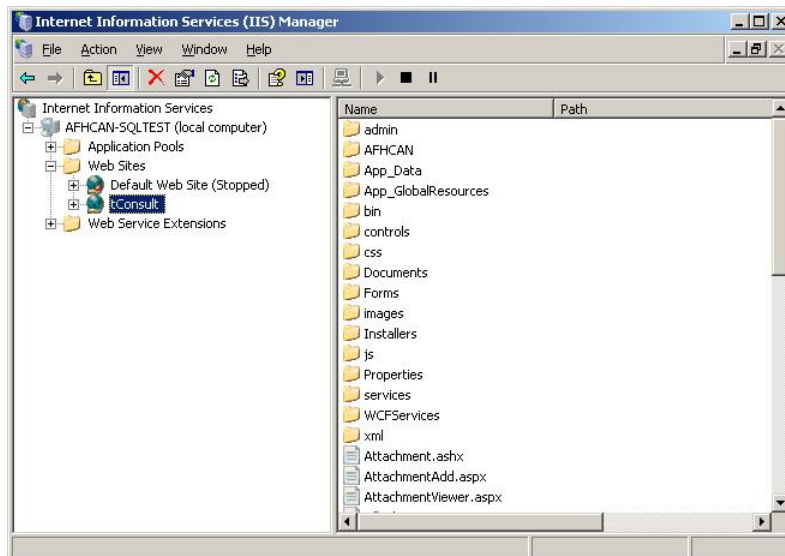


Figure 1 – IIS Manager

2. Do a right mouse-click on the tConsult website and select Properties. Click on the Directory Security tab. Click on the Server Certificate button.

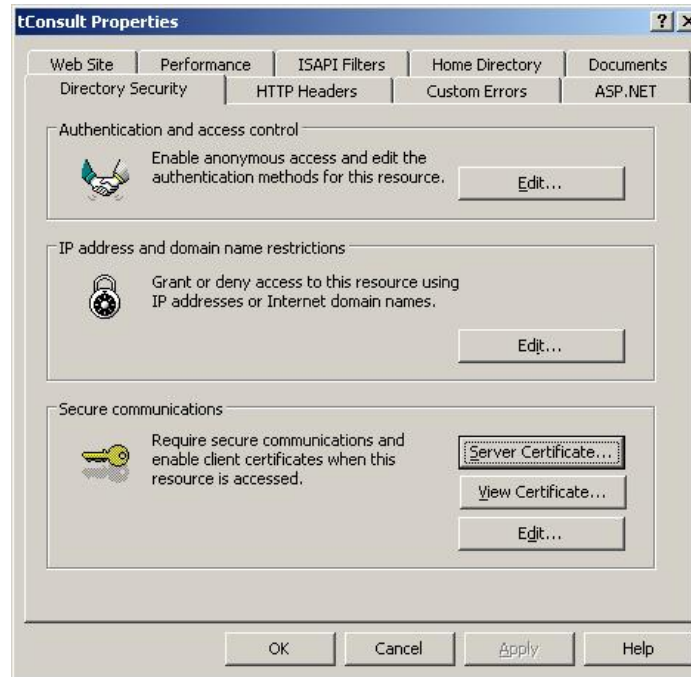


Figure 2 – Directory Security tab of the tConsult Website Properties

3. This will open the Web Server Certificate Wizard. Click on Next.



Figure 3 – Web Server Certificate Wizard

4. There is an AFHCAN Telehealth Signing Certificate currently installed. This needs to be removed from within IIS in order to request a new certificate from a third party. Ensure the Remove the current certificate radio button is selected and click on Next.

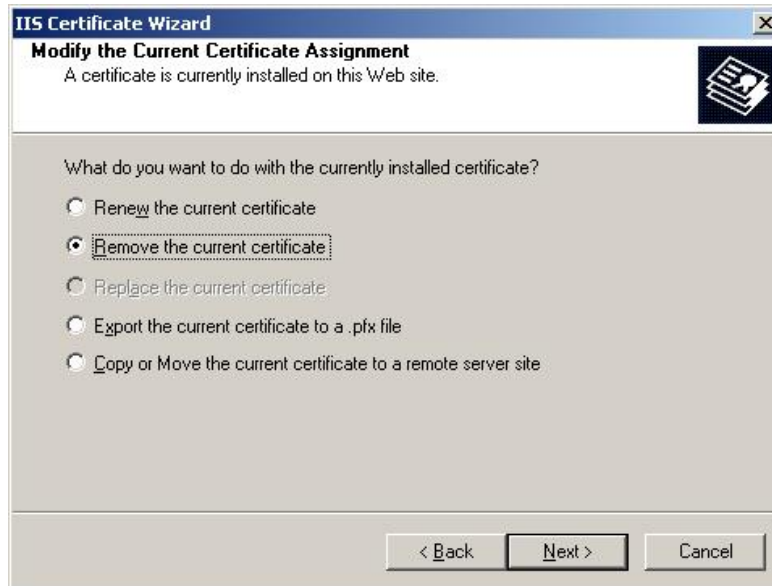


Figure 4 – Removing the Current Certificate

5. A verification of the removing of the current certificate is displayed. Click on Next.

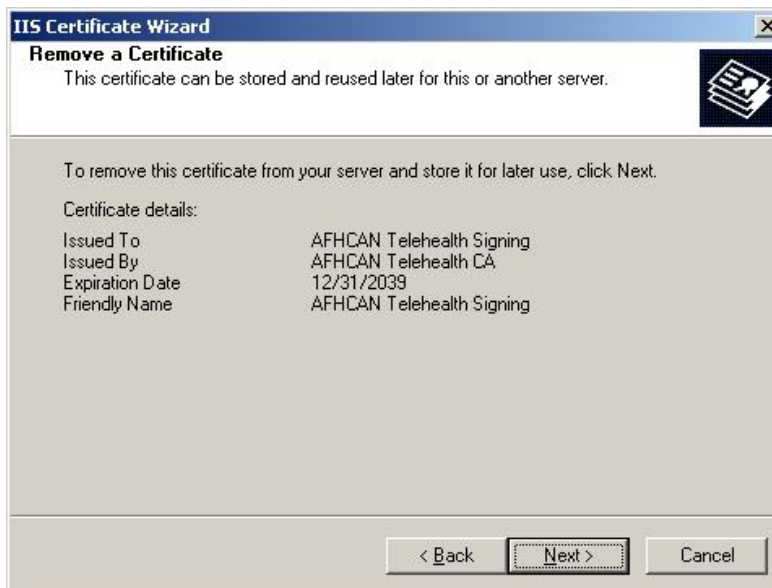


Figure 5 – Verifying the Removal of the Current Certificate

6. Click on Finish to complete the removal process.



Figure 6 – Completing the Removal of the Current Certificate

Requesting a Third Party SSL Certificate

This section details the steps for generating a CSR (Certificate Signing Request) from the tConsult Server.

2. Still using IIS Manager on the tConsult Server, right mouse on the tConsult Website and select Properties. Click on the Directory Security tab and click on the Server Certificate button.

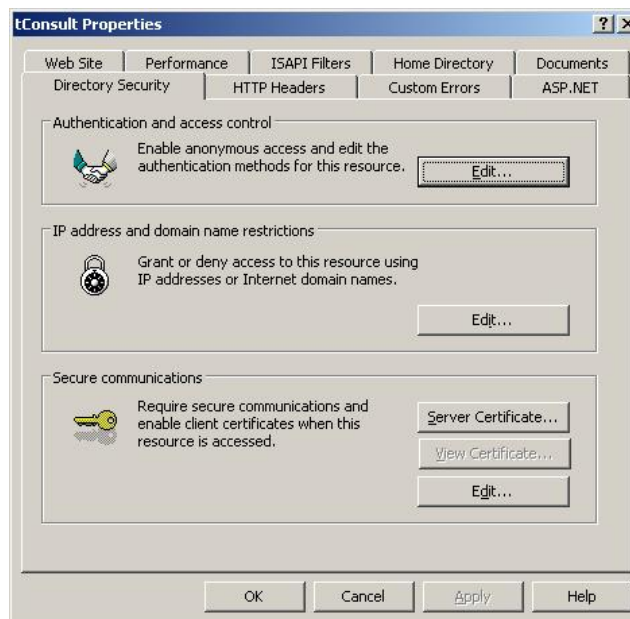


Figure 7 – Directory Security tab of the tConsult Website Properties

3. The Welcome to the Web Security Wizard will start up. Click on Next.



Figure 8 – Web Server Certificate Wizard

4. Select the radio button in front of Create a new certificate as shown in Figure 9 below, and then click on Next.



Figure 9 – Creating a New Certificate

5. Accept the default “Prepare the request now, but send it later” and click on Next.

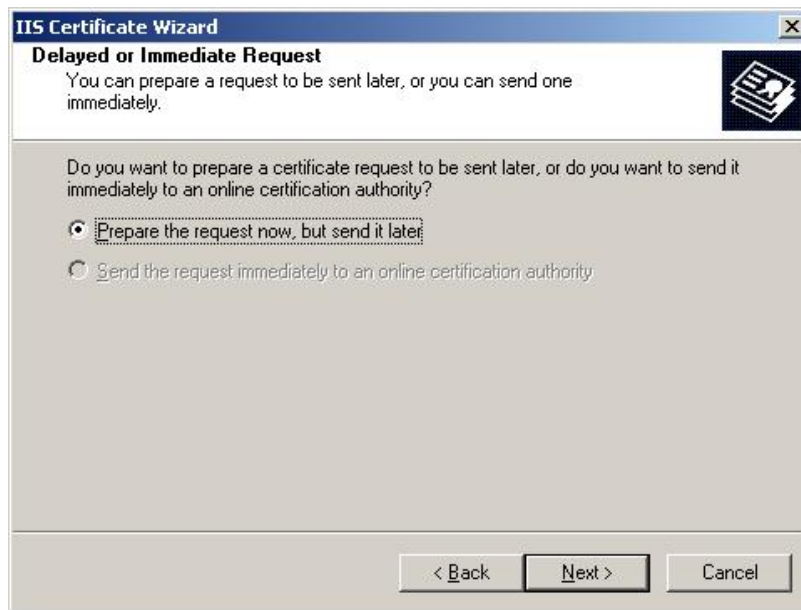


Figure 10 – Delayed or Immediate Request

6. Enter a name for this certificate, then click on Next.
Note: The name in Figure 11 is an example only.

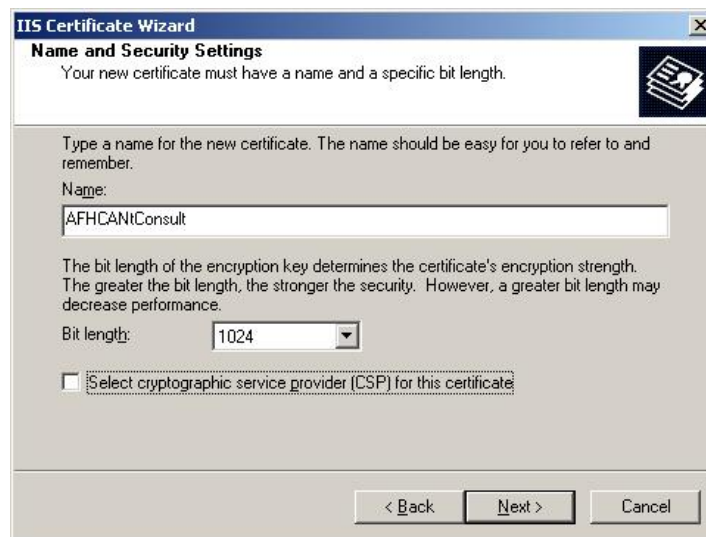
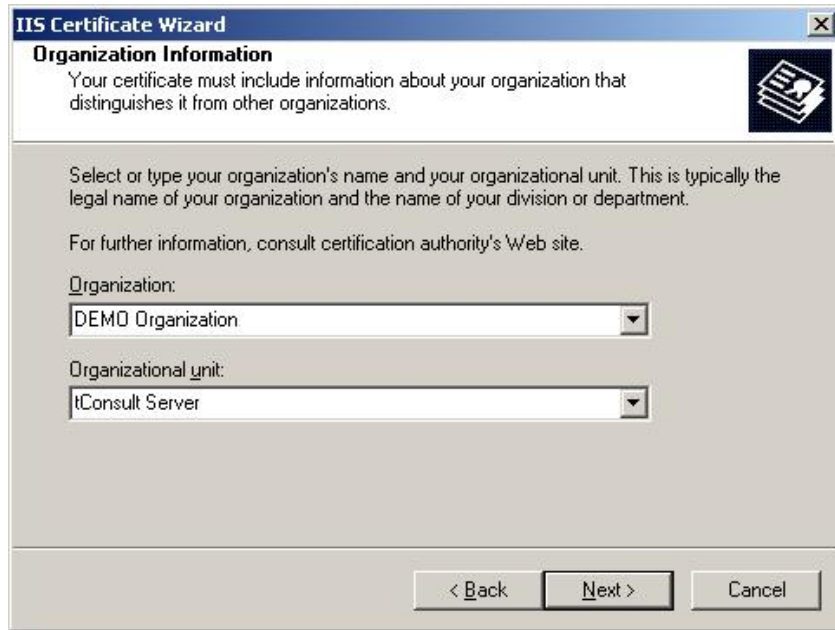


Figure 11 – Naming the Certificate

7. Enter the name of the Organization and the Organizational Unit. The Organizational Unit is whichever branch of the Organization that is ordering the certificate such as accounting, marketing, etc.



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Organization Information' and 'Your certificate must include information about your organization that distinguishes it from other organizations.' There is a small icon of a certificate on the right. The main area contains instructions: '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.' and 'For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization:' with 'DEMO Organization' selected, and 'Organizational unit:' with 'tConsult Server' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 12 – Organizational Information

8. Enter the FQDN (Fully Qualified Domain Name) for which you are requesting the SSL Certificate. Some third party vendors do allow the use of IP addresses – check with the third party certificate company where submitting this request.



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Your Site's Common Name' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Your Site's Common Name' and 'Your Web site's common name is its fully qualified domain name.' There is a small icon of a certificate on the right. The main area contains instructions: '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.' and 'If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' containing the text 'alfhcan-sqltest or IP Address'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 13 – Entering the FQDN

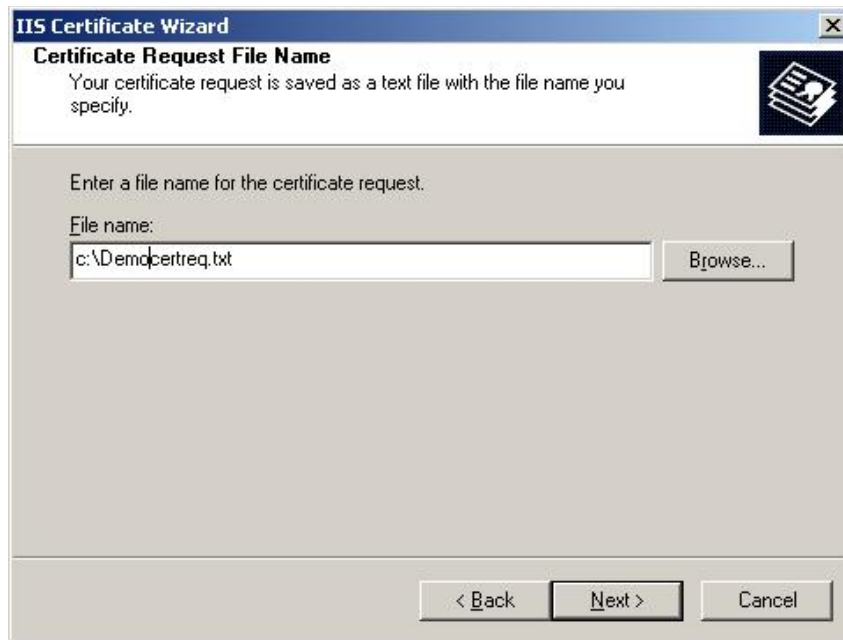
9. Select the Country/Region, enter the State/province and City/locality and then click on Next. This information is specific to the company and domain name and is collectively known as a Distinguished Name or DN. It is encoded within the certificate request.



The screenshot shows the 'IIS Certificate Wizard' window at the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Geographical Information' and 'The certification authority requires the following geographical information.' There is a small icon of a document with a key in the top right corner. The form contains three dropdown menus: 'Country/Region' with 'US (United States)' selected, 'State/province' with 'Alaska' selected, and 'City/locality' with 'Anchorage' selected. Below these is a note: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 14 – Information Specific to the Company and Domain Name

10. Enter a file name and location for this file to store this certificate request.



The screenshot shows the 'IIS Certificate Wizard' window at the 'Certificate Request File Name' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Certificate Request File Name' and 'Your certificate request is saved as a text file with the file name you specify.' There is a small icon of a document with a key in the top right corner. The form contains a text box labeled 'File name:' with the text 'c:\Dem\certreq.txt' entered. To the right of the text box is a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 15 – File Name and Location of Certificate Request

11. Request the file summary, and then click on Next.

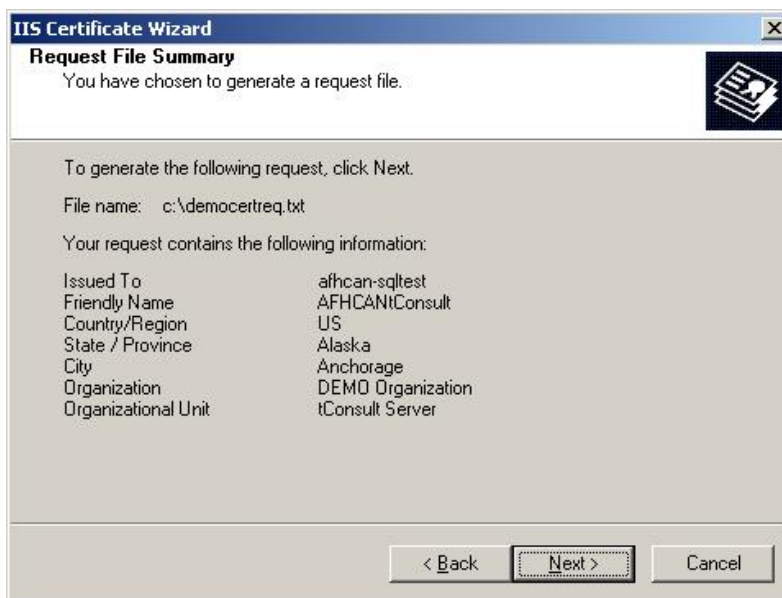


Figure 16 – Reviewing the Request File Summary

12. Click Finish at the Completion of the Web Server Certificate Wizard.



Figure 17 – Completing the Web Server Certificate Wizard

13. Create an email and submit the Certificate Request to the Third Party SSL Vendor who will be fulfilling this order. Upon receipt of a valid certificate from the Third Party SSL Vendor, place the certificate in the root of the C:\drive of the tConsult Server.

Installing the Third Party SSL Certificate into the Certificate Personal Store

The steps listed here install the Third Party SSL Certificate into the Certificate Personal Store on the tConsult Server.

1. Open an MMC (Microsoft Management Console) and select Add/Remove Snap-in, then click on Add.

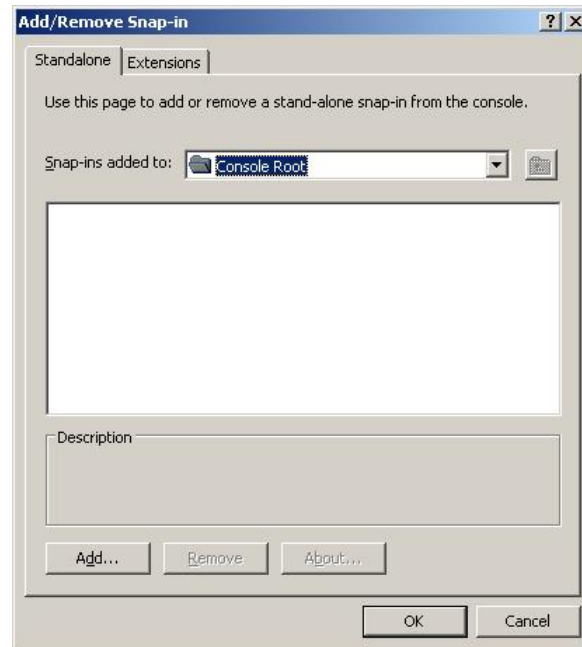


Figure 18 – Add/Remove Snap-In Dialog Box

2. Select Certificates then click on Add.



Figure 19 – Selecting Certificates

3. Ensure the radio button for Computer account is selected. Click on Next.

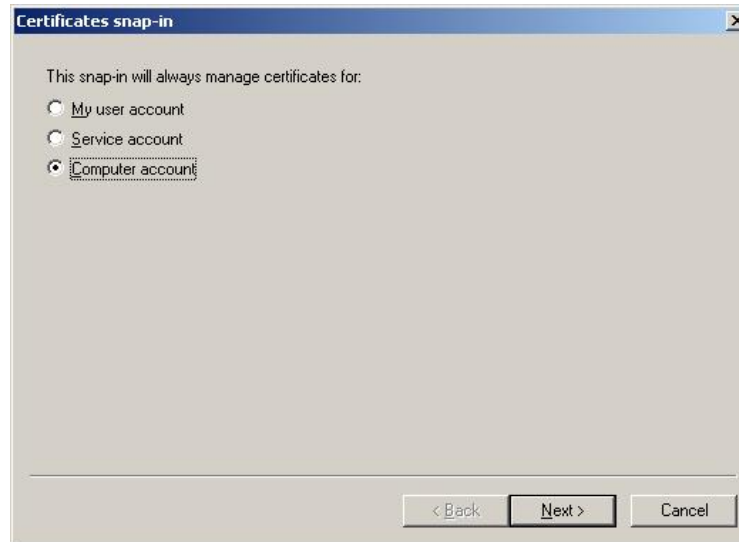


Figure 20 – Managing Certificates for Computer Account

4. Select Local computer, then click on Finish.



Figure 21 – Designating Local Computer to Manage

5. Click on the Close button to close the Add Standalone Snap-in dialog box.

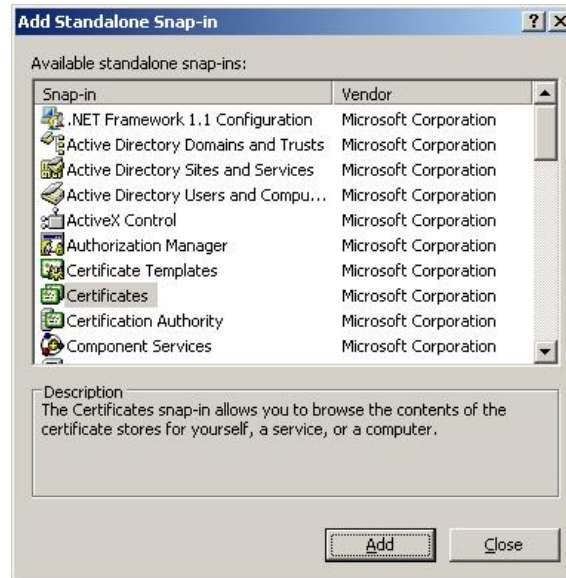


Figure 22 – Close the Add Standalone Snap-In

6. Click on Ok to return to view the Certificates MMC.

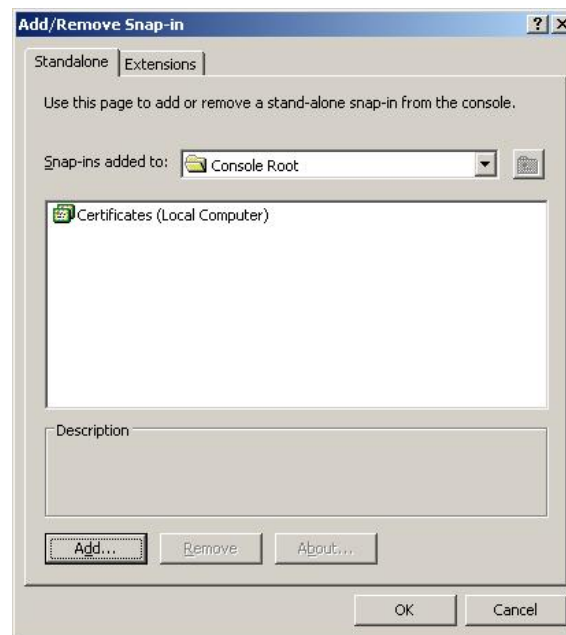


Figure 23 – Close Add/Remove Snap-in to view Certificates MMC

7. Expand the Console Root in the left pane to reveal Personal Certificates under Certificates (Local Computer). AFHCAN Telehealth Signing will show in the pane to the right.

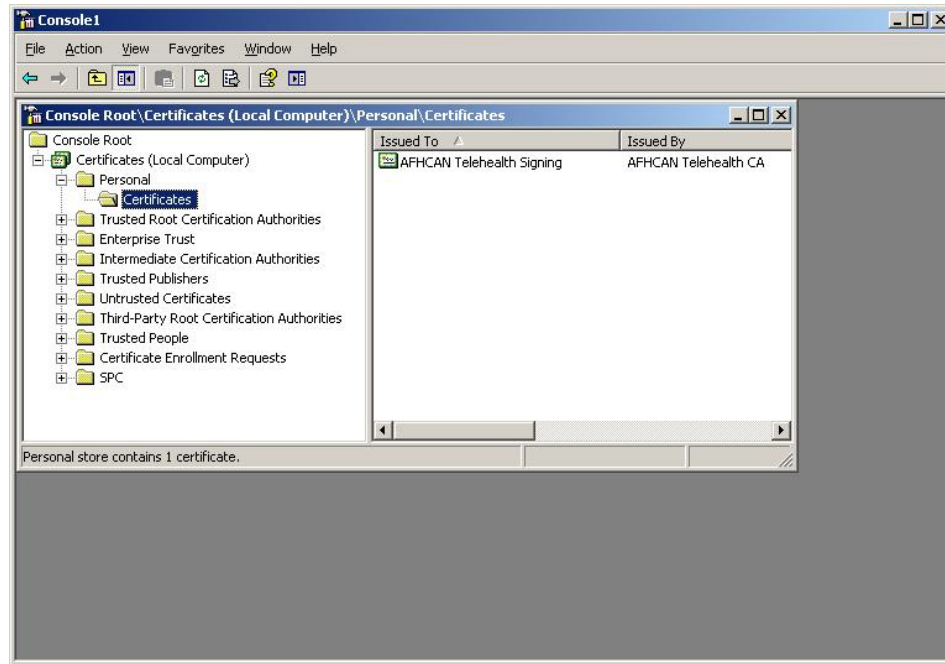


Figure 24 – Certificates MMC

8. With Certificates highlighted as shown in Figure 24, do a right mouse-click and choose Import. The Certificate Import Wizard will open. Click on Next.



Figure 25 – Certificate Import Wizard Welcome Screen

9. Browse to the location where the Third Party SSL Certificate was placed on the tConsult Server. Change the Files of type to Personal Information Exchange (*.pfx,*.p12) to see the certificate. Select the certificate and click on Open.

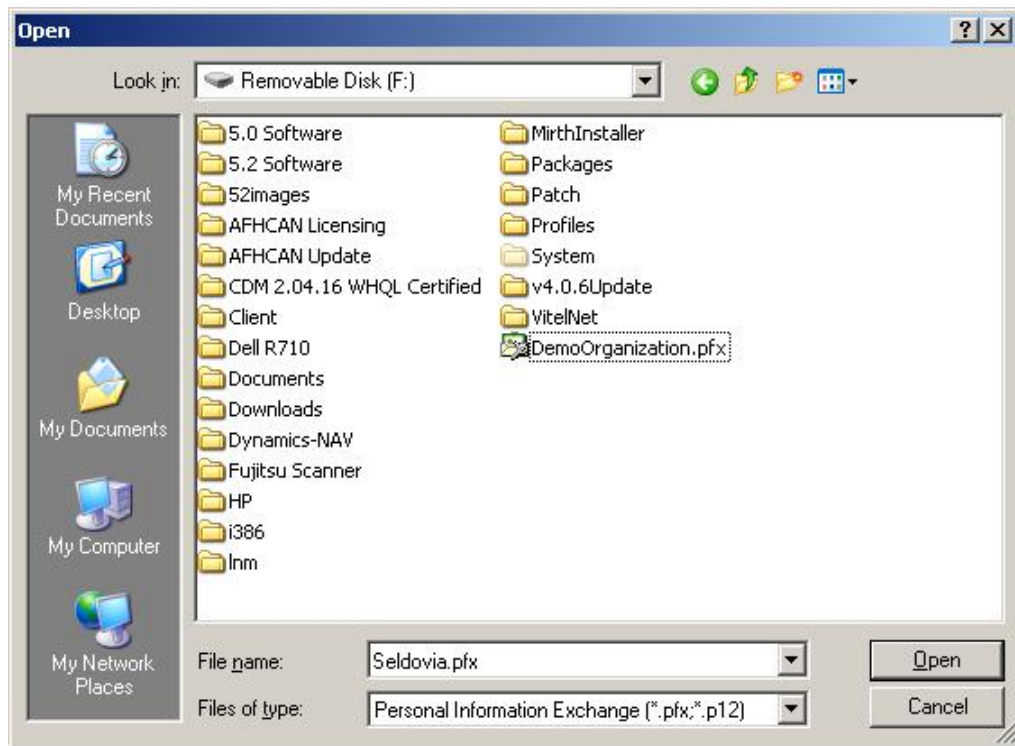


Figure 26 – Browsing to the Third Party SSL Certificate

10. Click on Next.

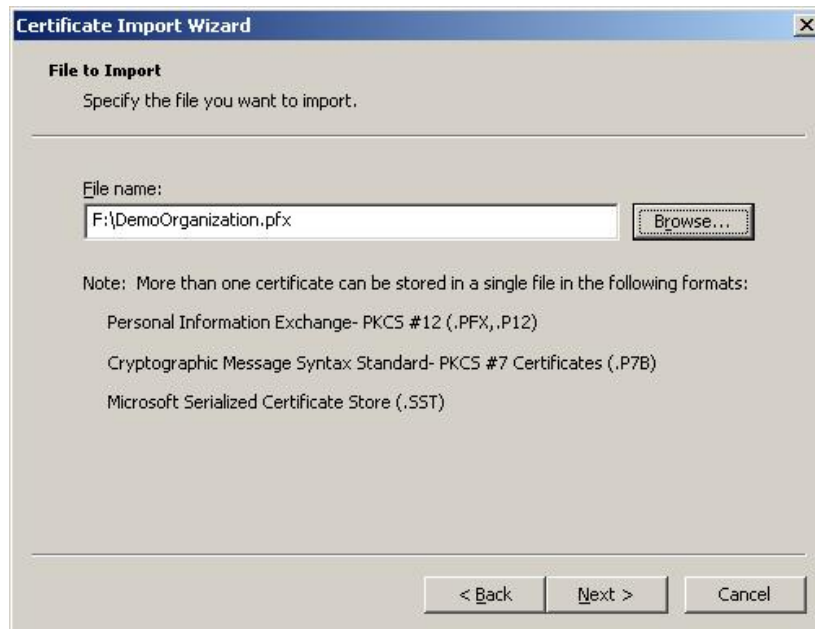


Figure 27 – Specifying the Correct Certificate to be Imported

11. Leave the password field blank. Place a checkmark in front of “Mark this key as exportable. This will allow you to back up or transport your keys at a later time”. Click on Next.



Figure 28 – Marking the Key Exportable

12. Place the Certificate into the Certificate Personal Store, and then click on Next.



Figure 29 – Placing the Certificate into the Certificate Personal Store

13. After verifying the settings, click on Finish to complete the Certificate Import Wizard.



Figure 30 – Completing the Certificate Import Wizard

14. By default, a tConsult Server built to AFHCAN specifications will have the Update Root Certificates turned off. There are two steps to enabling Update Root Certificates:

a. Using Control Panel, click on Add/Remove Programs:

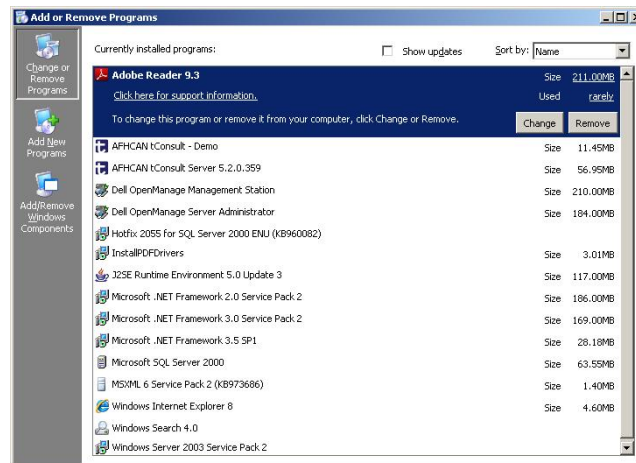


Figure 31 – Add or Remove Programs

b. Click on Add/Remove Windows Components. As seen on the bottom left of Figure 31. Scroll down to place a checkmark in front of Update Root Certificates, then click on Next.

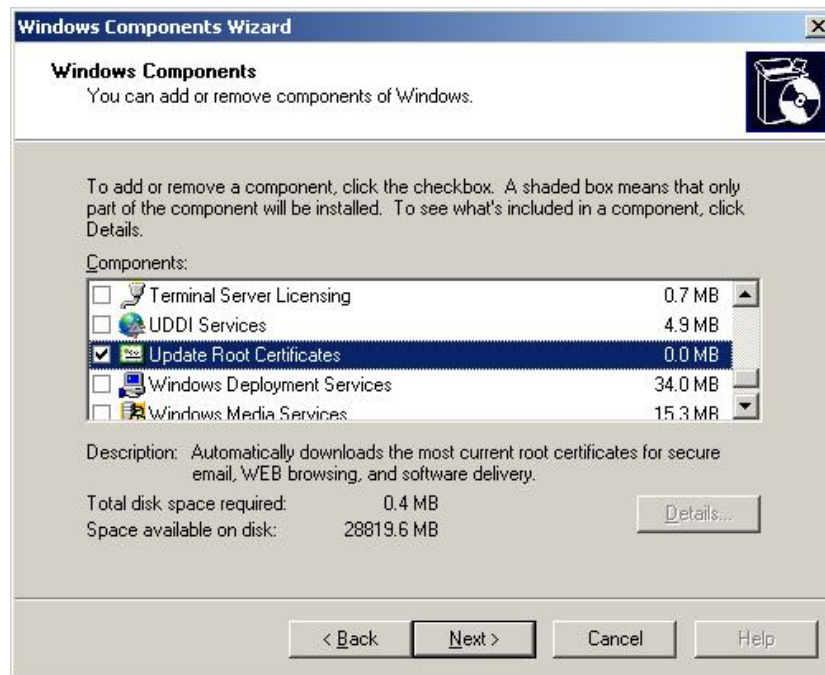


Figure 32 – Enabling Update Root Certificates

- c. Click on Finish when the Windows Components install is complete.



Figure 33 – Completing the Windows Components Wizard

- d. Within Computer Management under Services, ensure the Windows Update Service is enabled, set to Automatically start up, and start the service.

15. There now will show two certificates in the Certificate Personal Store. To verify that there is a trusted cert in the trusted root certification store; double-click on the imported personal certificate. Close the MMC by clicking on the X in the upper right hand corner.

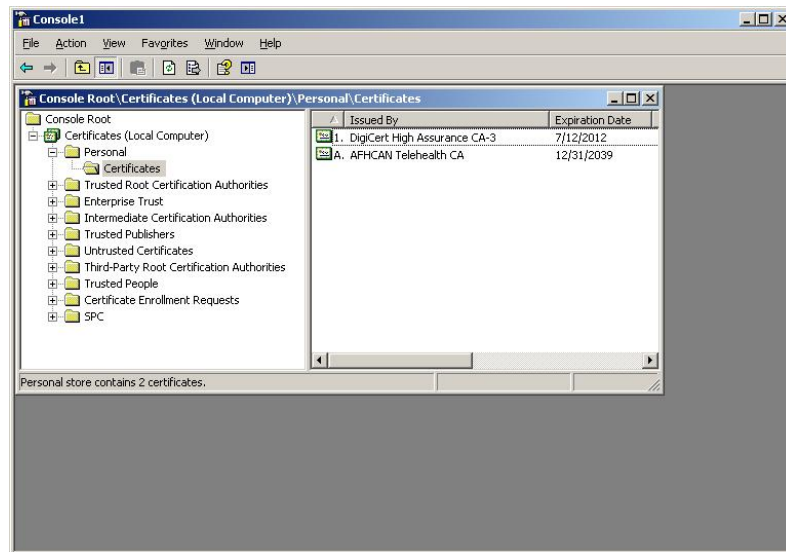


Figure 34 – Certificates MMC

Installing the Third Party SSL Certificate into IIS

1. Using IIS Manager on the tConsult Server, expand the Web Sites until tConsult website is located.

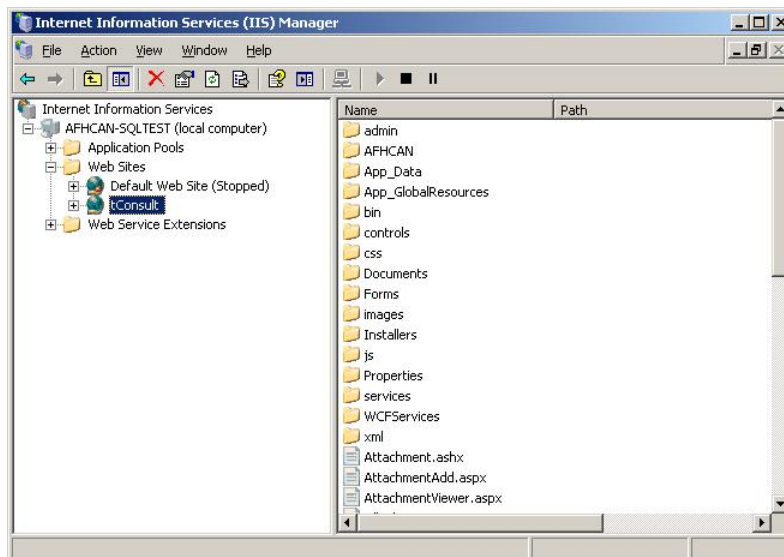


Figure 35 – IIS Manager

2. Do a right mouse-click on the tConsult website and select Properties. Click on the Directory Security tab. Click on the Server Certificate button.

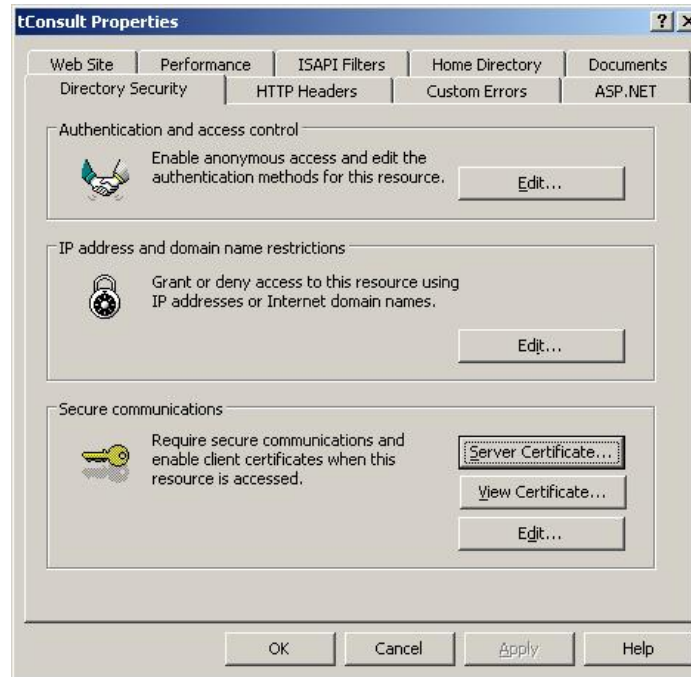


Figure 36 – Directory Security tab of the tConsult Website Properties

3. This will open the Web Server Certificate Wizard. Click on Next.



Figure 37 – Web Server Certificate Wizard

4. With the “Process the pending request and install the certificate” radial button selected, click on Next.

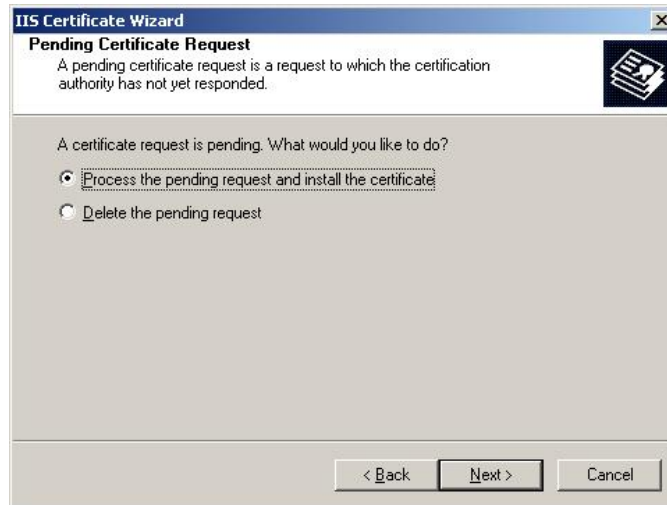


Figure 38 – Pending Certificate Request Dialog Box

5. Browse to the location where the Third Party SSL Certificate was placed on the tConsult Server and click on Next.

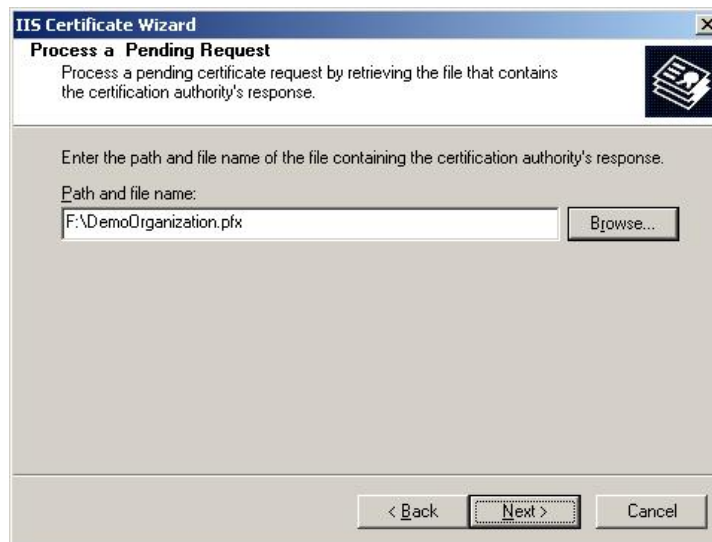


Figure 39 – Entering the Path and File Name of the Third Party SSL Certificate

6. Accept the default port the tConsult Website should use and click on Next.

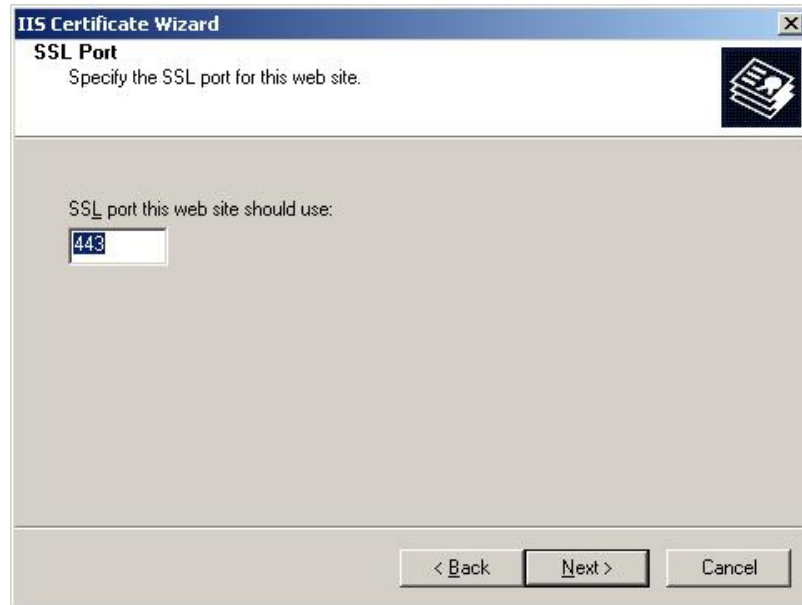


Figure 40 – SSL Port for tConsult Website

7. A review of the SSL Certificate will display. Click on Next.

NOTE: The illustration in Figure 41 is a representative example.



Figure 41 – Web Server Certificate Summary

8. Click on Finish to complete the Web Server Certificate Wizard.

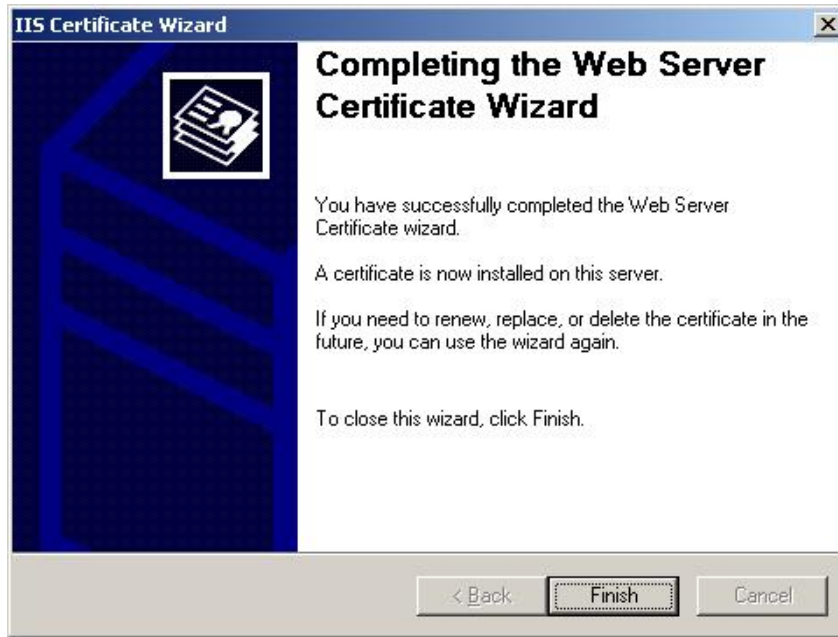


Figure 42 – Completing the Web Server Certificate Wizard

End of procedure.