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

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



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.

🔁 Web Applications Manage	ement		🏠 • 🖻 - 🖃 🖶	• Page • Safety • Tools • 🕡 • 🎽
Site Actions 🕶 😏 Bro	wse Web Applications			DOMAIN\Administrator 🗸
New Extend Delete	General Settings - Operations	Authentication Self-Service Site Providers	User Anonymous Permission Policy Policy	
Contribute	Manage	Security	Policy	A
Administration	Name		URL	Port
Application Managemen	t SharePoint - 80		http://serverb/	80
System Settings	SharePoint Central Administra	ation v4	http://serverb:3694/	3694
Monitoring				
Backup and Restore				
Security				
Upgrade and Migration				
General Application Settings				
Configuration Wizards				

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,



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.

Extend Web Application	to Another IIS Web Site	□ ×
IIS Web Site Choose between using an existing IIS web site or create a new one to serve the Microsoft SharePoint Foundation application. If you select an existing IIS web	O Use an existing IIS web site Default Web Site O Create a new IIS web site Name SharePoint - SSL	×
site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed. If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.	Port 443 Host Header Path C:\inetpub\wwwroot\wss\VirtualDirector	

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 which 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 t	o 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: O 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 https://serverb:443 Zone Intranet]

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

Web Applications Manager	nent		🏠 🕶 🖾 👻 🚍 🖶	• Page • Safety • Tools • 🕡 •
Site Actions 🕶 🐋 Brow	se Web Applications			DOMAIN\Administrator +
New Extend Delete Contribute	General ettings - Questions Managed Paths Manage	Authentication Self-Service Site Providers Self-Service Site Creation Security	User Policy Policy	
Central Administration	Name		URL	Port
Application Management	SharePoint - 80		http://serverb/	80
System Settings	SharePoint Central Administra	ation v4	http://serverb:3694/	3694
Monitoring				
Backup and Restore				
Security				
Upgrade and Migration				
General Application Settings				
Configuration Wizards				

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**.

SharePoint 2010	Central Administr	ation → Alternate Ac	ccess Mappings		•
Central Administration	😡 Edit Public URLs	🚔 Add Internal URLs	🖷 Map to External Resource	Alternate Access Mapping Collection: Show All	•
System Settings	Internal URL		Zone	Public URL for Zone	
Monitoring Backup and Restore	http://serverb https://serverb		Default Intranet	http://serverb https://serverb	
Security Upgrade and Migration General Application Settings	http://serverb:3694		Default	http://serverb:3694	
Configuration Wizards					

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*).

Site	e Binding	gs				?×
ł	Type https	Host Name	Port 443	IP Address	Binding	Add
	(Þ	Remove Browse
						Close

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.

Edit Site Binding			<u>? ×</u>
Type: https	IP address:		Port:
Host name:			
SSL certificate:			
WMSvc-SERVERB		_	View
		ОК	Cancel

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



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.

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*.

Si	te Bindin	gs				?×
	Туре	Host Name	Port	IP Address	Binding	Add
	http		80			Edit
						Remove
						Browse
	•					
						Close

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

Add Site Binding				<u>?</u> ×
Type: https	IP address: All Unassigned		Port:	
Host name:				
SSL certificate:				
WMSvc-SERVERB		•	View	
		ОК	Cance	ł

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.

Si	te Bindin	igs				<u>?</u> ×
	Type http https	Host Name	Port 80 443	IP Address *	Binding	Add Edit Remove Browse
	•				Þ	Close

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

Press the **Close** button to continue.

Site Actions - 😢 Brows	se Page Central A	Idministration			DOMAIN\Administrator +	
					6	
Central Administration		Application Management	ŝ	System Settings	Resources	
Application Management System Settings Monitoring		Manage web applications Create site collections Manage service applications Manage content databases		Manage servers in this farm Manage services on server Manage farm features Configure alternate access	There are currently no favorite links to display. To add a new link, click "Add new link".	
Backup and Restore Security Upgrade and Migration	M	Monitoring Review problems and solutions Check job status	<u>*</u>	mappings Backup and Restore Perform a backup Restore from a backup	🖶 Add new link	
General Application Settings Configuration Wizards		Security Manage the farm administrators group Configure service accounts		Perform a site collection backup Upgrade and Migration Check product and patch installation status		
		General Application Settings Configure send to connections		Check upgrade status Configuration Wizards		

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

Central Administration		Web Applications Manage web applications Configure alternate access mappings
Application Management		
System Settings	5	Site Collections
Monitoring		Specify quota templates Configure quotas and locks
Backup and Restore		Change site collection administrators View all site collections
Security		Configure self-service site creation
Upgrade and Migration		Service Applications
General Application Settings	V	Manage service applications Configure service application associations Manage services on server
Configuration Wizards		
	Ţ	Databases Manage content databases Specify the default database server Configure the data retrieval service

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

Central Administration	🐺 Edit Public URLs 🖷 Add Internal URLs	🚔 Map to External Resource	Alternate Access Mapping Collection: Show All -
System Settings	Internal URL	Zone	Public URL for Zone
Monitoring	http://serverb	Default	http://serverb
Backup and Restore	http://serverb:3694	Default	http://serverb:3694
Security			
Upgrade and Migration			
General Application Settings			
Configuration Wizards			

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.

Alterna	te 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 W	/ebpage Dialog	X	
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

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.

🐺 Edit Public URLs	🚔 Add Internal URLs	Map to External Resource	Alternate Access Mapping Collection: SharePoint - 80 -
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.

https://serv	verb/SitePages/Home.aspx	🕶 😵 Certificate Error 😽 🗙
🖕 Favorites 🛛 👍 🙋 Sugg	ested Sites 🔻 🙋 Web Slice Gallery 👻	
🔠 👻 📴 Alternate Access I	Mappings OIntranet - Home X	<u>a</u>
You may be trying to acces	is this site from a secured browser on the server. Please enable scr	ipts and reload this page.
Site Actions 👻 📝	Browse Page	
🚹 Intranet 🕨 Ho	me	
Home		
Libraries		
Site Pages	Welcome to your site!	(Aller and all and all all all all all all all all all al
Shared Documents		(CTURN)
Lists	Add a new image, change this welcome text or add new lists to this page by clicking the edit button above. You can click on	24
Calendar	Shared Documents to add files or on the calendar to create new team events. Use the links in the detting started section to share	

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.