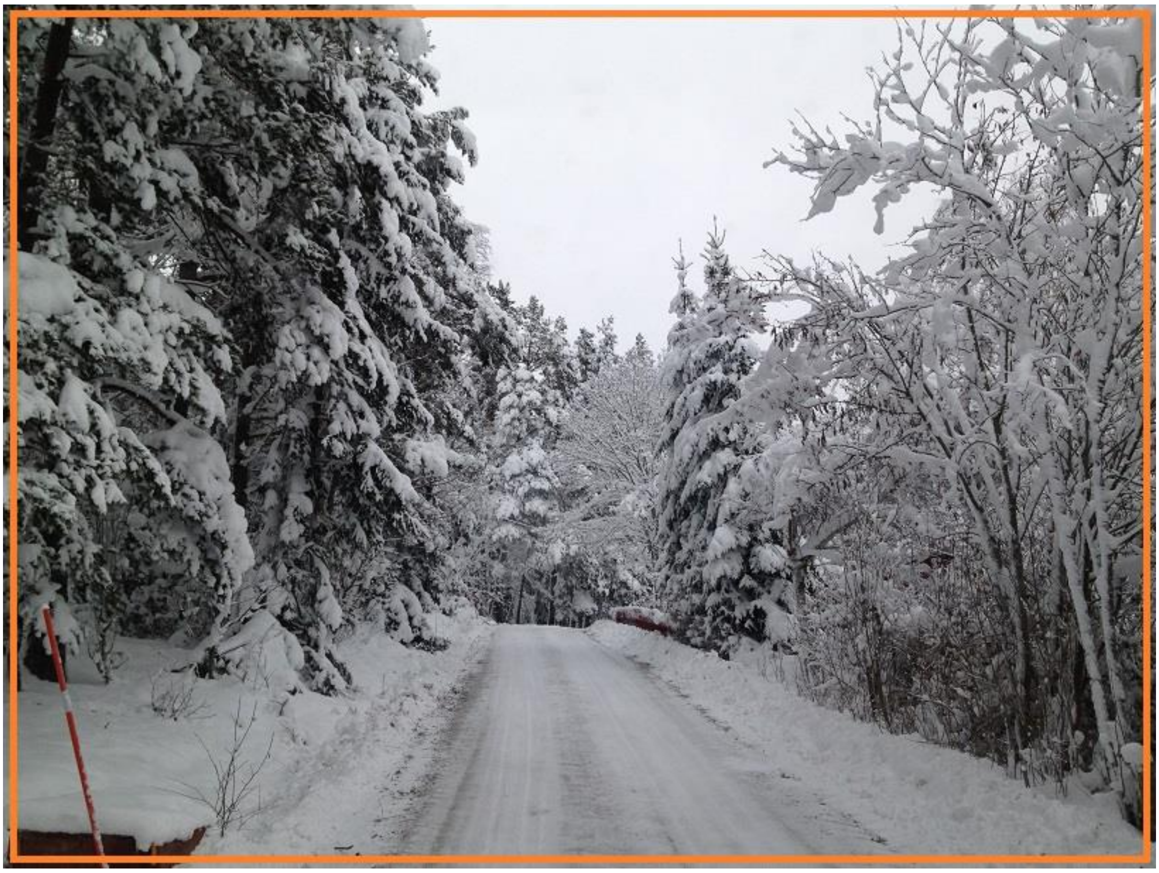
BLKSTHL

A guide to https and Secure Sockets Layer in SharePoint 2013

Release 1.0

https / Secure Sockets Layer

It has become something of a habit of mine, to jump over the tougher more difficult topics, the ones that I have spent a lot of energy avoiding before. Kerberos must be the worst of them all, and since I feel that I have Kerberos pretty much covered, I know everything and I can do anything...
This topic is something that I always avoided doing myself as well, if in production or in the lab, since certificates are difficult to understand and hard to come by for tests, I never got to try it much and thus it stayed a bit of a grey area for long.
But no more, by publishing this guide, I hope that I and you can all get over the fear of https/SSL together.
(This whitepaper is based on a blog post with the same title: http://blog.blksthl.com/2012/12/20/a-guide-to-https-and-secure-sockets-layer-in-sharepoint-2013)



This guide was created far from the ultrafast fibreoptic gigabit internet Connections

Contents

One important thing to remember though, this guide is only meant to be used in test or lab, it is not recommended to use exactly this setup in production. If you are looking to setup https in production, then you should have a certificate issued by your own Certificate Authority or have one bought from a trusted certificate issuer such as Verisign for example. I don't know all the downsides, but for one, you cannot revoke a self-signed cert.

My requirements for https in testing are these:
- They should look and behave the same as it would in production
- It should be a real DNS URL or a real URL added to the host file
- It should not cause any red warnings in the browser
- IIS and SharePoint must be configured the same way as if it were a real life scenario

How do we do this? Let me show you how I would do it...

First we need a proper environment, in my setup I have:
- A single SharePoint 2013 server on Windows Server 2012 running all roles but the DB.
- A SQL server 2008 R2 on Windows Server 2008 R2 (OS here is irrelevant)
- A Windows Server 2012 DNS server
- A Windows Server 2012 Domain Controller (Any DC will do...)
- A Windows 7 client with Internet Explorer 9. (Most common customer setup, works from the server as well with loopback check disabled)

I am also using a utility from the IIS 6.0 Resource kit, download that before we start from this link:
Download IIS 6.0 Resource Kit

In order for https / SSL and SharePoint to work we need a few things, lets add it all up in a checklist:

- A Web Application with a root site already created
- A URL (FQDN preferred)
- A DNS entry to go with the URL
- A Self-signed Certificate (or from a trusted issuer)
- AAM
- IIS Binding
- Certificate added to trusted authority on the client/server
- URL added to the local intranet zone in Internet Explorer for auto-logon

In my example, I will use the following:

Requirement	In my test environment
- A URL (FQDN preferred)	sharepoint2013.corp.balkestahl.se
- A DNS entry to go with the URL	sharepoint2013.corp.balkestahl.se -> 192.168.1.130
- A Certificate (Self-signed or from a trusted issuer)	certificate created using the IIS 6.0 RK utility SelfSSL.
- AAM	Internal http and https, Public https only
- IIS Binding	Bind my site to https and all IP using the created certificate

These are the steps we need to take:

1. Create a new Web Application or use an existing one (use port 80 initially and not https/443 for this guide.)
2. DNS, create an A-Record
3. Create the certificate (or request, buy, get any way you choose the real deal)
4. Add IIS Binding with Host-Header (this has to be done manually)
5. AAM, Add the necessary Alternate Access Mappings
6. Add the certificate to the Trusted Certificate store on the client
7. Test functionality
8. T-Shooting
9. References and recognitions

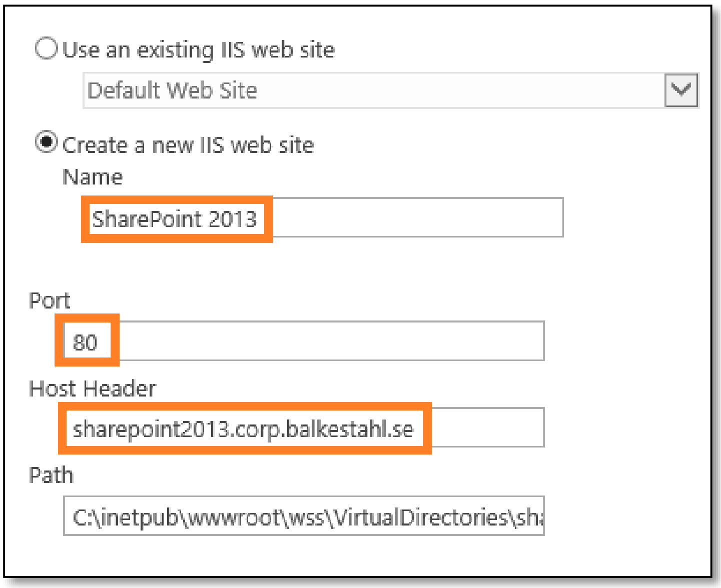
Note: If there is something that I have missed in this guide, or that should be done differently, please let me know.
I will reply to any comment and feedback that you submit at my blog: blog.blksthl.com.

1. Web Application

This step can be skipped completely if you already have a working Web Application with http on port 80 with an existing Site Collection.
If you do not have that or don't feel Confident that it will be adequate, follow these simple steps.

1.1 In Central Admin, go to Application Management, then Manage Web Applications, in the ribbon, click on new, fill in the form using your own values.

Note: The Name value is what the Web Application will be shown as in CA and in IIS.



○ Use an existing IIS web site
Default Web Site

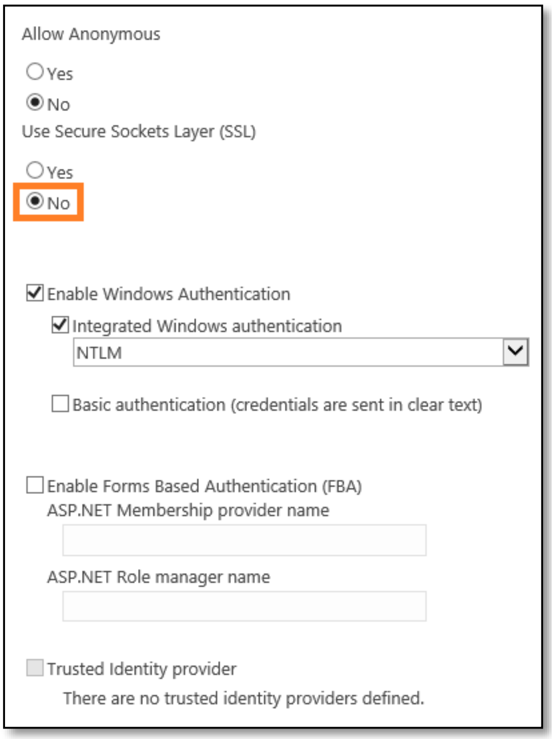
● Create a new IIS web site
Name
SharePoint 2013

Port
80

Host Header
sharepoint2013.corp.balkestahl.se

Path
C:\inetpub\wwwroot\wss\VirtualDirectories\sh

1.2 Note that I have not chosen to use SSL here, this will be added at a later time. Leave these choices as default.



Allow Anonymous

○ Yes
● No

Use Secure Sockets Layer (SSL)

○ Yes
● No

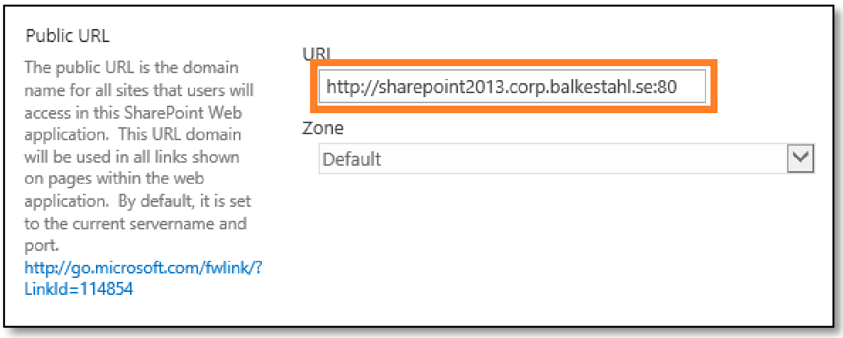
☑ Enable Windows Authentication
☑ Integrated Windows authentication
NTLM
☐ Basic authentication (credentials are sent in clear text)

☐ Enable Forms Based Authentication (FBA)
ASP.NET Membership provider name

ASP.NET Role manager name

☐ Trusted Identity provider
There are no trusted identity providers defined.

1.3 The http URL for this web application. As we set this up initially on port 80 and using http only, this could be anything, I have chosen to use the same FQDN as my https address will use.



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
http://sharepoint2013.corp.balkestahl.se:80

Zone
Default

Leave all other settings as is, the default values will do just fine for this test. The default is in 2013 using claims as authentication provider and this will serve our goal well.
I will not show you step by step how to create a Site Collection in the Web Application, something that you must do in order for the browser to later access the URL. But the steps are something like this:

1.4 Create a new Site Collection: In Central Admin select Application Management

1.5 Under Site Collections section, click on Create Site Collection.

1.6 In the dropdown, select the proper Web Application.

1.7 Enter a Name, Address and Description.

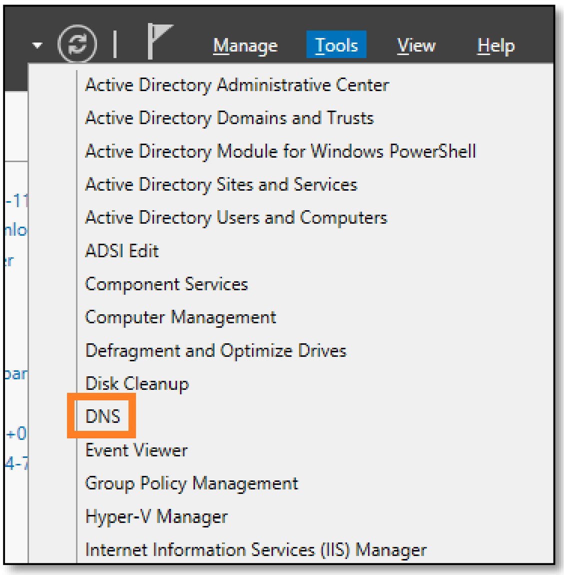
1.8 If only for test, use the Team site template under the Collaboration tab.

1.9 Add yourself as a site Collection administrator, or the account that will test access from a client, or add both in the primary and secondary fields.

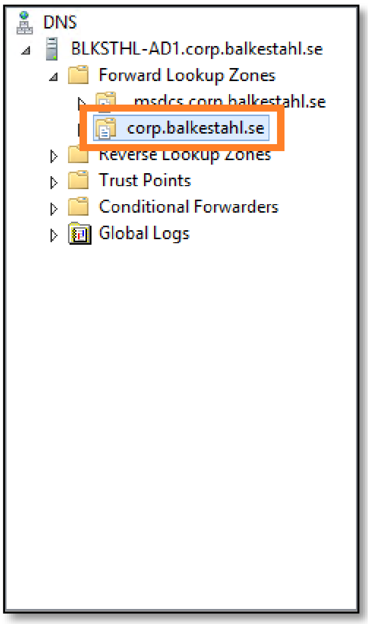
1.10 Click OK. Wait until it has been created. Done!

2. DNS

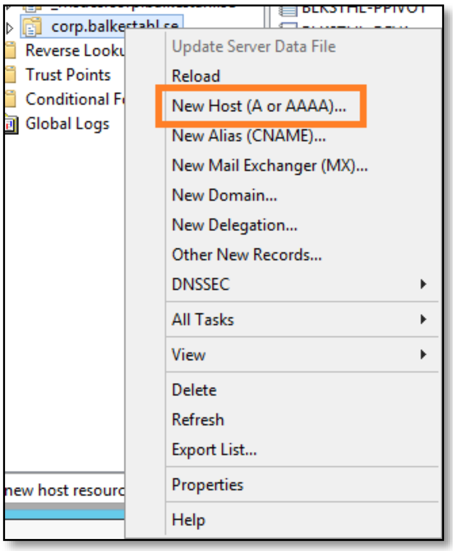
2.1 On your Windows Server 2012 running the DNS service, start server manager, then click on Tools and select DNS:


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Hyper-V Manager
Internet Information Services (IIS) Manager

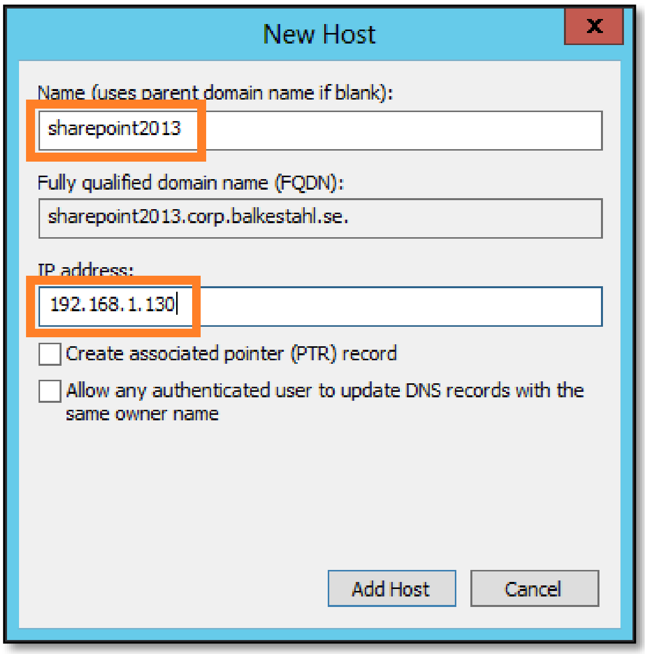
2.2 Locate the forward lookup zone for your domain:



2.3 Right click the zone and select New Host (A or AAAA)...



2.4 Enter the name of your site, this together with the full domain path will form the FQDN, Fully Qualified Domain Name. In the IP address field you enter the IP address of the SharePoint web server:


New Host

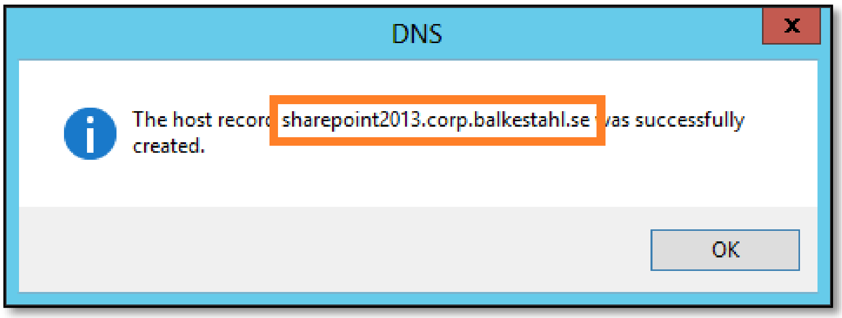
Name (uses parent domain name if blank):
sharepoint2013

Fully qualified domain name (FQDN):
sharepoint2013.corp.balkestahl.se.

IP address:
192.168.1.130

□ Create associated pointer (PTR) record
□ Allow any authenticated user to update DNS records with the same owner name

2.5 Click on Add Host and then Done, when you see this and verify that the FQDN shown is correct, you are done with the DNS part.



The host record sharepoint2013.corp.balkestahl.se was successfully created.

3. Create a certificate

In my test setup, I will create my own certificate but use a properly named one, this makes it feel more like the real thing. If you have not already done so, download and install the IIS 6.0 Resource kit that comes with the nifty little util called SelfSLL. This allows you to create a self-signed certificate that has a proper URL, a requirement if you want to avoid the red warning in the browser that a regular self-signed cert would give you. The RK can be downloaded here:
Download IIS 6.0 Resource Kit

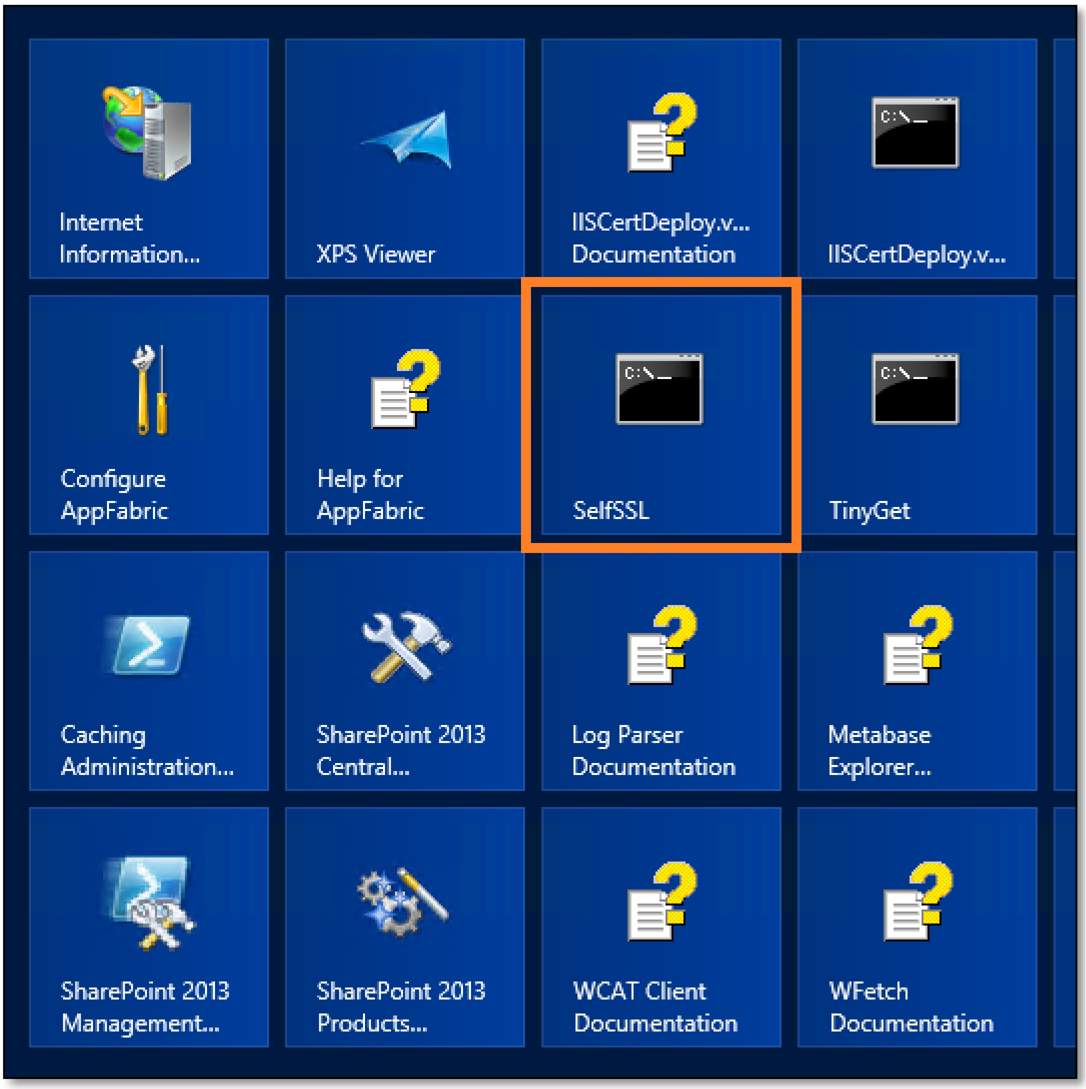
Content of the IIS 6.0 Resource Kit - the following tools are available in this package:

- IIS 6.0 Migration Tool Version 1.0 Version 1.1 Now Available!
- Apache to IIS 6.0 Migration Tool Version 1.0
- CustomAuth Version 1.0
- IISCertDeploy.vbs Version 1.0
- IIS Host Helper Service Version 1.0
- IISState Version 3.0
- Log Parser Version 2.1 Version 2.2 Now Available!
- Metabase Explorer Version 1.6
- Permissions Verifier Version 1.0
- RemapUrl Version 1.0
- SelfSSL Version 1.0
- TinyGet Version 5.2
- Web Capacity Analysis Tool Version 5.2
- WFetch Version 1.3

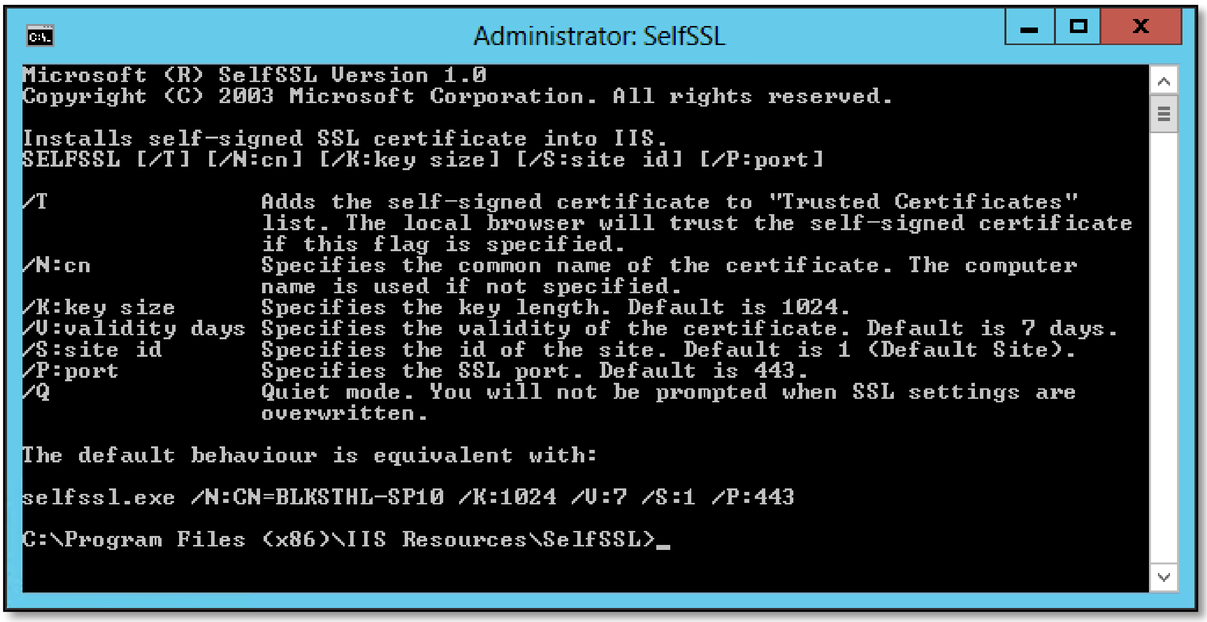
What we really want out of all this this time, is the small util called SelfSSL in bold. This little util allows you like I said before, to create a self-signed cert using an FQDN of choice. In my example, I want to use the URL: sharepoint2013.corp.balkestahl.se and have the cert created with the same URL. I'll show you how step by step.
It's really quite simple.

Note: You might consider even in a lab Environment, to install your own Certificate Authority and issue your own private Certificates, the following links will be of help when doing that:
Install the Certification Authority (Windows Server 2012)
Install a Root Certification Authority (Windows Server 2008 R2)
Active Directory Certificate Services Overview (Windows Server 2012)

3.1 Run the tool from the start menu:



3.2 The command-line tool does not look much to the world:

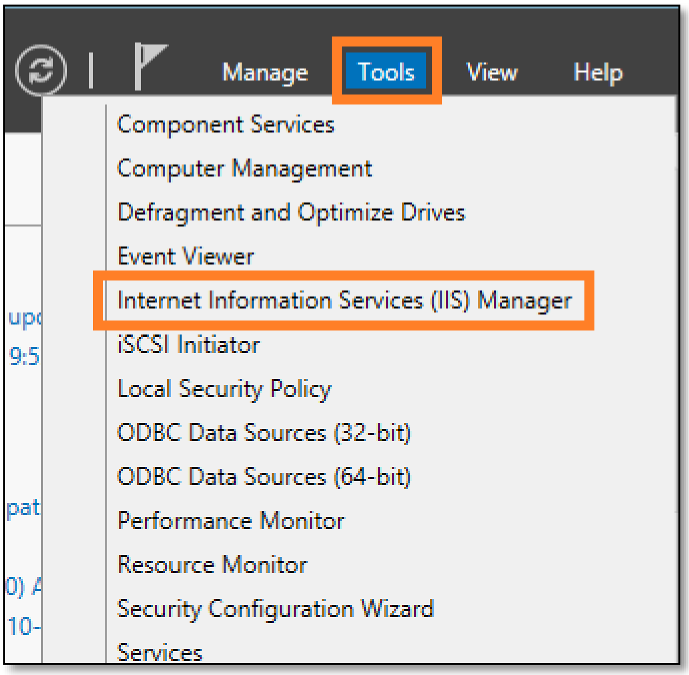


```
Microsoft (R) SelfSSL Version 1.0
Copyright (C) 2003 Microsoft Corporation. All rights reserved.

Installs self-signed SSL certificate into IIS.
SELFSSL [/T] [/N:cn] [/K:key size] [/S:site id] [/P:port]

/T               Adds the self-signed certificate to "Trusted Certificates"
                 list. The local browser will trust the self-signed certificate
                 if this flag is specified.
/N:cn            Specifies the common name of the certificate. The computer
                 name is used if not specified.
/K:key size      Specifies the key length. Default is 1024.
/V:validity days Specifies the validity of the certificate. Default is 7 days.
/S:site id       Specifies the id of the site. Default is 1 (Default Site).
/P:port          Specifies the SSL port. Default is 443.
/Q               Quiet mode. You will not be prompted when SSL settings are
                 overwritten.

The default behaviour is equivalent with:

selfssl.exe /N:CN=BLKSTHL-SP10 /K:1024 /V:7 /S:1 /P:443

C:\Program Files (x86)\IIS Resources\SelfSSL>_
```

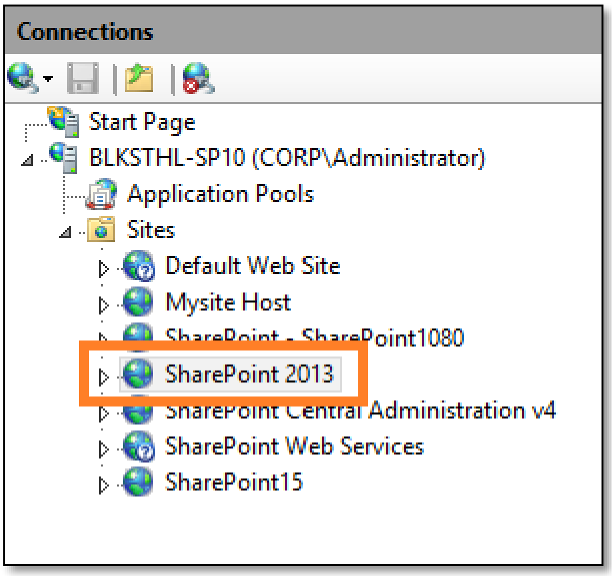
Note: You need to be logged on with an account that is a member of the local administrators Group in order to use this tool.

It gives you some options and I'm not going to go into what can be done with this tool, I'll just go with the default and create a certificate using the suggested settings with one exception, we need to use the proper site ID.
Every site in IIS gets an ID, this is in this case used to put the certificate in the correct place on the correct site.

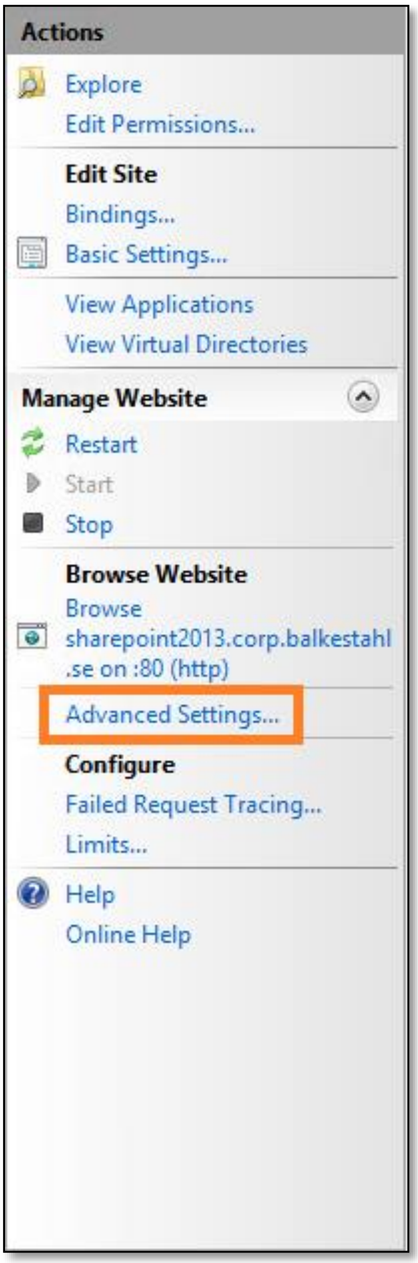
3.3 Get the correct ID from IIS, open up the IIS Manager, in server manager, click on Tools and then on Internet Information Services Manager:


Manage
Tools
View
Help
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services

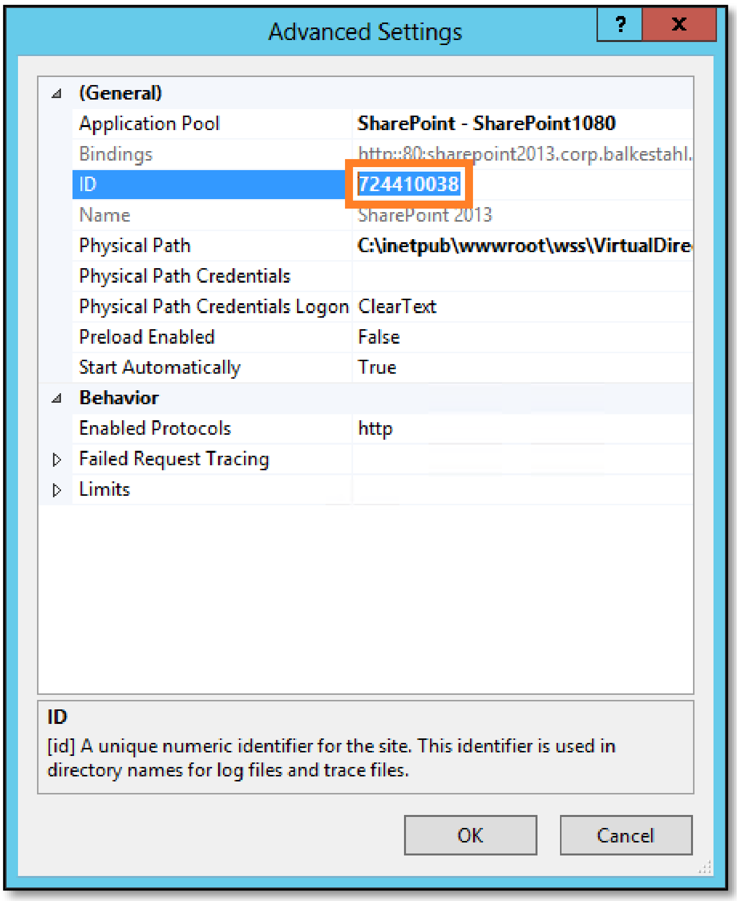
3.4 In Internet Information Services Manager, select your site:



3.5 On the right pane, near the bottom, click on Advanced Settings...:



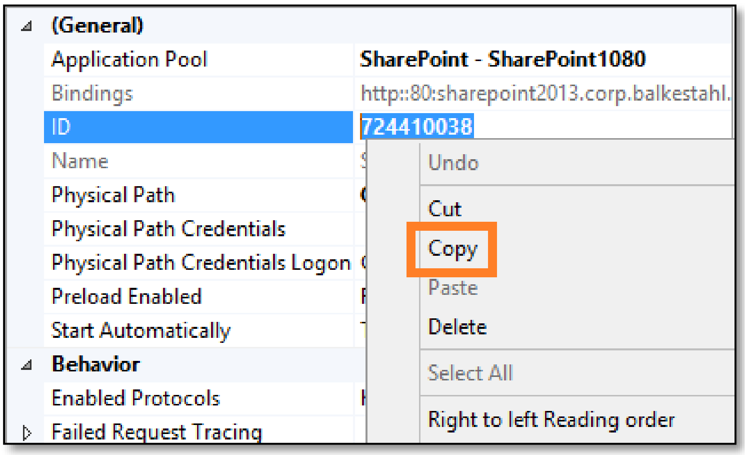
3.6 In the next dialog, you will see a row called simply ID:



(General)	
Application Pool	**SharePoint - SharePoint1080**
Bindings	http::80:sharepoint2013.corp.balkestahl.
ID	724410038
Name	SharePoint 2013
Physical Path	**C:\inetpub\wwwroot\wss\VirtualDire**
Physical Path Credentials	
Physical Path Credentials Logon	ClearText
Preload Enabled	False
Start Automatically	True
Behavior	
Enabled Protocols	http
Failed Request Tracing	
Limits	

ID
[id] A unique numeric identifier for the site. This identifier is used in directory names for log files and trace files.

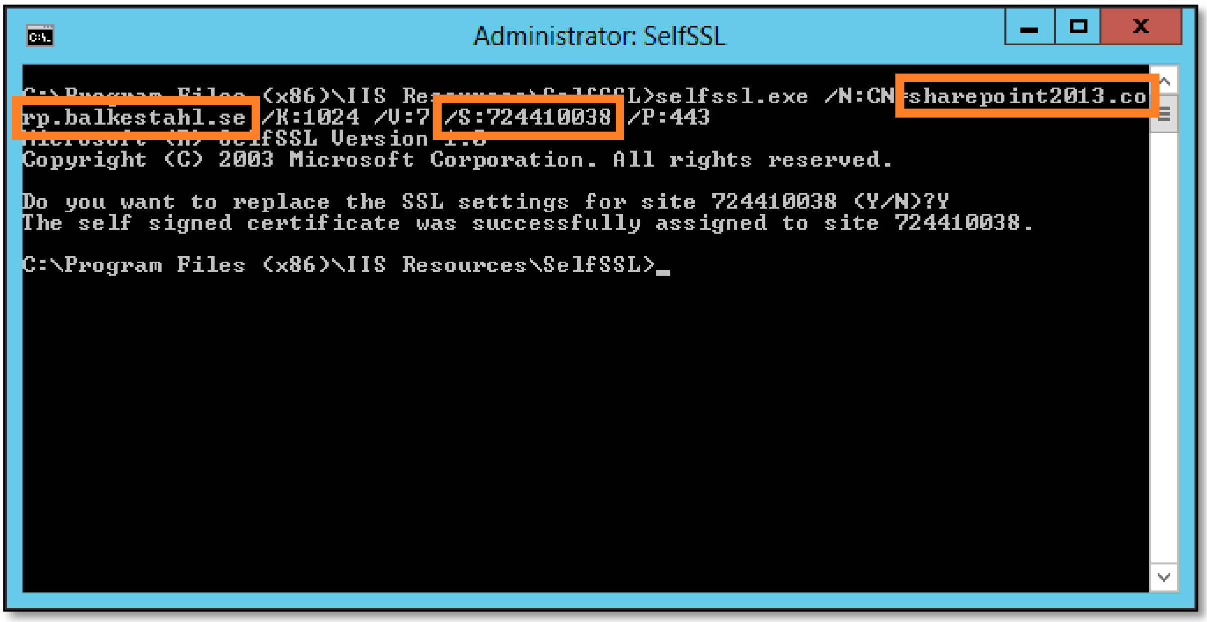
3.7 Select the number in the field and right click and copy:



(General)	
Application Pool	**SharePoint - SharePoint1080**
Bindings	http::80:sharepoint2013.corp.balkestahl.
ID	724410038
Name	
Physical Path	
Physical Path Credentials	
Physical Path Credentials Logon	
Preload Enabled	
Start Automatically	
Behavior	
Enabled Protocols	
Failed Request Tracing	

3.8 Paste the ID after the /S: switch. You should also change the value for the /V: setting, this represents how many days the certificate will be valid, the default 7 is ok for me in a very temporary setup, but for longer test runs, make it 90 Days or so.
Now you have all you need to proceed. Run the SelfSSL util and use the site ID but leave everything else default.
Answer yes to the question - Do you want to replace the SSL settings for site 724410038.

selfssl.exe /N:CN=SharePoint2013.corp.balkestahl.se /K:1024 /V:7 /S:724410038 /P:443



```
C:\Program Files (x86)\IIS Resources\SelfSSL>selfssl.exe /N:CN=sharepoint2013.co
rp.balkestahl.se /K:1024 /V:7 /S:724410038 /P:443
Microsoft (R) SelfSSL Version 1.0
Copyright (C) 2003 Microsoft Corporation. All rights reserved.

Do you want to replace the SSL settings for site 724410038 (Y/N)?Y
The self signed certificate was successfully assigned to site 724410038.

C:\Program Files (x86)\IIS Resources\SelfSSL>_
```

Note: One option that could be useful, if you add the /T to the command the certificate will be added to the local Machines trusted authority certificates list. This makes it trusted in the servers browser.

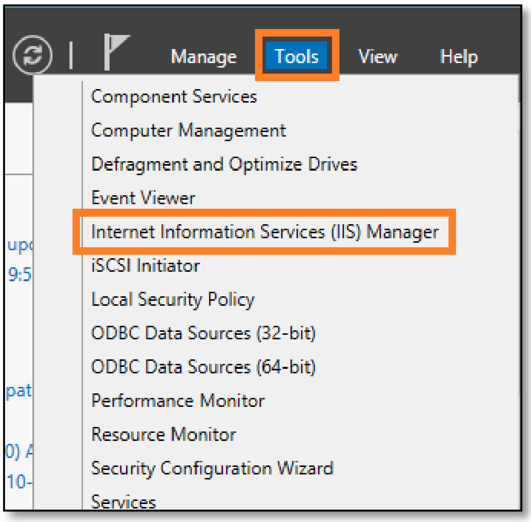
The certificate is now created and put into the personal store for this computer.
If you get an error here stating that the certificate could not be assigned to the site, then you most likely already have an instance of the same certificate name, locate any existence of the certificate and delete it. (See how later in the post under chapter 8. T-shooting)

Move on to Chapter 4.

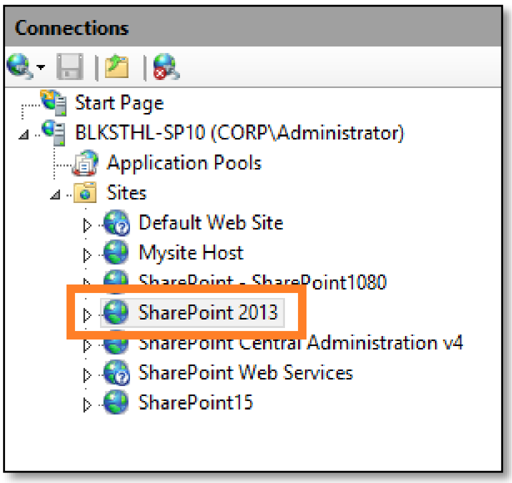
4. IIS Binding

In order for the web server, IIS, to recognize any incoming traffic and locate the proper site to direct it to, IIS uses Host header bindings. This is done so that you can have more than one site on port 80 in the same web server. The default site has a blank Host header binding which will in affect make it claim all incoming requests as its own.
SharePoint stops the Default Web Site so that does not affect us now, but we need to take care of our own IIS Web Site that in reality is our SharePoint Web Application.
What we have to do, is make our IIS Web Site answer to all incoming traffic with a host header of https and the FQDN created in Chapter 2. DNS - sharepoint2013.corp.balkestahl.se

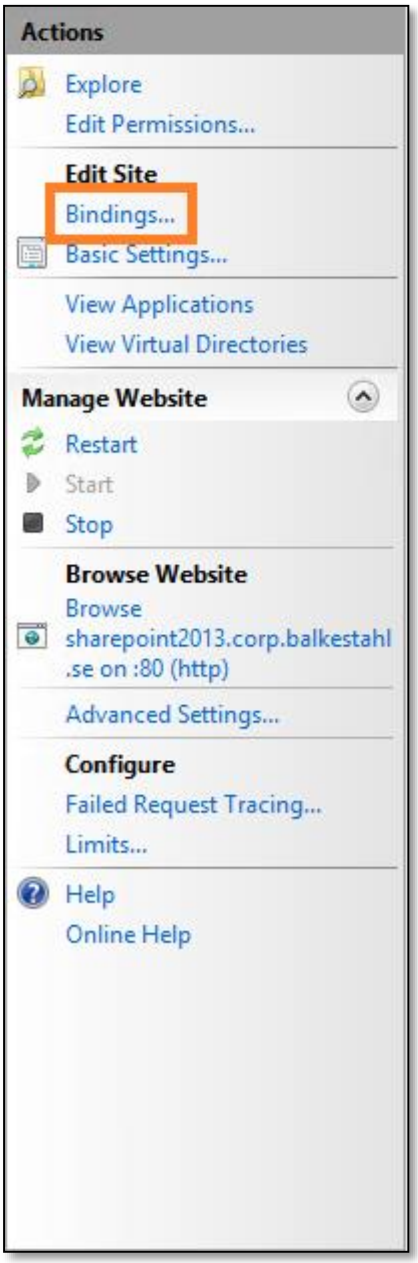
4.1 Start by opening up your IIS manager, in Server Manager, click on tools and the on Internet Information Services (IIS) Manager:


Manage
Tools
View
Help
Component Services
Computer Management
Defragment and Optimize Drives
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services

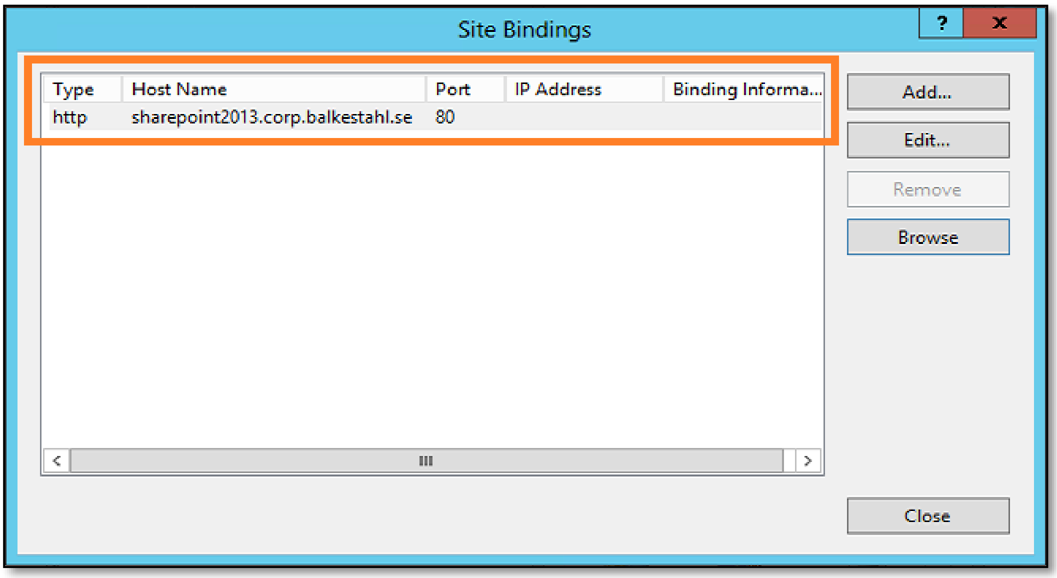
4.2 Locate your Web Site:



4.3 In the right hand pane, locate Bindings:

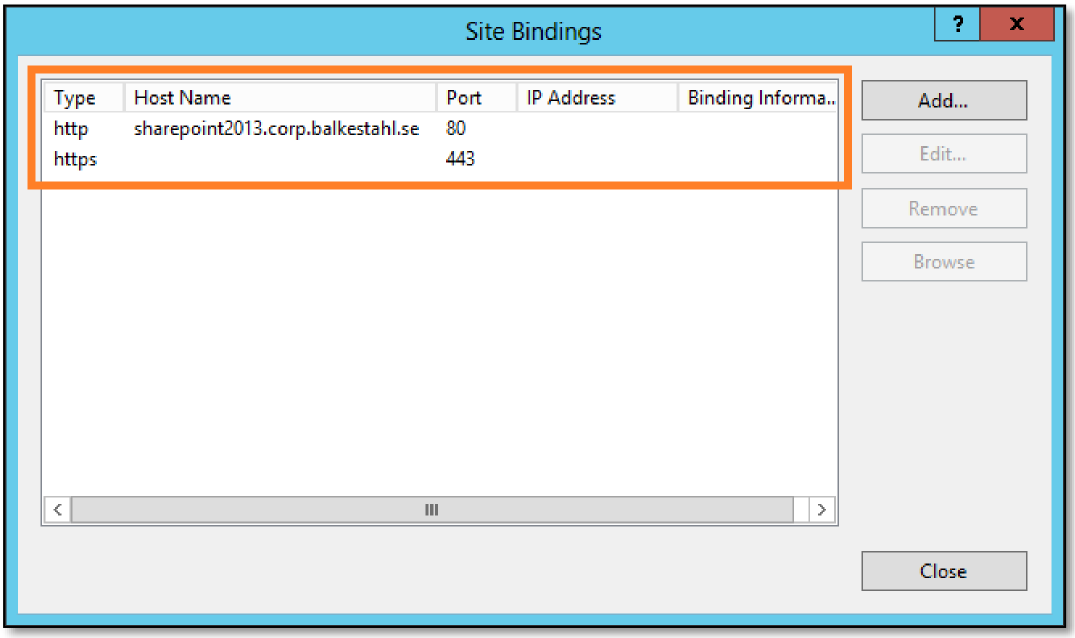


4.4 What you see here is a list of the existing Bindings for this site, Type, Host Name, Port and IP address. If you have created the certificate using the SelfSSL util and added the ID of the Web Site, then you will most likely see at least two rows here (see 4.5).



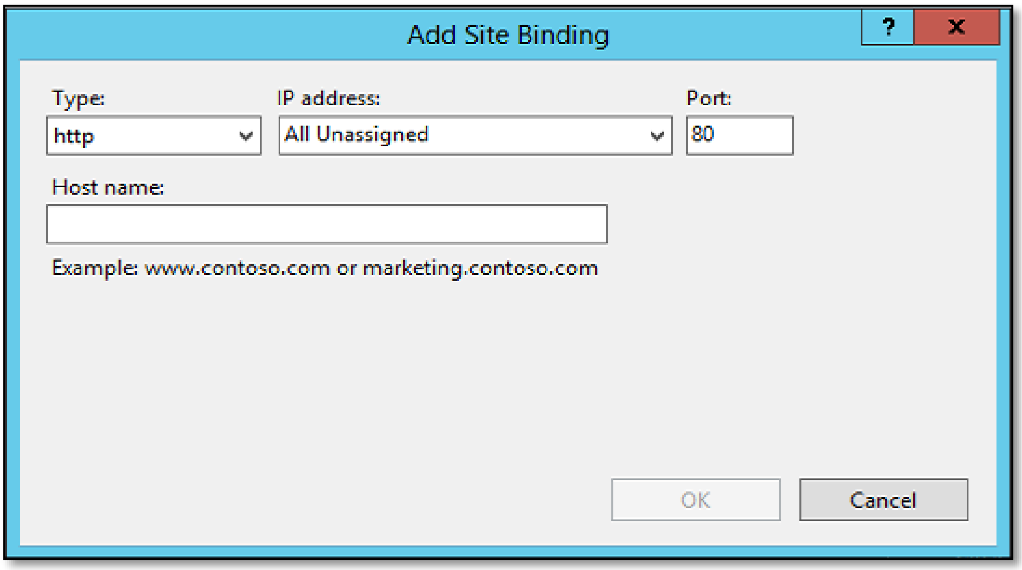
Type	Host Name	Port	IP Address	Binding Informa...
http	sharepoint2013.corp.balkestahl.se	80		

4.5 This is what you will have if the SelfSSL successfully added the cert to the site using its ID: If this is what you have, select the second row with the https/443 and click on Edit, then scroll down to step 4.11 in this guide.



Type	Host Name	Port	IP Address	Binding Informa..
http	sharepoint2013.corp.balkestahl.se	80		
https		443		

4.6 Assuming that it was not added, we have to add the cert to the site. Click on Add.


Add Site Binding

Type: http

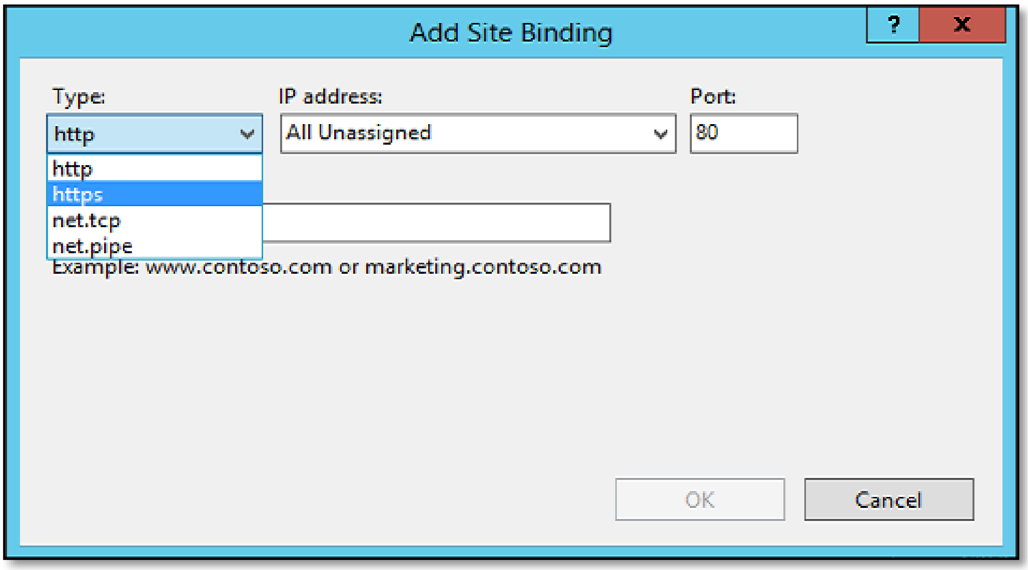
IP address: All Unassigned

Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

4.7 In this dialog, we must first select the proper protocol, https. Use the drop down:


Add Site Binding

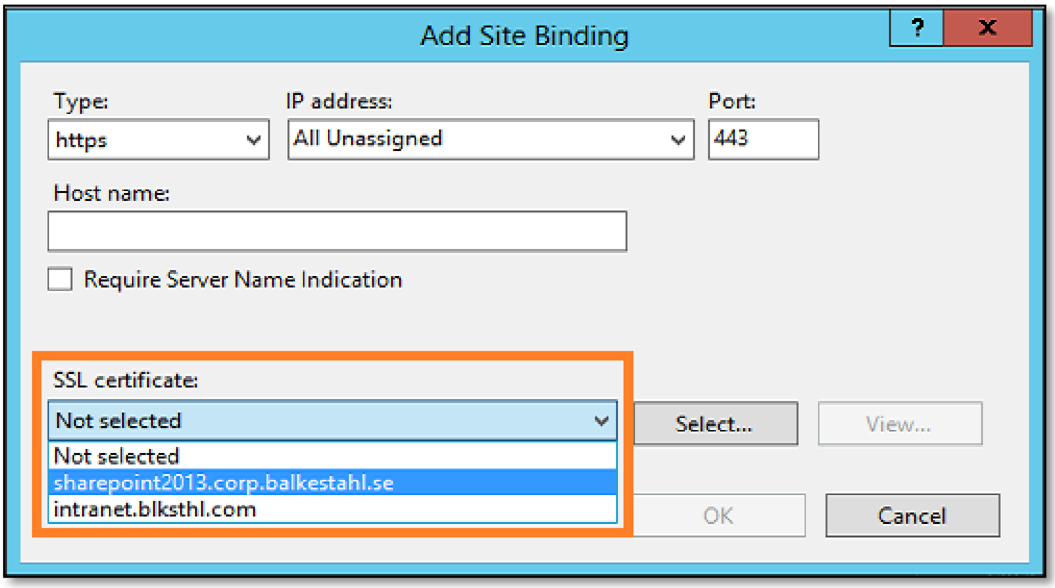
Type: http

IP address: All Unassigned

Port: 80

Example: www.contoso.com or marketing.contoso.com

4.8 Once you have selected https as the protocol, you will find that a new field appears. This is where you select the certificate to use.



Type: https

IP address: All Unassigned

Port: 443

Host name:

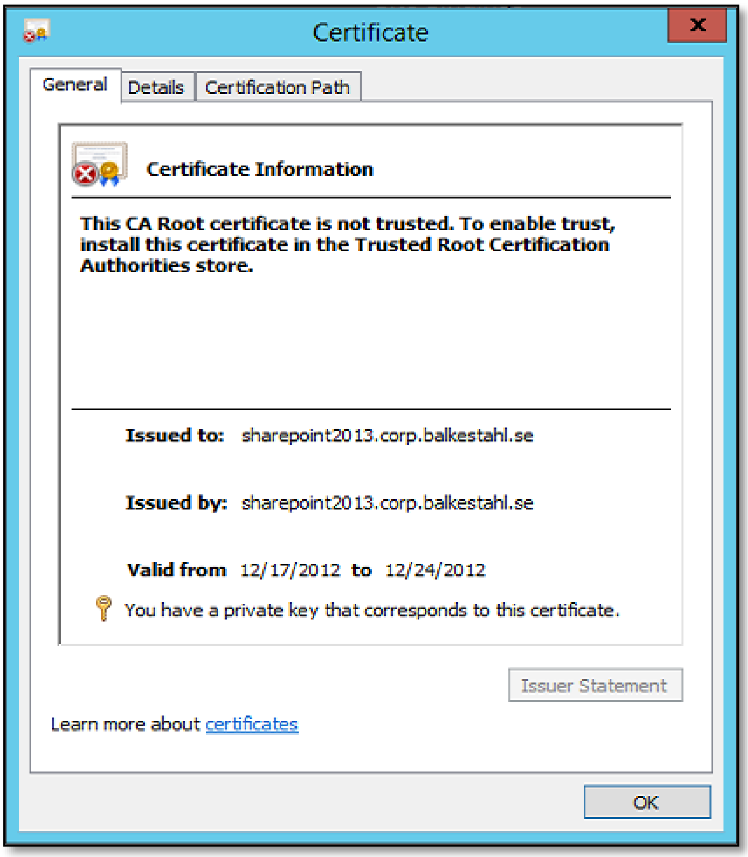
□ Require Server Name Indication

SSL certificate: Not selected

- Not selected
- sharepoint2013.corp.balkestahl.se
- intranet.blksthl.com

4.9 Select the certificate created in *Chapter 3. Create a Certificate*, in my environment, that is the sharepoint2013.corp.balkestahl.se certificate listed.

4.10 Once selected, you can click on View to verify that it really is the correct certificate and that everything looks to be in order, click on OK.



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

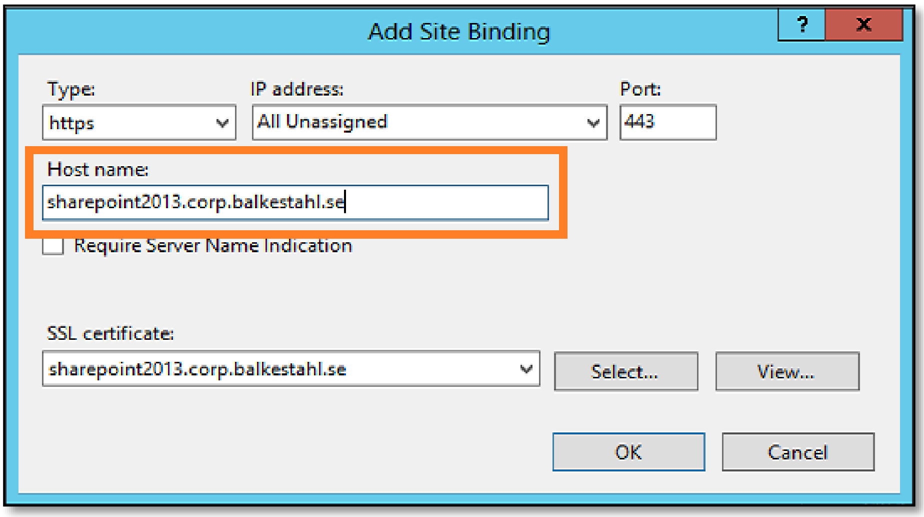
Issued to: sharepoint2013.corp.balkestahl.se

Issued by: sharepoint2013.corp.balkestahl.se

Valid from 12/17/2012 to 12/24/2012

You have a private key that corresponds to this certificate.

4.11 Next we add the Host Name that this Binding will be matched on, same as the certificate name, sharepoint2013.corp.balkestahl.se, click OK.



Type: https

IP address: All Unassigned

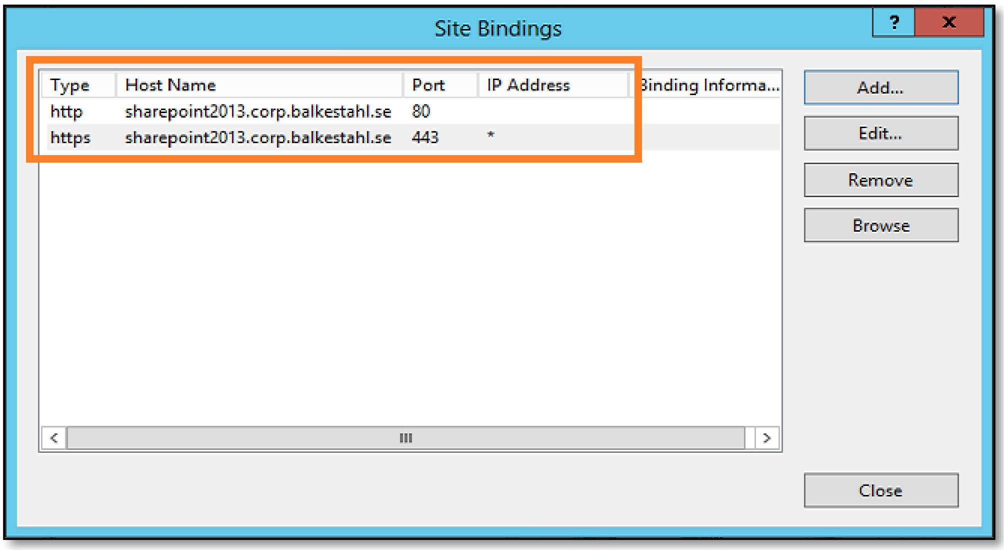
Port: 443

Host name: sharepoint2013.corp.balkestahl.se

□ Require Server Name Indication

SSL certificate: sharepoint2013.corp.balkestahl.se

4.12 Now you should see two rows in the bindings list for this Web SIte. One for the initial http/80 and one for https/443. This is goOoOod!



Type	Host Name	Port	IP Address	Binding Informa...
http	sharepoint2013.corp.balkestahl.se	80		
https	sharepoint2013.corp.balkestahl.se	443	*	

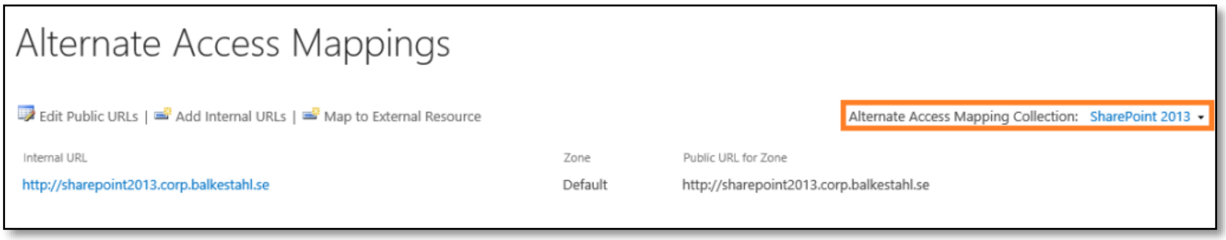
4.13 Now click on Close and Close the IIS manager.

Move on to Chapter 5.

5. Alternate Access Mappings - AAM

In order for SharePoint to know how to handle the incoming requests for this new URL, we need to add/configure Alternate Access Mappings, this basically tells SharePoint how to handle all URLs. AAMs Control if SharePoint should do a redirect or a translation of the incoming address. AAMs can be configured from Central Administration and using PowerShell, I will in this guide use only CA.

5.1 Open up your Central Administration site and click on Configure Alternate Access Mappings located under the System Settings category.
This will show you all Alternate Access Mappings for all of your Web Applications in the farm. In the top right dropdown, click on Change Alternate Access Mapping Collection and select the correct Web Application.
Now, it will look like this:

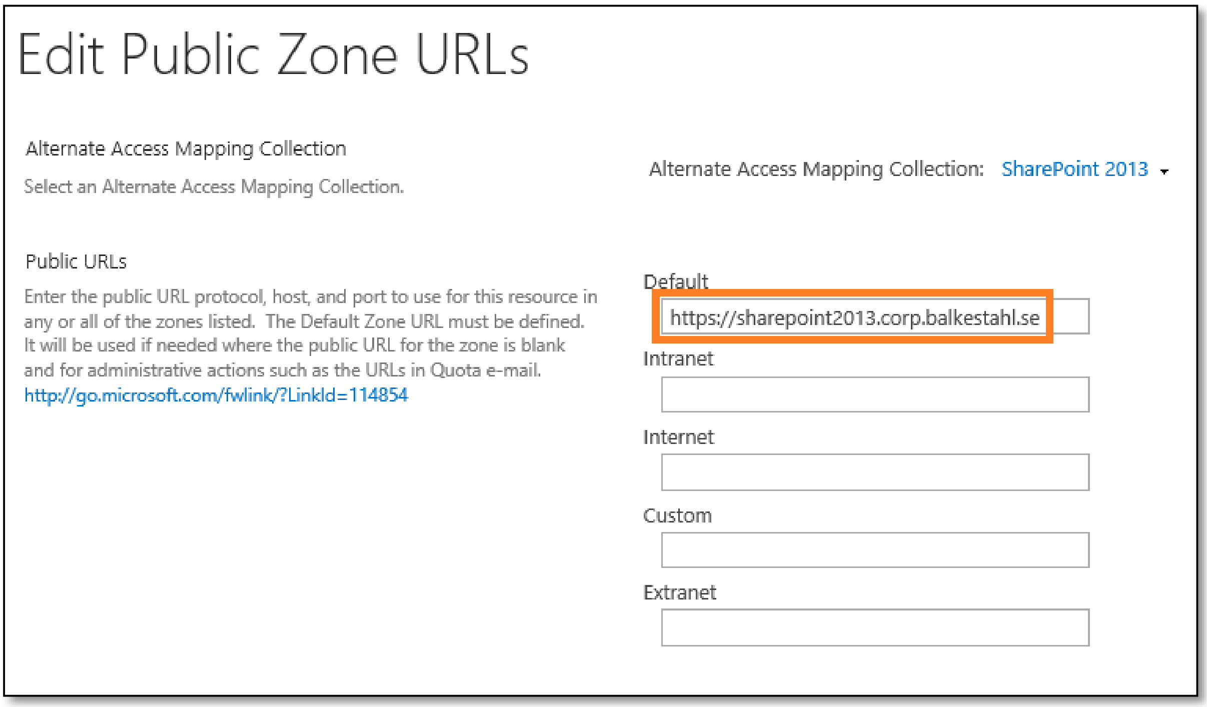


Alternate Access Mappings

Edit Public URLs | Add Internal URLs | Map to External Resource
Alternate Access Mapping Collection: SharePoint 2013

Internal URL	Zone	Public URL for Zone
http://sharepoint2013.corp.balkestahl.se	Default	http://sharepoint2013.corp.balkestahl.se

5.2 Next thing we want to do, is to alter the existing Public URL so that it uses https instead of http. Since all else is ok, add the s...



Edit Public Zone URLs

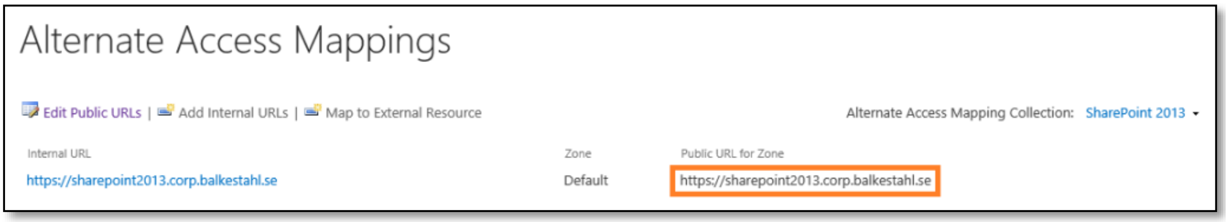
Alternate Access Mapping Collection
Select an Alternate Access Mapping Collection.

Alternate Access Mapping Collection: SharePoint 2013

Public URLs
Enter the public URL protocol, host, and port to use for this resource in any or all of the zones listed. The Default Zone URL must be defined. It will be used if needed where the public URL for the zone is blank and for administrative actions such as the URLs in Quota e-mail.
http://go.microsoft.com/fwlink/?LinkId=114854

Default: https://sharepoint2013.corp.balkestahl.se
Intranet:
Internet:
Custom:
Extranet:

5.3 Ok on that will give you this view, note that both the Internal URL and the Public URL has changed. This site is now only accessible by the https protocol. (Not entirely true, but true enough)



Alternate Access Mappings

Edit Public URLs | Add Internal URLs | Map to External Resource

Alternate Access Mapping Collection: SharePoint 2013

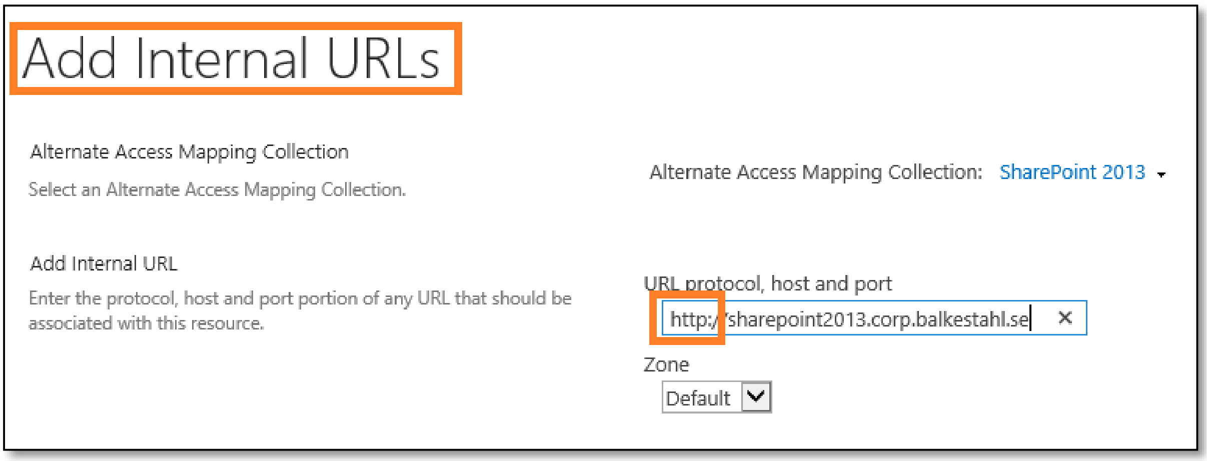
Internal URL	Zone	Public URL for Zone
https://sharepoint2013.corp.balkestahl.se	Default	https://sharepoint2013.corp.balkestahl.se

5.4 I always like to be able to type in the default http URL in my browser, and if the site uses https, be redirected automatically. This is rather easy to do in SharePoint, simply add an Internal URL using http and add it to the Default zone which will direct us to the Public URL using https. It may sound difficult but trust me, it just works.

If you are interested in Learning more about Alternate Access Mappings and the inner workings, I have a free whitepaper published on the subject for 2010 Here and a basic post for 2013 Here.

Anyways, click on the Add Internal URLs link and simply add the same URL using http, make sure that the default zone is selected.

Note: The zones used in AAM has NO RELATION with the zones in Internet Explorer, they are named similar, but they have no connection whatsoever.



Add Internal URLs

Alternate Access Mapping Collection
Select an Alternate Access Mapping Collection.

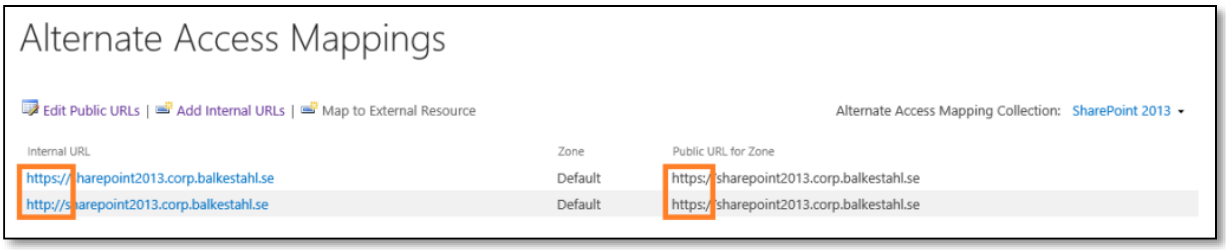
Alternate Access Mapping Collection: SharePoint 2013

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: http://sharepoint2013.corp.balkestahl.se

Zone: Default

5.5 Now the list should look like this, note that you have http and https on the left (incoming traffic) and only https on the right (target):



Alternate Access Mappings

Edit Public URLs | Add Internal URLs | Map to External Resource

Alternate Access Mapping Collection: SharePoint 2013

Internal URL	Zone	Public URL for Zone
https://sharepoint2013.corp.balkestahl.se	Default	https://sharepoint2013.corp.balkestahl.se
http://sharepoint2013.corp.balkestahl.se	Default	https://sharepoint2013.corp.balkestahl.se

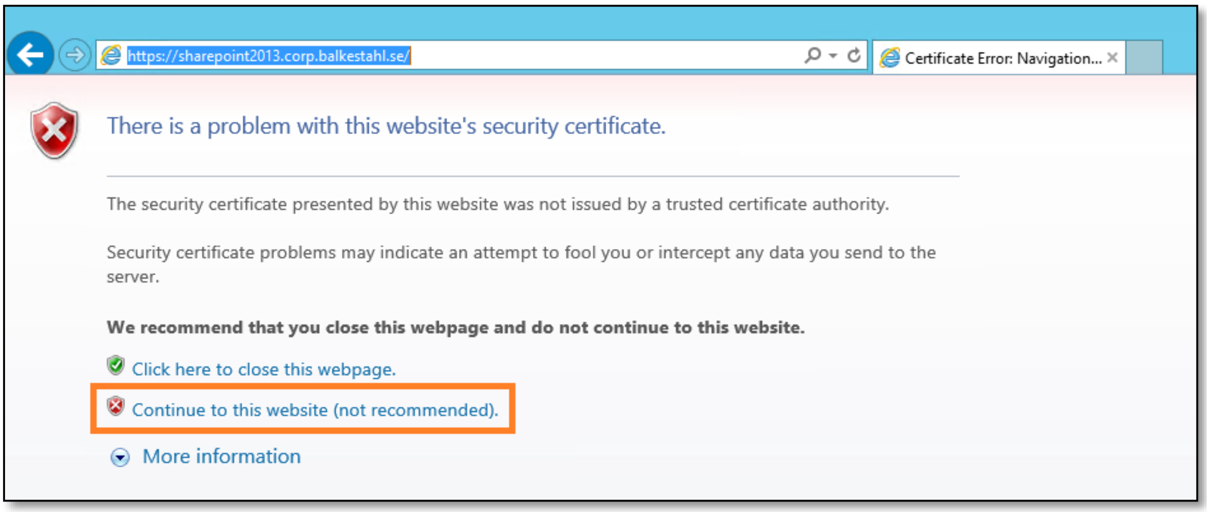
You are now done configuring your Alternate Access Mappings! Let’s move on to testing, start with Chapter 6.

6. Add the Certificate to the Trusted Authorities store.

If we do nothing else from here, we will be able to access the site using https, but it will not be pretty...in order to mimic https using a 'real' certificate we need to also add the certificate to the trusted store. This will make the browser trust the cert as authentic and it will stop throwing us the errors.

Note: If you are doing these tests on the server itself, you will need to disable the loopback check Before accessing the site, else it will fail. See Chapter 8. T-shooting for information on how to do this.

6.1 Try it first, open a browser, type in the address of the https URL and hit enter. You will first see this warning. Click on Continue to this website.


https://sharepoint2013.corp.balkestahl.se/
Certificate Error: Navigation...

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

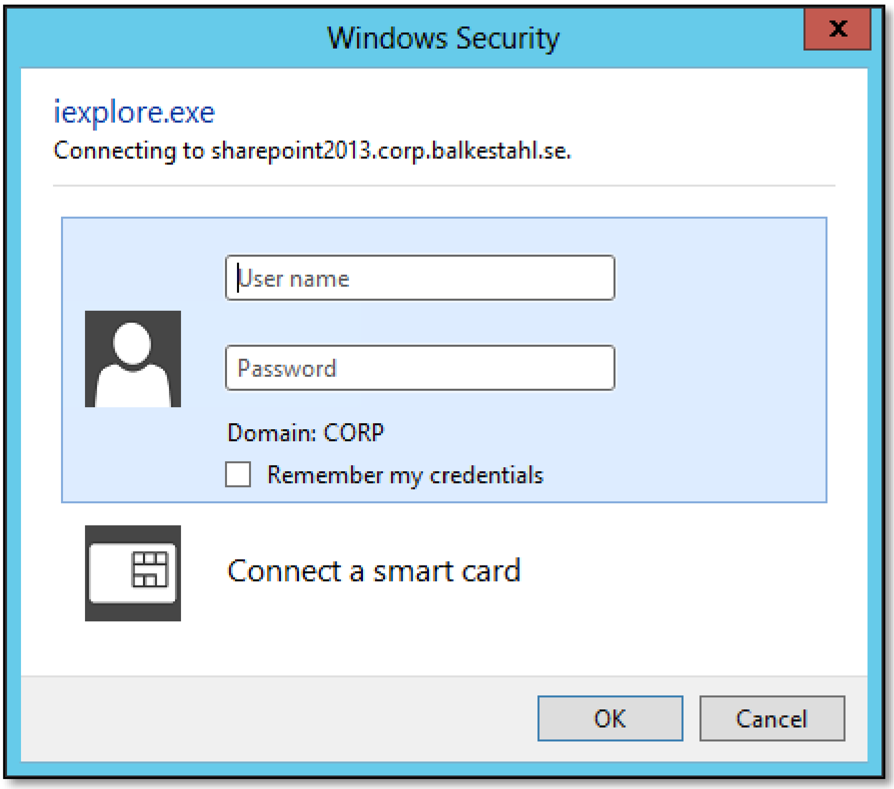
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

6.2 This will lead to a login prompt. This is to be expected at this Point, login using your credentials that you have made site Collection admin or that have access to the site Collection.



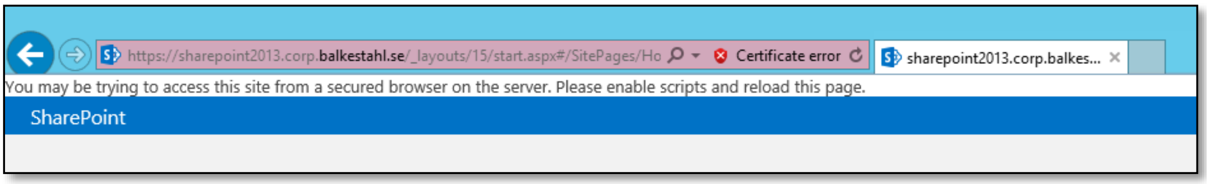
iexplore.exe
Connecting to sharepoint2013.corp.balkestahl.se.

Domain: CORP

6.3 Access! Yeay! or...no...hang on?! that's not the way I pictured it...we don't have access and we have a red certificate error. This is not what we want our users to see...
Two things cause this:

6.3.1. The White ribbon telling us that this is a secured browser comes from that the server in this case, has IE ESC - Internet Explorer Enhanced Security Configuration enabled.
If you are using a client like Windows 7 or 8, you will not see this but should actually see the site content.
To fix this, follow the steps in this blog post:
How to disable IE Enhanced Security in Windows Server 2012
http://blog.blksthl.com/2012/11/28/how-to-disable-ie-enhanced-security-in-windows-server-2012

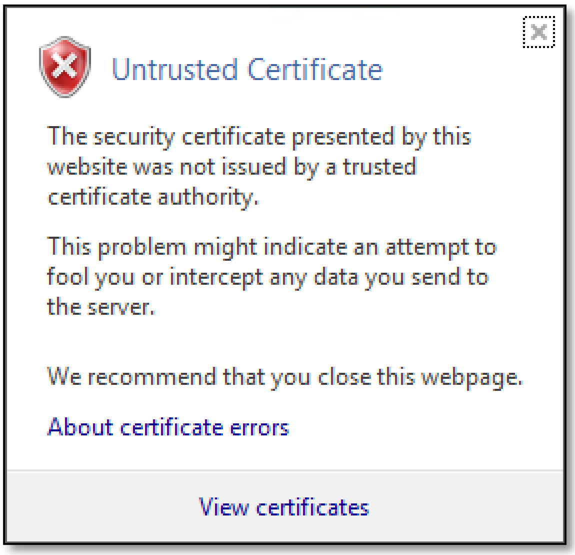
6.3.2. The red Certificate error is there because the certificate comes from an untrusted source. This is as it should be, and can be fixed.
To fix this, keep reading...



https://sharepoint2013.corp.balkestahl.se/_layouts/15/start.aspx#/SitePages/Ho

You may be trying to access this site from a secured browser on the server. Please enable scripts and reload this page.

6.4 There are several ways to add the certificate to the trusted store, I will show you the easiest of them all. Click on the Certificate Error to the right of the red shield symbol. This will show this:



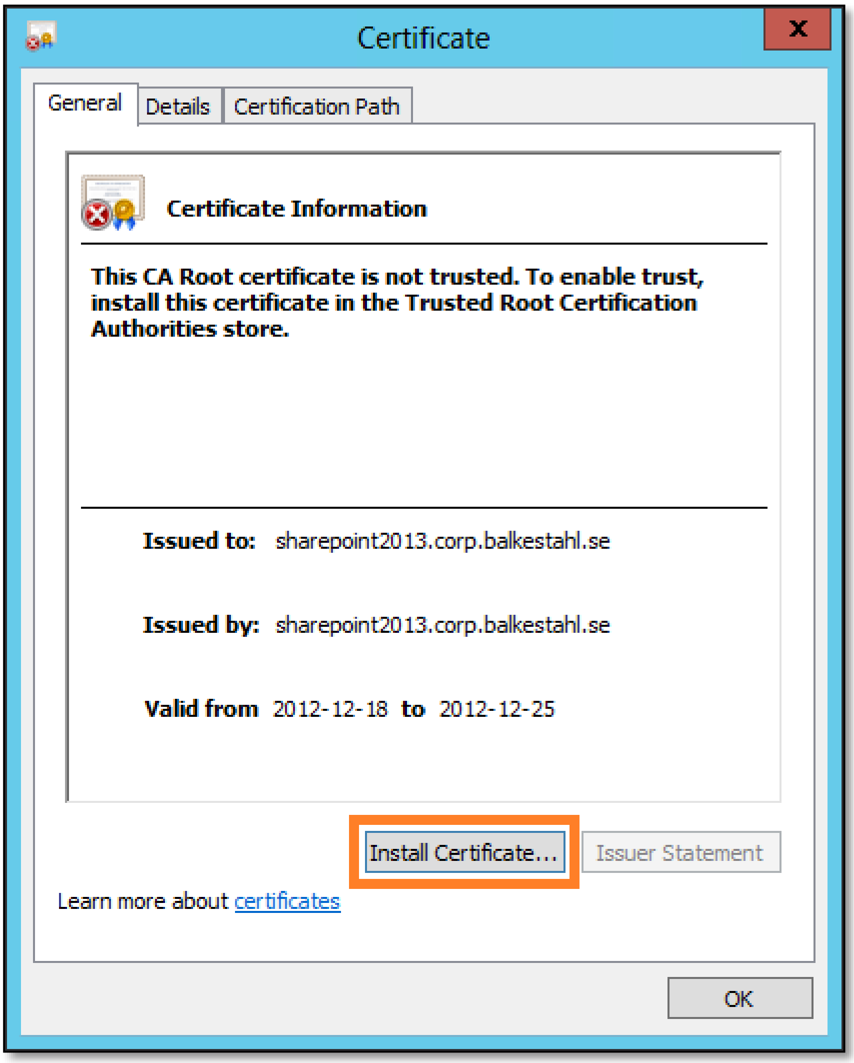
Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

6.5 It is all true what it says, except that nobody is trying to fool us...Click on View Certificates to show this dialog:



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

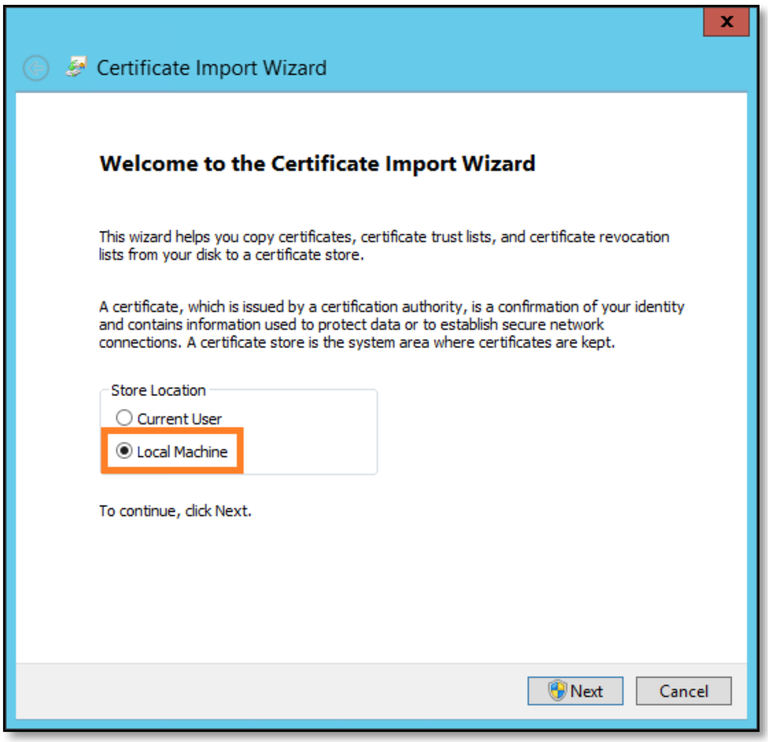
Issued to: sharepoint2013.corp.balkestahl.se

Issued by: sharepoint2013.corp.balkestahl.se

Valid from 2012-12-18 **to** 2012-12-25

Learn more about certificates

6.6 You can probably guess what the next step is going to be? Click on Install Certificate...



Welcome to the Certificate Import Wizard

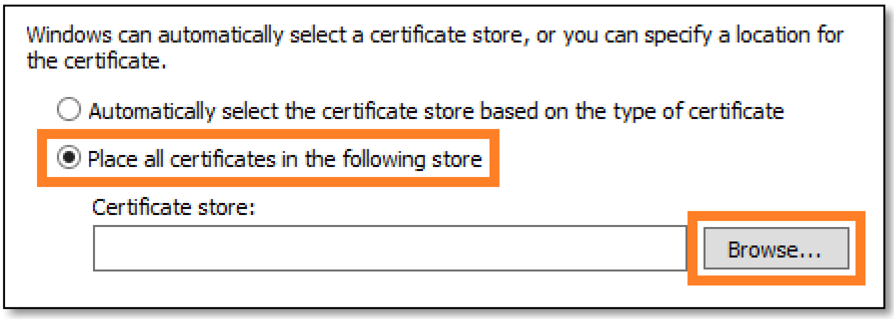
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

6.7 We want the certificate to be in the Computers store, select Local Machine and click Next.

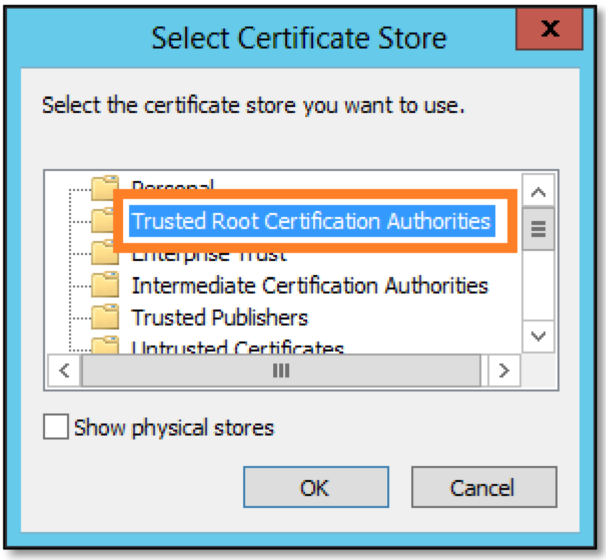


Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store:

6.8 Select Place all Certificates in the following store and hit the Browse button.



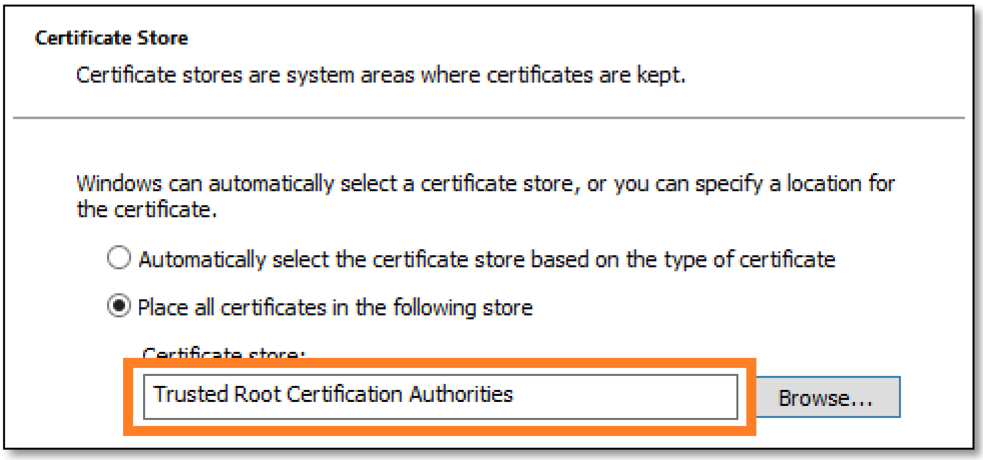
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

6.9 Now, locate the 'Trusted Root Certification Authorities' and make sure it is selected, click OK.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

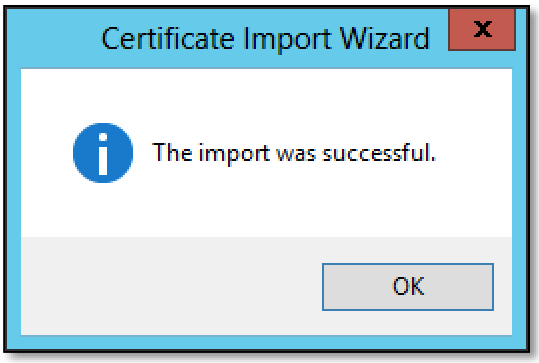
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

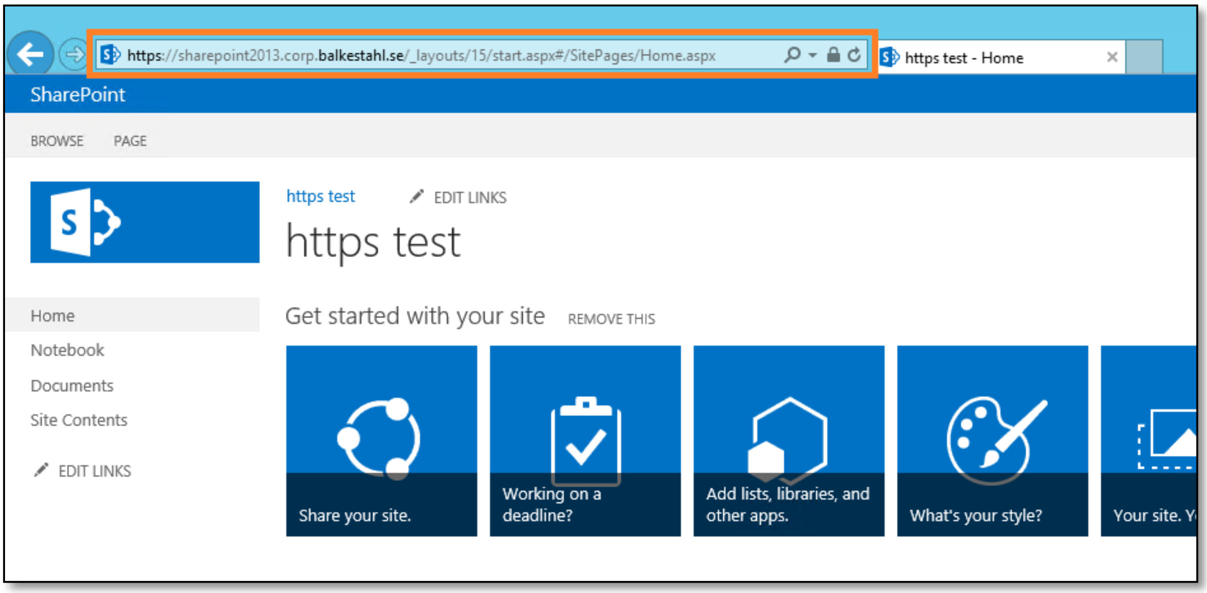
6.10 Verify that this is what you see as well. Click on OK.



Certificate Import Wizard

The import was successful.

6.11 **Success!** Try again to browse to the site, you should probably close the browser and start a new browser window.



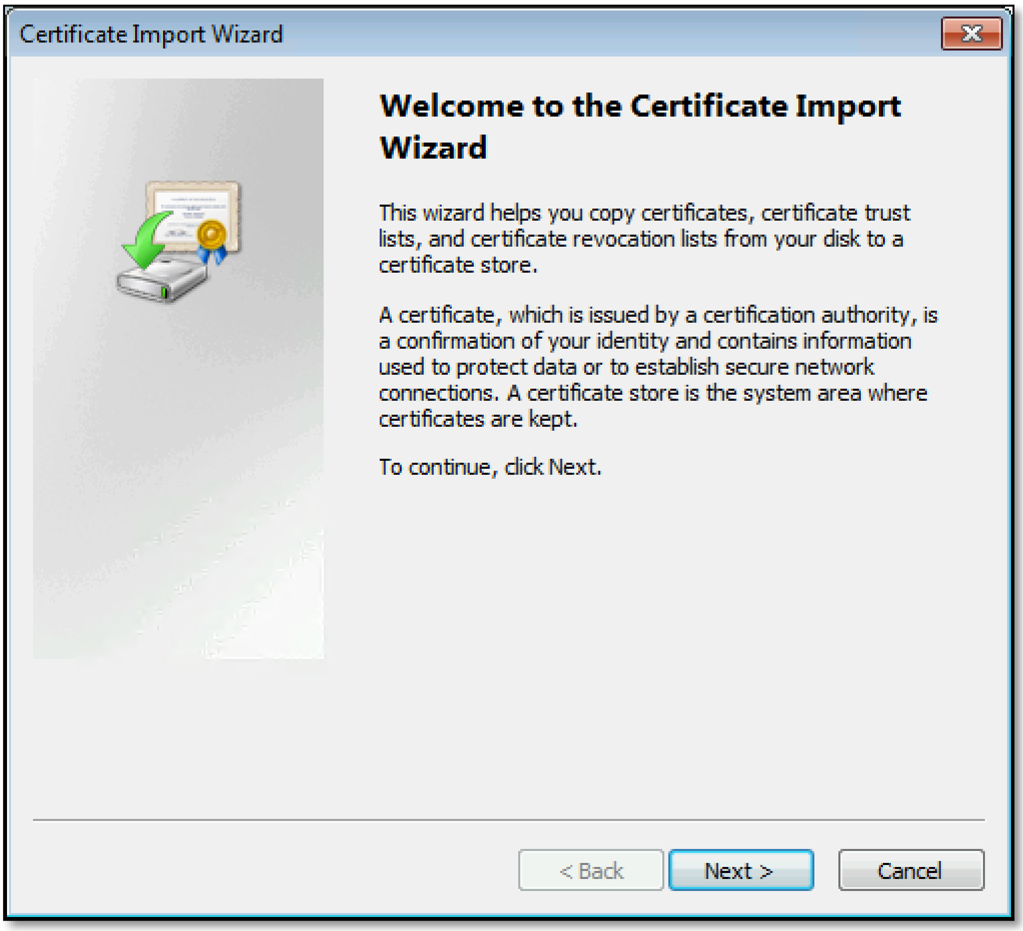
https://sharepoint2013.corp.balkestahl.se/_layouts/15/start.aspx#/SitePages/Home.aspx

6.12 Now we're talking! That's more like it, no red errors, no banner preventing us from loading the content...all is good, Life is GOOD!

Note: On my own server, it simply took a while for the error to go away, the IE cache has a renewal cycle of 50 minutes, to force a renewal, press Ctrl F5. That should do it.

7. Test functionality

Testing has really already been taken care of in Chapter 6, but if you did what I did and used the server's browser (not recommended in production) to test access, then you really should test from a client to get the proper feel for it.
Use the steps described in Chapter 6 on the client computer as well. The dialog may look a bit of, but it's the same steps basically. Sample dialog:



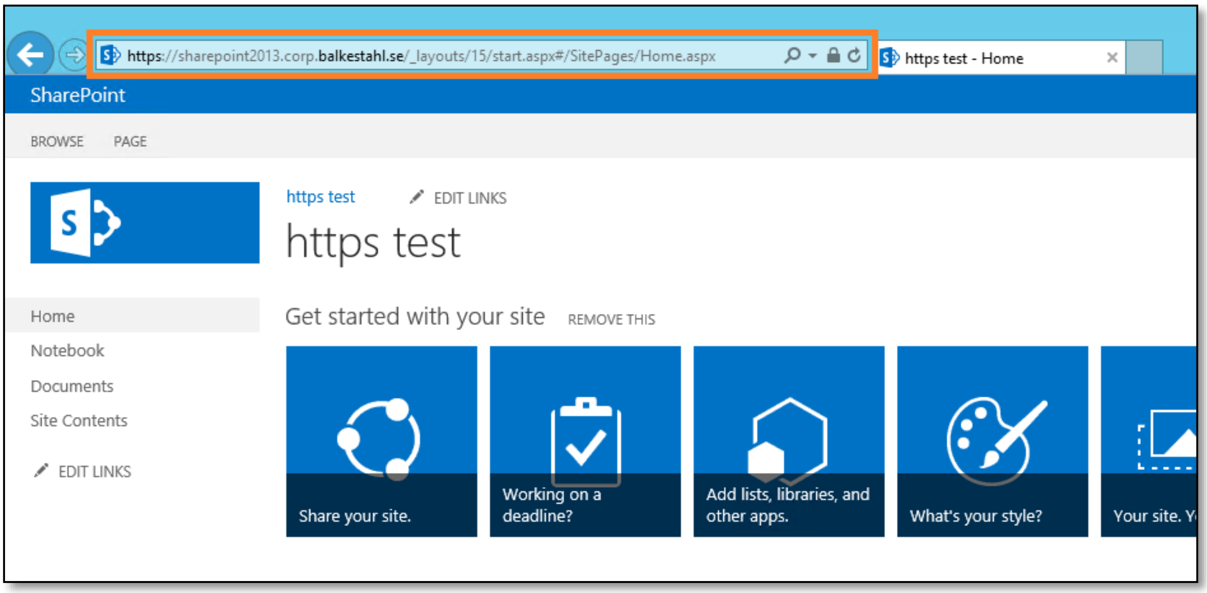
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

You will get the Picture if you use the steps in Chapter 6. Once you see the image below in your browser, you are OK!



https://sharepoint2013.corp.balkestahl.se/_layouts/15/start.aspx#/SitePages/Home.aspx

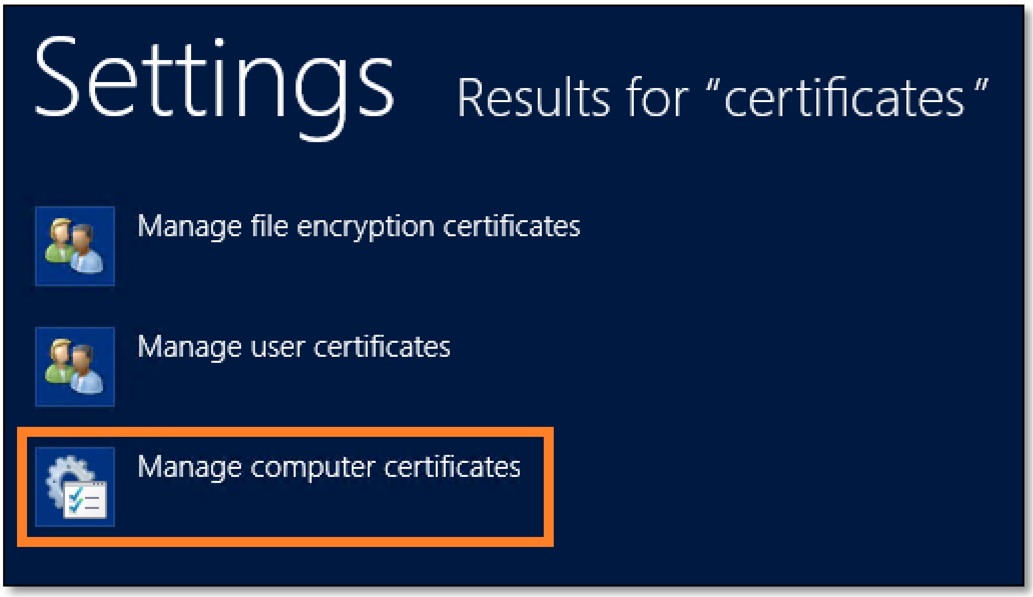
8. T-shooting

T-shooting scenarios covered so far:
- 8.1 Delete redundant certificates
- 8.2 Configure Loopback check

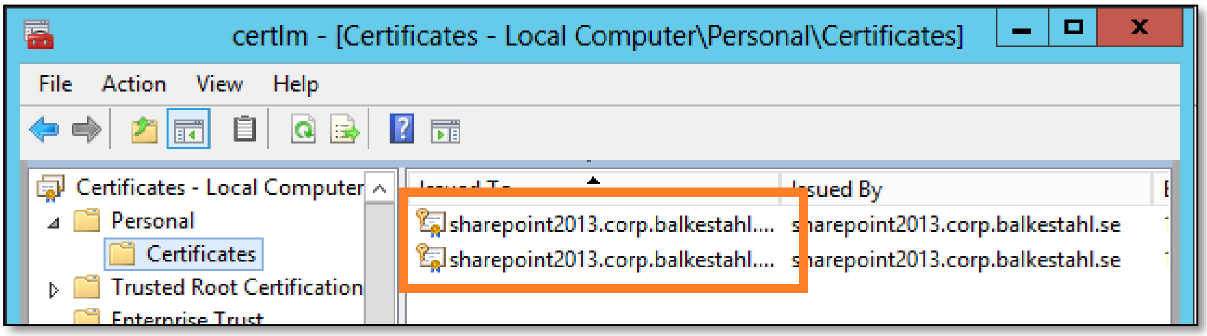
8.1 Delete redundant certificates

If adding the cert fails and you want to delete every copy, do this:

8.1.1 Press the start button, type Certificates...

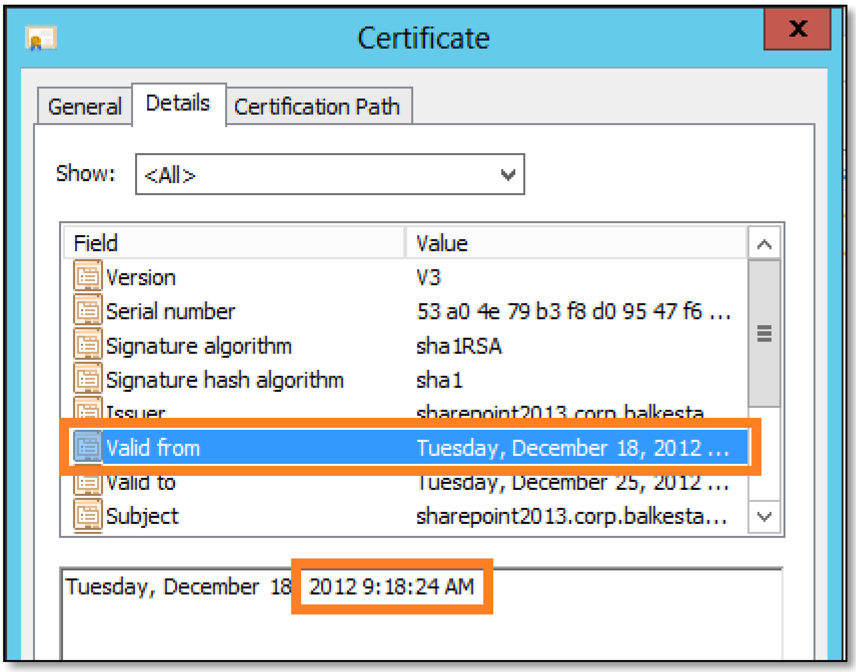

Settings
Results for "certificates"
Manage file encryption certificates
Manage user certificates
Manage computer certificates

8.1.2 Select Manage computer certificates.


certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification
Enterprise Trust

Issued To	Issued By
sharepoint2013.corp.balkestahl....	sharepoint2013.corp.balkestahl.se
sharepoint2013.corp.balkestahl....	sharepoint2013.corp.balkestahl.se

8.1.3 This will open up the 'Certificates Manager'//MMC Certificates Snap in. Locate the Personal, Certificates folder. In the content, either delete them both, or, find out which is the newer and delete the old one.

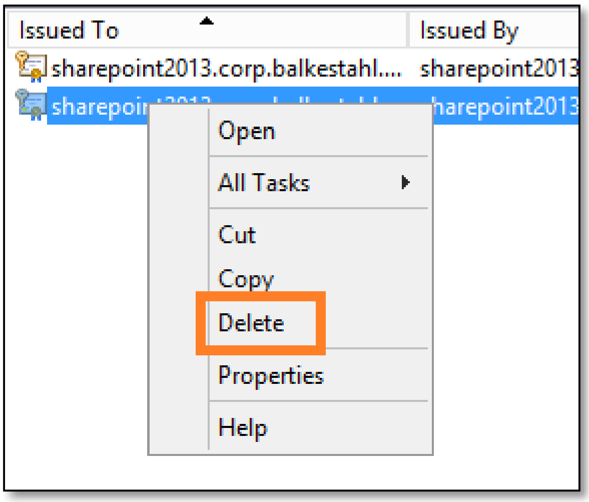


Show: <All>

Field	Value
Version	V3
Serial number	53 a0 4e 79 b3 f8 d0 95 47 f6 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	sharepoint2013.corp.balkesta...
Valid from	Tuesday, December 18, 2012 ...
Valid to	Tuesday, December 25, 2012 ...
Subject	sharepoint2013.corp.balkesta...

Tuesday, December 18, 2012 9:18:24 AM

8.1.4 In the Certificate Details, you will see the Valid from timestamp, this is from when the certificate was created.



Issued To	Issued By
sharepoint2013.corp.balkestahl....	sharepoint2013
sharepoi...	...harepoint2013

8.1.5 When you know which one to keep, delete the other, right click delete.
Done.

8.2 Configure Loopback check.

Note: Remember that the loopback check is a security feature that has been put there for a reason, it protects the server from a certain form of attacks. Disabling it will open up the server for such attacks. Read Spencer Harbar's post at the link below for a deeper understanding of this concept.

Are you planning to do one of two things on your SharePoint server, then you need to configure this, configure, not necessarily disable it.
- If you have search on the server and the Content source Points to the server itself using an FQDN.
- If you want to use the servers browser to test functionality or to access CA using an FQDN. (This is us in this guide...)

Note: I strongly recommend against using any browser on any server! It is a security risk since use of the browser opens up new ways for unwanted code to enter the server. Always access the server from a client browser!

I use the server's browser in my lab to make it easier, but it is a contained lab environment and the accounts used do not have access to anything outside this particular lab environment. Furthermore, the lab environment cannot be reached from outside nor can it access the Internet.

(Thanks Anders Janson, UAG/TMG/Security expert at Enfo Zipper for great feedback!)

Two links will tell you all you need to know:

8.2.1
DisableLoopbackCheck & SharePoint: What every admin and developer should know.
http://www.harbar.net/archive/2009/07/02/disableloopbackcheck-amp-sharepoint-what-every-admin-and-developer-should-know.aspx
(Spencer Harbar explains it all)

8.2.2
http://support.microsoft.com/kb/896861 (the best KB out there, it is old but still relevant)

9. Resources and Recognitions

Don't know who the author is, but this article gave me the last piece in the https puzzle.

How to Create a Self-signed Certificate in IIS 7
http://www.sslshopper.com/article-how-to-create-a-self-signed-certificate-in-iis-7.html

My thanks to the following individuals who have in different ways helped me in my ambitions to create these guides on difficult subjects for SharePoint:

Anders Janson (Enfo Zipper) Thanks Anders for very good and constructive feedback!
Hasain Alshakarti (TrueSec) Blog
Mattias Gutke (Enfo Zipper)
Anders Grönlund (Enfo Sweden)
Andrija Marcic (Microsoft)
Mattias Karlsson (Microsoft)
Herakles (Unknown)