



Lab - Create Self-Signed Certificate in IIS

Overview

In this lab, you will learn how to create a self-signed certificate and bind to a site in IIS. A self-signed certificate is a certificate that is signed by itself rather than a trusted third party such as Microsoft or VERITAS.

By using self-signed certificates, no PKI (Public Key Infrastructure) needs to be deployed before/after deployment of server-side applications. However, using self-signed certificates has both advantages and disadvantages.

Advantages

1. No PKI (Public Key Infrastructure) is needed.
2. Automatic deployment (Usually Self-signed certificates are created automatically during the installation process of the server-side applications).

Disadvantages

1. Other applications/operating systems will not trust the certificates. This may lead to authentication errors etc.

Note: To overcome this limitation, some IT staff add the self-signed certificates to the Trusted Roots Certificate Authorities. However, using this workaround may take additional time that is needed for management and troubleshooting. **(Covered in this lab)**

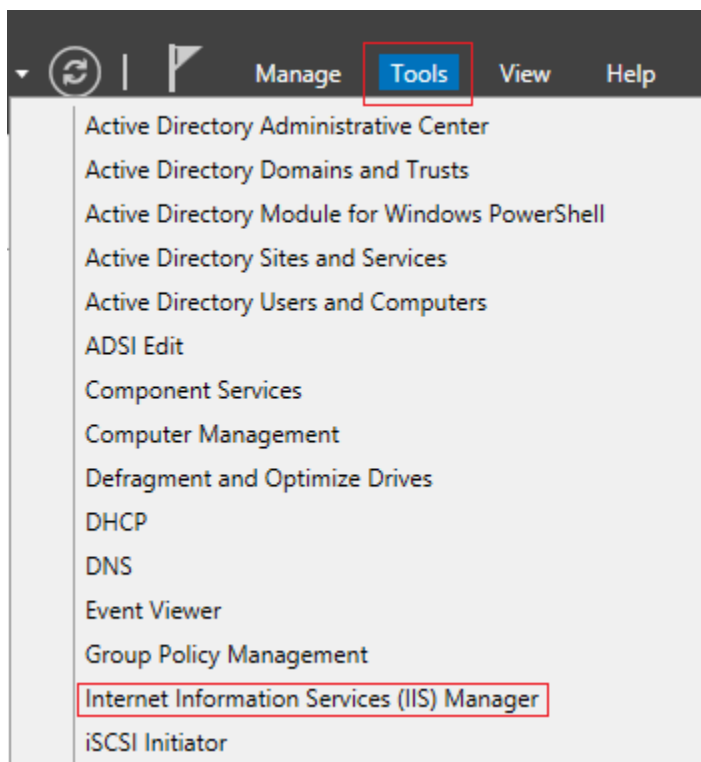
2. Self-signed certificates lifetime is usually one year. Before the year has ended, the certificate may need to be renewed/replaced.
3. Self-signed certificates may use low hash and cipher technologies. Due to this, the security level that is implemented by self-signed certificates may not satisfy the current Security Policy.
4. No support for advanced PKI (Public Key Infrastructure) functions (e.g., Online checking of the revocation list, etc.).
5. Most of the advanced features of server-side applications require a PKI (Public Key Infrastructure). Self-signed certificates can't be used.

Lab Requirements

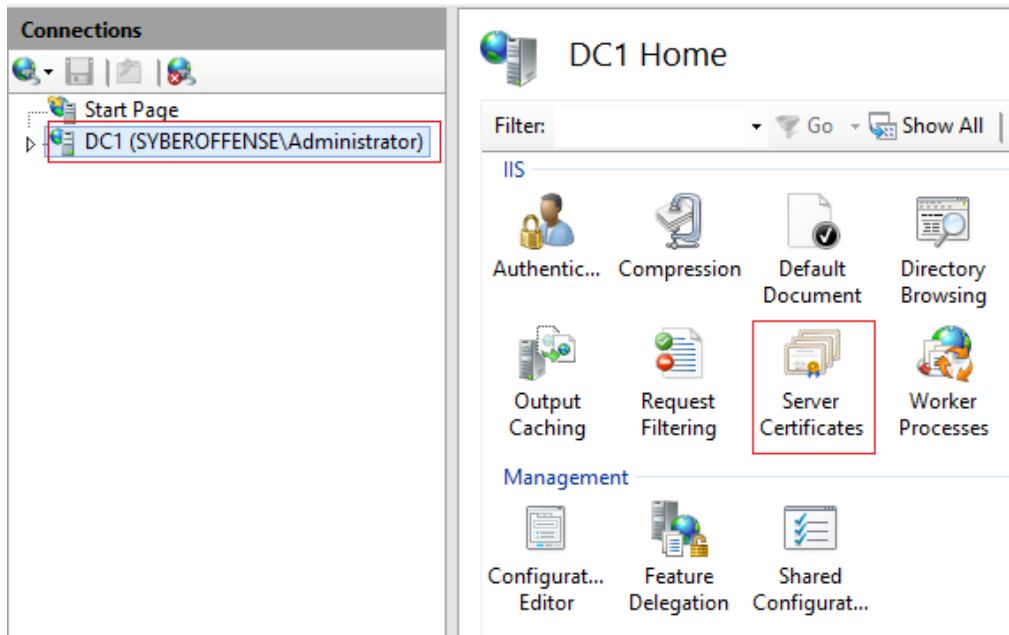
- One virtual install of Server 2012 or 2016 Full GUI running as a domain controller
- Web Services (IIS) installed

Begin the lab

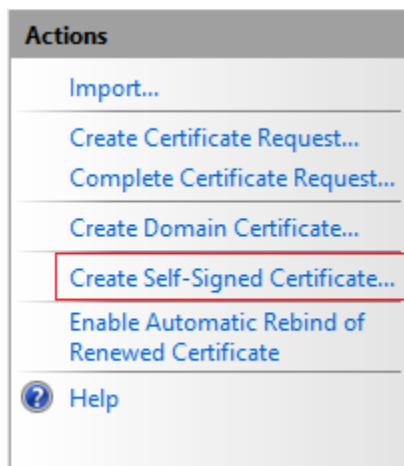
From Server Manager, go to the top right corner and click on tools. From the selection of snap-ins, Internet Information Services (IIS) Manager.



Inside the left window pane of your IIS management console, click on the name of your server. From the right window pane, click on Server Certificates.



In the far-right window pane, click on Create a self-signed Certificate.

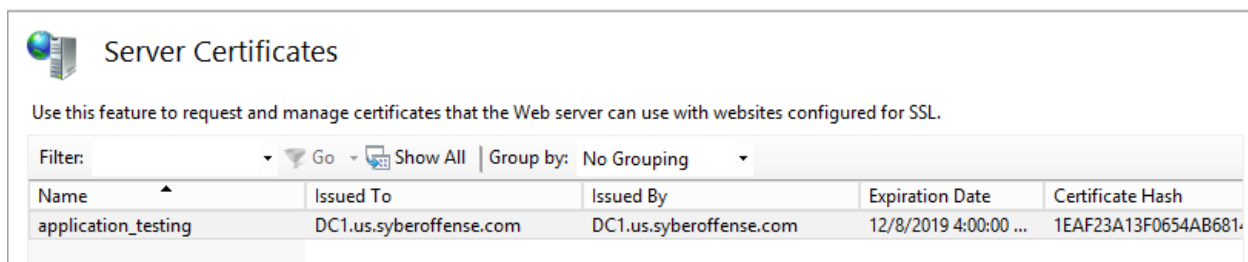


In the specify a Specify a Friendly Name window, type a name the signifies what the certificate will be used for. In this example, we are using this certificate for the testing of an application being developed in-house. This makes sense as we would not want to purchase a certificate from a trusted source just for testing purposes.

Leave the certificate store location as personal. If the certificate were to be used for hosting a website, we would change the location from personal to web hosting.

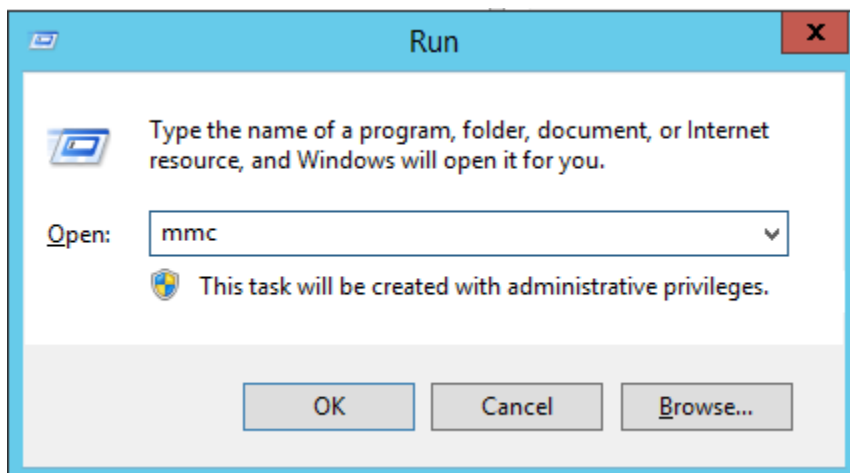


The certificate appears in the center window pane.

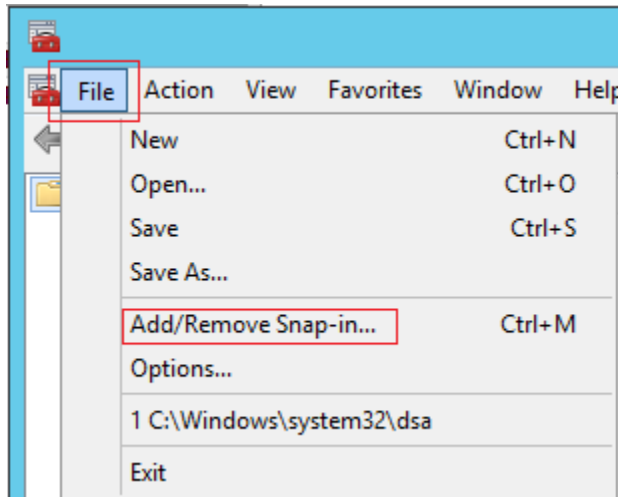


We can now go to the certificate store to view the certificate.

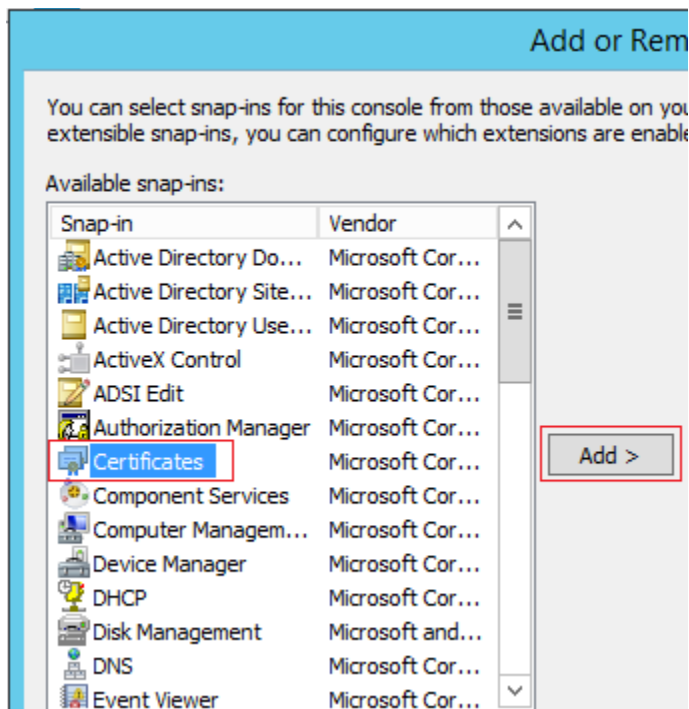
From your keyboard, press the Window+R key to open a run line. In the run line, type MMC, short for Microsoft Management Console. Click OK.



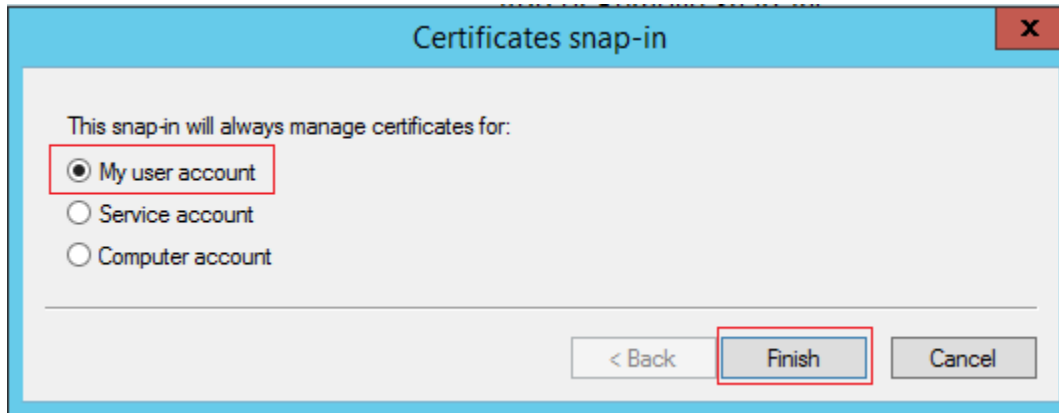
Click on File>Add/Remove Snap-in



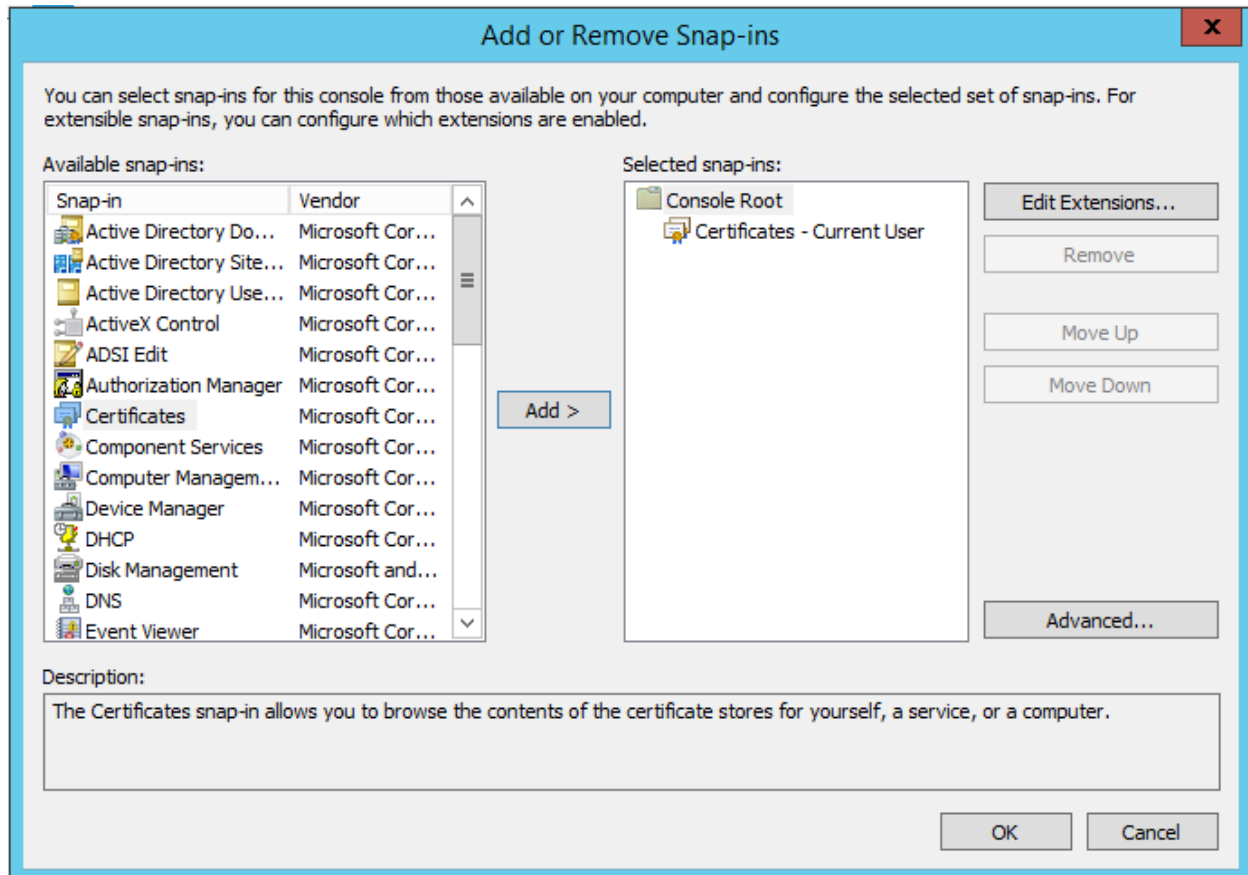
From the list of available snap-ins, click on Certificates and then the Add> button.




On this next screen, accept the default for My user account and click finish



The snap-in is now ready to be added to the MMC console. Click OK.



Expand the Certificate-Current User and the Trusted Root container. In the center window pane, you can see the certificate we just created.

 **Server Certificates**

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate Hash
application_testing	DC1.us.syberoffense.com	DC1.us.syberoffense.com	12/8/2019 4:00:00 ...	1EAF23A13F0654AB681...

Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certifi...]

File Action View Favorites Window Help

Console Root

- Certificates - Current User
 - Personal
 - Trusted Root Certification Authorities
 - Certificates
 - Enterprise Trust
 - Intermediate Certification Authorities
 - Active Directory User Objects
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certificates
 - Trusted People
 - Client Authentication Issuance
 - Smart Card Trusted Root Certificates

Issued To	Issued By	Expiration Date	Actions
Class 3 Public Primary Certif...	Class 3 Public Primary Certificatio...	8/1/2028	Certifica... More ...
Class 3 Public Primary Certif...	Class 3 Public Primary Certificatio...	1/7/2004	
Copyright (c) 1997 Microsof...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	
DC1.us.syberoffense.com	DC1.us.syberoffense.com	12/8/2019	
Microsoft Authenticode(tm)...	Microsoft Authenticode(tm) Root...	12/31/1999	
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	
Microsoft Root Certificate A...	Microsoft Root Certificate Authori...	5/9/2021	
Microsoft Root Certificate A...	Microsoft Root Certificate Authori...	6/23/2035	
Microsoft Root Certificate A...	Microsoft Root Certificate Authori...	3/22/2036	
NO LIABILITY ACCEPTED, (c)...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	
VeriSign Class 3 Public Prim...	VeriSign Class 3 Public Primary Ce...	7/16/2036	
VeriSign Universal Root Certi...	VeriSign Universal Root Certificati...	12/1/2037	

From the certificate snap-in, right click on our new certificate and select All Tasks > Export.

Issued To	Issued By	Expiration Date
Class 3 Public Primary Certif...	Class 3 Public Primary Certificatio...	8/1/2028
Class 3 Public Primary Certif...	Class 3 Public Primary Certificatio...	1/7/2004
Copyright (c) 1997 Microsof...	Copyright (c) 1997 Microsoft Corp.	12/30/1999
DC1.us.syberoffense.com	DC1.us.syberoffense.com	12/8/2019
Microsoft A...	Microsoft Authenticode(tm) Root...	12/31/1999
Microsoft R...	Microsoft Root Authority	12/30/2020
Microsoft R...	Microsoft Root Certificate Authori...	5/9/2021
Microsoft R...	Microsoft Root Certificate Authori...	6/23/2035
Microsoft R...	Microsoft Root Certificate Authori...	3/22/2036
NO LIABILI...	BILITY ACCEPTED, (c)97 V...	1/7/2004
Thawte Tim...	Timestamping CA	12/31/2020
VeriSign Cla...	Class 3 Public Primary Ce...	7/16/2036
VeriSign Uni...	VeriSign Universal Root Certificati...	12/1/2037

Right-click context menu for DC1.us.syberoffense.com:

- Open
- All Tasks
 - Open
 - Export...
- Cut
- Copy
- Delete
- Properties
- Help

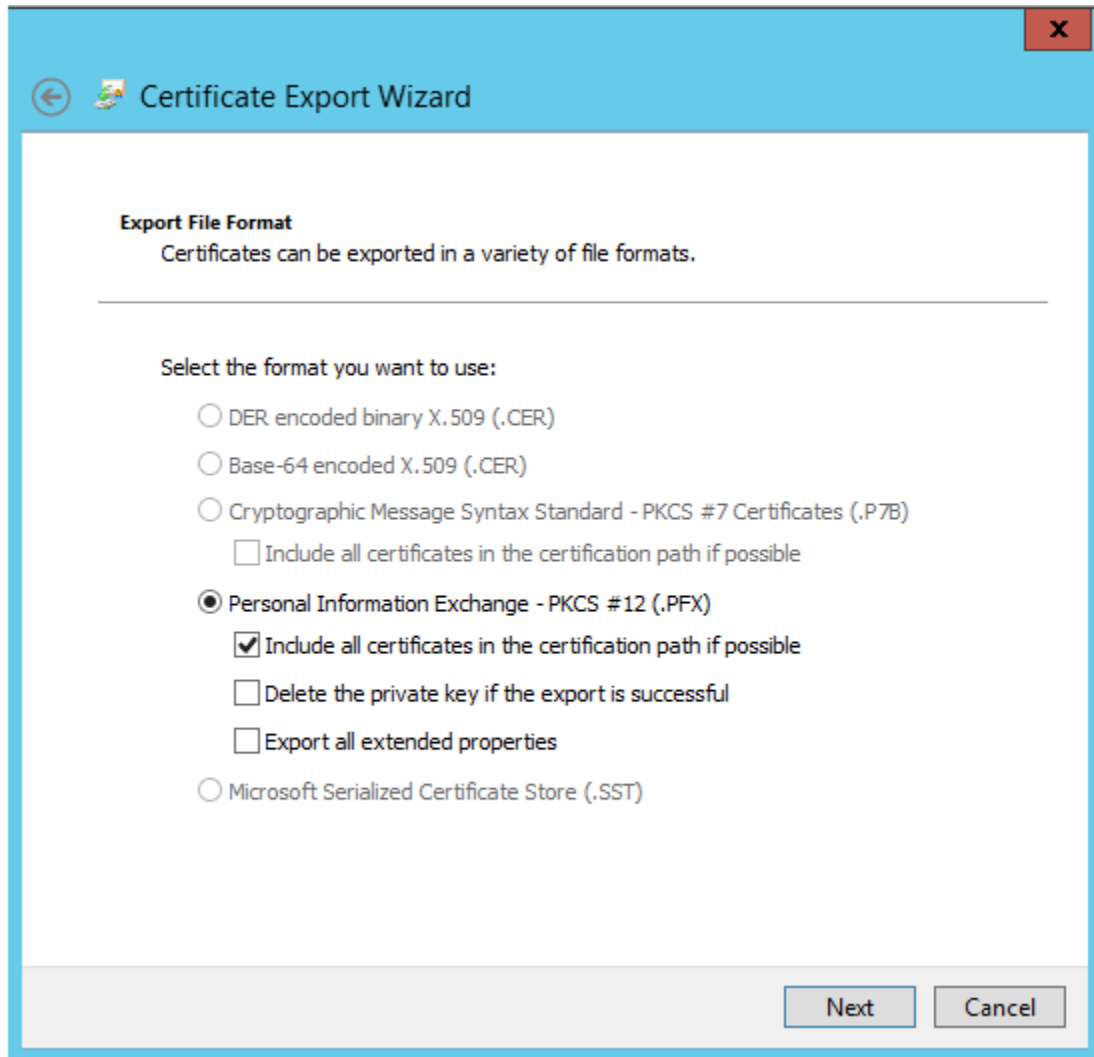
This brings up the Certificate Export Wizard.



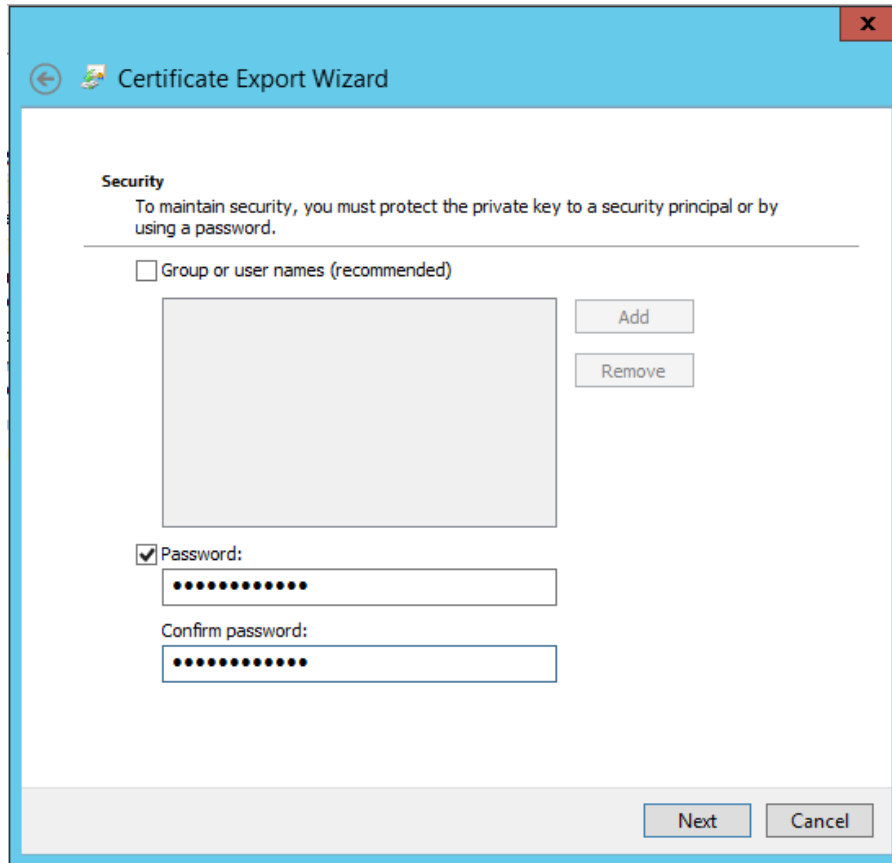
Click next and on the next window, select Yes, export the private key and click next.



Ensure the Personal Information Exchange -PKCS #12 (.PFX) option is selected and the box the first box from the list of options is checked as well. Click next.

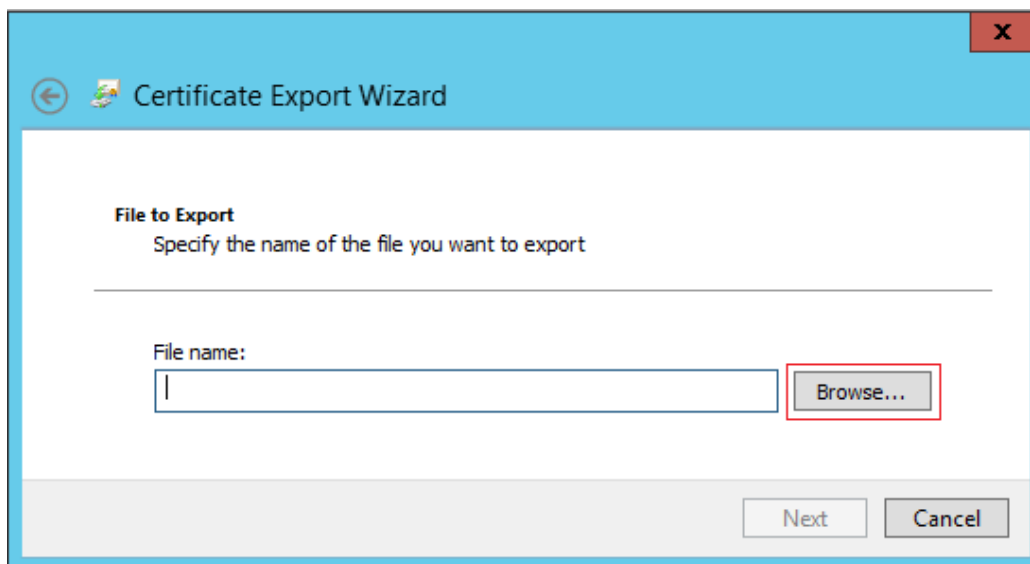


On the next screen, check the box for using a password. Type in any password you want.



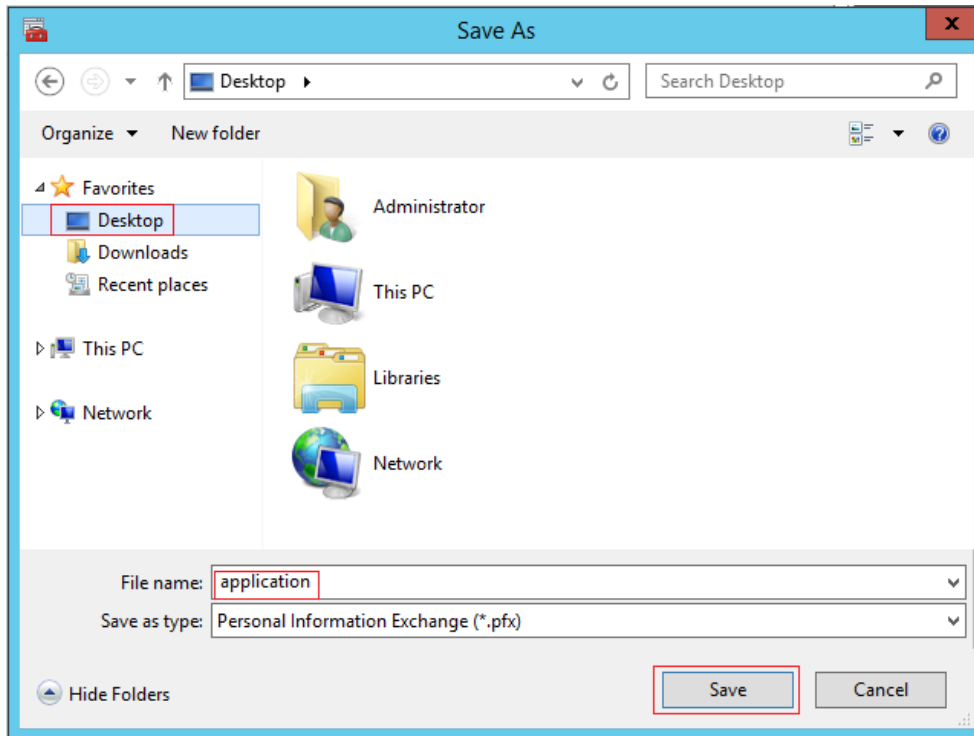
The screenshot shows the 'Security' step of the 'Certificate Export Wizard'. The window has a blue title bar with a back arrow, a forward arrow, and a close button. The title is 'Certificate Export Wizard'. Below the title bar, there's a section titled 'Security' with the instruction: 'To maintain security, you must protect the private key to a security principal or by using a password.' There are two options: 'Group or user names (recommended)' which is unchecked, and 'Password' which is checked. The 'Group or user names' option has a large empty box and 'Add' and 'Remove' buttons. The 'Password' option has two text boxes: 'Password:' and 'Confirm password:', both filled with dots. At the bottom right, there are 'Next' and 'Cancel' buttons.

On the next screen, click the browse button.

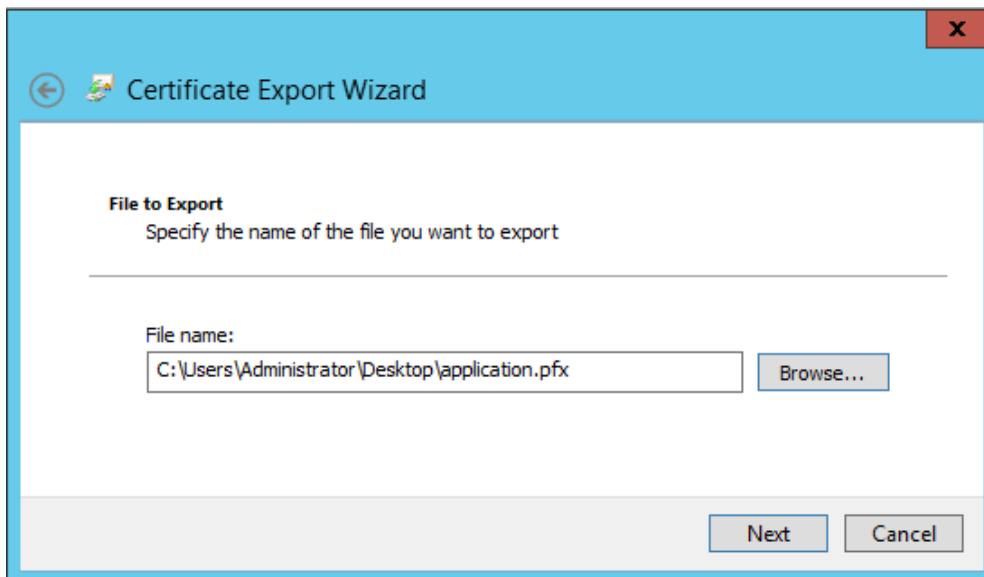


The screenshot shows the 'File to Export' step of the 'Certificate Export Wizard'. The window has a blue title bar with a back arrow, a forward arrow, and a close button. The title is 'Certificate Export Wizard'. Below the title bar, there's a section titled 'File to Export' with the instruction: 'Specify the name of the file you want to export'. There is a text box labeled 'File name:' which is empty. To the right of the text box is a 'Browse...' button, which is highlighted with a red rectangle. At the bottom right, there are 'Next' and 'Cancel' buttons.

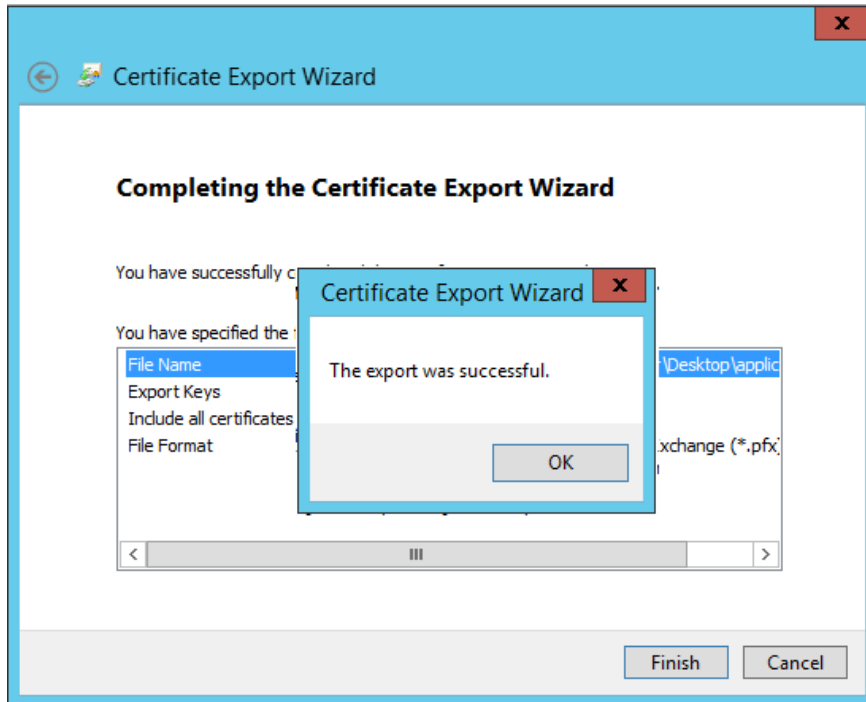
On the next screen, select the Desktop. Choose a file name to use for the export. In this example, I have named the exported file, application and saved it to the servers Desktop.



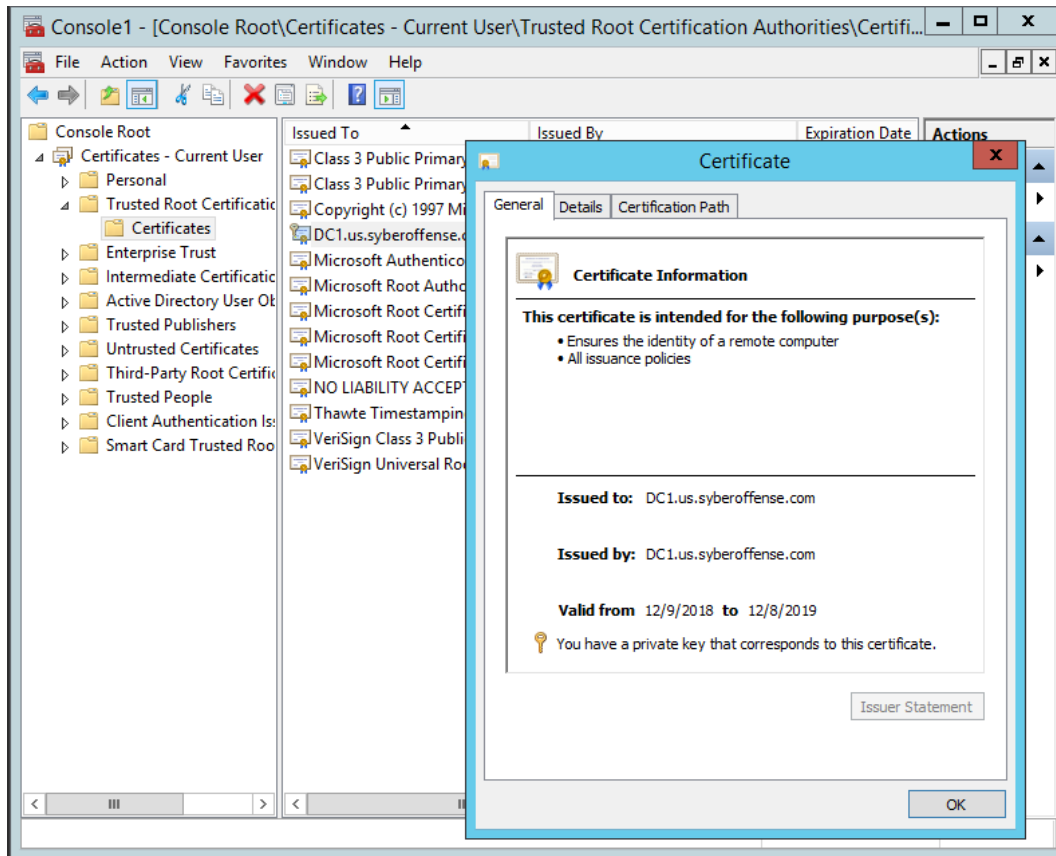
On the next screen, click the Next button.



On the Complete the Certificate Export Wizard screen, click finish and then click OK.

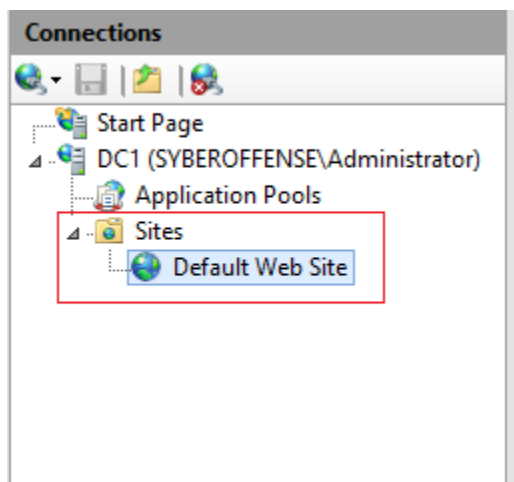


Minimize any open windows and find the certificate saved the desktop. To view the certificate, bring up your certificate snap-in, find the certificate and x2 click to view.

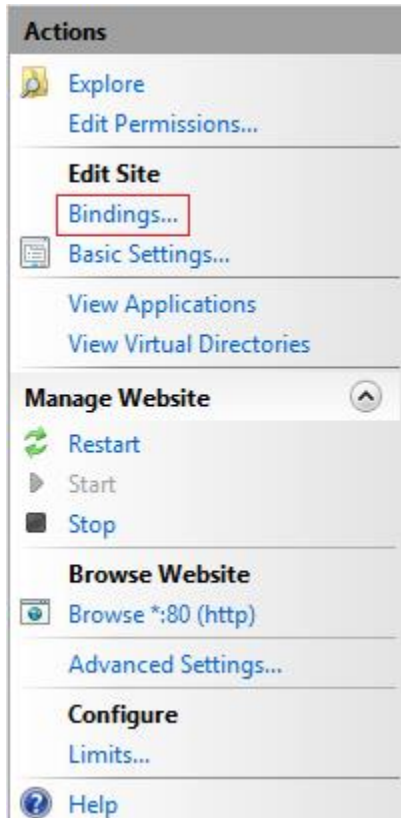


Bind a Certificate to a site

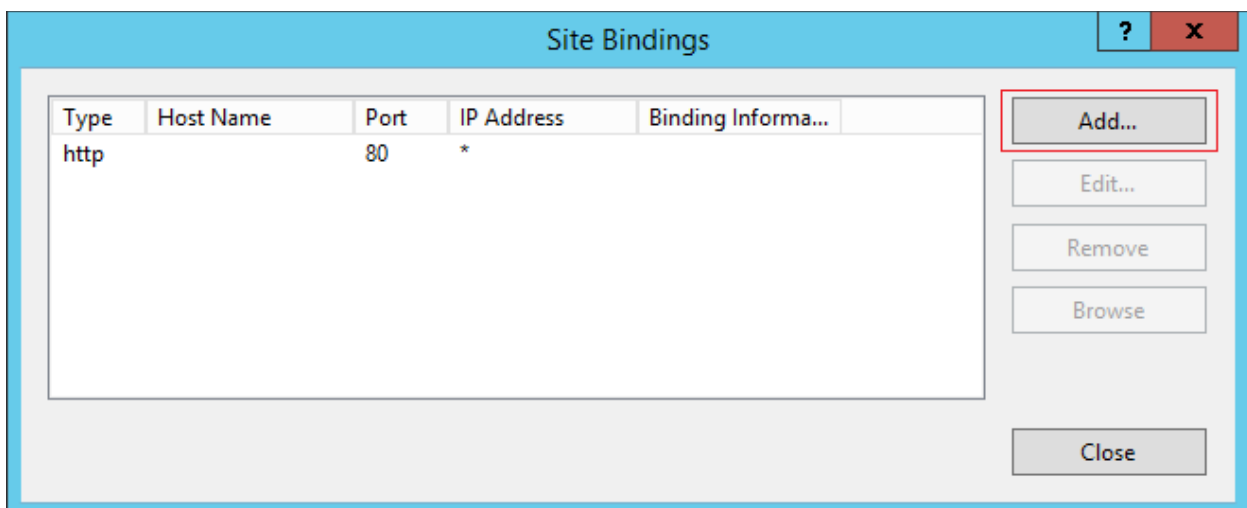
Bring up your IIS management console. In the left windows pane, click on Sites and then click on your Default Web Site.



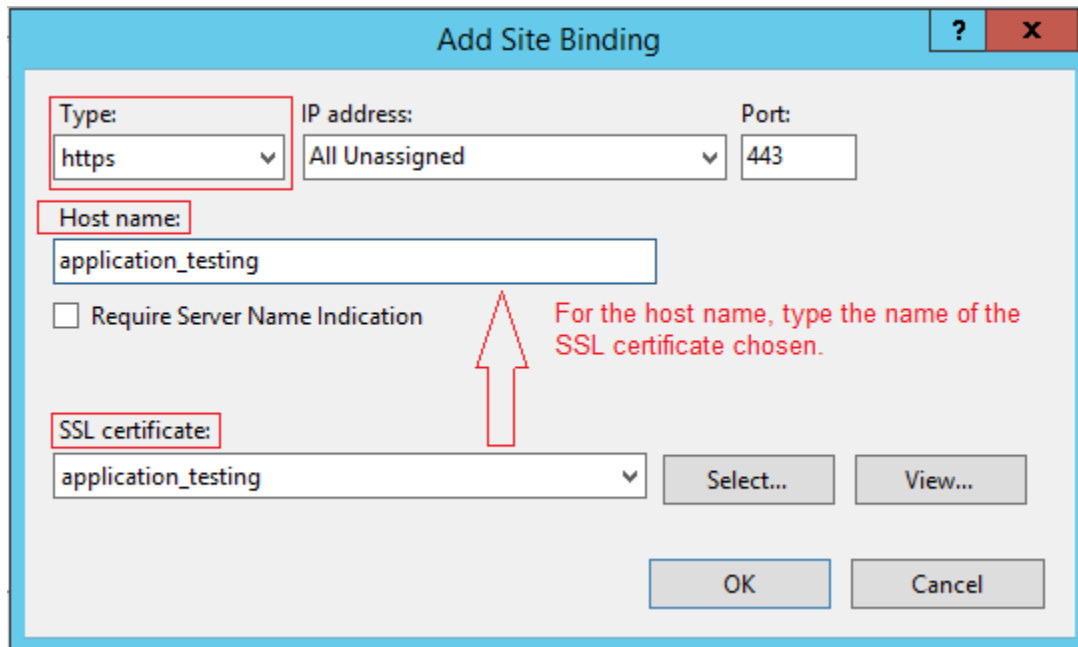
Over on the far-right Action window pane, click on bindings.



On the next window, click the Add button.



On the next screen, under the Type option, pull down the windows and select https. Under the SSL certificate, pull down the window and select the name of the certificate we created. Under Host names, type the name of the SSL certificate you selected. Click OK.

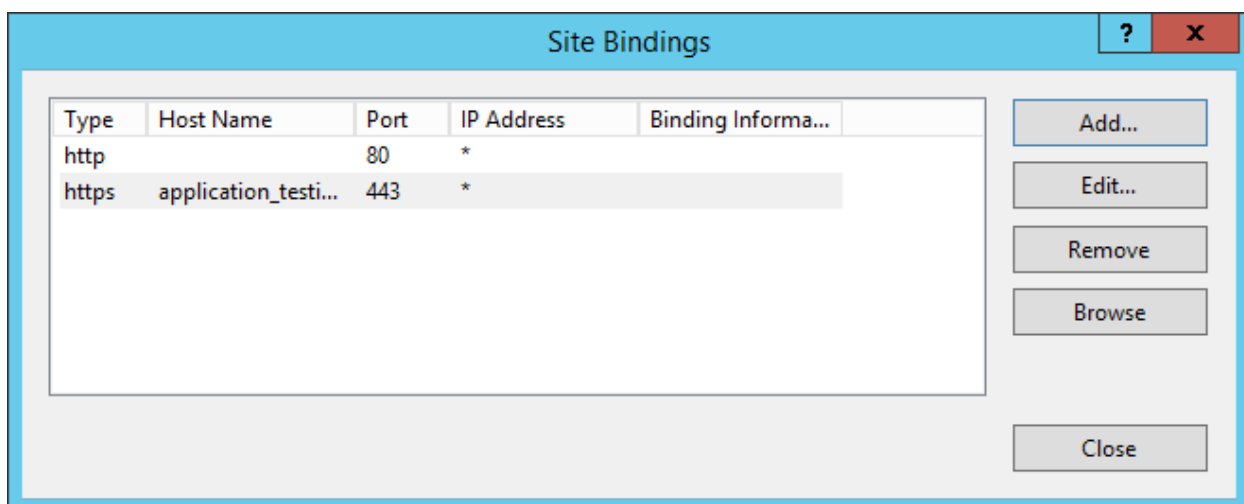


The 'Add Site Binding' dialog box contains the following fields and controls:

- Type:** A dropdown menu with 'https' selected.
- IP address:** A dropdown menu with 'All Unassigned' selected.
- Port:** A text box containing '443'.
- Host name:** A text box containing 'application_testing'.
- ☐ **Require Server Name Indication**
- SSL certificate:** A dropdown menu with 'application_testing' selected.
- Select...** and **View...** buttons next to the SSL certificate dropdown.
- OK** and **Cancel** buttons at the bottom.

A red arrow points from the text 'For the host name, type the name of the SSL certificate chosen.' to the 'Host name' text box.

On the next window, click close.



The 'Site Bindings' dialog box displays a table of bindings and a set of action buttons on the right.

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https	application_testi...	443	*	

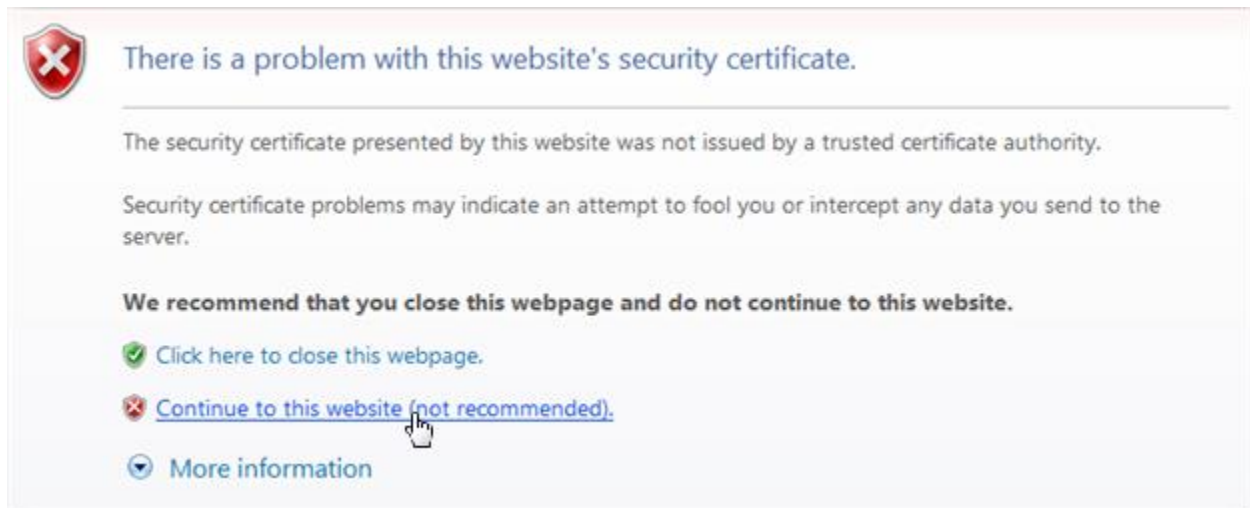
Buttons on the right: **Add...**, **Edit...**, **Remove**, **Browse**, and **Close**.

Users can now use HTTPS to browse the default web site.

Summary

In this lab, we learned how to generate a self-signing certificate using IIS removing the need of having to create a PKI infrastructure and manage a certificate server. For creating a temporary certificate for an application or website development, this a quick and easy way to create an SSL certificate for an internal trusted source. The trick is to ensure the certificate is placed inside the trusted root certificate folder on the web server and the user can import the certificate to their local machine using their browser.

With a self-signing certificate from an untrusted source, the user will see the following security warnings in most browsers.

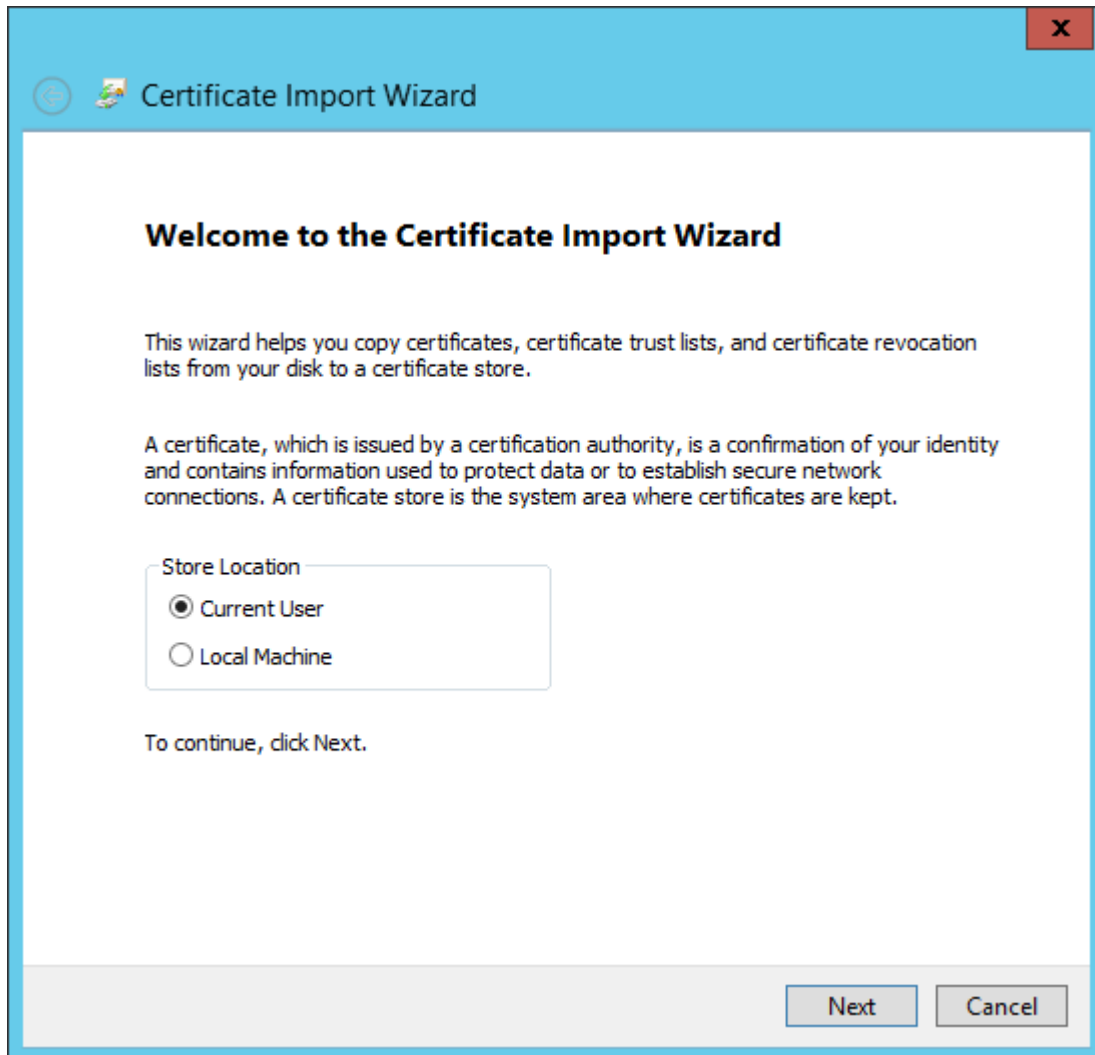


The user can proceed onto the website or import the self-signed certificate to their local machine.

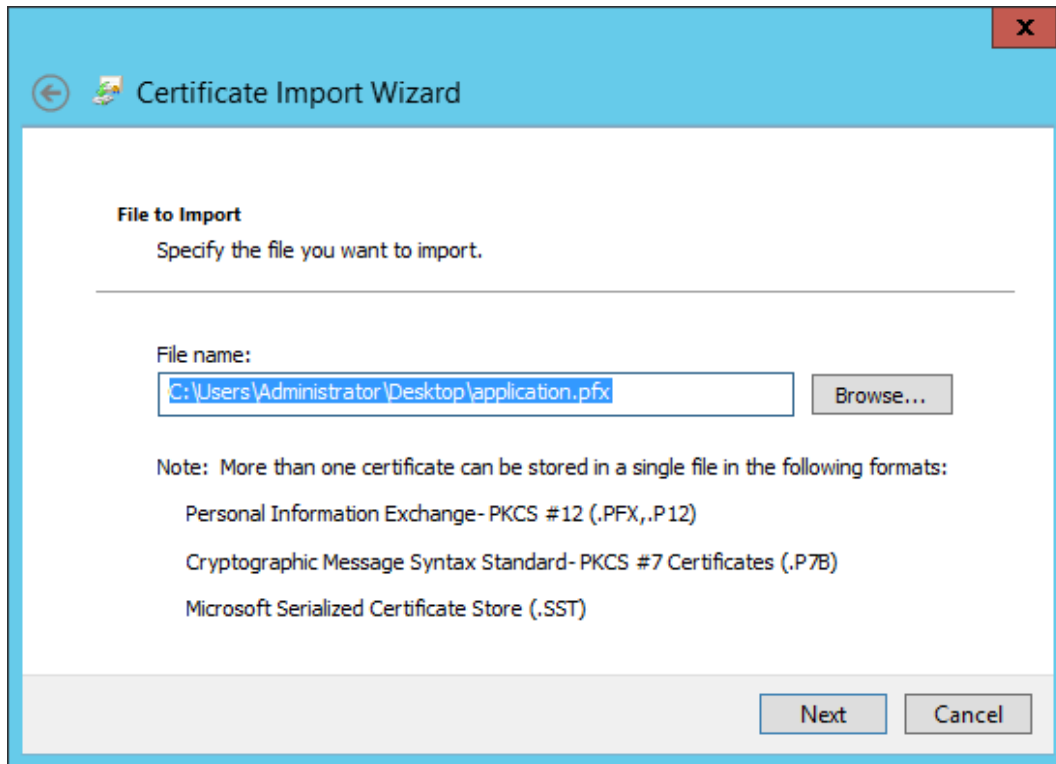
Importing the self-signed certificate to the client machine

Copy the certificate which was exported from the server (the PFX file) to the client's machine or ensure it is available from a network path.

From the client's machine, right click on the certificate and select install. On the first screen, select Current User.



On the next screen, verify the certificate you are importing.



The image shows a Windows-style dialog box titled "Certificate Import Wizard". It has a blue header bar with a back arrow icon and a close button (X). The main content area is white and contains the following text:

File to Import
Specify the file you want to import.

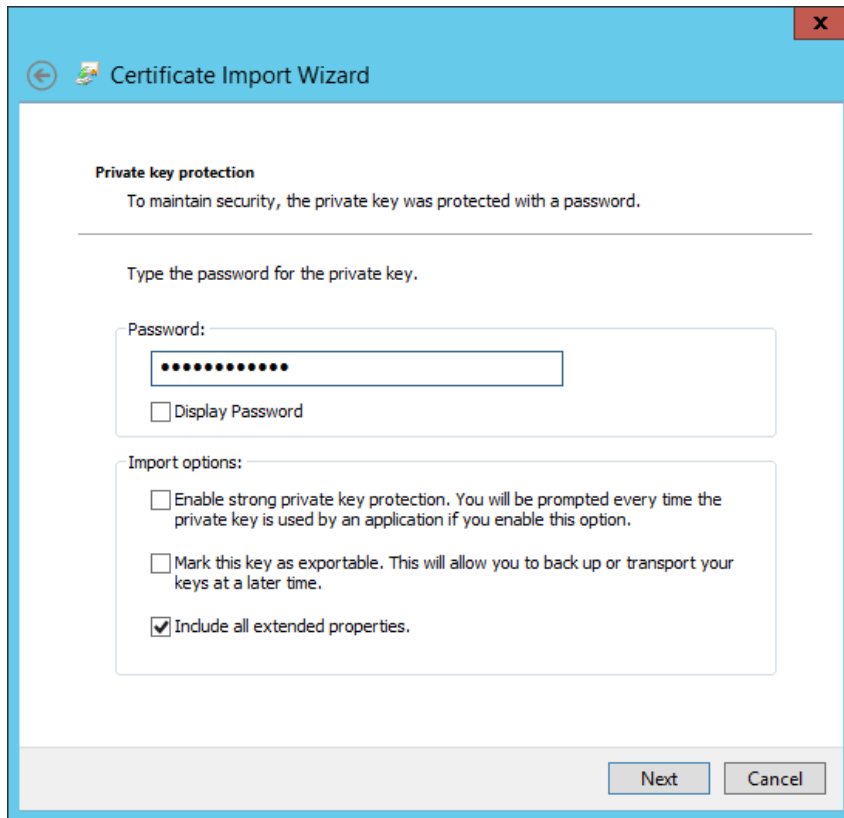
File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

At the bottom right, there are two buttons: "Next" and "Cancel".

Type in the certificate's password we create at the beginning of the lab.

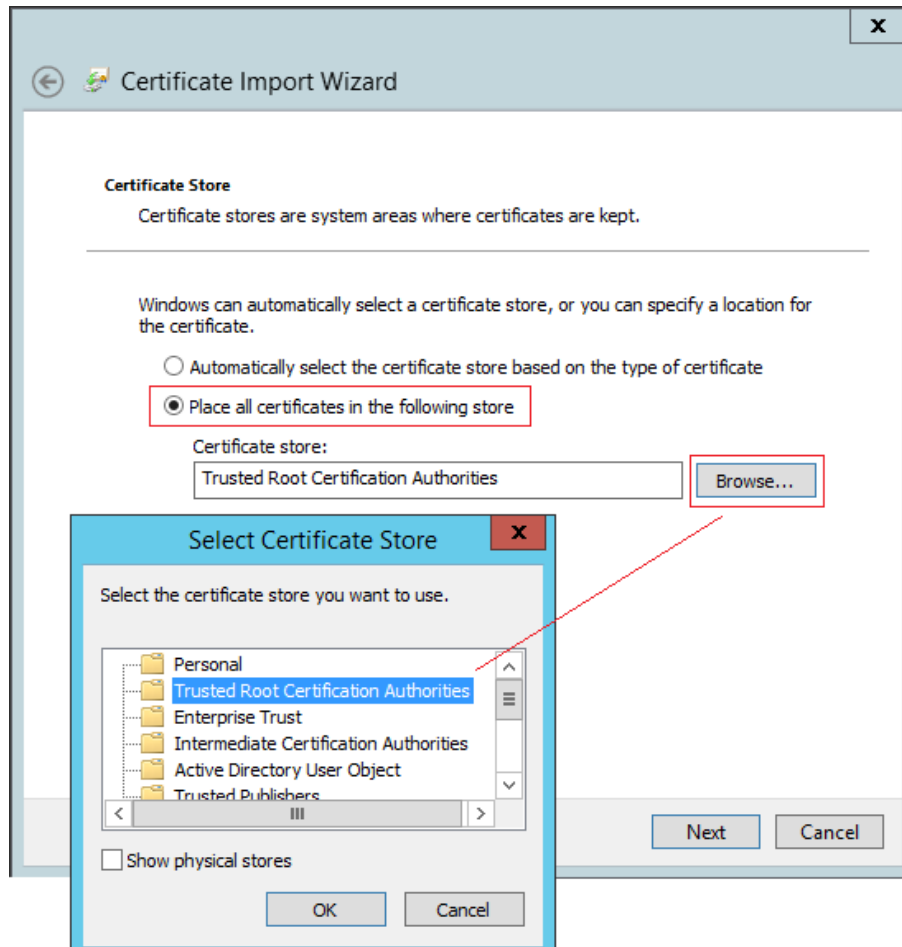


The image shows a Windows-style dialog box titled "Certificate Import Wizard". It has a blue header bar with a back arrow icon and a close button (X) in the top right corner. The main content area is white and contains the following elements:

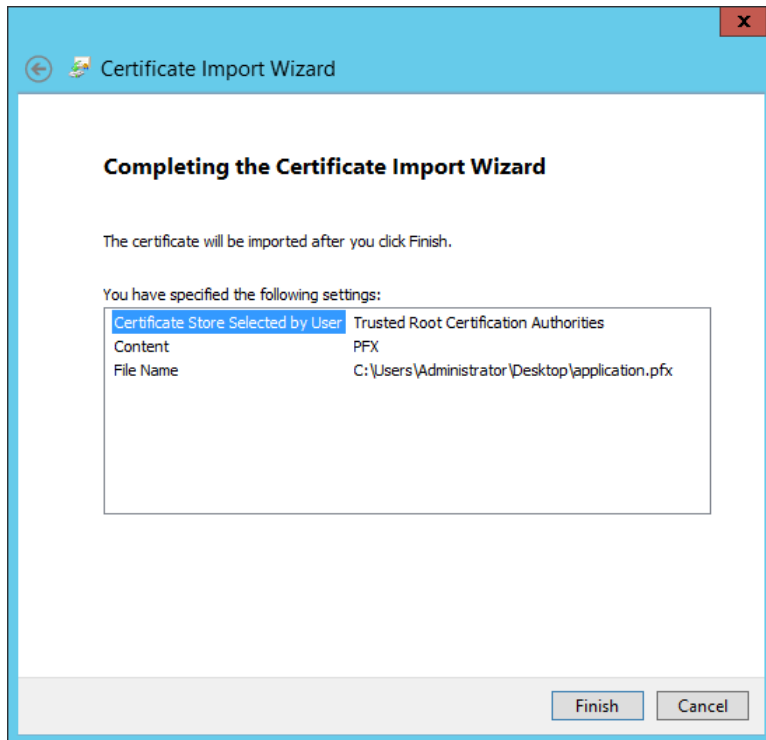
- Private key protection**
To maintain security, the private key was protected with a password.
- A horizontal line separator.
- Text: "Type the password for the private key."
- A label "Password:" followed by a text input field containing ten black dots.
- A checkbox labeled "Display Password" which is currently unchecked.
- A section titled "Import options:" containing three checkboxes:
 - ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
 - ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
 - ☒ Include all extended properties.

At the bottom right of the dialog box, there are two buttons: "Next" and "Cancel".

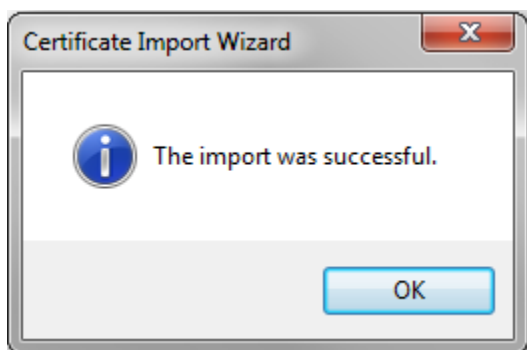
On the next screen, select the second radio button and browse to the local certificate store and select the Trusted Root Certification Authorities container.



On the next screen, click Finish to import the certificate.



Say ok to the confirmation message.



Once this is done, users should be able to browse to an HTTPS site which uses these certificates and receive no warnings or prompts.

Important Note: Users should *never* install a security certificate from an unknown source. In practice, you should only install a certificate locally if you generated it. No legitimate website would require you to perform these steps.