

Chapter 9 – Advanced configuration

Terms

This Windows SharePoint Services Operations Guide (WSSOPS) from the Computer Information Agency is provided as is. Every effort has been made by the author to ensure that information provided is correct however this cannot be guaranteed.

By using the Guide you also acknowledge that any work performed on production systems is a potentially dangerous act and may involve significant business risk and downtime. You hereby agree to release, waive and discharge the Computer Information Agency and/or the author from any liability incurred to yourself, your business or customers for any and all loss or damage, and any claims or demands therefore on account of problems arising from the use of this Guide.

By using this guide you hereby assume full responsibility for any risk to computer systems, now and forever arising out of, or related to the use of this Guide on any computer system.

Distribution and Duplication Guidelines

This document is copyright and only available directly from the Computer Information Agency. This work is now licensed under Creative Commons.



<http://creativecommons.org/licenses/by-nc-sa/4.0/>

By using this Guide you agree to these terms.

Index

- 9.1 Scope
- 9.5 Configuring SSL
- 9.99 Conclusion

Chapter 9 – Advanced configuration

9.1 Scope

There generally are not a lot of problems getting SharePoint Foundation 2010 installed onto a Windows Server.

9.5 Configuring SSL

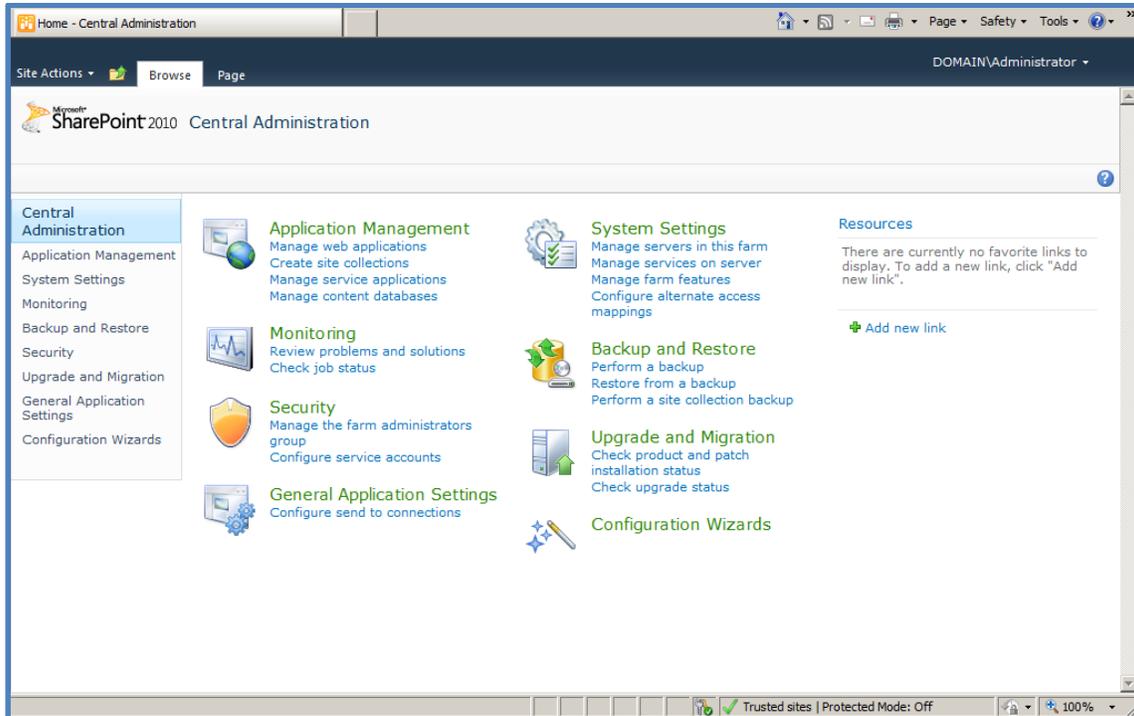
There are a number of ways that WSF can be utilized with SSL for secure communications. The first method will show you how to “extend” an existing WSF site to SSL. This means that the original WSF site (unencrypted) remains unchanged but the same content can also be accessed through an SSL connection. The second method will show you how to simply bind the SSL protocol to the existing WSF web site and configure SharePoint Alternate Access Mappings to allow access.

Your WSF server will require an SSL certificate to already be in place if you plan to use SSL. Most IIS Servers already have a self signed certificate configured and that is what will be used in these examples. If you require a public certificate you will need to request, purchase and configure one. The information here will not cover how to configure a public certificate on your server.

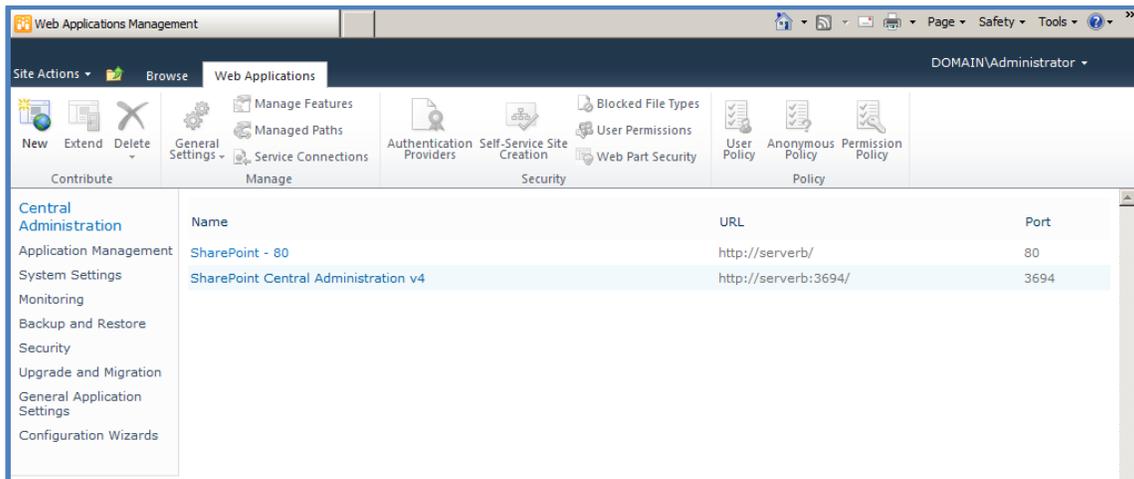
It is important to keep in mind that using SSL with WSF will slow the site down simply due to the SSL encryption and the graphical nature of WSF. This will be more evident if you have large documents and images because these too must be encrypted by SSL before they are transmitted. Also be aware that some custom web parts from third parties may not function over SSL. In this event you will be give the option to close the offending web part to display the page.

Method 1 – Extending existing web application

Chapter 9 – Advanced configuration

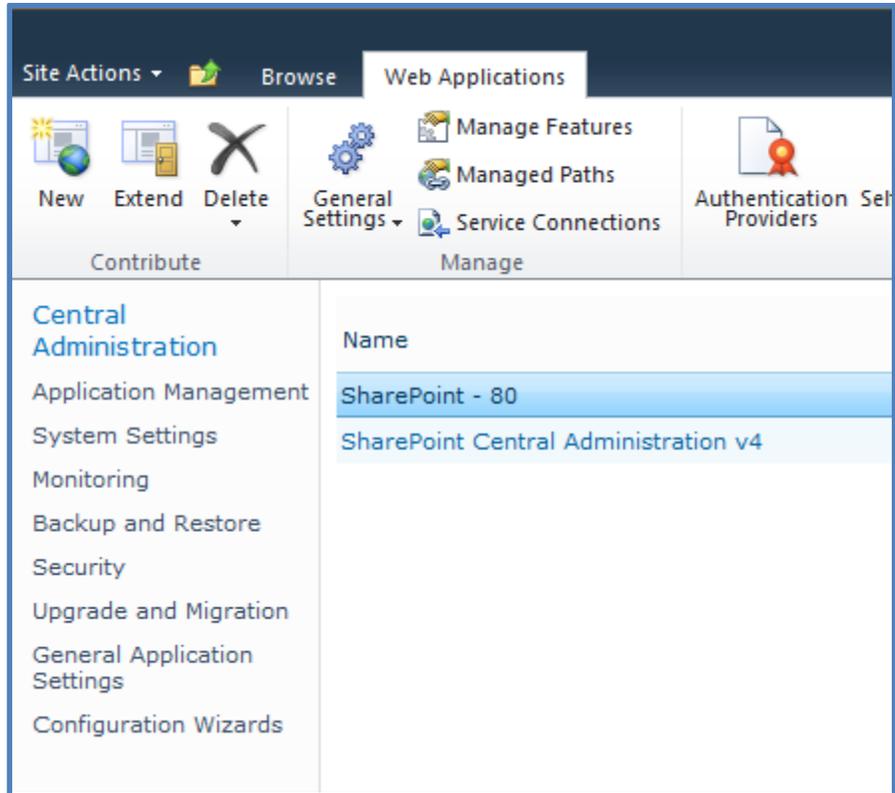


Run the *SharePoint Central Administration* by logging into the WSF server as an administrator and running **Start | SharePoint 2010 | SharePoint 2010 Central Administration**. Once this is opened select the **Manage web application** option from under the Application Management section in the top left.

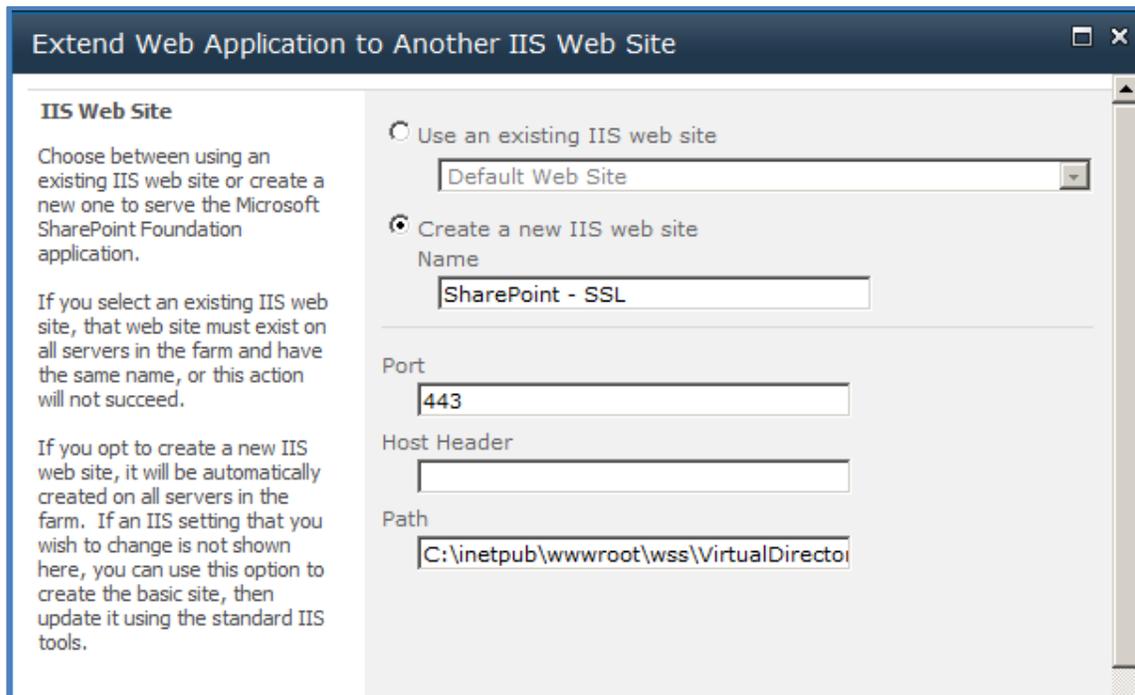


Now select the SharePoint web application you wish to extend (in this case SharePoint – 80). Once selected the line listing that web application should be highlighted,

Chapter 9 – Advanced configuration



The buttons in the ribbon menu should also now activate. With the SharePoint web application to be extended selected, press the **Extend** button on the left of the ribbon menu.



Chapter 9 – Advanced configuration

Select the option to *Create a new IIS web site* and give the site a meaningful name (in this case SharePoint – SSL). Next, select the port over which you wish to run SSL. The SSL port by default is 443 however in many cases you may want to select another port. This is especially true with Windows Small Business Server 2003 which uses port 443 for Outlook Web Access and Remote Web Workplace.

Set the other options as required but ensure that the option *Use Secure Sockets Layer (SSL)* is set to **Yes**. Select **OK** when complete.

Extend Web Application to Another IIS Web Site

Security Configuration

Kerberos is the recommended security configuration to use with Integrated Windows authentication. Kerberos requires the application pool account to be Network Service or special configuration by the domain administrator. NTLM authentication will work with any application pool account and the default domain configuration.

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Authentication provider:

Negotiate (Kerberos)

NTLM

Allow Anonymous

Yes

No

Use Secure Sockets Layer (SSL)

Yes

No

Public URL

The public URL is the domain name for all sites that users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port.

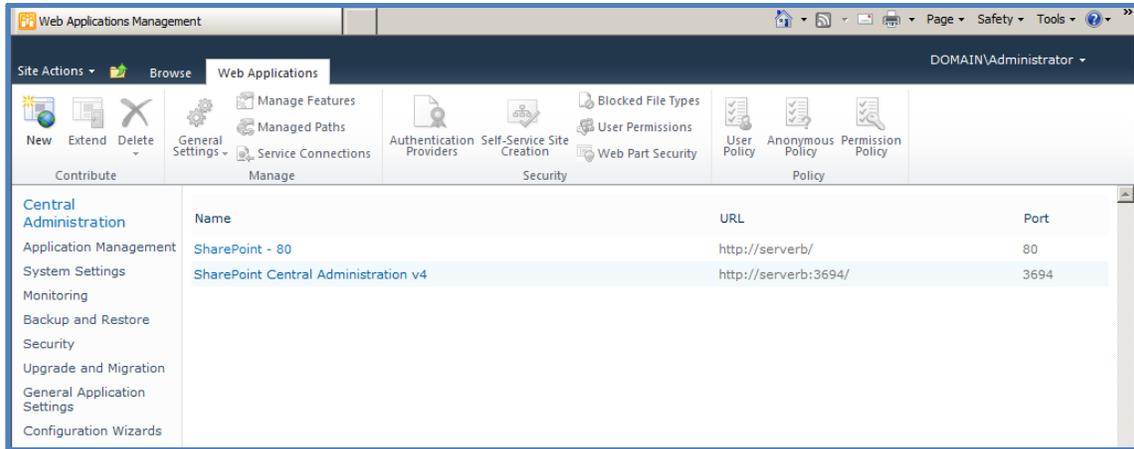
<http://go.microsoft.com/fwlink/?LinkId=114854>

URL

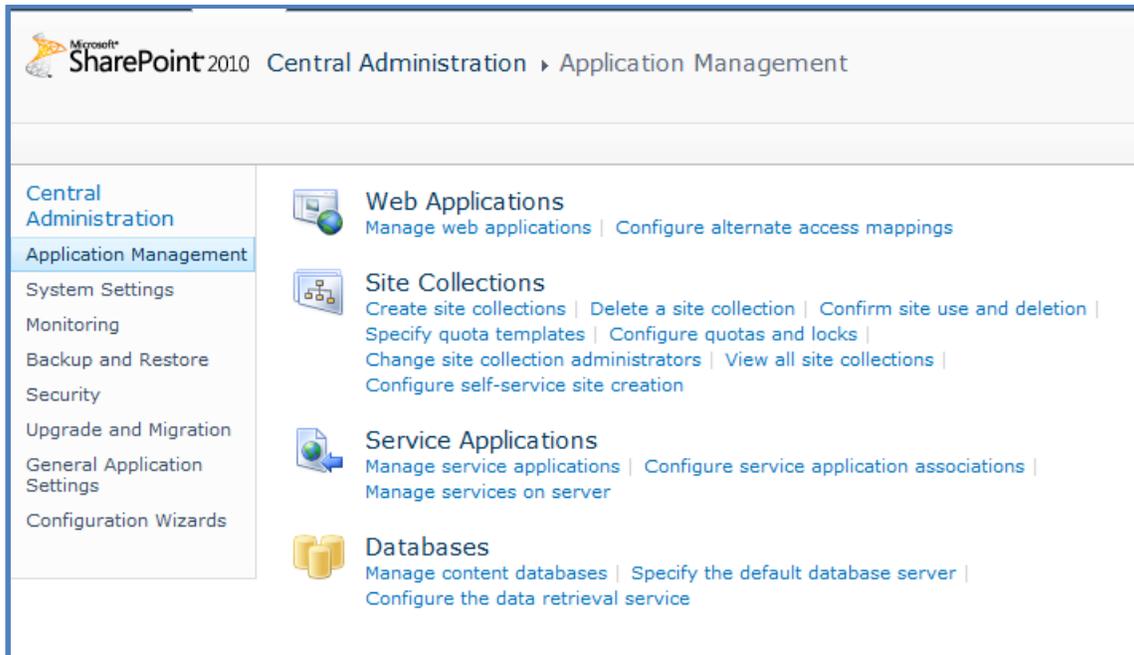
Zone

Press the **Save** button to complete the configuration.

Chapter 9 – Advanced configuration

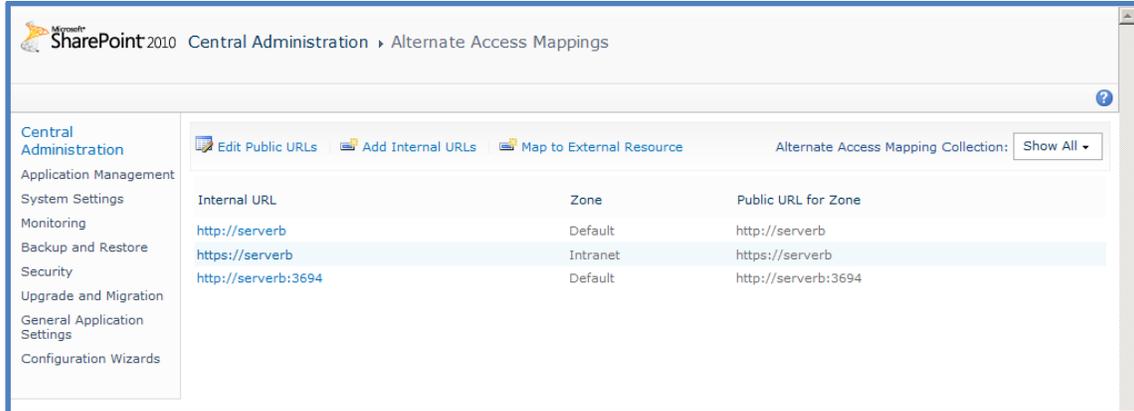


You will then be returned to the Web Application area.

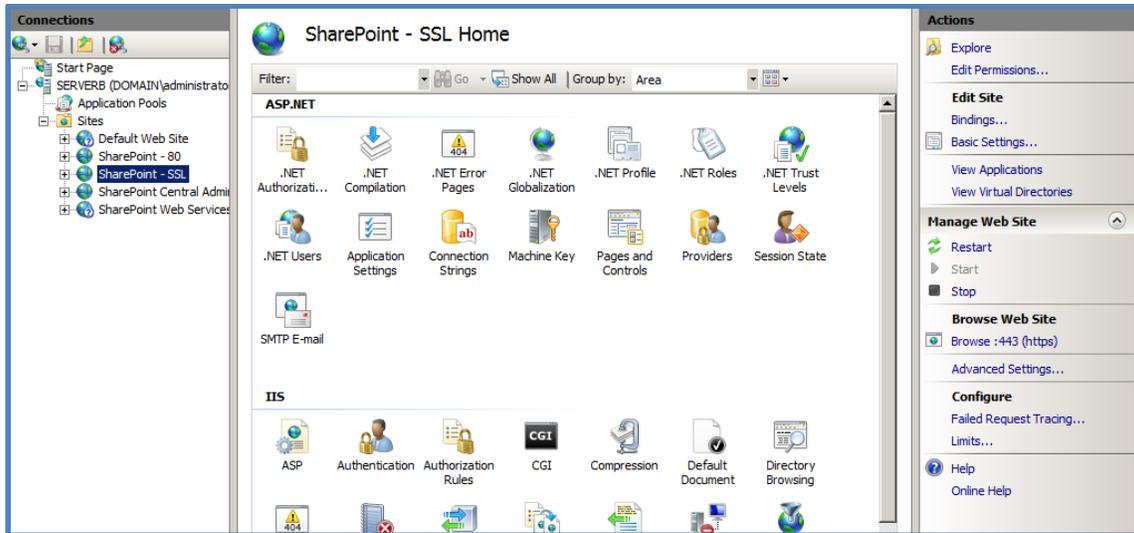


From the menu on the left hand side select **Application Management**. From under the *Web Applications* section at the top of the page select **Configure alternate access mappings**.

Chapter 9 – Advanced configuration

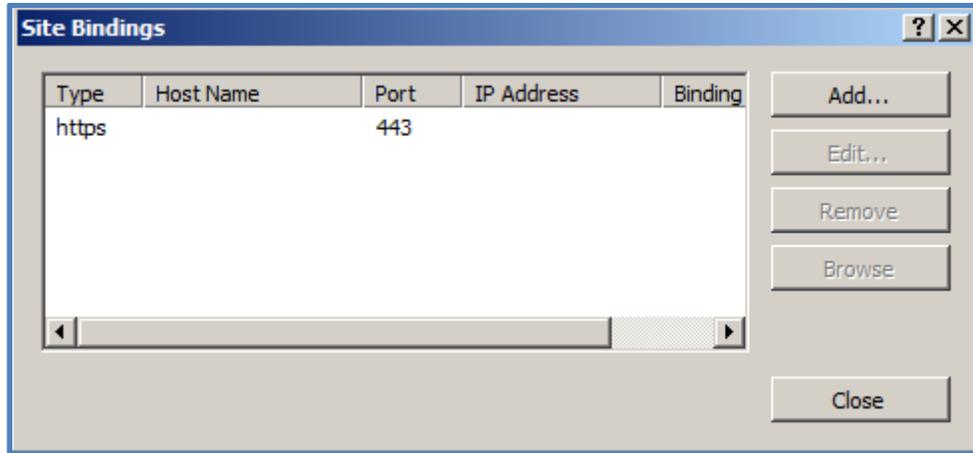


In this list you should see the new https:// address (here https://serverb).



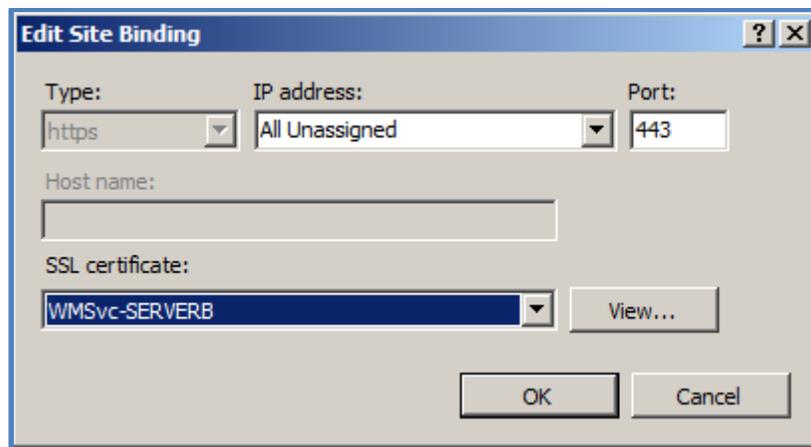
If you now open the *Internet Information Services (IIS) Manager* via **Start | Administrative tools** you should see that there is now an additional web site with the name you just created in the *SharePoint Central Administration* (in this case *SharePoint -SSL*).

Chapter 9 – Advanced configuration



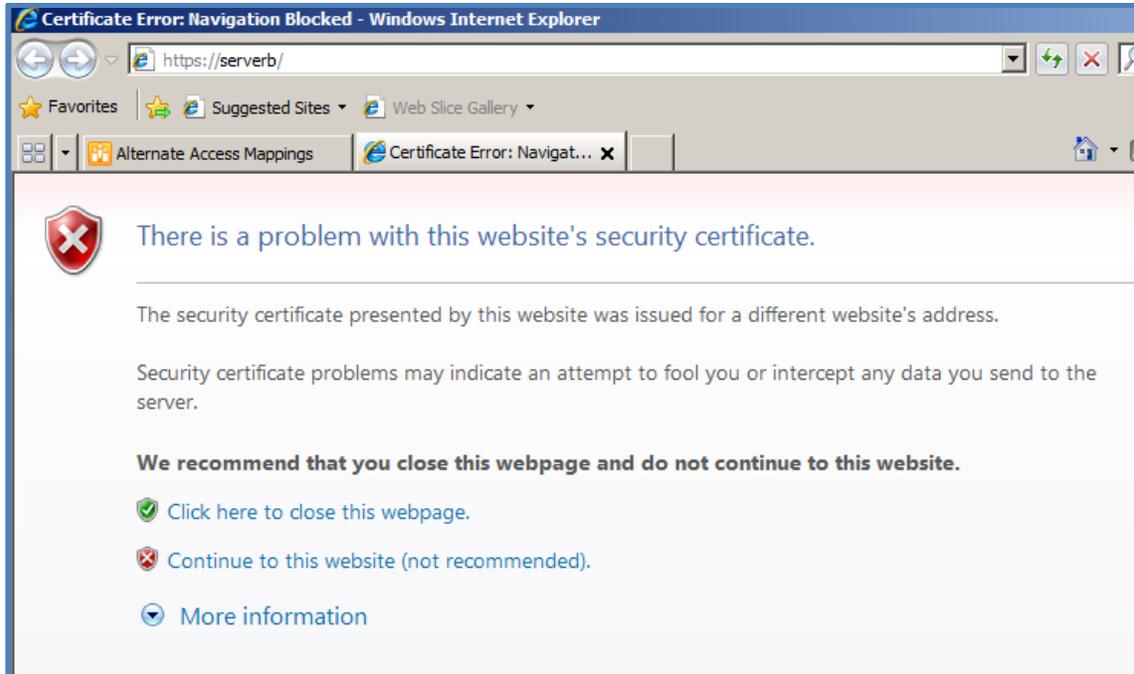
Under the *Edit Site* heading on the right, select **Bindings**.

At the *Site Bindings* window that appears select the https entry and then press the **Edit** button on the right.



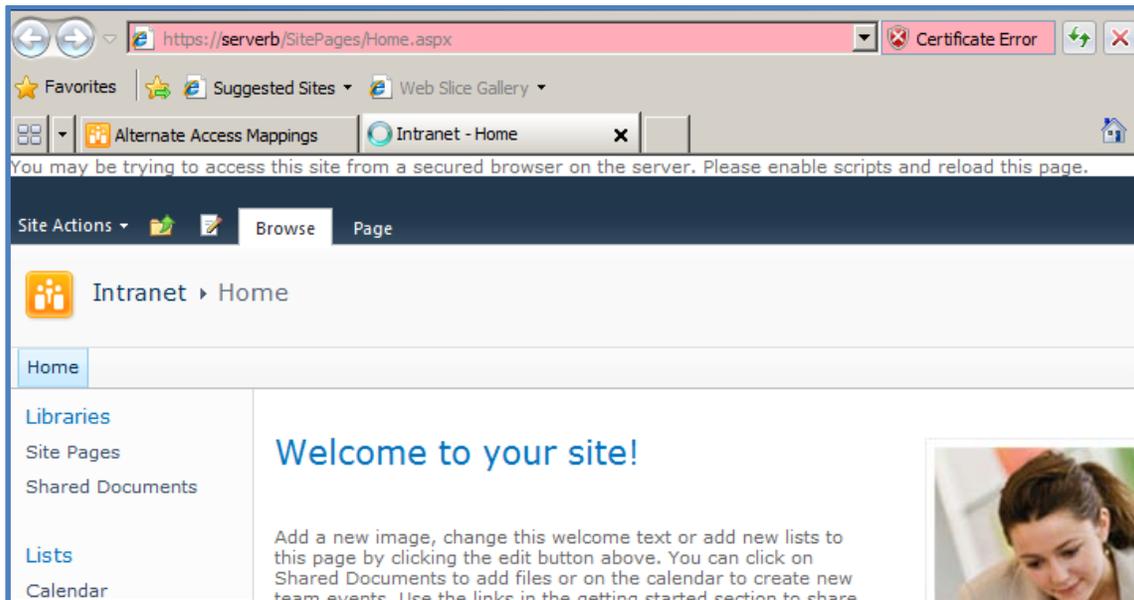
In the *Edit Site Binding* window select the SSL certificate you wish to use. Press **OK** when complete.

Chapter 9 – Advanced configuration



Open a browser and type the address of your new SSL WSF site into the address line. Remember you'll have to use `https://` as the prefix.

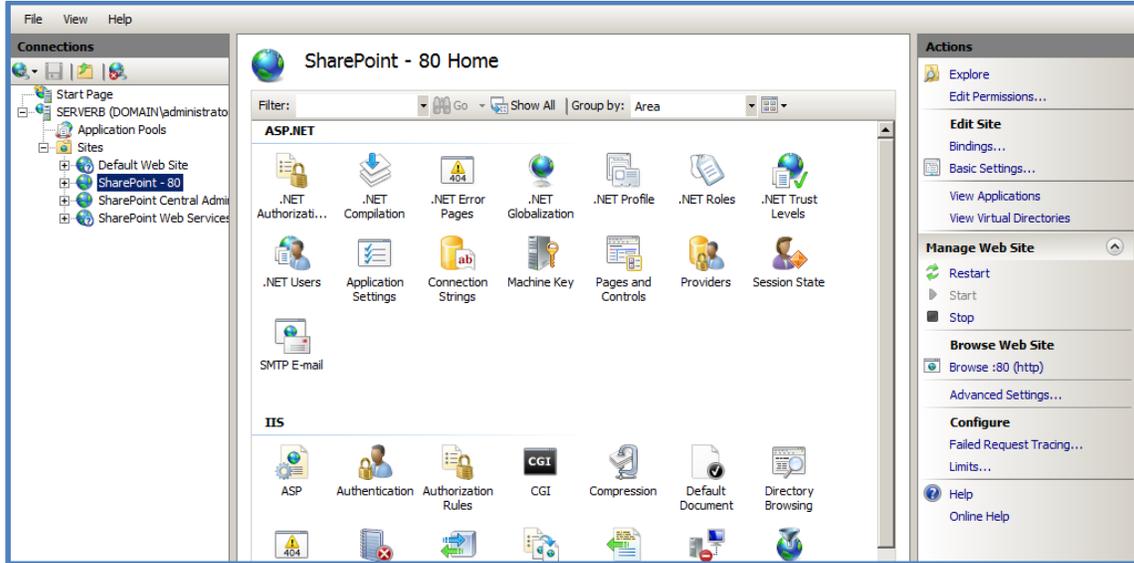
Prior to the site displaying you may see a certificate warning like that shown above. This error occurs in this situation because a self-signed server certificate has been used. If you use a commercial SSL certificate this should not occur.



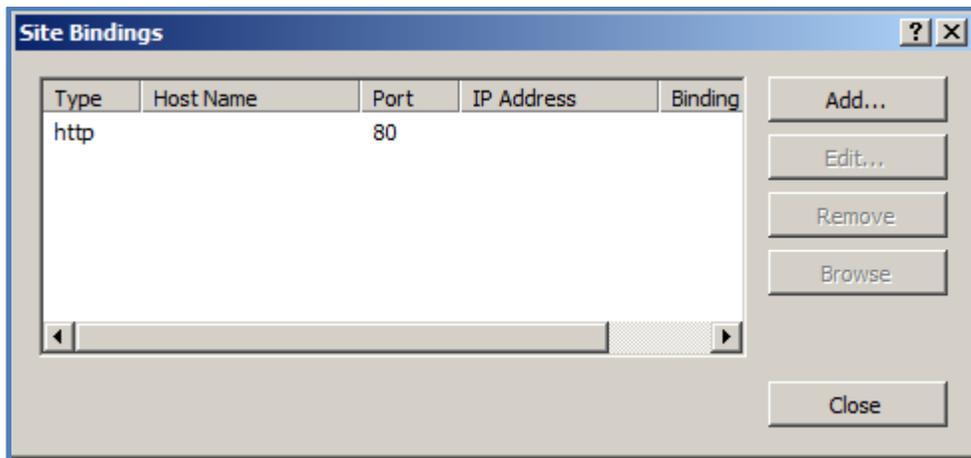
You should now see your existing site displayed as it was before but now all the traffic will be sent via SSL.

Chapter 9 – Advanced configuration

There is another way to configure SSL on an existing SharePoint site without 'extending' the site SharePoint. Instead all the configuration is done via Windows *Internet Information Services (IIS)*.

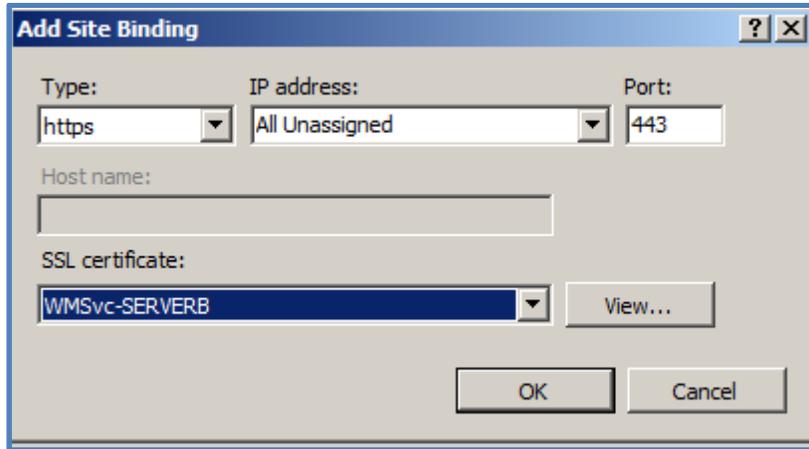


Select the existing SharePoint site in IIS (here **SharePoint – 80**). Select **Bindings** on the right hand side under *Edit Site*.



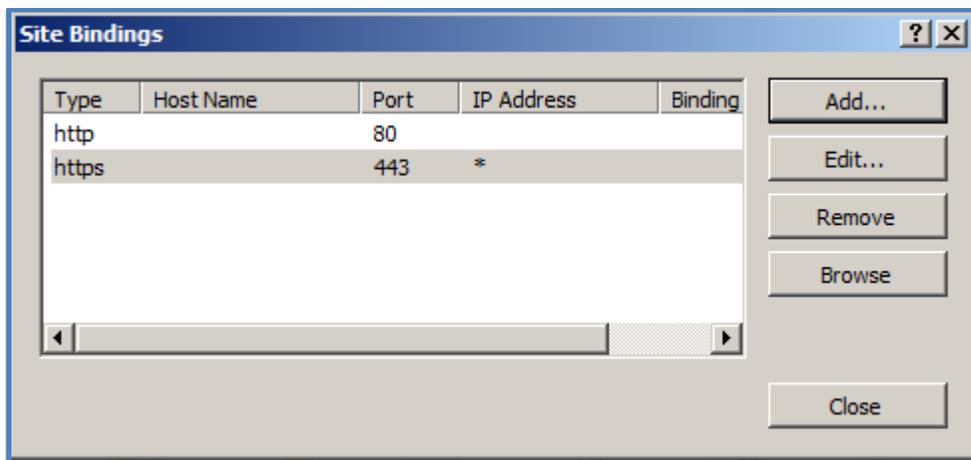
In the *Site Bindings* window select the **Add** button on the right.

Chapter 9 – Advanced configuration



In the *Type* field select **https** and ensure the *Port* is set to 443. In the SSL certificate field select the certificate you wish to use.

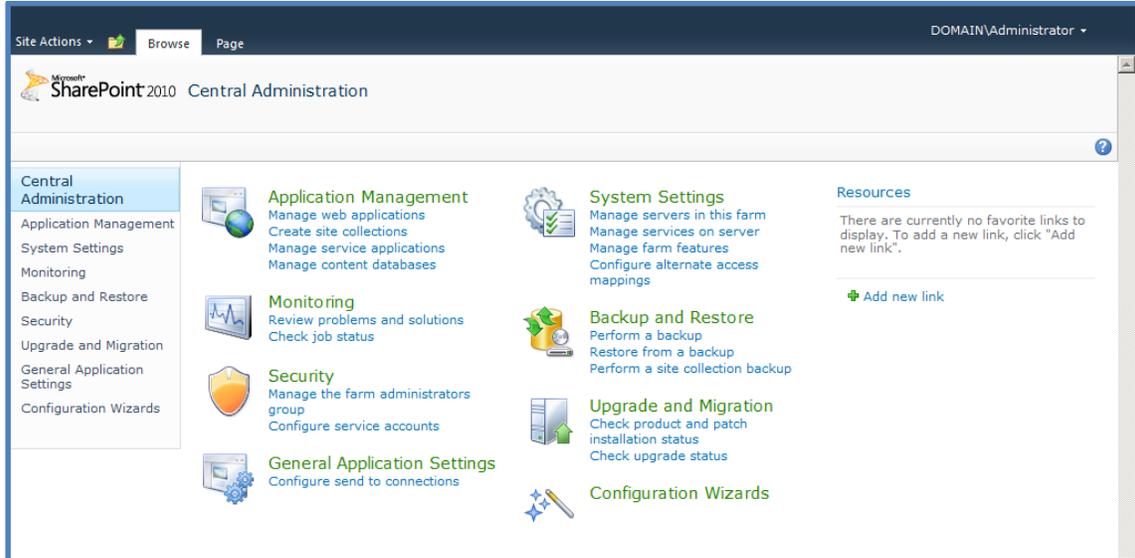
Press the **OK** button when complete.



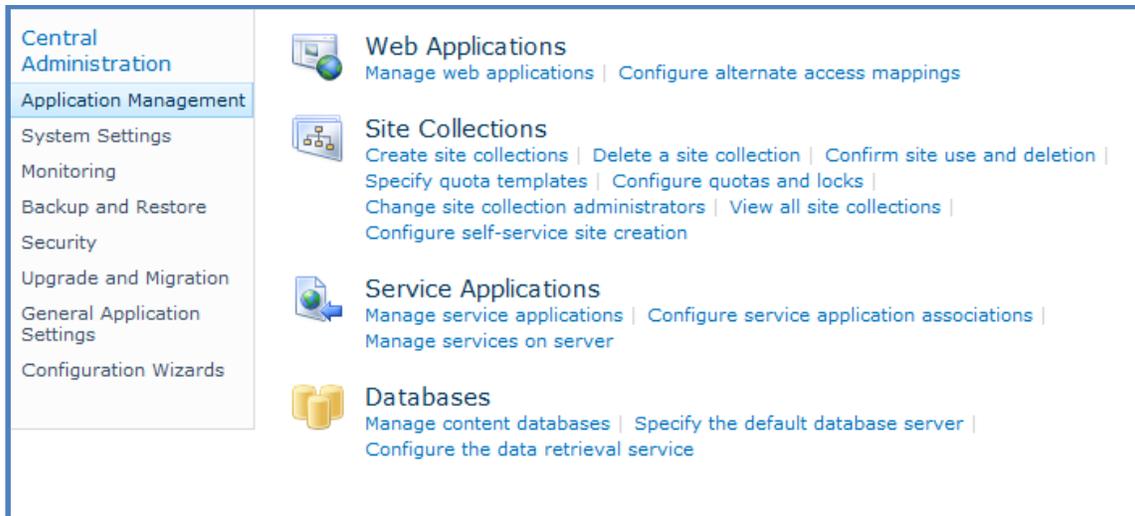
You should now see an additional *https* line appear in the *Site Bindings* as shown above.

Press the **Close** button to continue.

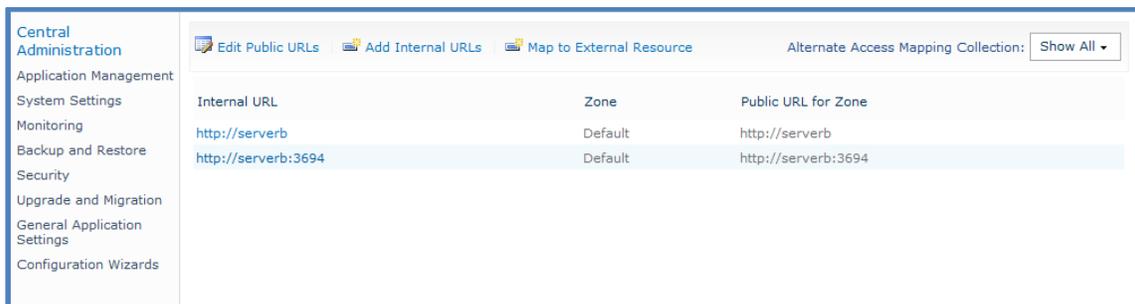
Chapter 9 – Advanced configuration



Select **Application Management** from the menu on the left hand side.



Then select **Configure alternate access** mappings from under the *Web Applications* heading at the top of the page.



Chapter 9 – Advanced configuration

Select **Add Internal URLs** from the menu across the top.

Alternate Access Mapping Collection
Select an Alternate Access Mapping Collection.

Alternate Access Mapping Collection: **No selection**

Add Internal URL
Enter the protocol, host and port portion of any URL that should be associated with this resource.

URL protocol, host and port

Zone
Default

Save Cancel

In the *Alternate Access Mapping Collection* at the top of the page ensure there is a site listed.

Alternate Access Mapping Collection: **No selection**

Change Alternate Access Mapping Collection

If it says *No Selection* then press the arrow to the right and select **Change Alternate Access Mapping Collection** for the menu that appears.

Select An Alternate Access Mapping Collection -- Webpage Dialog

Select An Alternate Access Mapping Collection

Name	URL
Central Administration	http://serverb:3694
SharePoint - 80	http://serverb

Cancel

Now select the existing SharePoint site you wish to map. In this case we select **SharePoint – 80**.

Alternate Access Mapping Collection
Select an Alternate Access Mapping Collection.

Alternate Access Mapping Collection: **SharePoint - 80**

Add Internal URL
Enter the protocol, host and port portion of any URL that should be associated with this resource.

URL protocol, host and port
https://serverb

Zone
Intranet

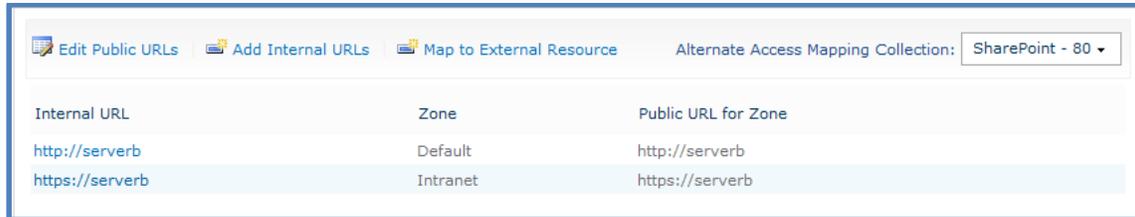
Save Cancel

Chapter 9 – Advanced configuration

This selection should now appear in the *Alternate Access Mapping Collection* in the top left.

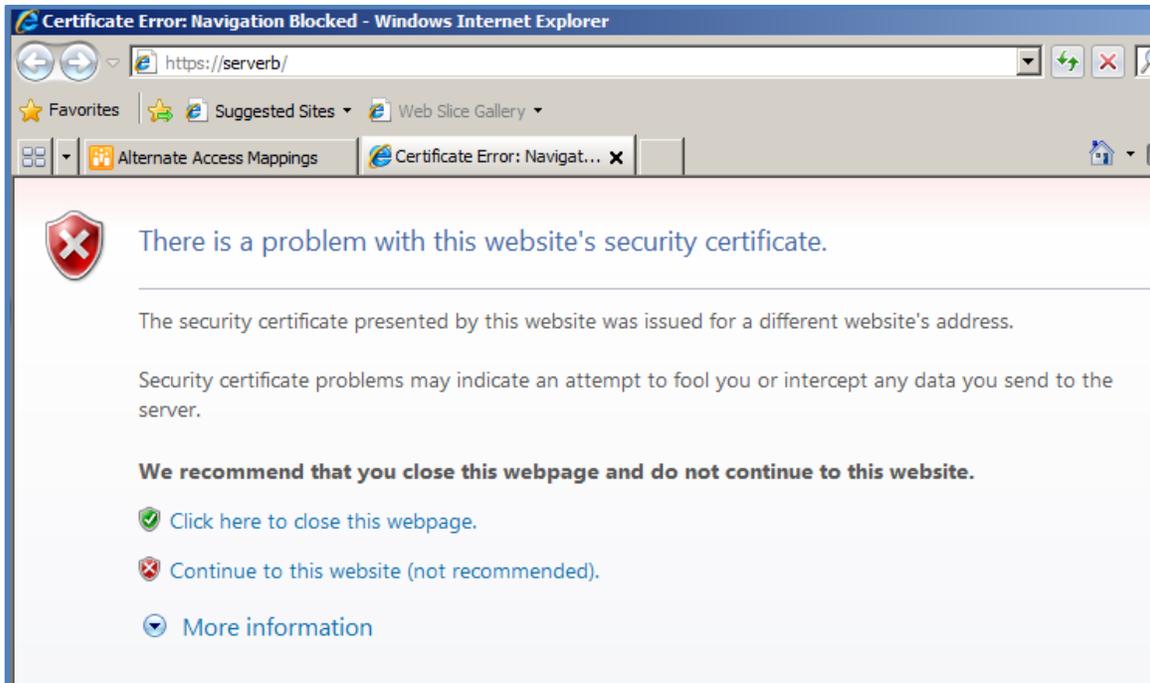
In the Add Internal URL section enter the SSL URL you wish to use (here **https://serverb**) and set the Zone to something that is free (say **Intranet**).

Press the **Save** button when the configuration is complete.



Internal URL	Zone	Public URL for Zone
http://serverb	Default	http://serverb
https://serverb	Intranet	https://serverb

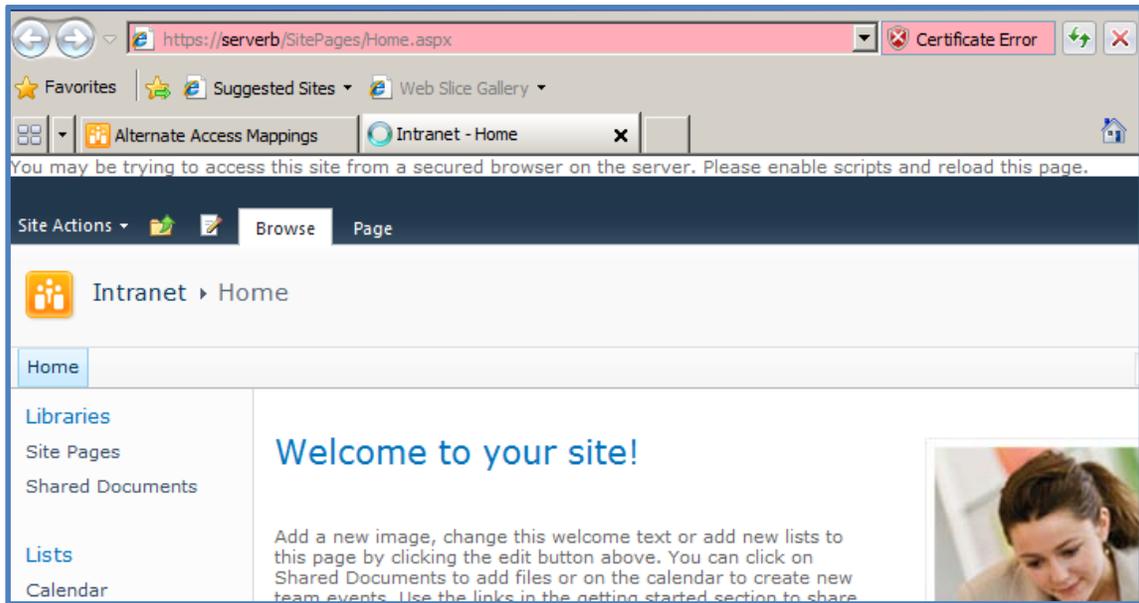
You should now see the mapped URL you just created appear in the listing (here *https://serverb*).



Open a browser and type the address of your new SSL WSF site into the address line. Remember you'll have to use **https://** as the prefix.

Prior to the site displaying you may see a certificate warning like that shown above. This error occurs in this situation because a self-signed server certificate has been used. If you use a commercial SSL certificate this should not occur.

Chapter 9 – Advanced configuration



You should now see your existing site displayed as it was before but now all the traffic will be sent via SSL.

So what is the difference between the two methods? The first method creates a completely independent web site in IIS for the SSL traffic. This means you can apply different securities and control without affecting the original site. It is normally best practice to configure an SSL site like this.

The second method is simply a duplicate mapping using the same IIS website that is already in use by port 80. This generally lacks the flexibility and security of the first method and should be considered the 'quick and dirty' method of achieving SSL configuration for your SharePoint web site.

9.99 Conclusion

This guide continues to be a work in progress and I encourage comments and feedback of any type. The only way that the Guide will improve if these is continued feedback.

Please send your comments and feedback to director@ciaops.com.