



The final guide to Alternate Access Mappings

Release 1.0

Alternate Access Mappings

In my opinion, this is another area within SharePoint which needs a good guide to how it works and how to configure it. Again, not to explain all about the inner workings of AAM, Host Headers, link translations, reverse proxies and so on, but a good, clean guide to how it is done in real life.

I got a lot of good feedback on my Final Kerberos guide, this gave me the idea of trying to cover yet another area that is a bit 'sticky' in SharePoint and make it simple to understand, Alternate Access Mappings. After you have finished this guide, or only parts of it, you will hopefully grasp the functionality of Alternate Access Mappings and what it's all about.



First I have added a checklist of things that must be done in order for any AAM to work, this can be used if you are comfortable with the steps. Second, a simple enough explanation as to how you should look at the Alternate Access Mappings table, it's not really that hard once you get the hang of it. After that I have added a few scenarios that hopefully will cover most real life circumstances that you can encounter out there. Lastly all the scenarios are added in PowerShell, the steps line by line.



Contents in this Guide

Contents in this Guide	2
Checklist	3
Basics	4
DNS	6
Scenario 1	10
Scenario 2	20
Scenario 3	25
Scenario 4	31
PowerShell	35
References	44
Thanks to, for technical and spiritual support:.....	44

Checklist

Item	Description
Web Application + Site Collection	A Web Application must exist with at least one Site Collection or it can't be accessed. The site collection is not a requirement to setup AAM but in order to verify functionality like in this guide, it must exist.
Name resolution	The selected URL to be used, must be resolved to an IP address, using DNS or the local Hosts file. This is true for Internal URL and Public URL both. Special circumstances like the use of a Load Balancer and more than one Web Server does apply. This guide does not cover that in this version.
Alternate Access Mapping	An Alternate Access Mapping must be added in SharePoint. An Internal URL must exist and be mapped to a Public URL using its zone. This will make sure that link translation is managed by SharePoint, as is the only recommended method for link translation. This can be done using Central Administration or PowerShell
Site Binding to Host Header. This is <u>not</u> handled by SharePoint	A binding on the IIS web site must be added same as the Alternate Access Mapping. Since SharePoint doesn't add a binding when a AAM is created, you must do this as a separate step, before or after creating the Alternate Access Mapping in SharePoint. This can be done using Central Administration or PowerShell
Verify access + functionality	Access the site using the Internal URL added, this should load the site and redirect/transform the URL to the proper Public URL. This can be done using a supported browser of choice, preferable Internet Explorer.

With all the steps in the checklist completed correctly, you will have configured Alternate Access Mappings correctly and can access your sites using a new name or URL.

The Basics section in this document will describe the functionality of Alternate Access Mappings in theory, and the 4 different scenarios will show you how to do it all, step by step.

Good Luck

Thomas Balkeståhl



Basics

Explains how you should look at Alternate Access Mapping – left to right.

- Left area Internal URL's
- Right area Public URL's with a zone
- Middle area Zones, is what connects Internal URL's to Public URL's, many to one.

An 'Internal URL' redirects or transforms to a Public URL, from left, to right. The URL on the left, is what you enter in the address field in your browser, the URL on the right is what you will see once there, this goes for visible and invisible links as well.

Internal URL format: Protocol + URL

A 'Public URL' is the address of the Web Application for one of the five zones available. The 'Default' must be filled out and the other four are optional. You can only have five Public URL's per Web Application. Public URL format: Protocol + URL

A "Zone is a label representing a Public URL, the zone is used to 'connect' an Internal URL to a Public URL. The zone names has no relation what so ever with the four Internet Explorer security zones (Internet, Local Intranet, Trusted sites and Restricted sites) and could just as easily been named 1,2,3,4 and 5. A zone can also represent an authentication provider.

Zones: Default, Intranet, Internet, Custom, Extranet

Example:

Internal URL	Internal URL zone	Public URL zone	Public URL
http://blksth-sp1	Default	Default	http://blksth-sp1
http://sharepoint	Default		
http://intranetportal	Intranet	Intranet	http://intranetportal
https://portal.balkestahl.se	Internet	Internet	https://portal.balkestahl.se
http://portal.balkestahl.se	Internet		
		Custom	Not used
		Extranet	Not used

Note: Based on the 'Zone' selected for every 'Internal URL', they will be connected to a 'Public URL'.
 From left – to right...

Translated to SharePoint GUI, this same setup would look like this:

Internal URL	Zone	Public URL for Zone
http://sharepoint	Default	http://blksth-sp1
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal
https://portal.balkestahl.se	Internet	https://portal.balkestahl.se
http://portal.balkestahl.se	Internet	https://portal.balkestahl.se

Note: Filtered on this Web Applications Alternate Access Mapping Collection only.
 Same Alternate Access Mappings as in the Example table above

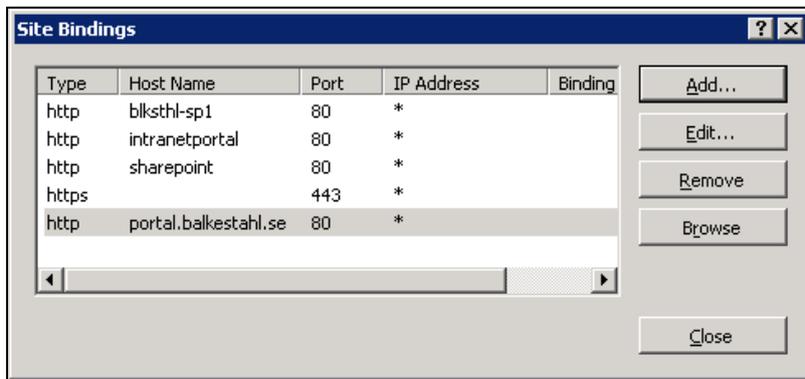
You will see that if you click on any of the 'Internal URLs' that you can select zone, and with the zone, the Public URL it will be connected to:



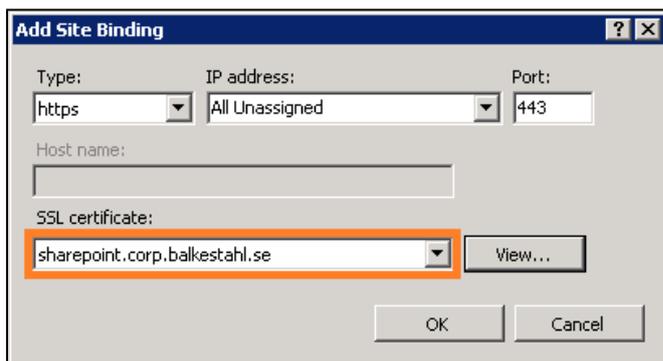
In addition to the actual Alternate Access Mapping in SharePoint Central Administration, you also have to add a Binding in IIS, contrary to what many believe, SharePoint does not do that for you so you have to do it manually.

Steps on how to do that is added to every scenario in this guide.

The example above would show up in IIS Bindings like this:



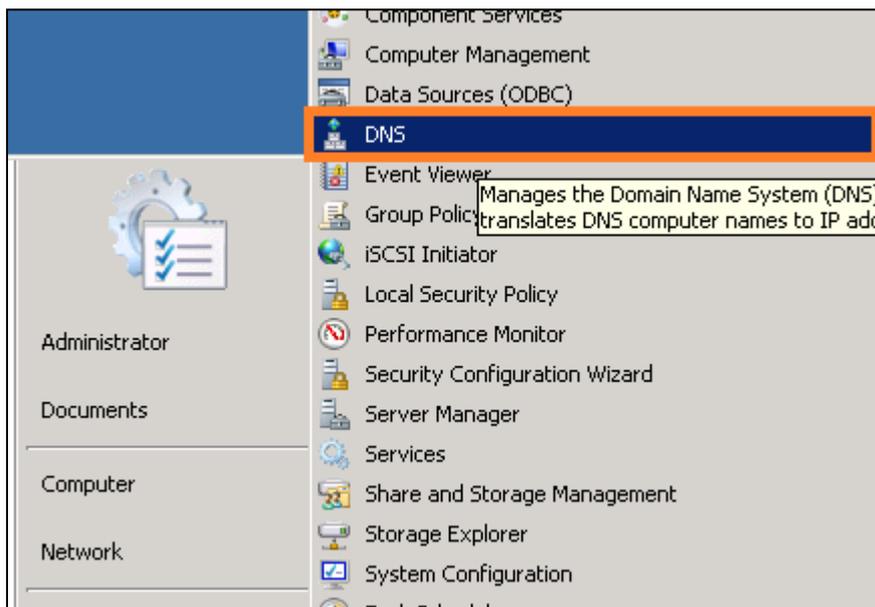
As you can see, the https binding does not show up as a hostname, the hostname is determined by the name configured in certificate used when adding that binding.



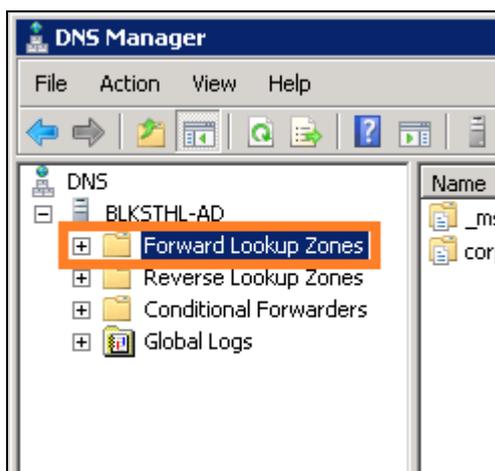
DNS

Since we are just starting up and we have just installed the SharePoint server and created a web application, only using the server name as URL, we need to add the more user friendly URL we want to use in DNS. In this scenario, we will use the URL <http://intranetportal> as the URL so that users easily understand the purpose of this site just by looking at the URL.

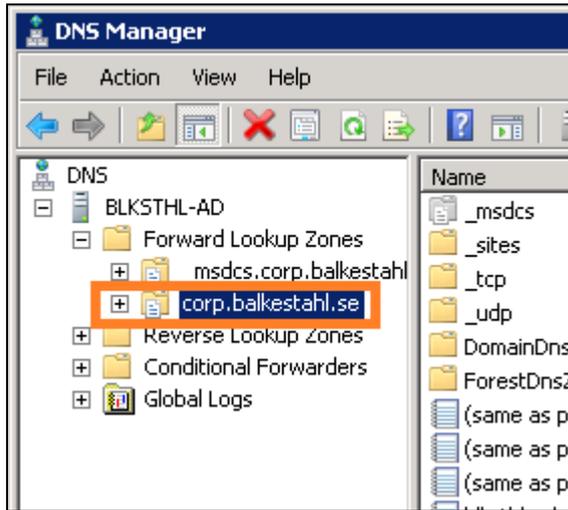
DNS.1 Under Administrative Tools, Open up the DNS Management tool



DNS.2 Expand the 'Forward Lookup Zones' container



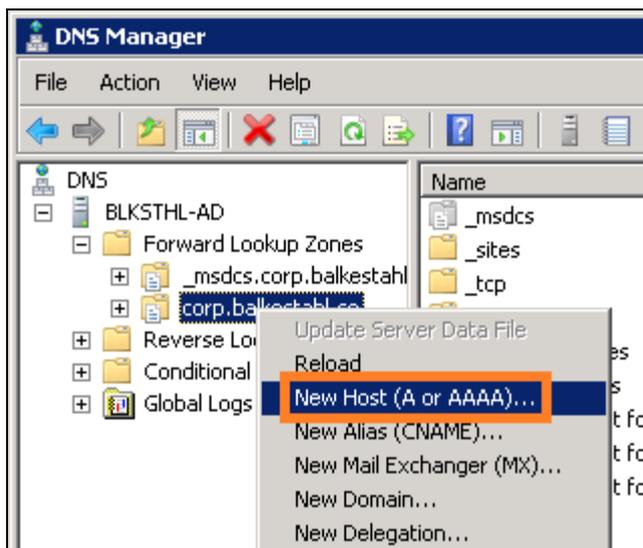
DNS.3 Select the zone for your domain



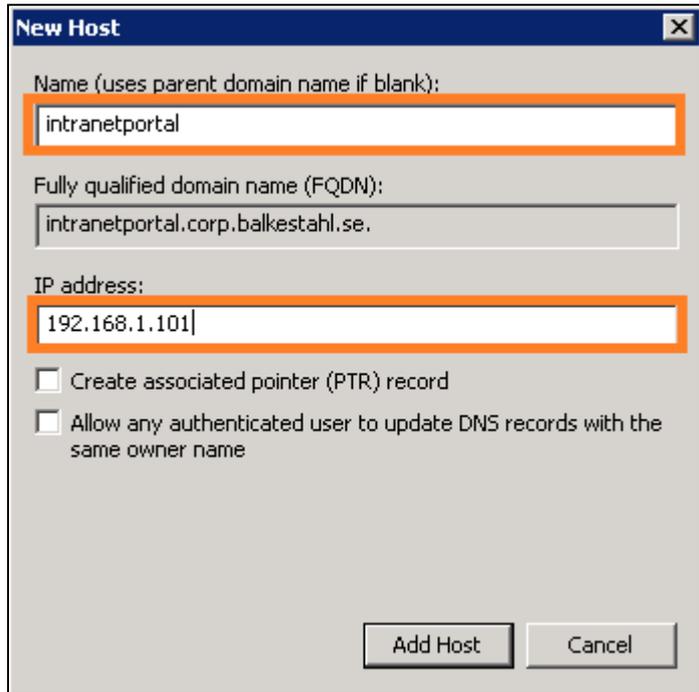
DNS.4 Verify the IP address for the server

(same as parent folder)	Host (A)	192.168.1.21
blksth-ad	Host (A)	192.168.1.21
BLKSTHL-DEV1	Host (A)	192.168.1.116
BLKSTHL-PPIVOT	Host (A)	192.168.1.113
BLKSTHL-SP1	Host (A)	192.168.1.101
BLKSTHL-SP2	Host (A)	192.168.1.110
BLKSTHL-SPF1	Host (A)	192.168.1.108
BLKSTHL-SQL	Host (A)	192.168.1.61

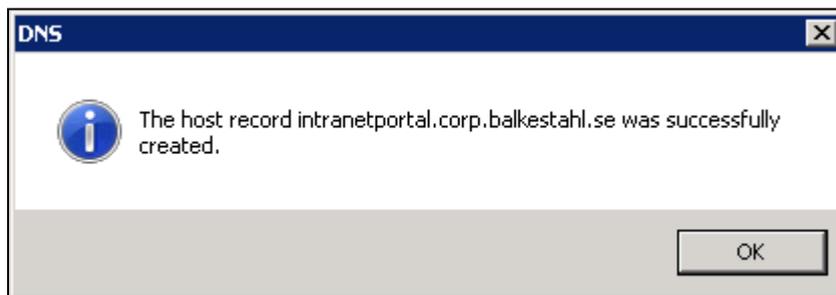
DNS.5 Right click on the zone and select 'New Host (A or AAAA)'



DNS.6 Fill in the Name we want to use, 'intranetportal' and add the IP address of the server



DNS.7 Click 'Add Host'



Click ok in the dialog, then click 'Done'

DNS.8 Verify that you see an entry for the name and the correct IP address.

BLKSTHL-SQL	Host (A)	192.168.1.61
blksth-tma2	Host (A)	192.168.1.115
intranetportal	Host (A)	192.168.1.101

These steps will automatically add an FQDN for 'intranetportal' as well since we are adding it as a host under the domain zone. This means that we in the example also get a DNS record for 'intranetportal.corp.balkestahl.se'

DNS.9 Verify the DNS entry by opening a Command prompt or Powershell prompt, then running the command 'ping intranetportal'. You should get a response from the servers IP address.

> ping intranetportal

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping intranetportal
Pinging intranetportal.corp.balkestahl.se [192.168.1.101] with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=5ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
PS C:\Users\Administrator>
```

DNS.10 Verify also that you can access the server using the FQDN for 'intranetportal'

> ping intranetportal.corp.balkestahl.se

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping intranetportal.corp.balkestahl.se
Pinging intranetportal.corp.balkestahl.se [192.168.1.101] with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator>
```

DNS.11 You have now successfully added a DNS (A) record for the address of your choice. Move along to the proper scenario 1-4 to configure Alternate Access Mappings.

Scenario 1

Add a user friendly NetBIOS name to the Web Application

In this scenario we want to add a more user friendly NetBIOS name to a Web Application so that the users don't have to use the server name to access SharePoint.

Like in the basic example previously we will use <http://intranetportal> as URL for our existing Web Application on port 80 on the server blksth-sp1.

I have added how this is done first using the graphical user interface, then how to do the same using only PowerShell.

Steps needed:

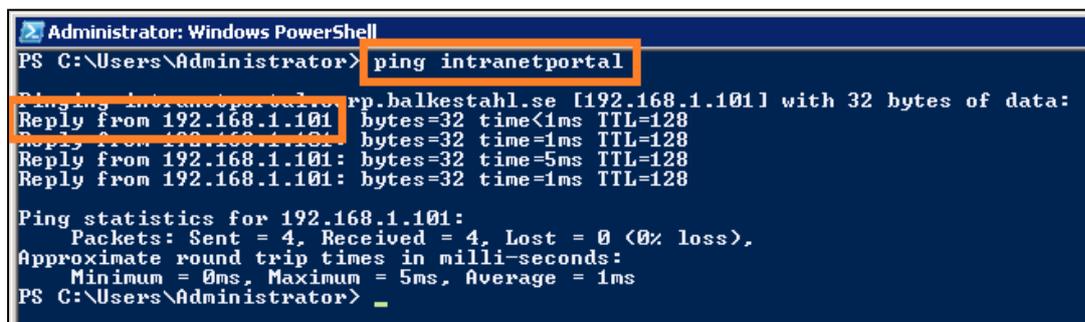
- 1.1 Add the URL to DNS with a pointer to the servers IP address. (See separate section).
- 1.2 Add a Public URL in Alternate Access Mappings (Internal URL is added automatically).
- 1.3 Add a Binding for the Web Site in Internet Information Services.
- 1.4 Verify access – **Done!**

In order to set a working friendly NetBIOS name as a URL of our Web Application, we need to add a public URL so that this friendly URL will be used as the URL everywhere and not be translated or redirected from.

- 1.1 Name Resolution. First simply verify that the name is added ok to the DNS.

Note: See separate section on [DNS](#) for a complete guide to adding a DNS record.

```
> ping intranetportal
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping intranetportal
Pinging intranetportal [192.168.1.101] with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=5ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
PS C:\Users\Administrator> _
```

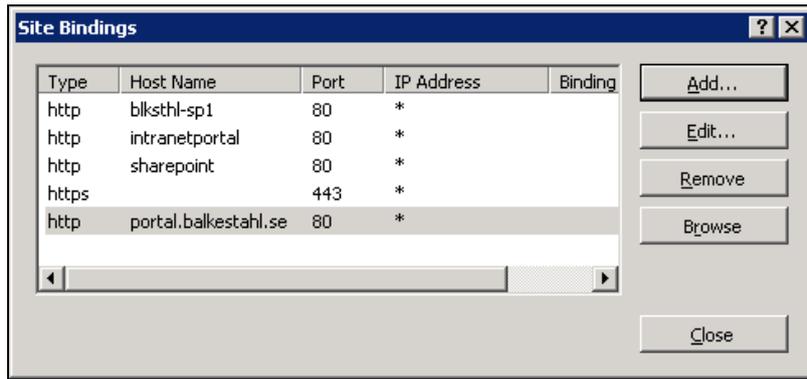
If you get a proper response with the SharePoint Web Servers IP address when you ping the URL, then DNS is set, if you don't, try first to flush the DNS cache.

```
> Ipconfig /flushdns
```

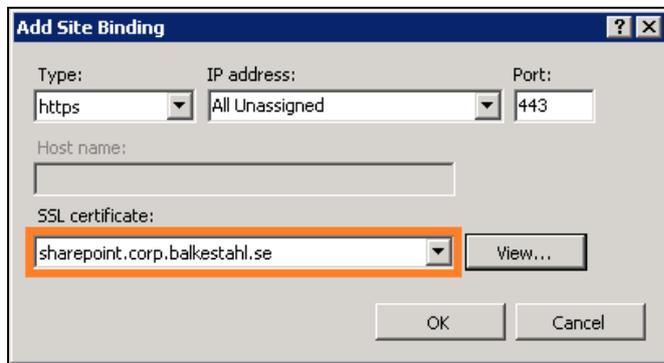
If ping still don't get you a response, recheck the In addition to the actual Alternate Access Mapping in SharePoint Central Administration, you also have to add a Binding in IIS, contrary to what many believe, SharePoint does not do that for you so you have to do it manually.

Steps on how to do that is added to every scenario in this guide.

The example above would show up in IIS Bindings like this:



As you can see, the https binding does not show up as a hostname, the hostname is determined by the name configured in certificate used when adding that binding.





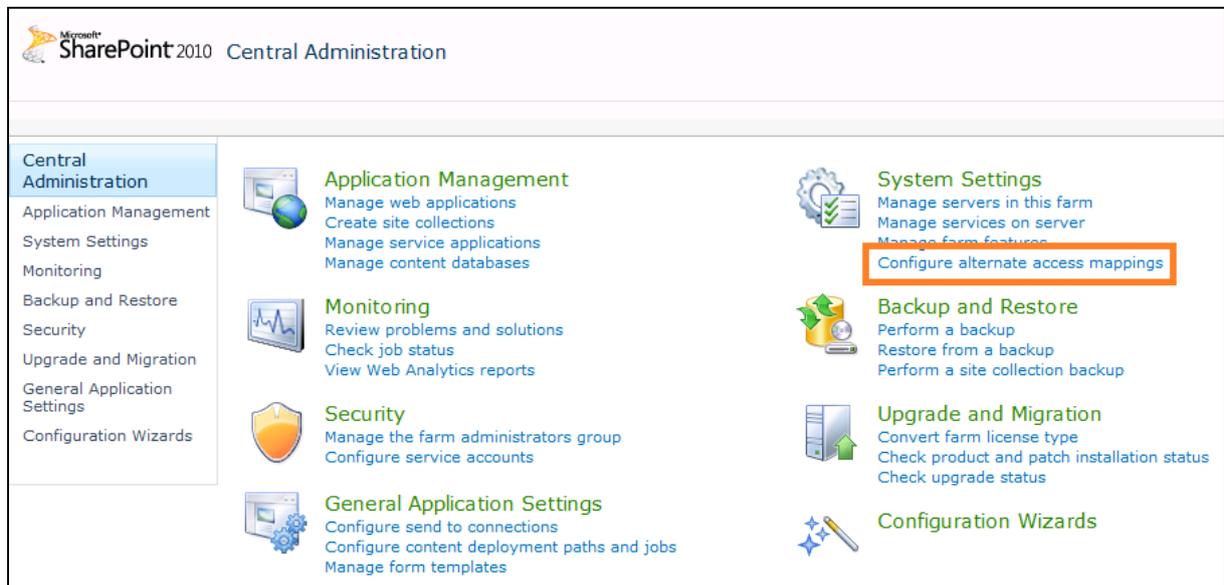
The final guide to Alternate Access Mappings
Release 1.0 - Whitepaper
By: Thomas Balkestahl - blog.blksth.com

17 October 2012

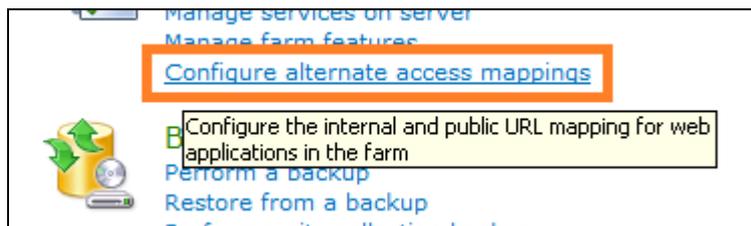
DNS section in this guide.

Thomas Balkestahl

1.2.0 After DNS is configured correctly and verified, open the 'Central Administration' site of your SharePoint Farm.



1.2.1 Click on 'Configure Alternate Access Mappings'.

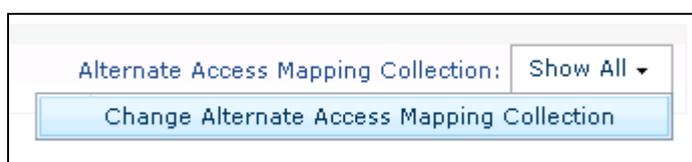


In this state we can see one line for the Central Administration Web Application and one for the Web Application on port 80. We only have the server name at this point.

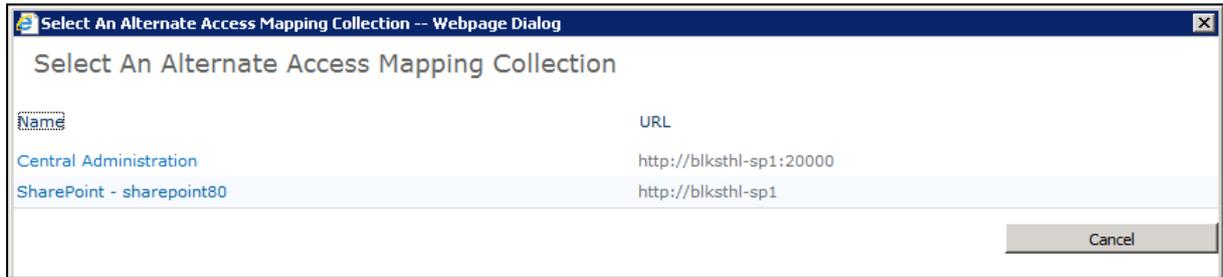
1.2.2 Note that the 'Alternate Access Mapping Collection' selector by default is set to 'Show All'.



1.2.3 Click on the 'Alternate Access Mapping Collection' selector and select 'Change Alternate Access Mapping Collection' in the dropdown.



1.2.4 Select our Web Application on port 80 by clicking on its link



1.2.5 Verify that the 'Alternate Access Mapping Collection' selection dropdown is set to the Web Application on port 80, in this example 'SharePoint - SharePoint80'



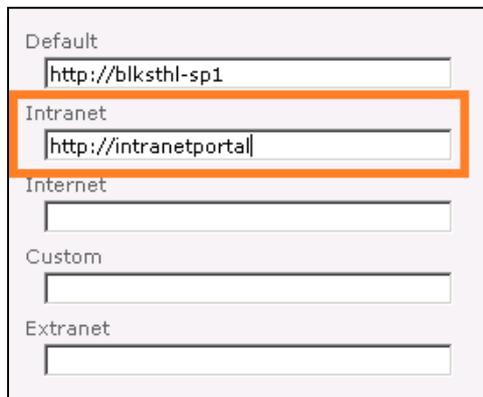
1.2.6 Now, we need to add a new Public URL to the Web Application, click on 'Edit Public URLs'



1.2.7 In the dialog for Public URLs you see that you have 5 different textboxes, each with a zone name in front of it. It does not matter which zone we select to use, but since it fits, we will use the 'Intranet' zone.



1.2.8 Type 'http://intranetportal' including the protocol – http, into the textbox named 'Intranet' and click on 'Save'



Default
http://blksth-sp1

Intranet
http://intranetportal

Internet

Custom

Extranet

1.2.9 Now, you will see that a new line has been added to the collection view, we now have a line for 'Default' zone and one for the 'Intranet' zone, the 'Internal URL' is added automatically, our example now looks like this.



Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal

1.2.10 Select again to 'Show All' in the 'Alternate Access Mapping Collection' selection dropdown.

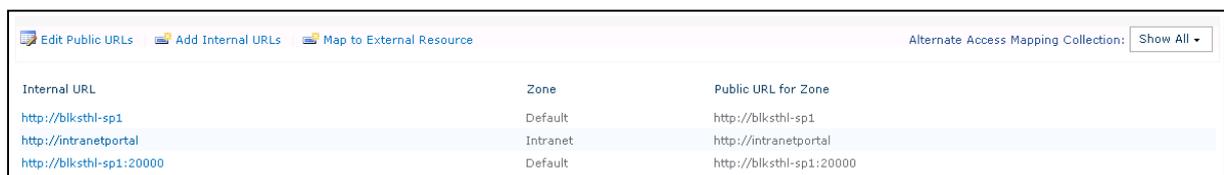


Alternate Access Mapping Collection: SharePoint - sharepoint80

Change Alternate Access Mapping Collection

Show All

1.2.11 Now, our Alternate Access Mappings looks like this.

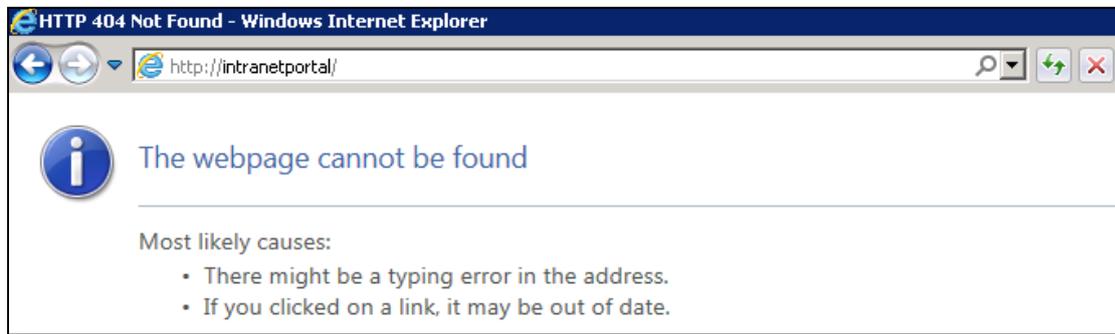


Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal
http://blksth-sp1:20000	Default	http://blksth-sp1:20000

1.2.12 So, we have an URL connected to the Web Application, let's try to access it in a browser.



1.2.13 'The webpage cannot be found'...this is to be expected. So no worries, things are like they should be. At least, this is how things work in SharePoint 2010.

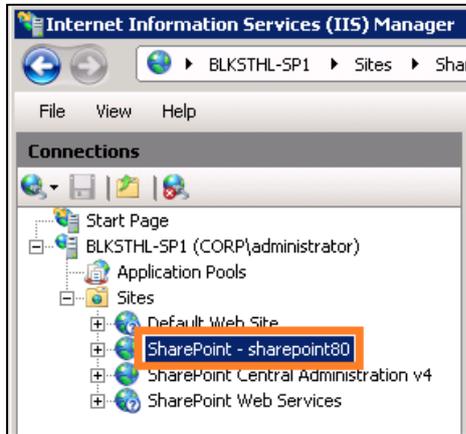


1.3.0 Bindings. What we need to do in addition, is to bind the new URL to the web site in Internet Information Services.

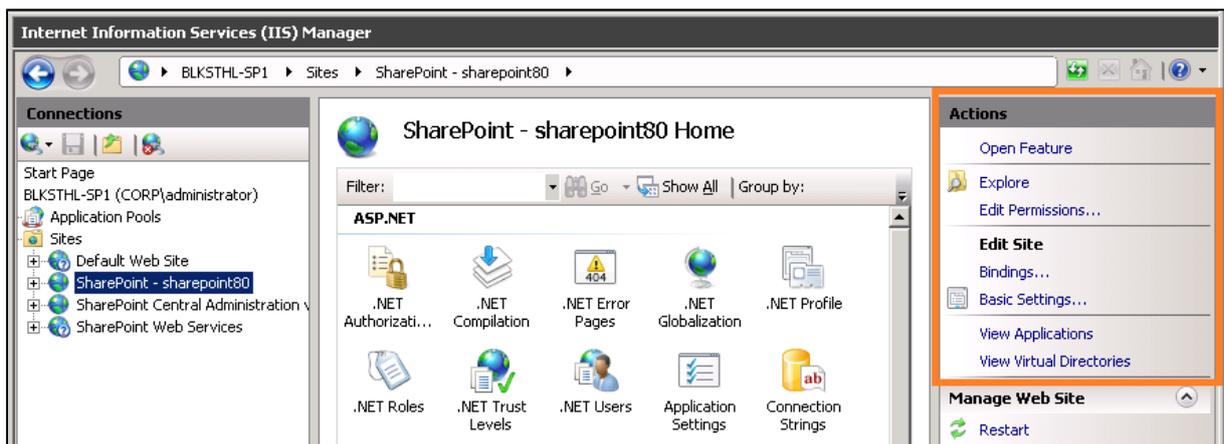
1.3.1 Start the 'Internet Information Services (IIS) Manager.



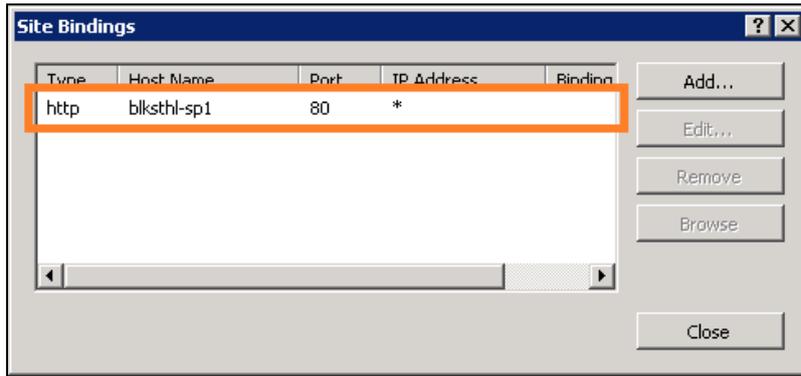
1.3.2 Expand the 'Servername' container and the 'Sites' container, then select your Web Application , in our example, 'SharePoint – sharepoint80' by simply clicking on it.



1.3.3 Now on the right hand side, you see the 'Actions' pane. In this list, click on 'Bindings...'



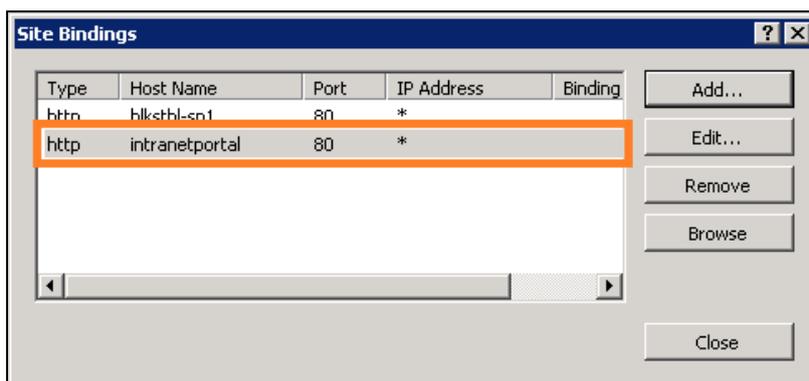
1.3.4 As you can see, we only have a binding for http and 'servername' and port 80.



1.3.5 Click on 'Add' and type in 'intranetportal' in the 'Host name:' textbox. Verify that http in the selected protocol and that 'All unassigned' as IP address and 80 as the port number. Click on 'OK'

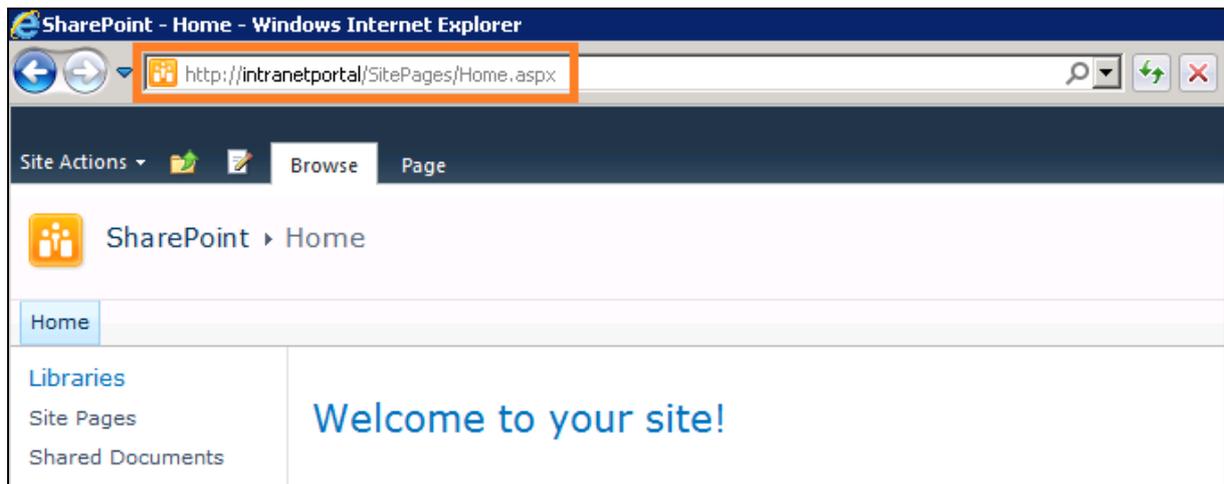


1.3.6 Verify that you can see the new binding in the list.



1.4.0 Verify access. Load the site in IE to verify that the Alternate Access Mapping and the Binding has been configured correctly.

Note: If this is done on the actual SharePoint Web server, make sure that the loopback-check has been configured or disabled to allow access using this URL. See [resolution section in this KB article](#)



Note: Since the address is a NetBIOS name, Internet Explorer will automatically recognize it as a local address and it will be a member of the 'Local intranet sites' zone. Internet Explorer will automatically logon using the currently logged on user to sites in the 'local intranet' zone in IE. (This zone is not related to the AAM zones in any way or form other than by name)

If the site loads, that's it! You are done. **Congratulations!**

1.4.1 Extra If you want to avoid users from using the server name at all, which in multi web server farms is a good idea, then replace the default zones public URL with the NetBIOS name or the primary URL you want users to use. When the Default Public URL is the NetBIOS name or a FQDN, simply put the server name as an Internal URL and connect it to the 'Default Zone'. This way, users who may have been used to typing in the server name will soon get used to only using the real address of the application, in our case, <http://intranetportal>.

Scenario 2

Add an FQDN to the Web Application

In this scenario we want to add an FQDN (i.e. <http://hostname.domain.com>) to a Web Application so that the Web Application may be accessed internally and or externally using the same URL.

We will use <http://portal.balkesth.se> as the URL for our existing Web Application on port 80 on the server blksth-sp1.

For detailed steps on where to do the different steps and how to access the different settings, see scenario 1. In Scenario 1 every step is well documented thru the entire way of the configurations.

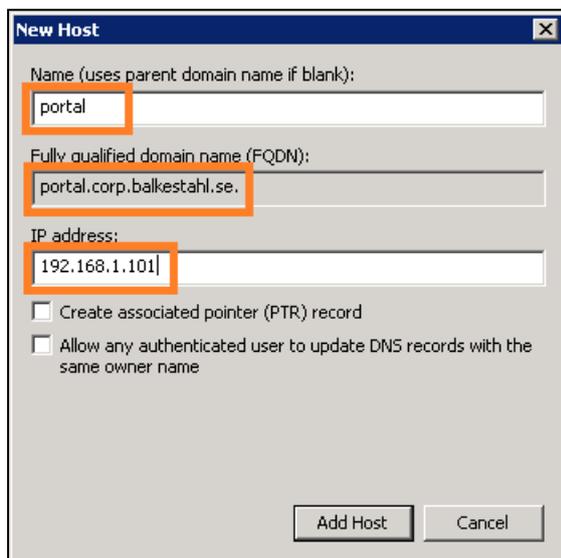
Steps needed:

- 2.1 Add the URL to DNS with a pointer to the servers IP address.
- 2.2 Add a Public URL in Alternate Access Mappings.
- 2.3 Verify that an Internal URL is created in Alternate Access Mappings.
- 2.4 Add a binding for the Web Site in Internet Information Services.
- 2.5 Add the site as a local intranet site in IE to avoid logon prompt. (Better: use a GPO)
- 2.6 Verify access

2.1.0 Make sure that the name 'portal' is added to the correct zone (domain name) in DNS.

For internet access, the FQDN must be accessible from the internet as well either by using a public IP address for the server or a forwarder in the externally accessible firewall/router.

Note: See separate section on [DNS](#) for a complete guide to adding a DNS record.



intranetportal	Host (A)	192.168.1.101
portal	Host (A)	192.168.1.101

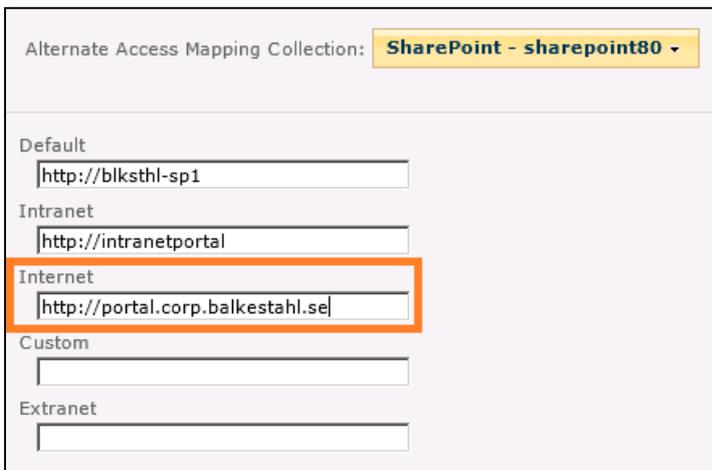
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ping portal.corp.balkestahl.se

Pinging portal.corp.balkestahl.se [192.168.1.101] with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator>
```

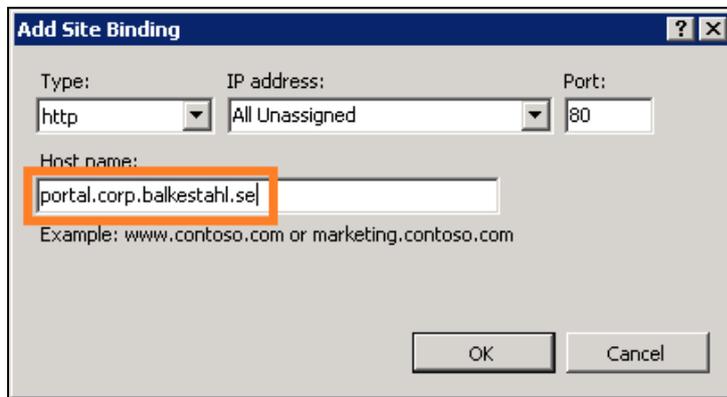
2.2.0 Add an Alternate Access Mapping Public URL to the Web Applications collection. In this case, we use the 'Internet' zone and we add the URL portal.corp.balkestahl.se.



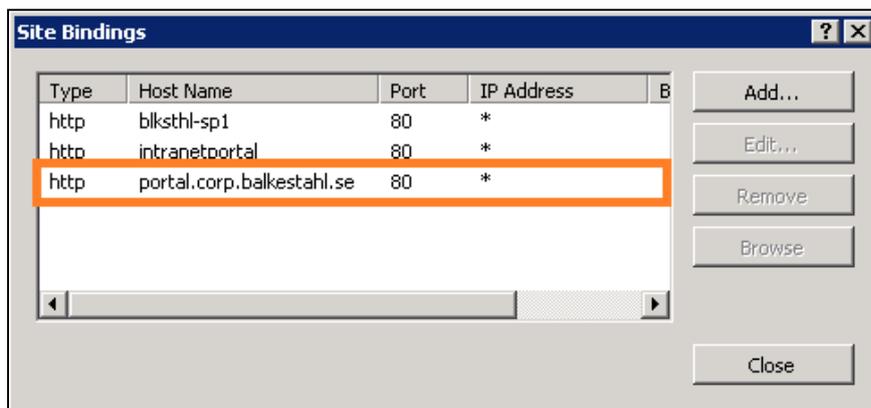
2.3.0 Verify that an Internal URL has been created and are connected to the Public URL we created via the 'Internet' zone.

Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal
http://portal.corp.balkestahl.se	Internet	http://portal.corp.balkestahl.se

2.4.0 Add a Binding to the Web Site in IIS. Use http and port 80 and all Ip addresses. Use the full FQDN as the Host Header.



2.4.1 Verify that the URL you have entered shows up in the list of bindings.

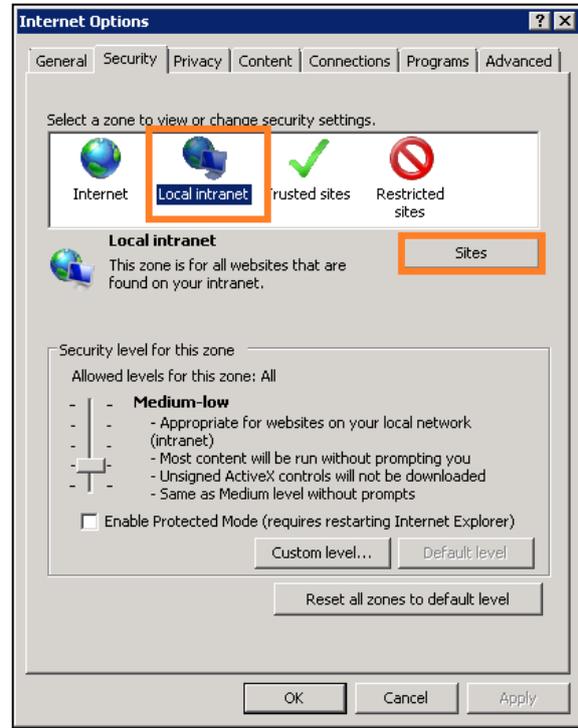


2.5.0 Add the site to IE's Local Intranet sites, this is to have IE automatically logon using logged on credentials. If you don't, the risk is that you get a login prompt every time you try to access the site.

2.5.1



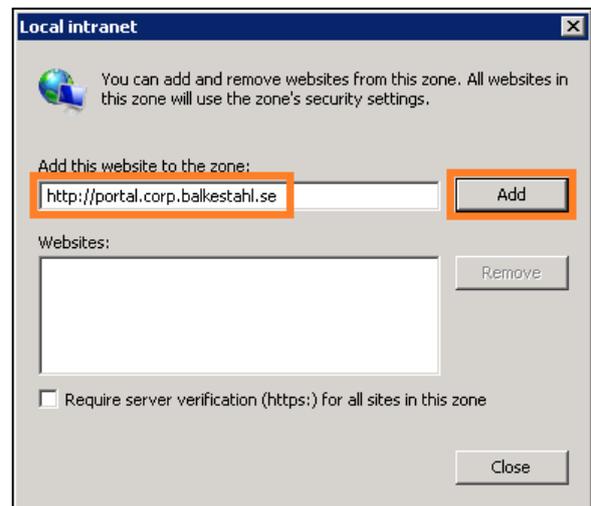
2.5.2



2.5.3



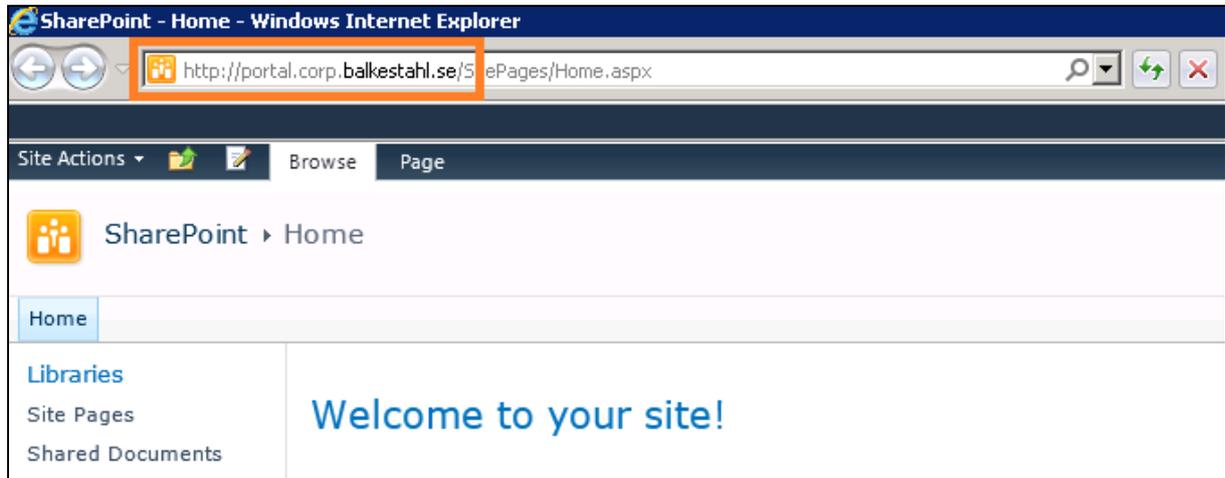
2.5.4



Note: It is recommended to do this in a larger environment using a GPO and Active Directory:
Edit your IE settings GPO (or create a new one) with the following - Computer Configuration - Administrative Templates - Windows Components - Internet Explorer - Internet Control Panel - Security Page - Site to Zone Assignment List - Enabled
Then click the Show button - and add the appropriate Value Name and Value - e.g.:
http://portal.corp.balkestahl.se with a value of 1 for Intranet Zone.

2.6.0 Verify functionality in a web browser.

Note: If this is done on the actual SharePoint Web server, make sure that the loopback-check has been configured or disabled to allow access using this URL. See [resolution section in this KB article](#)



Note: Internet Explorer will recognize this address as an internet address and it will be considered in the 'Internet' zone until we tell IE otherwise. See step 2.5

If the site loads, that's it! You are done. **Congratulations!**

Scenario 3

Add an https/SSL FQDN to the Web Application

In this scenario we want to add an https FQDN (i.e. <http://name.domain.com>) to a Web Application so that the Web Application may be accessed in an encrypted and safe manner using one URL. Like in the basic example previously we will use <http://intranetportal> as URL for our existing Web Application on port 80 on the server blksth-sp1.

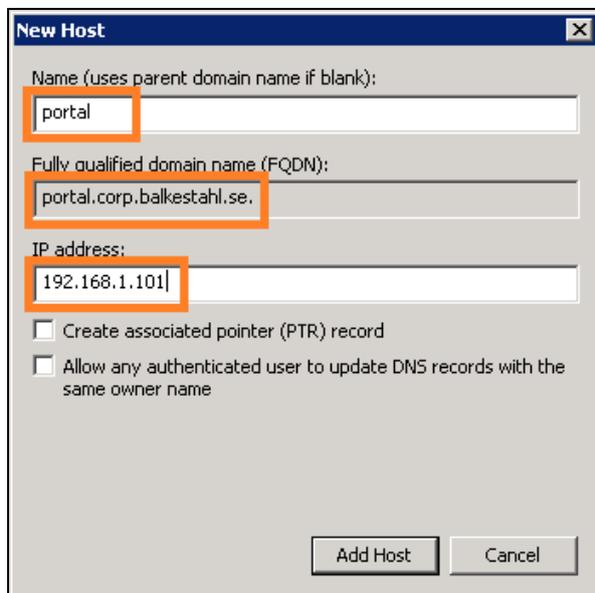
Steps needed:

- 3.1** Add the URL to DNS with a pointer to the servers IP address.
- 3.2** Add a Public URL in Alternate Access Mappings
- 3.3** Verify that an Internal URL is created.
- 3.4** Add a binding for the Web Site in Internet Information Services using an installed certificate
- 3.5** Add the site as a local intranet site in IE to avoid logon prompt. (AD Group policy)
- 3.6** Verify access

3.1.0 Make sure that the name 'portal' is added to the correct zone (domain name) in DNS.

For internet access, the FQDN must be accessible from the internet as well either by using a public IP address for the server or a forwarder in the externally accessible firewall/router.

Note: See separate section on [DNS](#) for a complete guide to adding a DNS record.



intranetportal	Host (A)	192.168.1.101
portal	Host (A)	192.168.1.101

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ping portal.corp.balkestahl.se

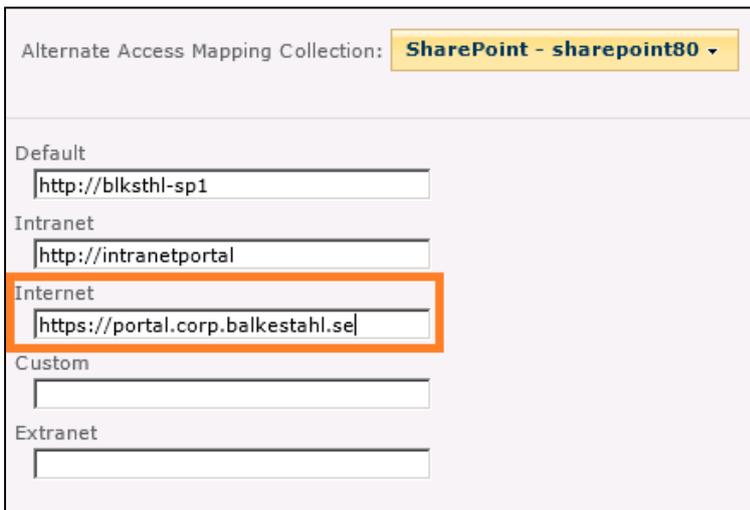
Pinging portal.corp.balkestahl.se [192.168.1.101] with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time<1ms TTL=128
Reply from 192.168.1.101: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator>
  
```

3.2.0 First we start of by having only URL's for the 'Default' and the 'Intranet' zones.

Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal

3.2.1 Add an Alternate Access Mapping Public URL to the Web Applications collection. In this case, we use the 'Internet' zone.



Alternate Access Mapping Collection: **SharePoint - sharepoint80**

Default:

Intranet:

Internet:

Custom:

Extranet:

3.3.0 Verify that an Internal URL has been created and are connected to the Public URL we created via the 'Internet' zone.

Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal
https://portal.corp.balkestahl.se	Internet	https://portal.corp.balkestahl.se

3.4.0 Add a Binding to the Web Site in IIS.

Note: You need to have a SSL certificate installed in order to complete this step.

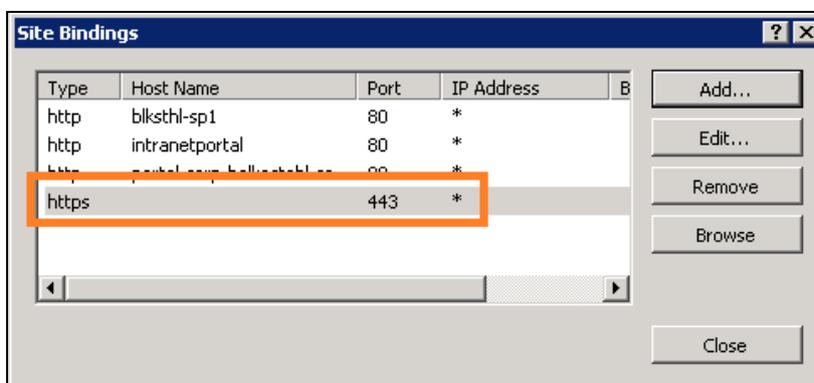
3.4.1 Select https and then the installed certificate in the dropdown list. The Host Header will be greyed out.



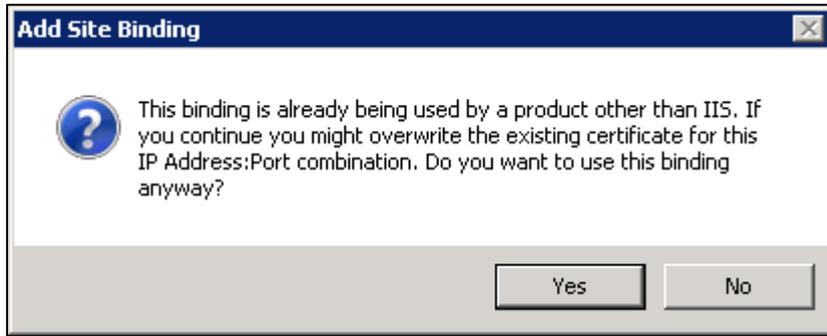
3.4.2 Select the certificate that is installed with your URL, note that the Host Header textbox is greyed out.



3.4.3 Note that the binding is added to the list with port 443.



3.4.4 If the certificate is or have been used in another application in this IIS, you may see this popup, simply click yes if everything feels ok and it will go away.

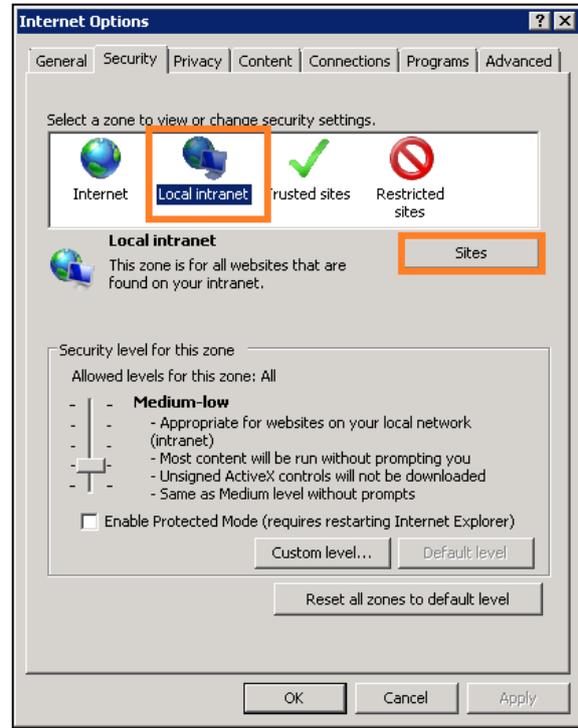


3.5.0 Add the site to IE's Local Intranet sites, this is to have IE automatically logon using logged on credentials. If you don't, the risk is that you get a login prompt every time you try to access the site.

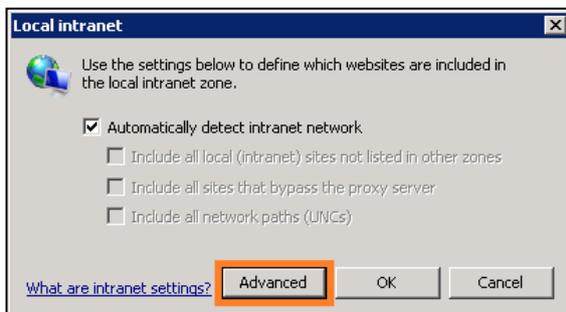
3.5.1



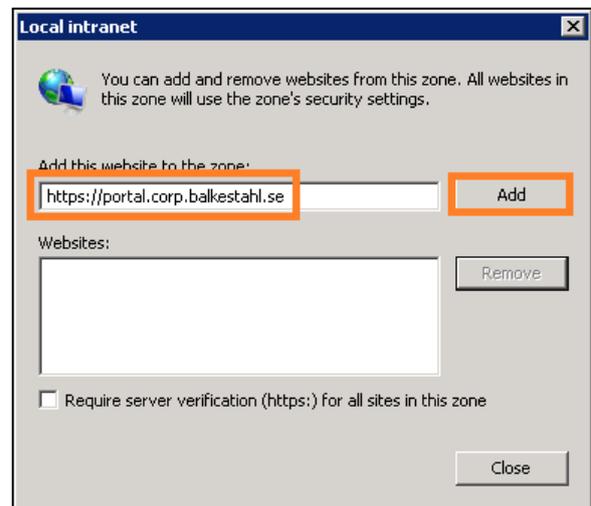
3.5.2



3.5.3



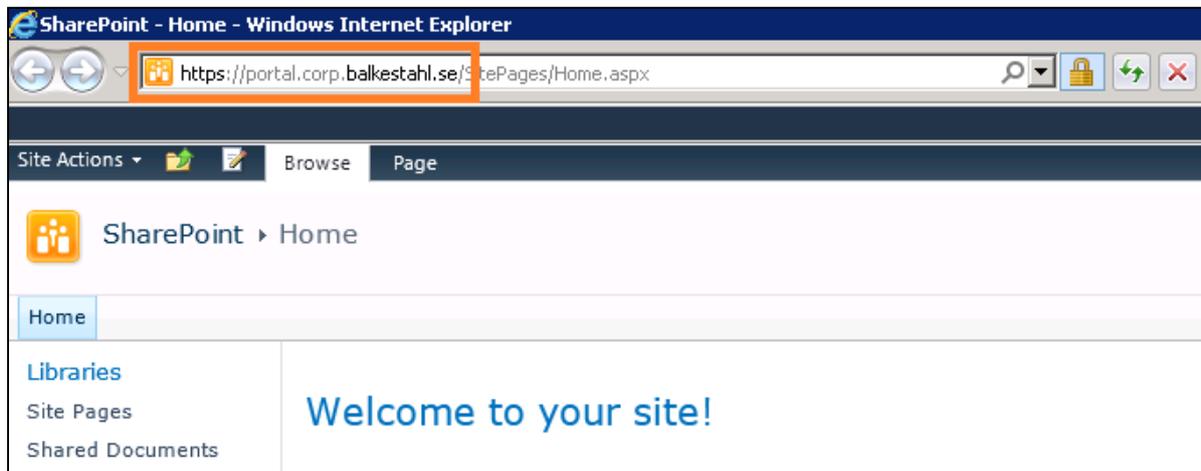
3.5.4



Note: It is recommended to do this in a larger environment using a GPO and Active Directory:
Edit your IE settings GPO (or create a new one) with the following - Computer Configuration - Administrative Templates - Windows Components - Internet Explorer - Internet Control Panel - Security Page - Site to Zone Assignment List - Enabled
Then click the Show button - and add the appropriate Value Name and Value – e.g.:
http://portal.corp.balkestahl.se with a value of 1 for Intranet Zone.

3.6.0 Verify functionality in a web browser.

Note: If this is done on the actual SharePoint Web server, make sure that the loopback-check has been configured or disabled to allow access using this URL. See [resolution section in this KB article](#)



Note: Internet Explorer will recognize this address as an internet address and it will be considered in the 'Internet' zone until we tell IE otherwise. See step 3.5

If the site loads, that's it! You are done. **Congratulations!**

Scenario 4

Add a redirect from http to https

In this scenario we assume that you have an https FQDN address configured and working as described in scenario 3. Now we want to add a redirect/transformation of all requests coming in on http to the https address, this since we want to keep our environment as secure as possible.

Steps needed:

4.1 Add an Internal URL in Alternate Access Mappings connected to the https address zone

4.2 Add the site as a local intranet site in IE to avoid logon prompt. (AD Group policy)

4.3 Verify access

Note: As a part of the prerequisites for this scenario, you need to have performed scenario 3, when that is configured, you will have a DNS record for the FQDN address (same regardless of the http or https protocol) and the FQDN using https is already up and running.

4.1.0 First, in Central administration and Alternate Access Mappings management, verify that the 'Alternate Access Mapping Collection' selection dropdown is set to the Web Application on port 80, in this example 'SharePoint – SharePoint80'.

Alternate Access Mapping Collection: SharePoint - sharepoint80 ▾

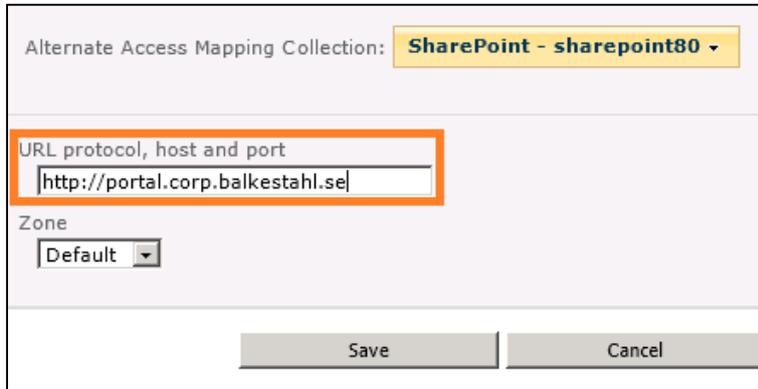
4.1.1 Before starting we can also note that we have the https FQDN address configured as described in Scenario 3. You can see that an 'Internal URL' is connected to a 'Public URL' via the 'Internet' zone. The 'Internet' zone is what we will use to connect our new http address later on.

Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal
https://portal.corp.balkestahl.se	Internet	https://portal.corp.balkestahl.se

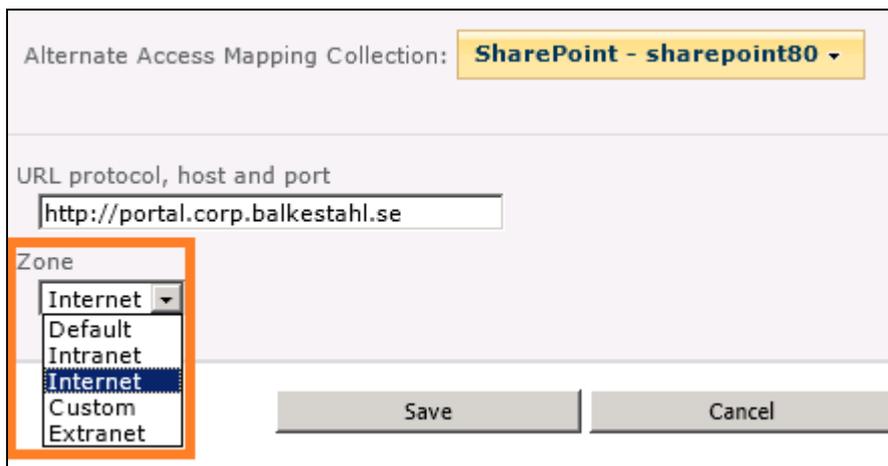
4.1.2 This time, we click on 'Add Internal URL' in order to add a URL that will only act as a pointer to an existing 'Public URL'.

 Add Internal URLs

4.1.3 In the 'URL protocol, host and port' textbox, enter the http address that you will redirect to the https address.



4.1.4 In the 'Zone' dropdown selection box, select the zone 'Internet' as this was the zone our https address was added to.



4.1.5 Click on 'Save' and verify that a new line has been added to our Alternate Access Mappings Collection, a line with an internal http address on the left and a Public https on the right. By selecting the 'Internet' zone when adding the 'Internal URL' we made the connection.



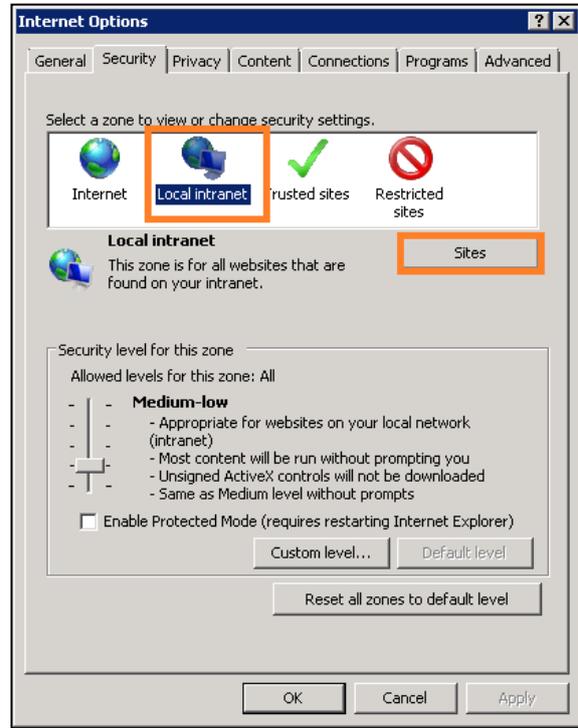
Internal URL	Zone	Public URL for Zone
http://blksth-sp1	Default	http://blksth-sp1
http://intranetportal	Intranet	http://intranetportal
https://portal.corp.balkestahl.se	Internet	https://portal.corp.balkestahl.se
http://portal.corp.balkestahl.se	Internet	https://portal.corp.balkestahl.se

4.2.0 Add the site to IE's Local Intranet sites, this is to have IE automatically logon using logged on credentials. If you don't, the risk is that you get a login prompt every time you try to access the site.

4.2.1



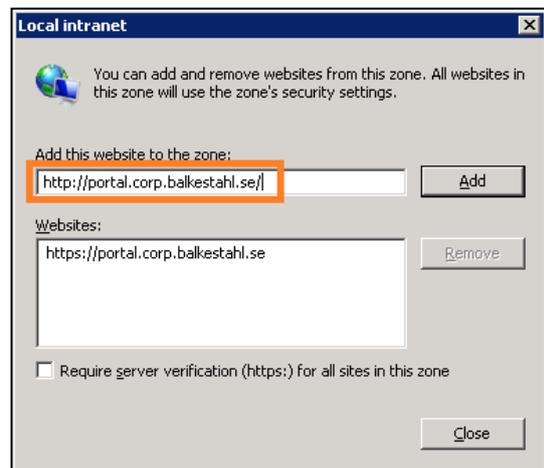
4.2.2



4.2.3



4.2.4



Note: It is recommended to do this in a larger environment using a GPO and Active Directory:
Edit your IE settings GPO (or create a new one) with the following - Computer Configuration - Administrative Templates - Windows Components - Internet Explorer - Internet Control Panel - Security Page - Site to Zone Assignment List - Enabled
Then click the Show button - and add the appropriate Value Name and Value - e.g.:
http://portal.corp.balkestahl.se with a value of 1 for Intranet Zone.

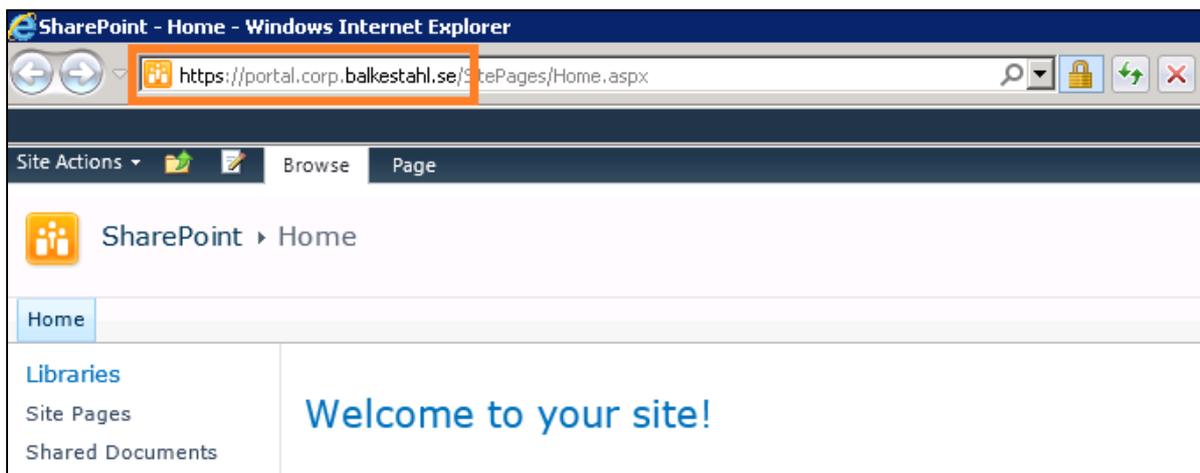
4.3.0 Verify functionality in a web browser.

Note: If this is done on the actual SharePoint Web server, make sure that the loopback-check has been configured or disabled to allow access using this URL. See [resolution section in this KB article](#)

4.3.1 Type in the http address in a new browser or tab and press enter.



4.3.2 Note that the page loads and redirects/transforms the address to https.



Note: Internet Explorer will recognize this address as an internet address and it will be considered in the 'Internet' zone until we tell IE otherwise. See step 3.5

If the site loaded, that's it! You are done. **Congratulations!**

PowerShell

PowerShell Doing the same thing as above using Powershell is not that complicated, the following commands takes care of it. In a PowerShell prompt or a SharePoint Management shell running 'as admin' the following steps will accomplish the same as using the graphical user interface. Follow the outlined steps:

5.1 Scenario 1 – Add a user friendly NetBIOS name to the Web Application

5.2 Scenario 2 – Add an http FQDN to the Web Application

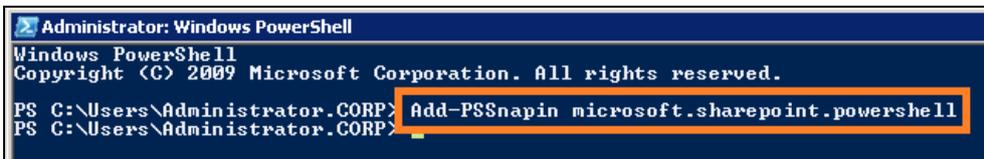
5.3 Scenario 3 – Add an https/SSL FQDN to the Web Application

5.4 Scenario 4 – Add a redirect from http to https

5.1.0 Add a user friendly NetBIOS name to the Web Application

5.1.1 Load the SharePoint PowerShell snapin.

> Add-PSSnapin Microsoft.sharepoint.powershell



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CORP> Add-PSSnapin microsoft.sharepoint.powershell
PS C:\Users\Administrator.CORP>
```

5.1.2 Lists the Web applications to get the 'Name/DisplayName':

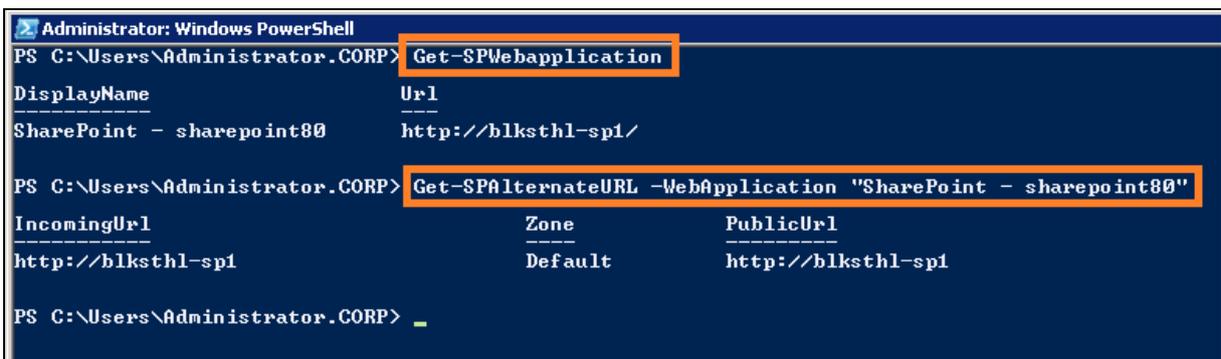
> Get-SPWebApplication

TechNet Reference: [Get-SPWebApplication](#)

5.1.3 Lists the AlternateAccess Mappings configured for the Web Application / Collection:

> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"

TechNet Reference: [Get-SPAlternateURL](#)



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPWebapplication
-----
DisplayName          Url
-----
SharePoint - sharepoint80  http://blksth1-sp1/

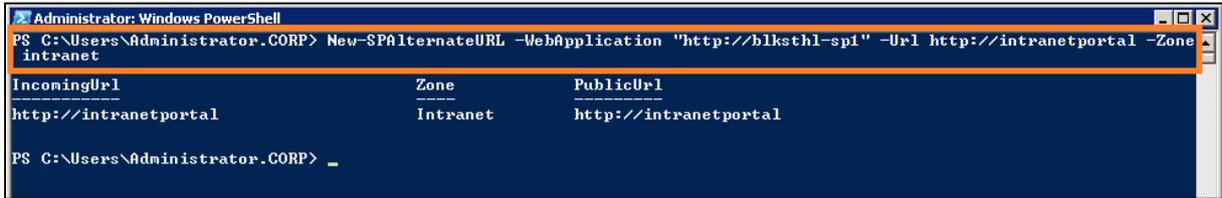
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"
-----
IncomingUrl          Zone          PublicUrl
-----
http://blksth1-sp1  Default      http://blksth1-sp1

PS C:\Users\Administrator.CORP>
```

5.1.4 Add the http://intranetportal URL as an Alternate Access Mapping:

```
> New-SPAlternateURL -WebApplication http://blksth1-sp1 -Url  
http://intranetportal -Zone intranet
```

TechNet Reference: [New-SPAlternateURL](#)



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> New-SPAlternateURL -WebApplication "http://blksth1-sp1" -Url http://intranetportal -Zone  
intranet
```

IncomingUrl	Zone	PublicUrl
http://intranetportal	Intranet	http://intranetportal

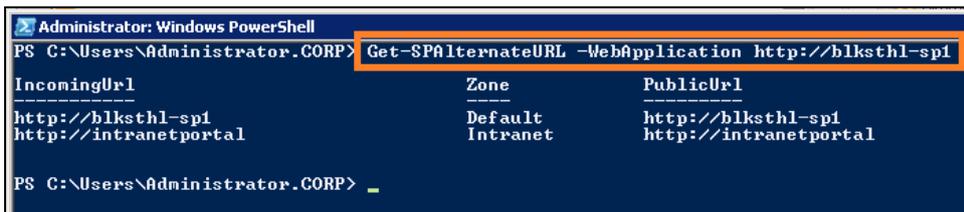
```
PS C:\Users\Administrator.CORP> _
```

5.1.5 Verify that it has been added:

```
> Get-SPAlternateURL -WebApplication http://blksth1-sp1
```

TechNet Reference: [Get-SPAlternateURL](#)

Now we are done with the SharePoint part. Next step is to add a binding in IIS.



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication http://blksth1-sp1
```

IncomingUrl	Zone	PublicUrl
http://blksth1-sp1	Default	http://blksth1-sp1
http://intranetportal	Intranet	http://intranetportal

```
PS C:\Users\Administrator.CORP> _
```

5.1.6 Loads the IIS administration module:

```
> Import-Module WebAdministration
```

TechNet Reference: [Import-Module](#)

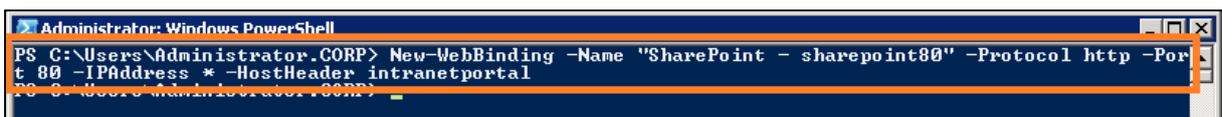


```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> Import-Module webadministration  
PS C:\Users\Administrator.CORP> _
```

5.1.7 Adds a binding with a specified protocol, IP address and Host Header to an IIS Web site by name:

```
> New-WebBinding -Name "SharePoint - sharepoint80" -Protocol http -Port 80  
-IPAddress * -HostHeader intranetportal
```

TechNet Reference: [New-WebBinding](#)

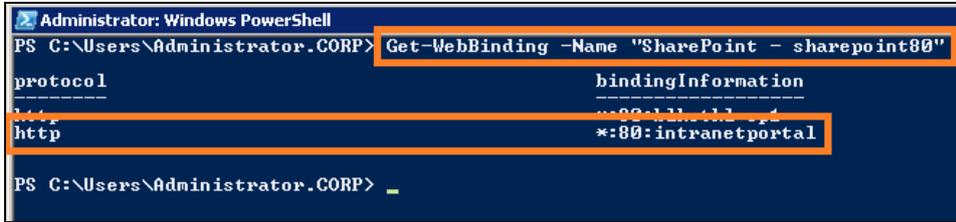


```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> New-WebBinding -Name "SharePoint - sharepoint80" -Protocol http -Port 80 -IPAddress * -HostHeader intranetportal  
PS C:\Users\Administrator.CORP> _
```

5.1.8 Verify that the Binding has been added correctly:

```
> Get-WebBinding -Name "SharePoint - sharepoint80"
```

TechNet Reference: [Get-WebBinding](#)



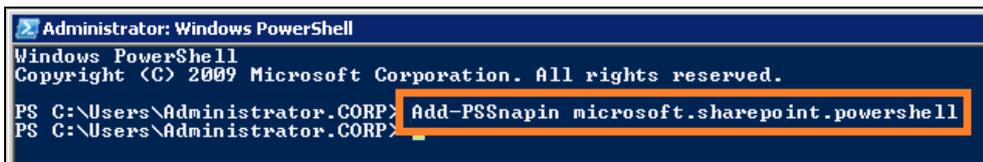
```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-WebBinding -Name "SharePoint - sharepoint80"
protocol bindingInformation
-----
http *:80:intranetportal
PS C:\Users\Administrator.CORP> _
```

5.1.9 Done!

5.2.0 Add an http FQDN to the Web Application

5.2.1 Load the SharePoint PowerShell snapin.

```
> Add-PSSnapin Microsoft.sharepoint.powershell
```



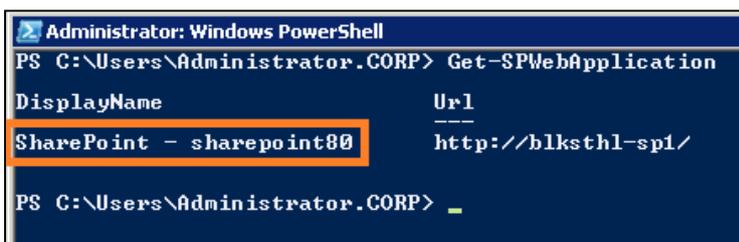
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CORP> Add-PSSnapin microsoft.sharepoint.powershell
PS C:\Users\Administrator.CORP> _
```

5.2.2 Lists the Web applications to get the 'Name/DisplayName':

```
> Get-SPWebApplication
```

TechNet Reference: [Get-SPWebApplication](#)

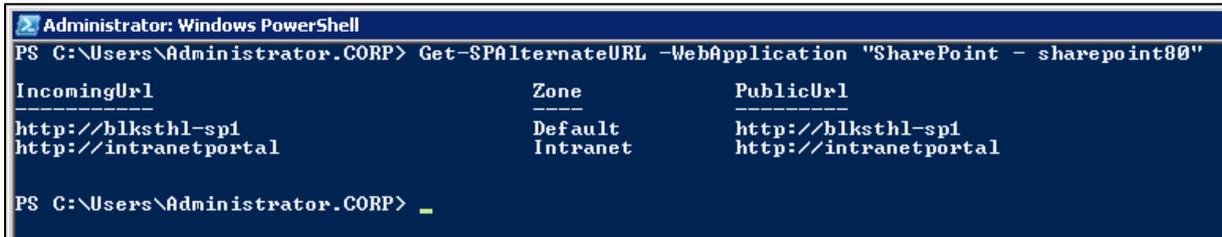


```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPWebApplication
DisplayName Url
-----
SharePoint - sharepoint80 http://blksth1-spl/
PS C:\Users\Administrator.CORP> _
```

5.2.3 Lists the AlternateAccess Mappings configured for the Web Application / Collection:

```
> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"
```

TechNet Reference: [Get-SPAlternateURL](#)



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"

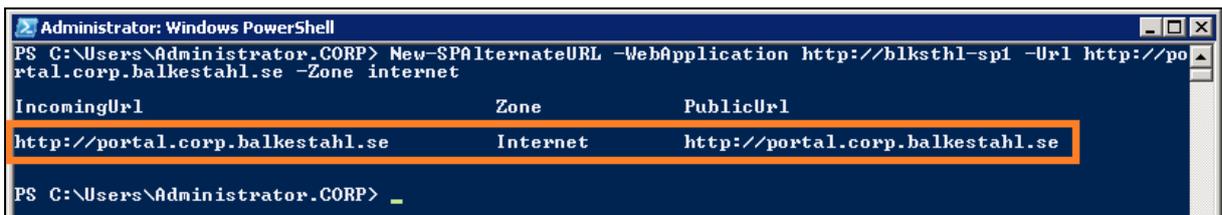
IncomingUrl                Zone                PublicUrl
-----
http://blksth1-spl         Default            http://blksth1-spl
http://intranetportal     Intranet          http://intranetportal

PS C:\Users\Administrator.CORP> _
```

5.2.4 Add the http://intranetportal URL as an Alternate Access Mapping:

```
> New-SPAlternateURL -WebApplication http://blksth1-spl -Url
http://portal.corp.balkestahl.se -Zone intranet
```

TechNet Reference: [New-SPAlternateURL](#)



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> New-SPAlternateURL -WebApplication http://blksth1-spl -Url http://portal.corp.balkestahl.se -Zone internet

IncomingUrl                Zone                PublicUrl
-----
http://portal.corp.balkestahl.se  Internet          http://portal.corp.balkestahl.se

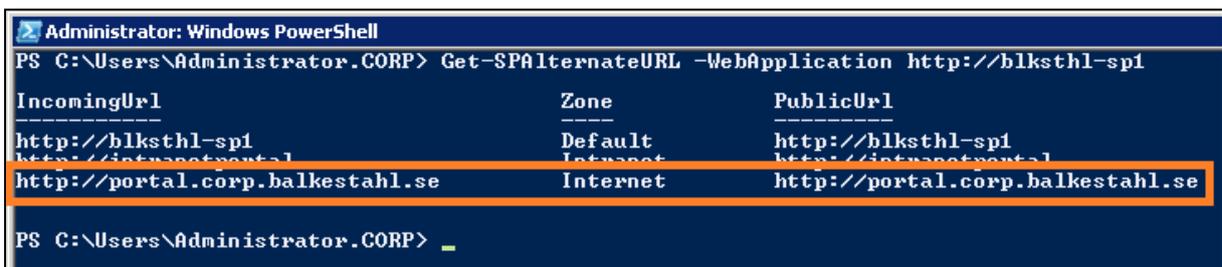
PS C:\Users\Administrator.CORP> _
```

5.2.5 Verify that it has been added:

```
> Get-SPAlternateURL -WebApplication http://blksth1-spl
```

TechNet Reference: [Get-SPAlternateURL](#)

Note: Now we are done with the SharePoint part. Next step is to add a binding in IIS.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication http://blksth1-spl

IncomingUrl                Zone                PublicUrl
-----
http://blksth1-spl         Default            http://blksth1-spl
http://intranetportal     Intranet          http://intranetportal
http://portal.corp.balkestahl.se  Internet          http://portal.corp.balkestahl.se

PS C:\Users\Administrator.CORP> _
```

5.2.6 Loads the IIS administration module:

```
> Import-Module WebAdministration
```

TechNet Reference: [Import-Module](#)



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Import-Module webadministration
PS C:\Users\Administrator.CORP>
```

5.2.7 Adds a binding with a specified protocol, IP address and Host Header to an IIS Web site by name:

```
> New-WebBinding -Name "SharePoint - sharepoint80" -Protocol http -Port 80
-IPAddress * -HostHeader portal.corp.balkestahl.se
```

TechNet Reference: [New-WebBinding](#)

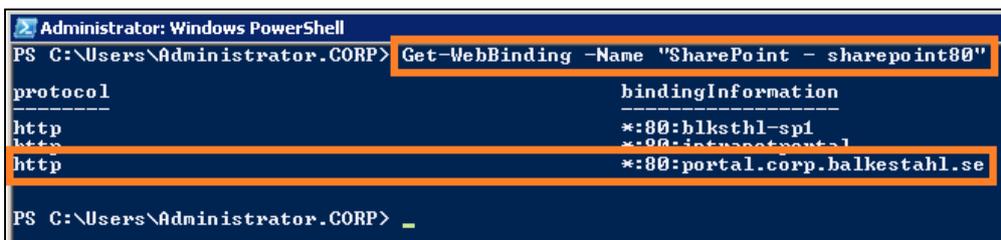


```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> New-WebBinding -Name "SharePoint - sharepoint80" -Protocol http -Port 80 -IPAddress * -HostHeader portal.corp.balkestahl.se
PS C:\Users\Administrator.CORP>
```

5.2.8 Verify that the Binding has been added correctly:

```
> Get-WebBinding -Name "SharePoint - sharepoint80"
```

TechNet Reference: [Get-WebBinding](#)



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-WebBinding -Name "SharePoint - sharepoint80"

protocol          bindingInformation
-----
http              *:80:blksth-spl
http              *:80:portal.corp.balkestahl.se
http              *:80:portal.corp.balkestahl.se

PS C:\Users\Administrator.CORP>
```

5.2.9 Done!

5.3.0 Adding a https/SSL FQDN Alternate Access Mapping

5.3.1 Load the SharePoint PowerShell snapin.

> Add-PSSnapin Microsoft.sharepoint.powershell

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CORP> Add-PSSnapin microsoft.sharepoint.powershell
PS C:\Users\Administrator.CORP> _
```

5.3.2 Lists the Web applications to get the 'Name/DisplayName':

> Get-SPWebApplication

TechNet Reference: [Get-SPWebApplication](#)

```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPWebApplication

DisplayName          Url
-----
SharePoint - sharepoint80  http://blksth1-sp1/

PS C:\Users\Administrator.CORP> _
```

5.3.3 Lists the AlternateAccess Mappings configured for the Web Application / Collection:

> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"

TechNet Reference: [Get-SPAlternateURL](#)

```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"

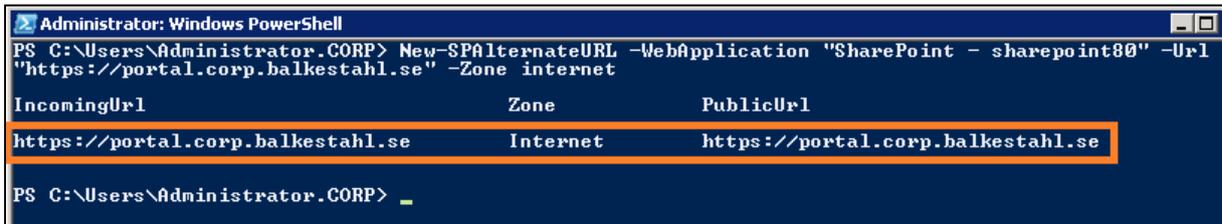
IncomingUrl          Zone          PublicUrl
-----
http://blksth1-sp1   Default      http://blksth1-sp1
http://intranetportal Intranet     http://intranetportal
http://portal.corp.balkestahl.se Internet     http://blksth1-sp1

PS C:\Users\Administrator.CORP> _
```

5.3.4 Add the http://intranetportal URL as an Alternate Access Mapping:

```
> New-SPAlternateURL -WebApplication "SharePoint - sharepoint80" -Url  
https://portal.corp.balkestahl.se -Zone internet
```

TechNet Reference: [New-SPAlternateURL](#)



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> New-SPAlternateURL -WebApplication "SharePoint - sharepoint80" -Url  
"https://portal.corp.balkestahl.se" -Zone internet
```

IncomingUrl	Zone	PublicUrl
https://portal.corp.balkestahl.se	Internet	https://portal.corp.balkestahl.se

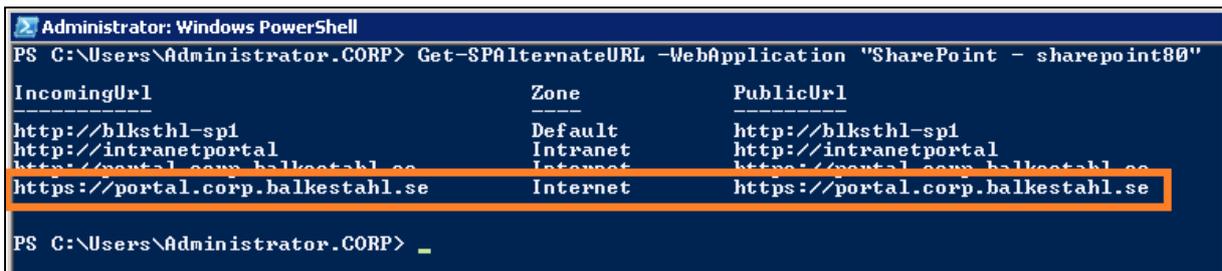
```
PS C:\Users\Administrator.CORP> _
```

5.3.5 Verify that it has been added:

```
> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"
```

TechNet Reference: [Get-SPAlternateURL](#)

Note: Now we are done with the SharePoint part. Next step is to add a binding in IIS.



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"
```

IncomingUrl	Zone	PublicUrl
http://blksth1-spi	Default	http://blksth1-spi
http://intranetportal	Intranet	http://intranetportal
https://portal.corp.balkestahl.se	Internet	https://portal.corp.balkestahl.se

```
PS C:\Users\Administrator.CORP> _
```

5.3.6 Loads the IIS administration module:

```
> Import-Module WebAdministration
```

TechNet Reference: [Import-Module](#)



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> Import-Module webadministration  
PS C:\Users\Administrator.CORP> _
```

5.3.7 Add a binding 'place holder' to the Web site in IIS, use the URL, port and protocol as below.

```
> New-WebBinding -Name "SharePoint - sharepoint80" -Port 443 -Protocol  
https -HostHeader portal.corp.balkestahl.se
```



```
Administrator: Windows PowerShell  
PS C:\Users\Administrator.CORP> New-WebBinding -Name "SharePoint - sharepoint80" -Port 443 -Protocol https -HostHeader portal.corp.balkestahl.se  
PS C:\Users\Administrator.CORP> _
```

5.3.8 Since we want to use an installed certificate to configure the https binding, we have to first get the cert to an object that we can refer to later.

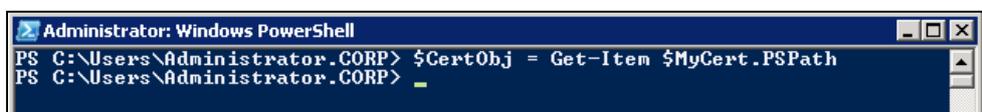
```
> $MyCert = Get-ChildItem cert:\localmachine\my | Where-Object {$_.Subject -eq "CN=portal.corp.balkestahl.se"}
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> $MyCert = Get-ChildItem cert:\localmachine\my | Where-Object {$_.Subject -eq "CN=portal.corp.balkestahl.se"}
PS C:\Users\Administrator.CORP> _
```

5.3.9 From the Certificate Object we pick the path to be used when creating the binding.

```
> $CertObj = Get-Item $MyCert.PSPath
```

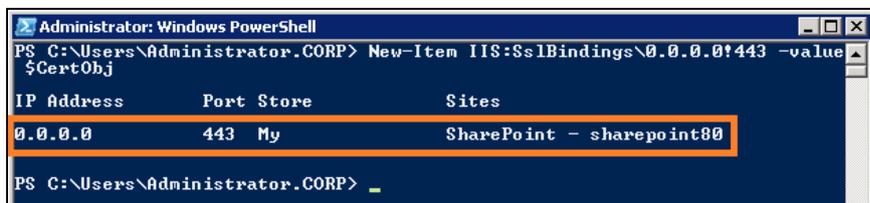


```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> $CertObj = Get-Item $MyCert.PSPath
PS C:\Users\Administrator.CORP> _
```

5.3.10 We create the actual binding to the certificate and the binding we created in the first step, so that the https binding and the certificate gets connected.

Note: In the graphical user interface we use '*' (wildcard) to represent all available IP Addresses, here '0.0.0.0' represents the same thing.

```
> New-Item IIS:SslBindings\0.0.0.0!443 -value $CertObj
```

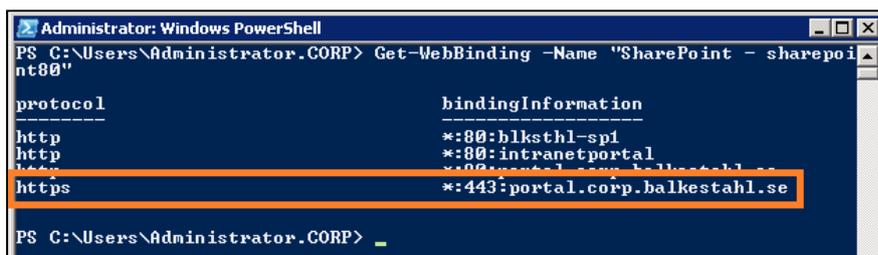


```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> New-Item IIS:SslBindings\0.0.0.0!443 -value $CertObj
IP Address      Port Store      Sites
-----
0.0.0.0         443 My           SharePoint - sharepoint80
PS C:\Users\Administrator.CORP> _
```

5.3.11 List all bindings on this Web Application to verify that the https/SSL binding has been added properly.

```
> Get-WebBinding -Name "SharePoint - sharepoint80"
```

TechNet Reference: [Get-WebBinding](http://technet.microsoft.com/en-us/library/ff730931.aspx)



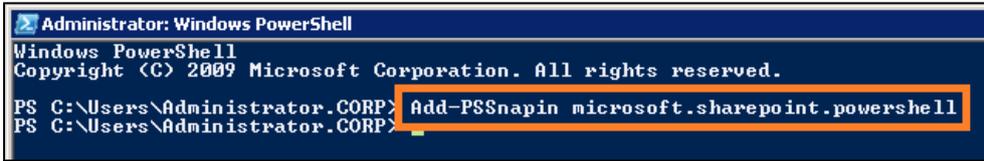
```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-WebBinding -Name "SharePoint - sharepoint80"
protocol      bindingInformation
-----
http          *:80:blksth1-spl
http          *:80:intranetportal
https        *:443:portal.corp.balkestahl.se
PS C:\Users\Administrator.CORP> _
```

5.3.12 Done!

5.4.0 Add a redirect from http to https

5.4.1 Load the SharePoint PowerShell snapin.

> Add-PSSnapin Microsoft.sharepoint.powershell



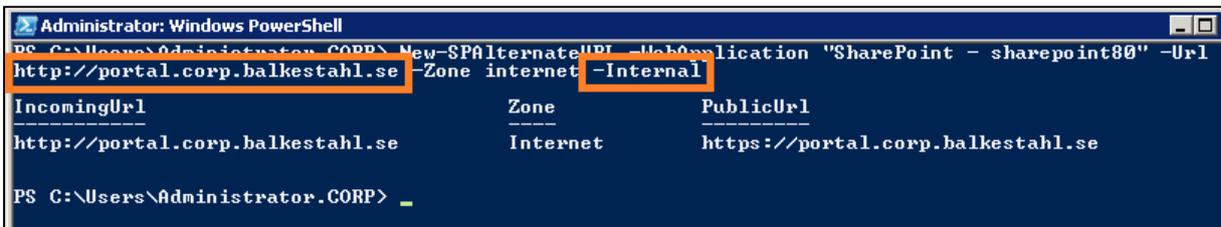
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CORP> Add-PSSnapin microsoft.sharepoint.powershell
PS C:\Users\Administrator.CORP>
```

5.4.2 Add the http://intranetportal URL as an Alternate Access Mapping:

> New-SPAlternateURL -WebApplication "SharePoint - sharepoint80" -Url http://portal.corp.balkestahl.se -Zone internet -Internal

TechNet Reference: [New-SPAlternateURL](#)



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> New-SPAlternateURL -WebApplication "SharePoint - sharepoint80" -Url http://portal.corp.balkestahl.se -Zone internet -Internal

IncomingUrl          Zone          PublicUrl
-----
http://portal.corp.balkestahl.se  Internet      https://portal.corp.balkestahl.se

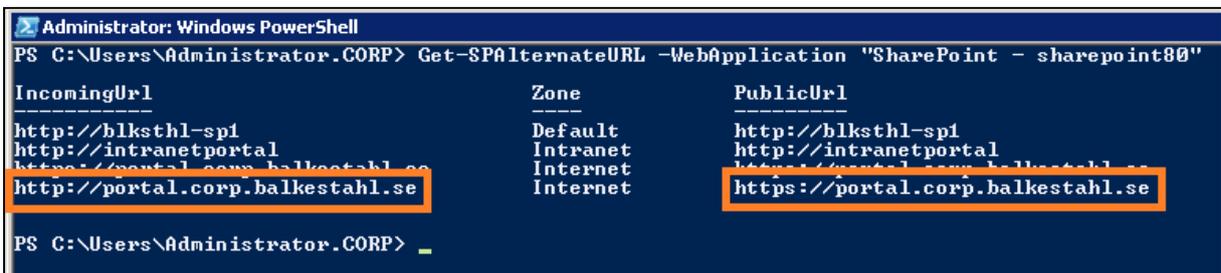
PS C:\Users\Administrator.CORP>
```

5.4.3 Verify that it has been added:

> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"

TechNet Reference: [Get-SPAlternateURL](#)

Note: The http is on the left and https on the right.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.CORP> Get-SPAlternateURL -WebApplication "SharePoint - sharepoint80"

IncomingUrl          Zone          PublicUrl
-----
http://blksth1-spi   Default       http://blksth1-spi
http://intranetportal Intranet      http://intranetportal
https://portal.corp.balkestahl.se Internet      https://portal.corp.balkestahl.se
http://portal.corp.balkestahl.se Internet      https://portal.corp.balkestahl.se

PS C:\Users\Administrator.CORP>
```

5.4.4 Done!



References

Plan alternate access mappings (Office SharePoint Server)

<http://technet.microsoft.com/en-us/library/cc261814.aspx>

KB: Configuring Alternate Access Mappings in SharePoint 2010

<http://support.microsoft.com/kb/2624320>

Disable the loopback check

<http://support.microsoft.com/kb/896861>

Self-signed cert (Outstanding post!!)

<http://www.sslshopper.com/article-how-to-create-a-self-signed-certificate-in-iis-7.html>

Thanks to, for technical and spiritual support:

Mattias Gutke - [Enfo Zipper](#)

A handwritten signature in orange ink, reading 'Thomas Balkeståhl'.