

# Configure IIS to use your self signed certificates with your application including IIS client certificate mapping authentication

⌚ October 27, 2014 - 📲 Elizabeth Andrews (<https://blog.jayway.com/author/elizabethandrews/>) - ☐ .Net (<https://blog.jayway.com/category/net/>) / Security (<https://blog.jayway.com/category/security-2/>) - 💬 75 Comments (<https://blog.jayway.com/2014/10/27/configure-iis-to-use-your-self-signed-certificates-with-your-application/#comments>)

I'm now assuming that you read my [previous post](http://blog.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/) (<http://blog.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/>) about how to create self signed certificates for development and it might've left you thinking "Yay great! ....But how do I actually use them?". This blog post will take you step by step through the manual process of configuring IIS on your PC or Windows Server to use your self signed certificates together with IIS client certificate mapping authentication.

**Please note** that I in my examples I use my localhost hosting and a random domain name but you can do this on your real server's IIS if you have a static IP address from your internet service provider or your



(<https://www.jayway.com>)

Search

[Subscribe via RSS](#)

(<https://blog.jayway.com/?feed=rss2>).

## CATEGORIES

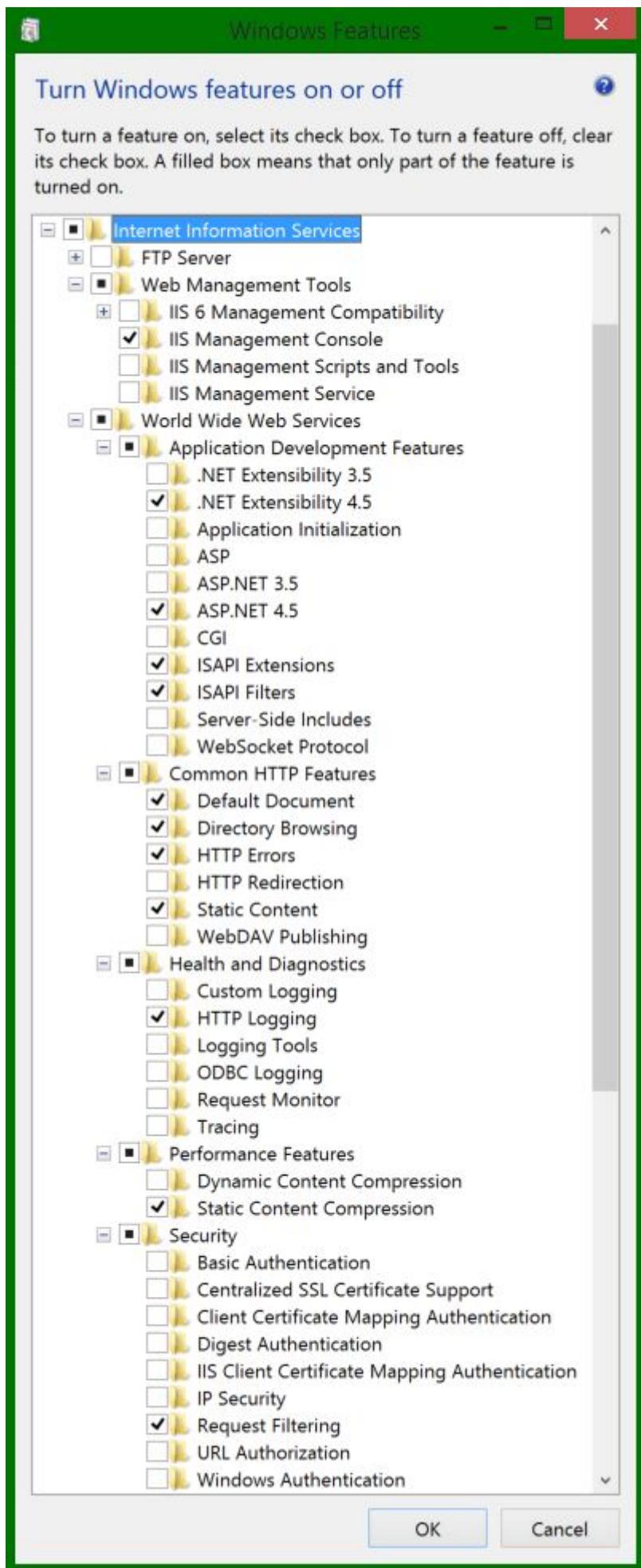
- [.Net](#) (<https://blog.jayway.com/category/net/>).
- [Agile](#) (<https://blog.jayway.com/category/agile/>).
- [Android](#) (<https://blog.jayway.com/category/android/>).
- [Architecture](#) (<https://blog.jayway.com/category/architecture/>).
- [Art](#) (<https://blog.jayway.com/category/uncategorized/art/>).

domain hosting company as well as configured your firewall, router etc. correctly where finally you can point your domain name to your that address. **BUT** I won't recommend either together with *self signed certificates* unless your clients/users are willing to receive and install your self-signed root and client certificate. A good example of this is in a closed intranet where you have access to all the end-user's computers because then you can install the certificates on their machines, which is necessary if you don't want your users to get a big fat warning about trust issues with your self signed server certificate. If you are looking for a commercial production-worthy solution you should purchase your certificates instead of self signing. So now we have that out of the way I'm using a PC with Windows 8.1 Pro, IIS 8.5 and Visual Studio Premium 2013. (I've also tested with a Windows Server 2012 R2 Hyper-V VM on my PC).

## **Installing IIS**

If you haven't already installed IIS on the machine that will act as the hosting server, please do so by pressing the Windows button for a PC and search "Turn Windows features on or off" (or go to Control Panel and search). Check Internet Information Services and the following childnodes.

[Aspect Oriented Programming](https://blog.jayway.com/category/aspect-oriented-programming/)  
(<https://blog.jayway.com/category/aspect-oriented-programming/>).  
[Assistants](https://blog.jayway.com/category/assistants/)  
(<https://blog.jayway.com/category/assistants/>).  
[Augmented Reality](https://blog.jayway.com/category/augmented-reality/)  
(<https://blog.jayway.com/category/augmented-reality/>).  
[Automotive](https://blog.jayway.com/category/automotive/)  
(<https://blog.jayway.com/category/automotive/>).  
[C++](https://blog.jayway.com/category/c/)  
(<https://blog.jayway.com/category/c/>).  
[Cloud](https://blog.jayway.com/category/cloud/)  
(<https://blog.jayway.com/category/cloud/>).  
[Cocoa](https://blog.jayway.com/category/cocoa/)  
(<https://blog.jayway.com/category/cocoa/>).  
[Competence Development](https://blog.jayway.com/category/competence-development/)  
(<https://blog.jayway.com/category/competence-development/>).  
[Data Science](https://blog.jayway.com/category/data-science/)  
(<https://blog.jayway.com/category/data-science/>).  
[Design](https://blog.jayway.com/category/design/)  
(<https://blog.jayway.com/category/design/>).  
[DevOps](https://blog.jayway.com/category/devops/)  
(<https://blog.jayway.com/category/devops/>).



[Dynamic languages](#)  
(<https://blog.jayway.com/category/dynamic-languages/>).

[Embedded](#)  
(<https://blog.jayway.com/category/embedded/>).

[Events](#)  
(<https://blog.jayway.com/category/events/>).

[Functional programming](#)  
(<https://blog.jayway.com/category/functional-programming/>).

[Generics](#)  
(<https://blog.jayway.com/category/swift/generics/>).

[Graphics](#)  
(<https://blog.jayway.com/category/graphics/>).

[iOS](#)  
(<https://blog.jayway.com/category/ios/>).

[IoT](#)  
(<https://blog.jayway.com/category/iot/>).

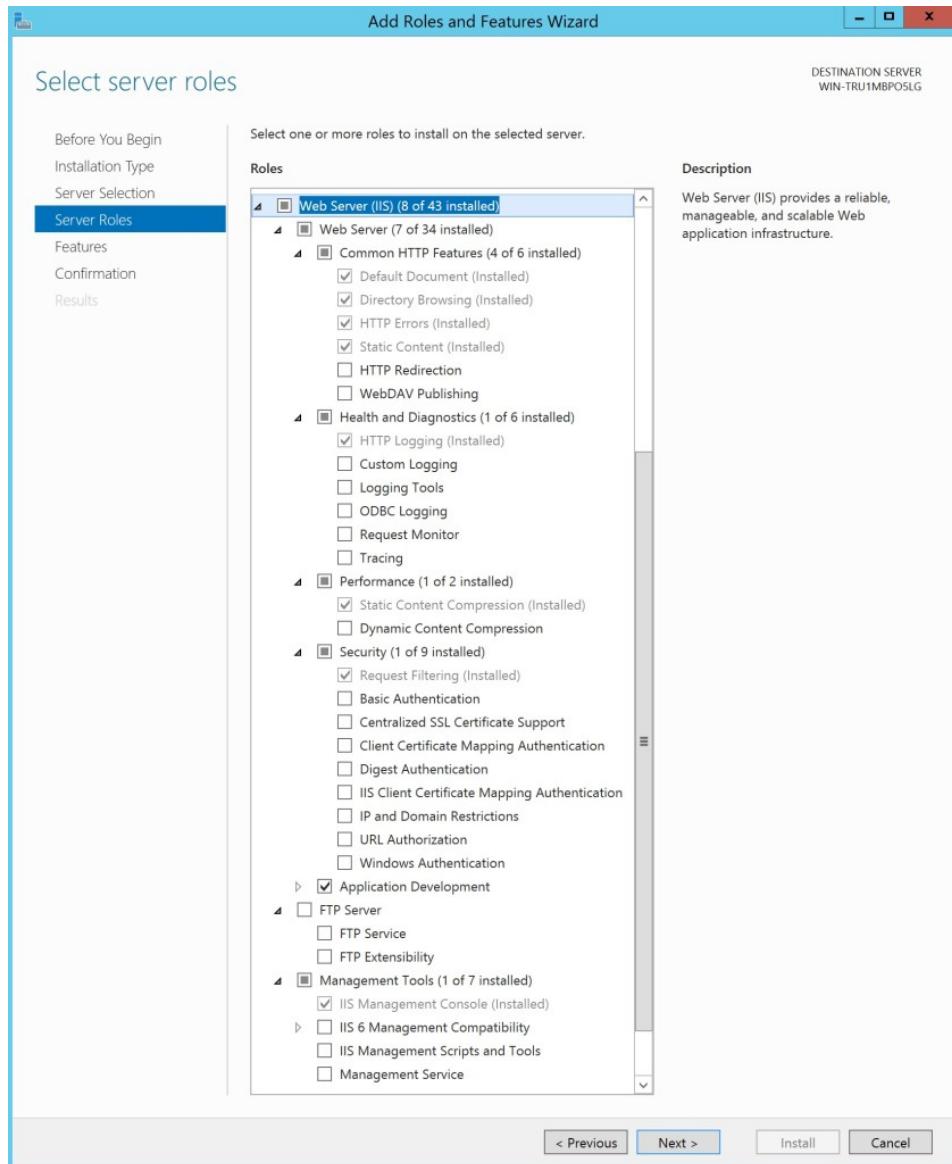
[Java](#)  
(<https://blog.jayway.com/category/java/>).

[JavaScript](#)  
(<https://blog.jayway.com/category/javascript/>).

[Kotlin](#)  
(<https://blog.jayway.com/category/kotlin/>).

(<http://blog.jayway.com/wp-content/uploads/2014/10/1-complete-IIS-install.jpg>) If you are running on .NET 3.5 you need to check the .NET Extensibility 3.5 and ASP.NET 3.5)

For Windows Server 2012 go to the Server Manager Dashboard → Click add roles and features → Choose role-based or feature-based installation and go next → Select the server → Enable the server role called Web Server (IIS) and following child elements



(<http://blog.jayway.com/wp-content/uploads/2014/10/Server-IIS.jpg>)

Also make sure Application Development is checked with the following childnodes

Linux

(<https://blog.jayway.com/category/linux/>)

Machine Learning

(<https://blog.jayway.com/category/data-science/machine-learning/>)

Other

(<https://blog.jayway.com/category/other/>)

python

(<https://blog.jayway.com/category/python/>)

React

(<https://blog.jayway.com/category/web/react/>)

Scala

(<https://blog.jayway.com/category/scala/>)

Security

(<https://blog.jayway.com/category/security-2/>)

Swift

(<https://blog.jayway.com/category/swift/>)

SwiftUI

(<https://blog.jayway.com/category/swift/swiftui/>)

Testing

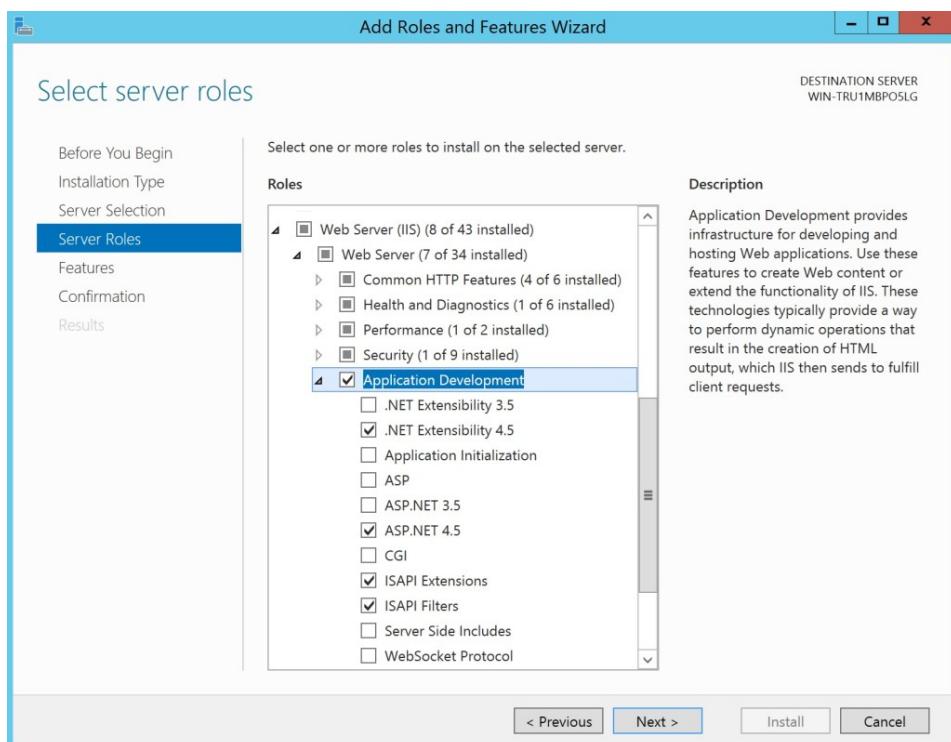
(<https://blog.jayway.com/category/testing/>)

Tips & Tricks

(<https://blog.jayway.com/category/tips-and-tricks/>)

Tools & Workflows

(<https://blog.jayway.com/category/tools-and-workflows/>)



(<http://blog.jayway.com/wp-content/uploads/2014/10/Server-IIS-application-dev.jpg>)

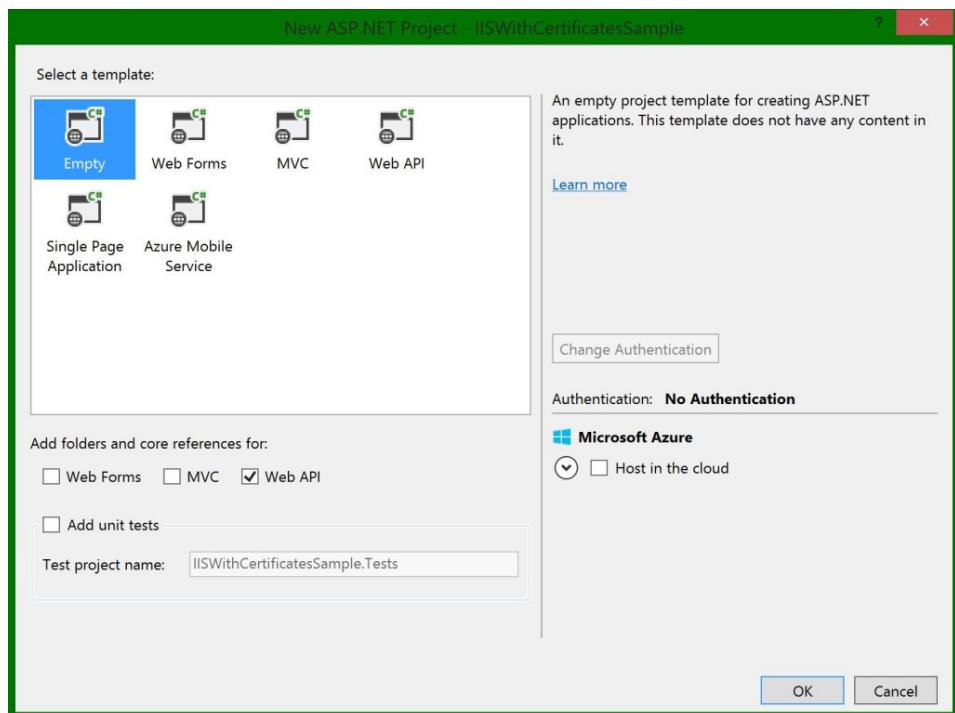
Click OK and let Windows install.

## Creating our sample project

For the sake of this demo we'll create a really simple mini application that we will be hosting in the local IIS. (You can also just [fork mine](https://github.com/LadyLizzy/IISWithCertificatesSample) (<https://github.com/LadyLizzy/IISWithCertificatesSample>) directly at Github)

In Visual Studio, create a new empty web application and reference web api

tegory/tools-and-workflows/),  
Tutorial  
(<https://blog.jayway.com/category/tutorial/>),  
Uncategorized  
(<https://blog.jayway.com/category/uncategorized/>),  
Unity  
(<https://blog.jayway.com/category/unity/>),  
User Experience  
(<https://blog.jayway.com/category/user-experience/>),  
VR/AR  
(<https://blog.jayway.com/category/vrar/>),  
Wearables  
(<https://blog.jayway.com/category/wearables/>),  
Web  
(<https://blog.jayway.com/category/web/>),  
  
TAGS  
.Net  
(<https://blog.jayway.com/tag/.net/>)  
Android  
(<https://blog.jayway.com/tag/android/>),



(<http://blog.jayway.com/wp-content/uploads/2014/10/5-New-Project.jpg>)

We'll just need a reeeeally simple controller:

```
using System.Web.Http;

namespace IISWithCertificatesSample.WebApi.Controllers
{
    public class CatsController : ApiController
    {
        public IHttpActionResult Get()
        {
            return Ok("A lot of cats meowing for food");
        }
    }
}
```

You should now be able to run both routes (F5) and surf to the localhost url with /api/cats (mine looks like <http://localhost:62172/api/cats>). Awesome, lets host this application using our local IIS.

aop

(<https://blog.jayway.com/tag/aop>)

automated testing

(<https://blog.jayway.com/tag/automated-testing/>)

aws

(<https://blog.jayway.com/tag/aws/>)

(<https://blog.jayway.com/tag/azure/>)

C#

(<https://blog.jayway.com/tag/c/>)

(<https://blog.jayway.com/tag/clojure/>)

(<https://blog.jayway.com/tag/closure/>)

(<https://blog.jayway.com/tag/conference/>)

conference)

frameworks

(<https://blog.jayway.com/tag/frameworks/>)

functional programming

([https://blog.jayway.com/tag/functional\\_programming/](https://blog.jayway.com/tag/functional_programming/))

git

(<https://blog.jayway.com/tag/git/>)

http

(<https://blog.jayway.com/tag/http/>)

iOS

(<https://blog.jayway.com/tag/ios/>)

iphone

(<https://blog.jayway.com/tag/iphone/>)

Java

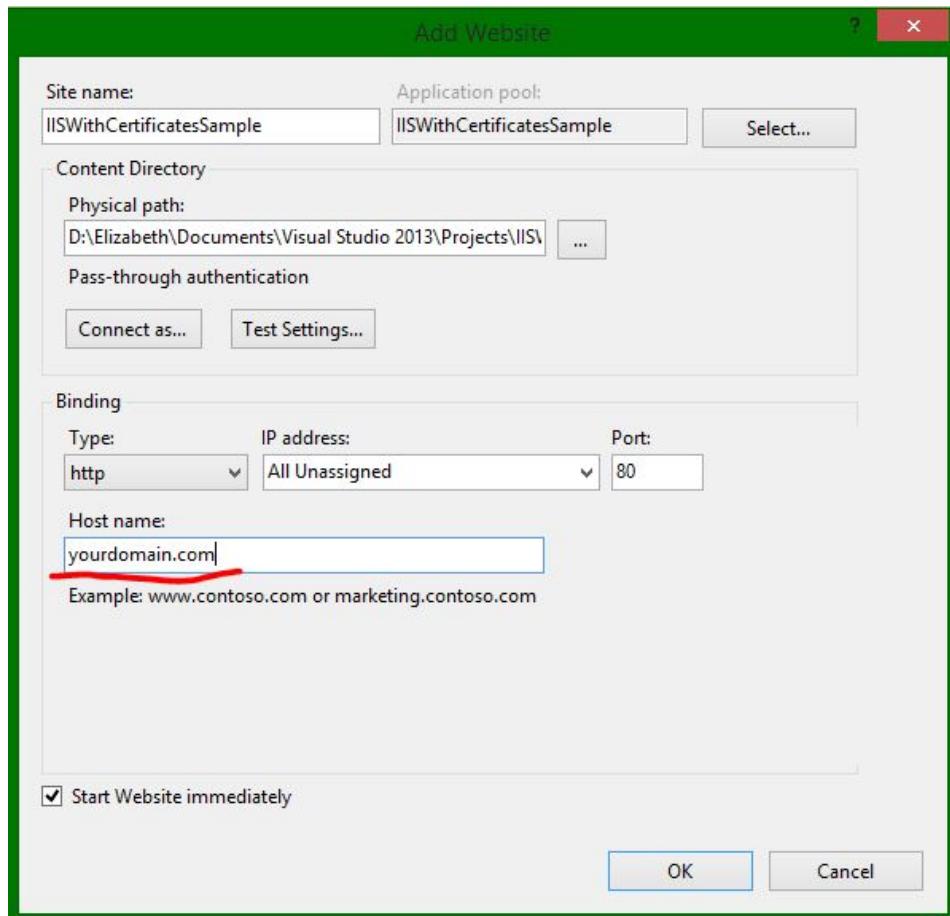
(<https://blog.jayway.com/tag/java/>)

**NOTE:** We will no longer be running the application directly from Visual Studio (F5) which is set to use IIS Express.

## Configuring IIS

Open your IIS Manager (Windows button + search for it). Add a new website and application pool with our sample application. (Right-click Sites → Add Website) The path needs to be the folder where your web site documents are located, so if you have published your website point the path there. I'm just going to use the direct path to the project in Visual Studio for this very simple example.

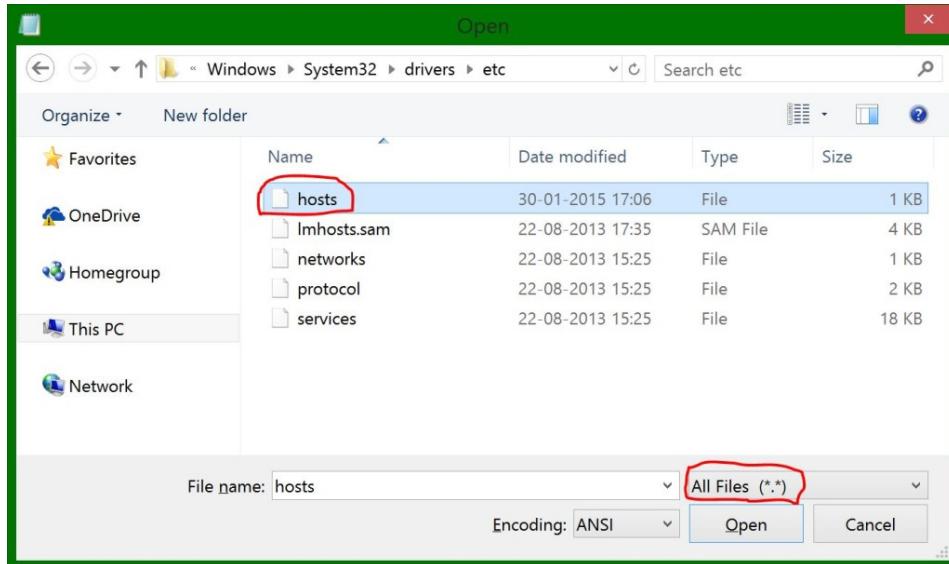
Now let's locally host this site by specifying the host name AKA. your domain name.



(<http://blog.jayway.com/wp-content/uploads/2014/10/7-yourdomain.com.jpg>).

[ava/\)](#)[javascript](#)  
(<https://blog.jayway.com/tag/javascript/>)  
[jayview](#)  
(<https://blog.jayway.com/tag/jayview/>)[junit](#)  
(<https://blog.jayway.com/tag/junit/>)  
[maven](#)  
(<https://blog.jayway.com/tag/maven/>)[metro](#)  
(<https://blog.jayway.com/tag/metro/>)[mobile](#)  
(<https://blog.jayway.com/tag/mobile/>)[node.js](#)  
(<https://blog.jayway.com/tag/nodejs/>)[objective-c](#)  
(<https://blog.jayway.com/tag/objective-c/>)[open](#)  
[source](#)  
(<https://blog.jayway.com/tag/open-source/>)[performance](#)  
(<https://blog.jayway.com/tag/performance/>)[powermock](#)  
(<https://blog.jayway.com/tag/powermock/>)  
[programming](#)  
(<https://blog.jayway.com/tag/programming/>)  
[pr](#)  
(<https://blog.jayway.com/tag/pr/>)

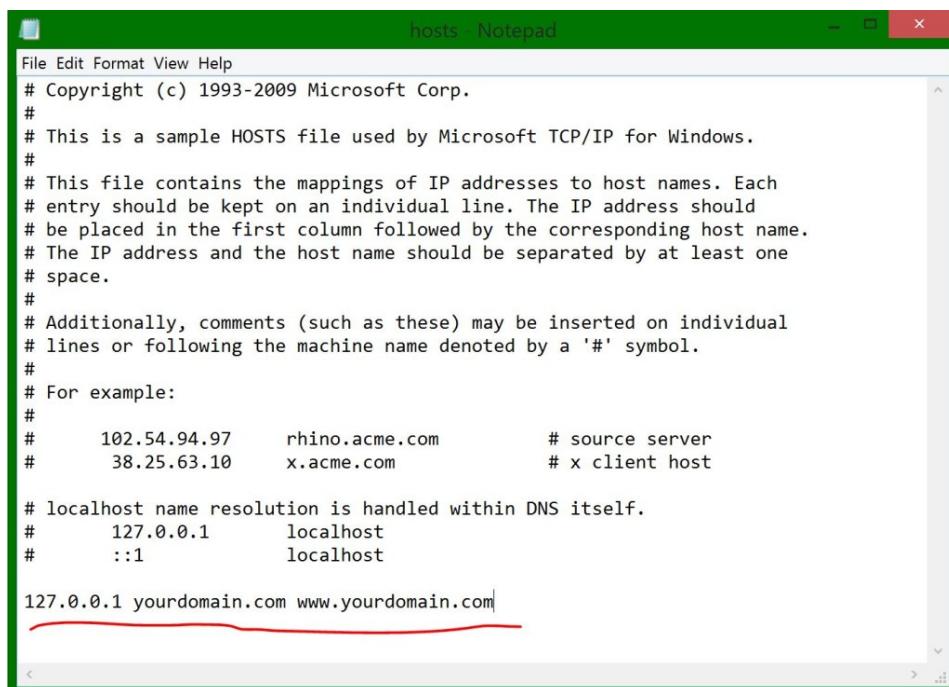
Since I'm just hosting locally I need to add the site to my local hosts file in order to bind my localhost IP address with the host name. This is done by running notepad as administrator and opening the hosts file in the path: %systemroot%\System32\drivers\etc



(<http://blog.jayway.com/wp-content/uploads/2014/10/hosts-file1.jpg>)

Adding the following at the end: 127.0.0.1 yourdomain.com

www.yourdomain.com



(<http://blog.jayway.com/wp-content/uploads/2014/10/8-hosts-file.jpg>)

Now whenever I surf to yourdomain.com and www.yourdomain.com on my machine it will resolve the site with my newly added bindings to the 127.0.0.1 IP address (which is localhost's IP).

ogramming/).rest

(<https://blog.jayway.com/tag/rest/>) Ruby

(<https://blog.jayway.com/tag/ruby/>) scala

(<https://blog.jayway.com/tag/scala/>) spring

(<https://blog.jayway.com/tag/spring/>) testing

(<https://blog.jayway.com/tag/testing-2/>) tips

(<https://blog.jayway.com/tag/tips/>) tools

(<https://blog.jayway.com/tag/tools/>) tutorial

(<https://blog.jayway.com/tag/tutorial/>) web

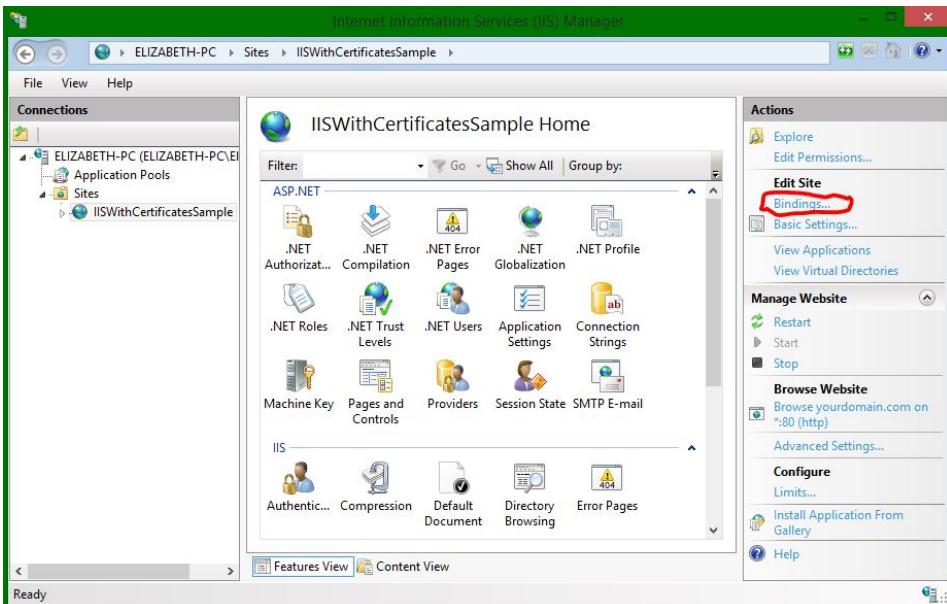
(<https://blog.jayway.com/tag/web/>) windows

(<https://blog.jayway.com/tag/windows-8/>) windows 8

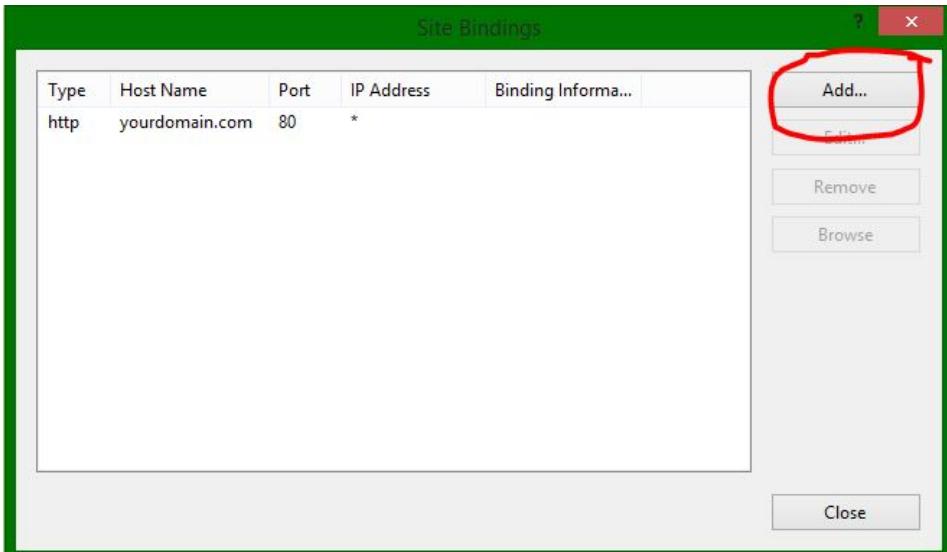
(<https://blog.jayway.com/tag/windows-8/>) windows phone

(<https://blog.jayway.com/tag/windows-phone/>) windows

Let's add the www. binding to your site in the IIS Manager as well



(<http://blog.jayway.com/wp-content/uploads/2014/10/9-IIS-bindings.jpg>)



(<http://blog.jayway.com/wp-content/uploads/2014/10/10-add-http-binding.jpg>)

phone 7

(<https://blog.jayway.com/tag/windows-phone-7/>)

phone 8.1

(<https://blog.jayway.com/tag/windows-phone-8-1/>)

(<https://blog.jayway.com/tag/winrt/>)

wp7dev

(<https://blog.jayway.com/tag/wp7dev/>)

xaml

(<https://blog.jayway.com/tag/xaml/>)

## AUTHORS

Adam Tibbing

(<https://blog.jayway.com/author/adam-tibbingjayway-com/>) (1)

Albin Theander

(<https://blog.jayway.com/author/albintheander/>) (1)

Alexander Persson

(<https://blog.jayway.com/author/alexanderpersson/>) (8)

Amir Moulavi

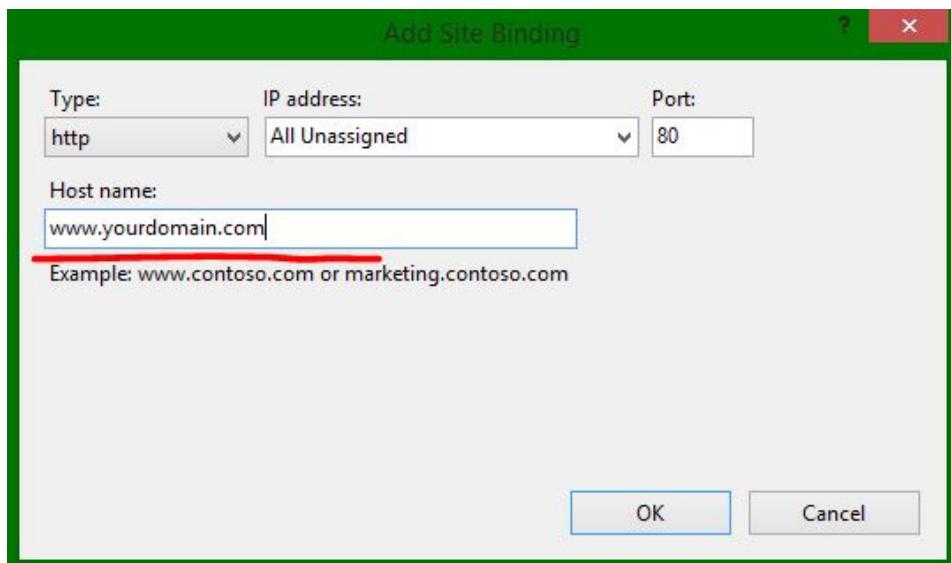
(<https://blog.jayway.com/author/amirmoulavi/>) (7)

Anders Ericsson

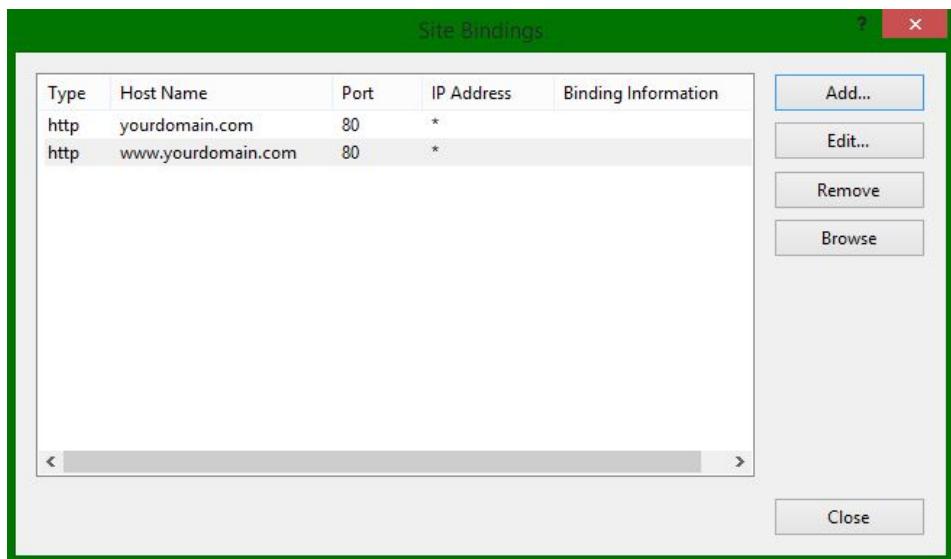
(<https://blog.jayway.com/author/andersericsson/>) (8)

Anders Eriksson

(<https://blog.jayway.com/author/andreseriksson/>)



(<http://blog.jayway.com/wp-content/uploads/2014/10/11-domain-with-www.jpg>)



(<http://blog.jayway.com/wp-content/uploads/2014/10/12-both-http-added.jpg>)

Surf to the domain name you set up in the bindings with or without www. and add the ending /api/cats and you should get the meowing cats. (If not try emptying the cache)

**IMPORTANT:** This is ONLY going to happen on the local machine because we altered the hosts file to redirect our requests of the domain name we added to the localhost IP address. It is meant for development and to be able to test your changes before deploying them to your real web hosting server.

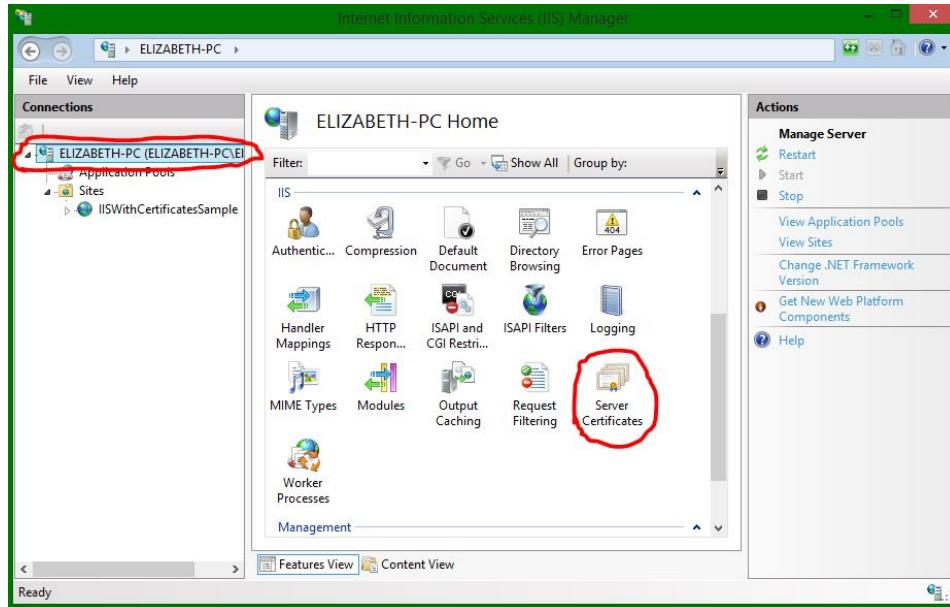
- [thor/anderseriksson/](#) (2)  
Anders Haahr  
(<https://blog.jayway.com/au/thor/anders-haahrjayway-com/>) (1)
- [Anders Janmyr](#)  
(<https://blog.jayway.com/au/thor/andersjanmyr/>) (57)
- [Anders Poulsen](#)  
(<https://blog.jayway.com/au/thor/anderspoulsen/>) (28)
- [Andreas Ekberg](#)  
(<https://blog.jayway.com/au/thor/andreasekberg/>) (4)
- [Andreas Hammar](#)  
(<https://blog.jayway.com/au/thor/andreashammar/>) (60)
- [Andreas Nilsson](#)  
(<https://blog.jayway.com/au/thor/andreasnilsson/>) (2)
- [Andreas Ronge](#)  
(<https://blog.jayway.com/au/thor/andreasronge/>) (6)
- [Anton Fagerberg](#)  
(<https://blog.jayway.com/au/thor/antonfagerberg/>) (6)
- [August Alfredsson](#)  
(<https://blog.jayway.com/au/thor/august-alfredssondevoteam-com/>) (1)
- [Binh Tu](#)  
(<https://blog.jayway.com/au/thor/binhtu/>) (2)
- [Björn Antonsson](#)  
(<https://blog.jayway.com/au/thor/bjornantonsson/>) (1)

## Securing the server with SSL

Now we want to secure the cats by adding a SSL certificate to our Server.

In your IIS Manager go to your server (The top of the tree to the left)

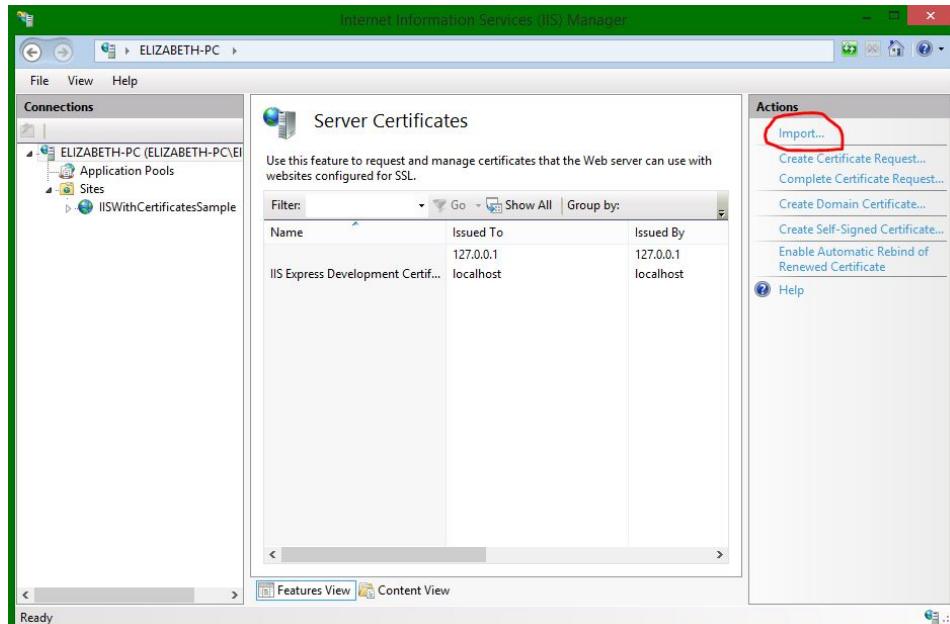
→ Scroll down and double-click Server Certificates.



(<http://blog.jayway.com/wp-content/uploads/2014/10/13-IIS-Server.jpg>)

(If your self signed certificate is already here, jump ahead to the bindings steps)

We need to import our self signed server certificate in order to enable https communication with SSL, so click Import...



[thor/bjornantonsson/](#)(1)

[Björn Carlsson](#)

(<https://blog.jayway.com/au thor/bjornCarlsson/>) (6)

[Björn Granvik](#)

(<https://blog.jayway.com/au thor/bjorngrankvik/>) (29)

[Carl Nordenfelt](#)

(<https://blog.jayway.com/au thor/carl-nordenfeltjayway- com/>) (4)

[Carl-Emil Kjellstrand](#)

(<https://blog.jayway.com/au thor/carlemilkjellstrand/>)

(14)

[Christian Hedin](#)

(<https://blog.jayway.com/au thor/christianhedin/>) (4)

[Christian Jacobsen](#)

(<https://blog.jayway.com/au thor/christianjacobsen/>) (16)

[Daniel Kleveros](#)

(<https://blog.jayway.com/au thor/danielkleveros/>) (4)

[Darius Katz](#)

(<https://blog.jayway.com/au thor/dariuskatz/>) (5)

[Davor Crnomat](#)

(<https://blog.jayway.com/au thor/davorcrnomat/>) (5)

[Dennis Overhage](#)

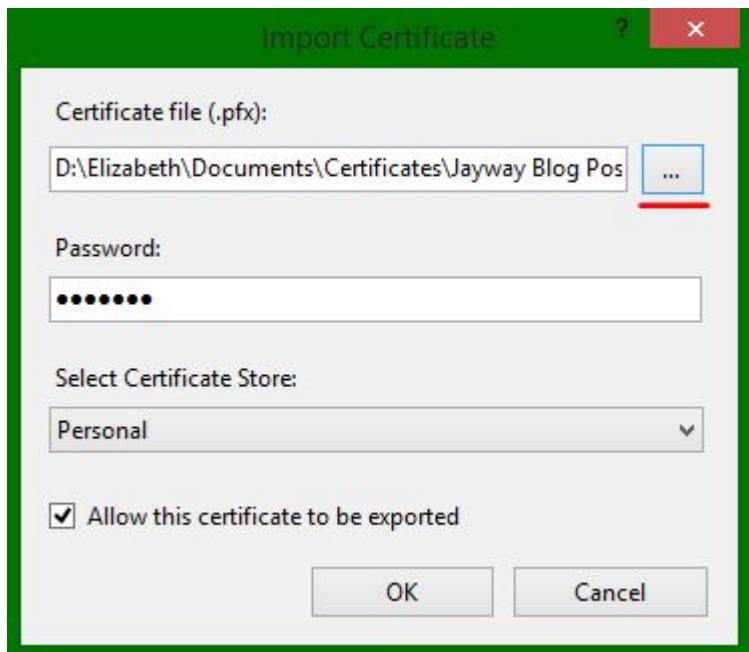
(<https://blog.jayway.com/au thor/dennis- overhagejayway-com/>) (2)

[Einar Valgeirsson](#)

(<https://blog.jayway.com/au thor/einarvalgeirsson/>)

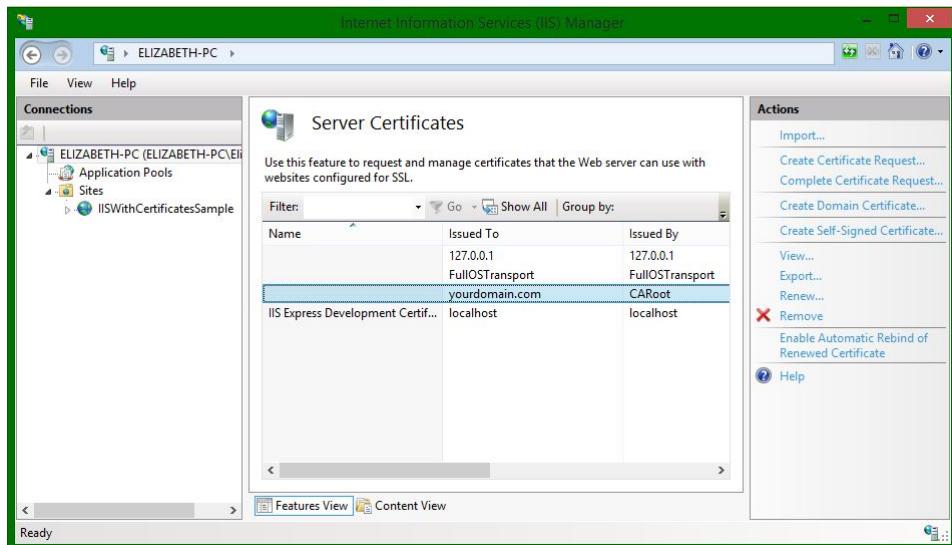
(<http://blog.jayway.com/wp-content/uploads/2014/10/14-Import-server-cert.jpg>)

Click the ... and find your .pfx file, fill out the password (the -po parameter in your command batch file) and click OK



(<http://blog.jayway.com/wp-content/uploads/2014/10/15-browse-server-cert.jpg>)

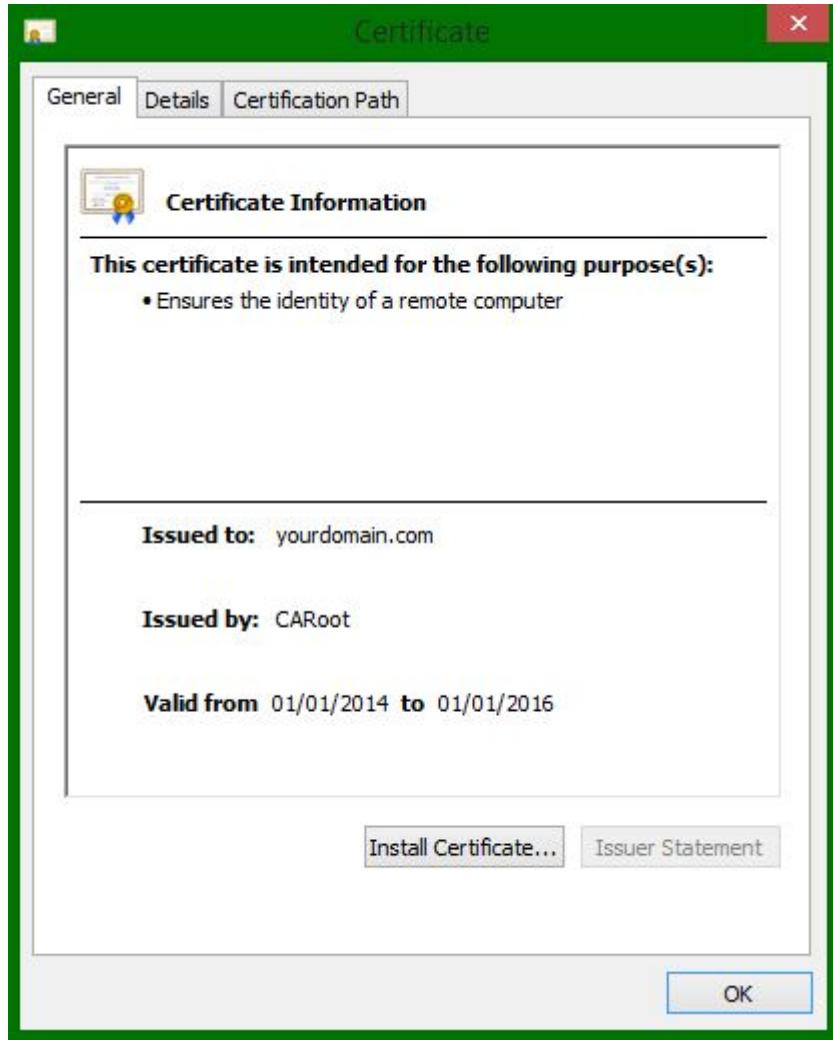
Your certificate is now added



(<http://blog.jayway.com/wp-content/uploads/2014/10/16-cert-added.jpg>)

thor/einar-  
[valgeirssonjayway.com/](https://blog.jayway.com/author/elizabethandrews/)) (2)  
Elizabeth Andrews  
[\(https://blog.jayway.com/au thor/elizabethandrews/\)](https://blog.jayway.com/author/elizabethandrews/) (6)  
Erik Ogenvik  
[\(https://blog.jayway.com/au thor/erikhjortsberg/\)](https://blog.jayway.com/author/erikhjortsberg/) (5)  
Ester Ytterbrink  
[\(https://blog.jayway.com/au thor/esterytterbrink/\)](https://blog.jayway.com/author/esterytterbrink/) (2)  
Fredrik Frodlund  
[\(https://blog.jayway.com/au thor/fredrikfrodlund/\)](https://blog.jayway.com/author/fredrikfrodlund/) (5)  
Fredrik Nannestad  
[\(https://blog.jayway.com/au thor/fredrik/\)](https://blog.jayway.com/author/fredrik/) (1)  
Fredrik Olsson  
[\(https://blog.jayway.com/au thor/fredrikolsson/\)](https://blog.jayway.com/author/fredrikolsson/) (31)  
Frida Bredberg  
[\(https://blog.jayway.com/au thor/fridabredberg/\)](https://blog.jayway.com/author/fridabredberg/) (1)  
Gina Adamova  
[\(https://blog.jayway.com/au thor/gina-adamovajayway- com/\)](https://blog.jayway.com/author/gina-adamovajayway-com/) (1)  
Gustaf Nilklin  
[\(https://blog.jayway.com/au thor/gustafnilklin/\)](https://blog.jayway.com/author/gustafnilklin/) (2)  
Gustaf Nilsson Kotte  
[\(https://blog.jayway.com/au thor/gustafnilssonkotte/\)](https://blog.jayway.com/author/gustafnilssonkotte/) (12)  
Håkan Reis  
[\(https://blog.jayway.com/au thor/hakanreis/\)](https://blog.jayway.com/author/hakanreis/)

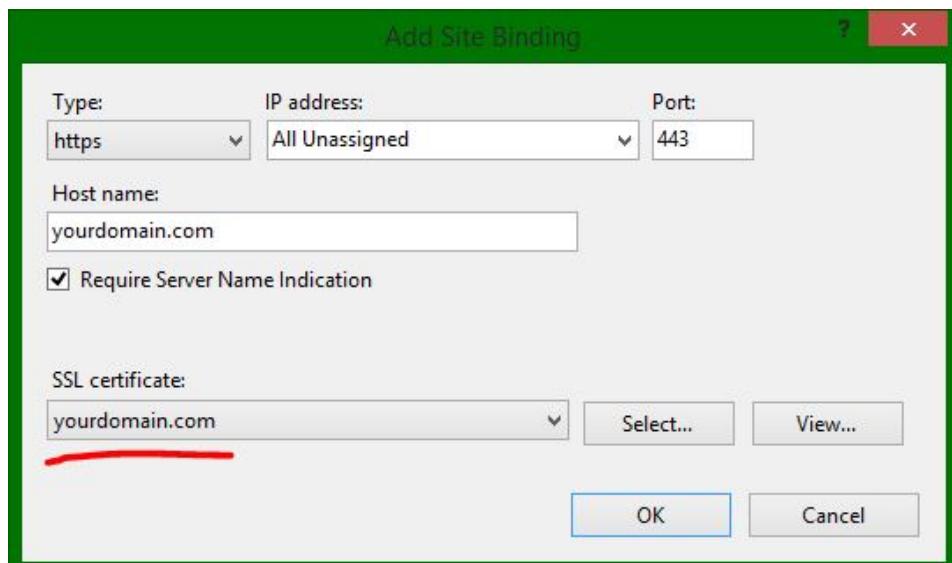
Double-click the newly added cert to verify that it is trusted (Your self signed certificates were added to the correct stores in my [previous post](#) (<http://blog.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/>), so again: read it if you are lost right now ;-))



(<http://blog.jayway.com/wp-content/uploads/2014/10/17-trusted-server-cert.jpg>)

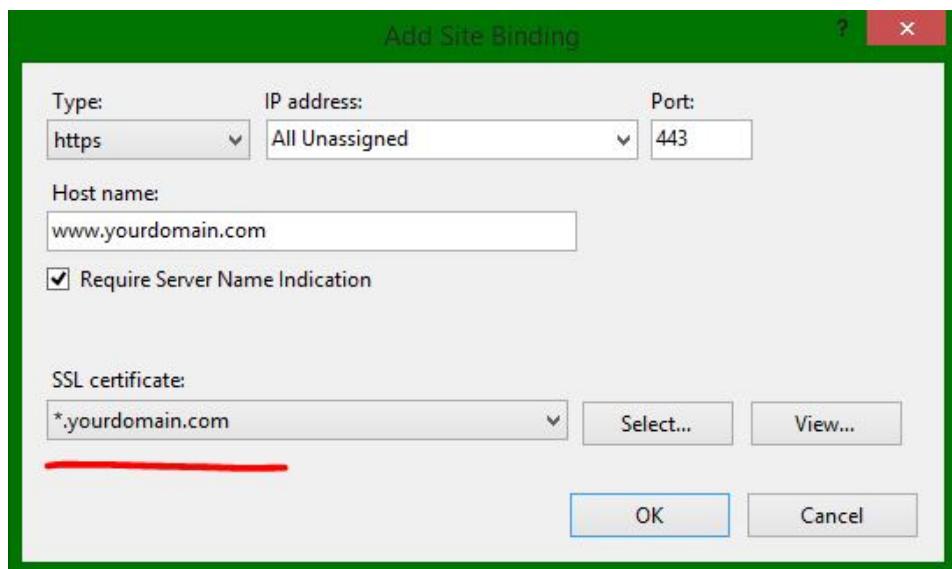
So far, so good! Now we can add the https binding, the same way as before but choose https with port 443, your domain as the host name and find your self signed certificate in the drop down list

thor/hakanreis/)(37)  
Hang Ruan  
(<https://blog.jayway.com/au/thor/hangruan/>)(3)  
Hanna Sahle  
(<https://blog.jayway.com/au/thor/hannasahle/>)(1)  
Hannes Gruber  
(<https://blog.jayway.com/au/thor/hannesgruber/>)(3)  
Henrik Andersson  
(<https://blog.jayway.com/au/thor/henrikandersson/>)(3)  
Henrik Bernstrom  
(<https://blog.jayway.com/au/thor/henrik-bernstromdevoteam-com/>)(5)  
Henrik Feldt  
(<https://blog.jayway.com/au/thor/henrikfeldt/>)(5)  
Henrik Larne  
(<https://blog.jayway.com/au/thor/henriklarne/>)(2)  
Henrik Lundahl  
(<https://blog.jayway.com/au/thor/henriklundahl/>)(4)  
Fredrik Henriksson  
(<https://blog.jayway.com/au/thor/fredrik-henricssonjayway-com/>)(2)  
Hugo Hjerten  
(<https://blog.jayway.com/au/thor/hugo-hjertenjayway-com/>)(3)



(<http://blog.jayway.com/wp-content/uploads/2014/10/18-bindings-add-ssl.jpg>).

Check the Server Name Indication box which enables our server to have multiple certificates installed on the same IP address by sending the hostname with the first stage of the SSL handshake. Repeat the same steps to add SSL for www.yourdomain.com but with a certificate where the CN name matches the domain name or a wildcard certificate



(<http://blog.jayway.com/wp-content/uploads/2014/10/19-https-www-with-wildcard.jpg>).

Our bindings are complete for now

Hugo Josefson  
(<https://blog.jayway.com/author/hugojosefson/>) (6)

Jacob Mattsson  
(<https://blog.jayway.com/author/jacobmattsson/>) (2)

Jakob Nilsson-Ehle  
(<https://blog.jayway.com/author/jakobnilssonehle/>) (4)

Jakob Wolman  
(<https://blog.jayway.com/author/jakobklamra/>) (3)

Jan Kronquist  
(<https://blog.jayway.com/author/jankronquist/>) (29)

Jan-Olof Eriksson  
(<https://blog.jayway.com/author/janoloferiksson/>) (1)

Jens Jakob Jensen  
(<https://blog.jayway.com/author/jensjakobjensen/>) (2)

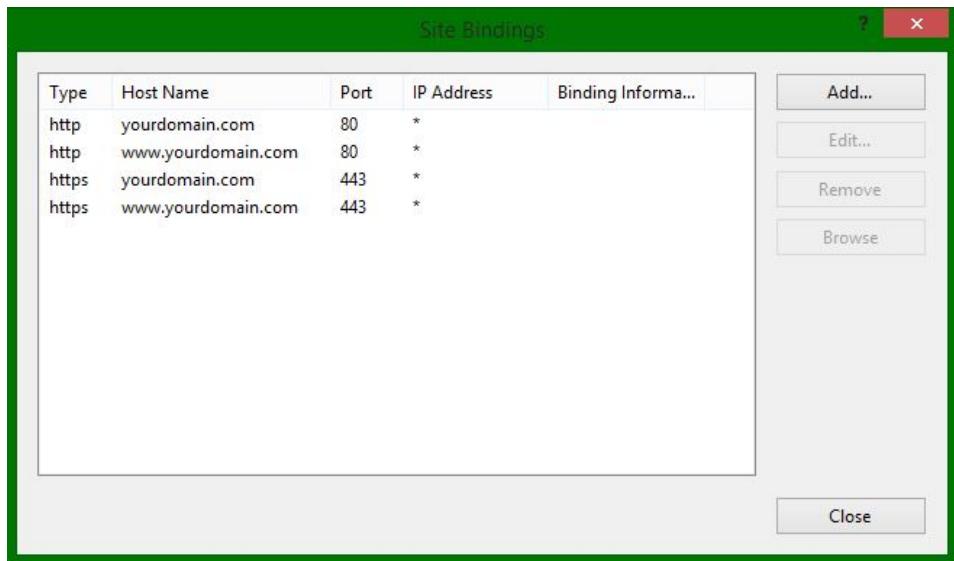
Jens Nordahl  
(<https://blog.jayway.com/author/jensnordahl/>) (2)

Jimmie Jensen  
(<https://blog.jayway.com/author/jimmiejensen/>) (3)

Jimmy Falkbjer  
(<https://blog.jayway.com/author/jimmyfalkbjer/>) (1)

Joacim Löwgren  
(<https://blog.jayway.com/author/joacimlowgren/>) (1)

joakim astbrant  
(<https://blog.jayway.com/author/joakimastbrant/>) (2)



(<http://blog.jayway.com/wp-content/uploads/2014/10/19-All-bindings.jpg>)

Tadaa, you can now use <https://yourdomain.com/api/cats> and  
<https://www.yourdomain.com/api/cats>

**NOTE:** Firefox doesn't use the Windows certificate store, so you will have to add your root CA manually. Go to Firefox Settings → Options → Advanced → View Certificates → Authorities → import your CARoot.cer file

### IIS Client Certificate Mapping Authentication

We have now been through the uses of the root and server certificates and you are probably wondering what to do with the client certificate we also created in my [previous post](#)  
(<http://blog.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/>). This is for situations when we for example need to authenticate clients without a user login and password approach but rather want the server to ask the client to show its certificate and if it's the correct one the client is allowed in. This can be done with a Many-To-One or a One-To-One mapping and I will show you how to do both manually in the IIS Manager.

[Joakim Back](#)

(<https://blog.jayway.com/au/thor/joakimback/>) (1)

[Joakim Hogart](#)

(<https://blog.jayway.com/au/thor/joakimhogart/>) (1)

[Johan Haleby](#)

(<https://blog.jayway.com/au/thor/johanhaleby/>) (50)

[Johan Karlsson](#)

(<https://blog.jayway.com/au/thor/johankarlsson/>) (3)

[Johan Lundahl](#)

(<https://blog.jayway.com/au/thor/johanlundahl/>) (5)

[Johan Måansson](#)

(<https://blog.jayway.com/au/thor/johan-manssonjayway-com/>) (1)

[Johan Nordenswan](#)

(<https://blog.jayway.com/au/thor/johannordenswan/>) (3)

[Johan Olsson](#)

(<https://blog.jayway.com/au/thor/johanolsson/>) (10)

[Johan Rask](#)

(<https://blog.jayway.com/au/thor/johanrask/>) (4)

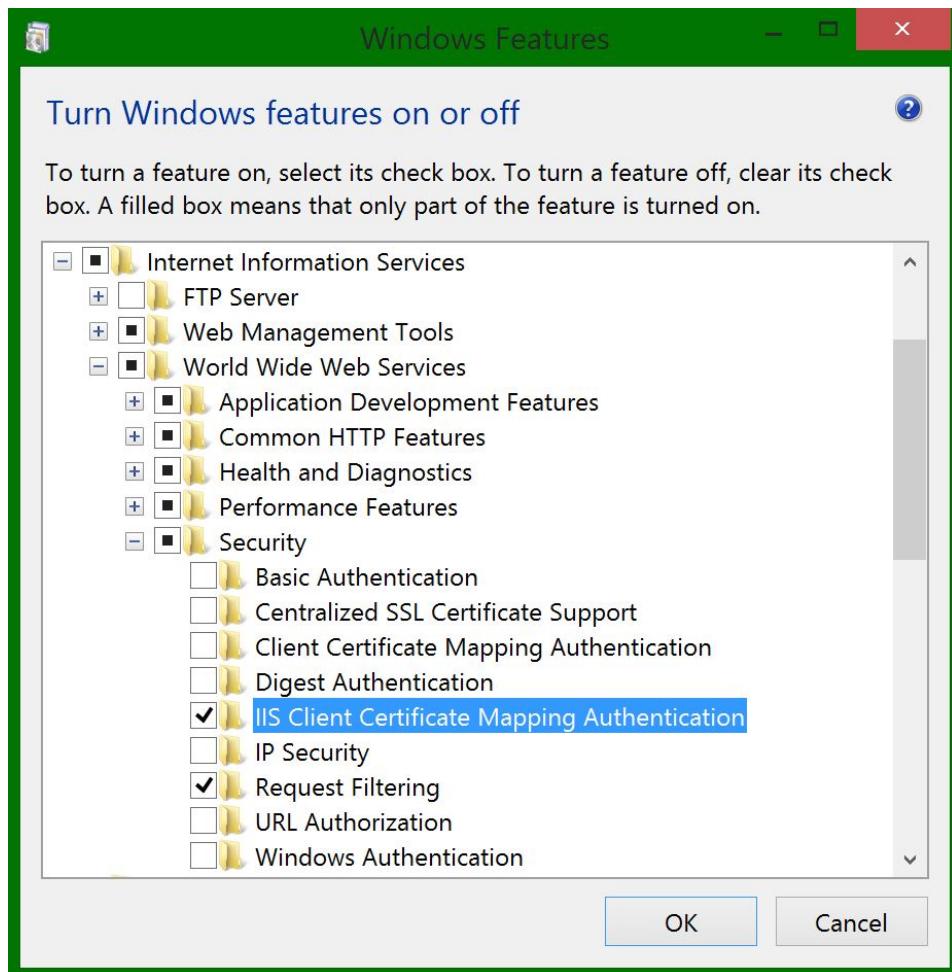
[Johan Silfversparre](#)

(<https://blog.jayway.com/au/thor/johansilfversparre/>) (13)

[Karin Hofbauer](#)

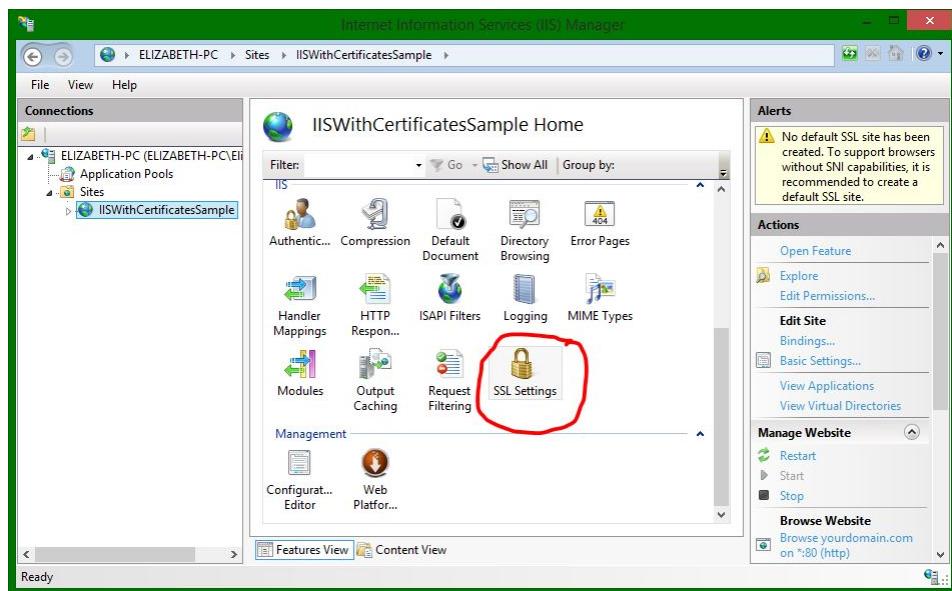
(<https://blog.jayway.com/au/thor/karinhofbauer/>) (1)

First we need to install the feature, so bring up the “Turn Windows features on or off” again and install the following



(<http://blog.jayway.com/wp-content/uploads/2014/10/20-IIS-client-cert-mapping.jpg>)

We'll tell our server to require a SSL certificate from the client



Karl Marhäll

(<https://blog.jayway.com/author/karl-marhall/>) (1)

Kenneth Andersson

(<https://blog.jayway.com/author/kennethandersson/>) (1)

Khalid Afridi

(<https://blog.jayway.com/author/khalid-afridi/>) (1)

Lars-Håkan Jönsson

(<https://blog.jayway.com/author/larshakanjonsson/>) (2)

László Urszuly

(<https://blog.jayway.com/author/laszlourszuly/>) (2)

Mads Enevoldsen

(<https://blog.jayway.com/author/madsenevoldsen/>) (7)

Magnus Mårtensson

(<https://blog.jayway.com/author/magnusmartensson/>)

(9)

Magnus Palmér

(<https://blog.jayway.com/author/magnuspalmer/>) (1)

Magnus Robertsson

(<https://blog.jayway.com/author/magnusrobertsson/>)

(3)

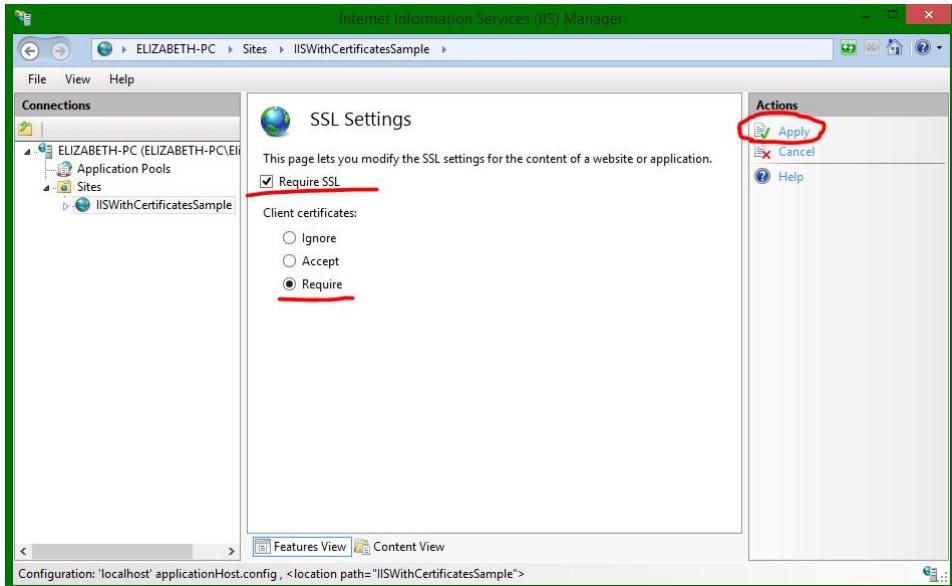
Magnus Rydin

(<https://blog.jayway.com/author/magnusrydin/>) (1)

Mario Boikov

(<https://blog.jayway.com/author/mario-boikov/>)

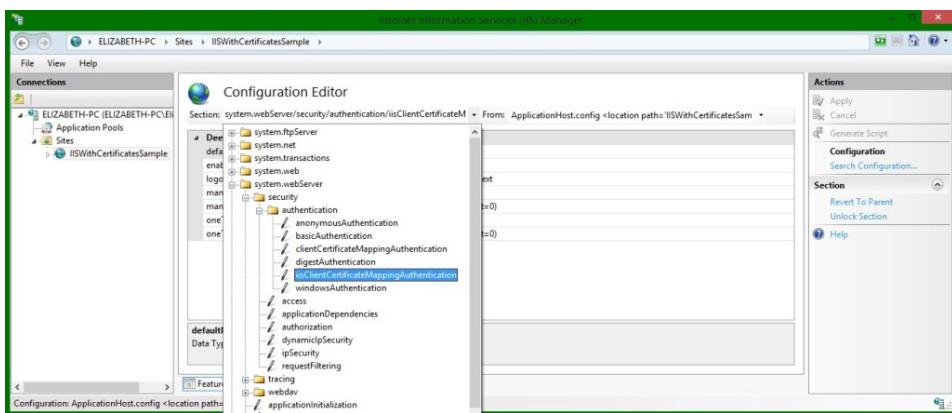
(<http://blog.jayway.com/wp-content/uploads/2014/10/21-SSL-Settings.jpg>)



(<http://blog.jayway.com/wp-content/uploads/2014/10/22-apply-require-ssl.jpg>)

Then we need to configure the server to know which client certificate it needs to validate, so go to the Configuration Editor and choose the iisClientCertificateMappingAuthentication section (you can also enter the path

system.webServer/security/authentication/iisClientCertificateMapping Authentication into the Section field)



(<http://blog.jayway.com/wp-content/uploads/2014/10/24-iisClientCertMapAuth-section.jpg>)

## Many-To-One Mappings

If you want to map multiple client certificate to a single user this approach is what you need. You can also share client certificates like this

[thor/mario-boikov/](#)) (3)

[Mårten Österberg](#)

(<https://blog.jayway.com/author/martenosterberg/>) (1)

[Mattias Ask](#)

(<https://blog.jayway.com/author/mattiasask/>) (8)

[Mattias Hellborg](#)

[Arthursson](#)

(<https://blog.jayway.com/author/mattiasarthursson/>)

(12)

[Mattias Lindskog](#)

(<https://blog.jayway.com/author/mattiaslindskog/>) (9)

[Mattias Rosberg](#)

(<https://blog.jayway.com/author/mattiasrosberg/>) (3)

[Mattias Severson](#)

(<https://blog.jayway.com/author/mattiasseverson/>) (39)

[Mattias Sjögren](#)

(<https://blog.jayway.com/author/mattias-sjogren/>) (4)

[Max Ringström](#)

(<https://blog.jayway.com/author/max-ringstromjayway-com/>) (1)

[Michael Kober](#)

(<https://blog.jayway.com/author/michaelkober/>) (5)

[Mikael Karlsson](#)

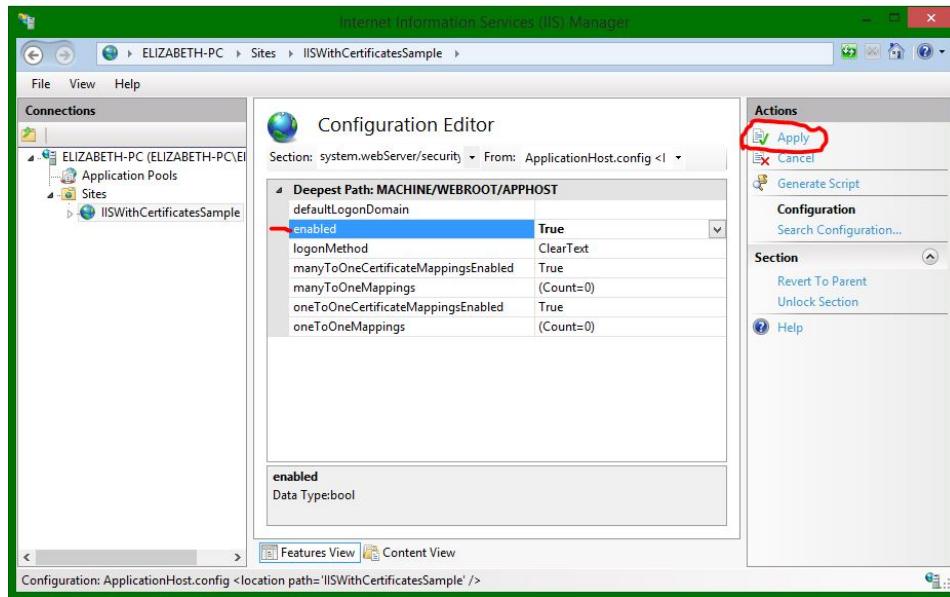
(<https://blog.jayway.com/author/mikaelkarlsson/>) (1)

[Mina Ashna](#)

(<https://blog.jayway.com/author/minashna/>)

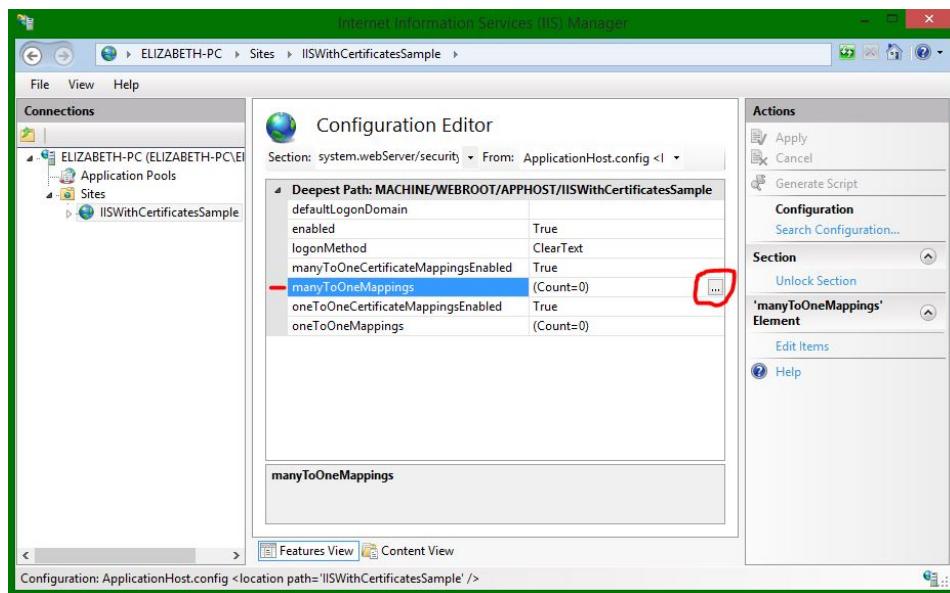
by installing the client certificate (and the CA Root, since we are self-signing certificate) on other users on whichever machine to gain access as long as the client certificate matches the rule criterias of the mapping. It would for example be useful in a situation where you would want all users in an organization to gain access through a single user mapping.

## Enable the client certificate mapping authentication



<http://blog.jayway.com/wp-content/uploads/2014/10/25-enable-client-auth.jpg>

To add a mapping click the ... of the manyToOneMappings



<http://blog.jayway.com/wp-content/uploads/2014/10/26-add-mapping.jpg>

thor/mina-ashnajayway-com/)(2)  
Mohsan Khan  
<https://blog.jayway.com/au/thor/mohsan-khanjayway-com/>(1)

Morten Faester  
<https://blog.jayway.com/au/thor/mortenfaester/>(1)

Niklas Lundberg  
<https://blog.jayway.com/au/thor/niklaslundberg/>(1)

Niklas Uhrberg  
<https://blog.jayway.com/au/thor/niklasuhrberg/>(2)

Nino Martinez  
<https://blog.jayway.com/au/thor/ninomartinez/>(1)

Oleksii Kulikov  
<https://blog.jayway.com/au/thor/oleksii-kulikovjayway-com/>(1)

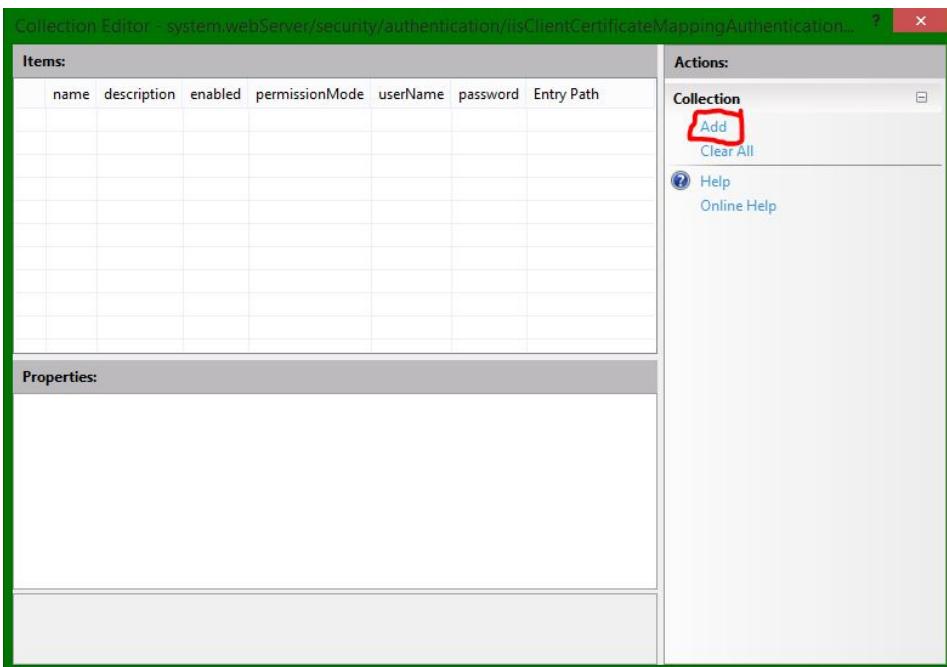
Olof Åkesson  
<https://blog.jayway.com/au/thor/olofakesson/>(2)

Ondrej Bendo  
<https://blog.jayway.com/au/thor/ondrej-bendojayway-com/>(1)

Oskar Wickström  
<https://blog.jayway.com/au/thor/oskarwickstrom/>(3)

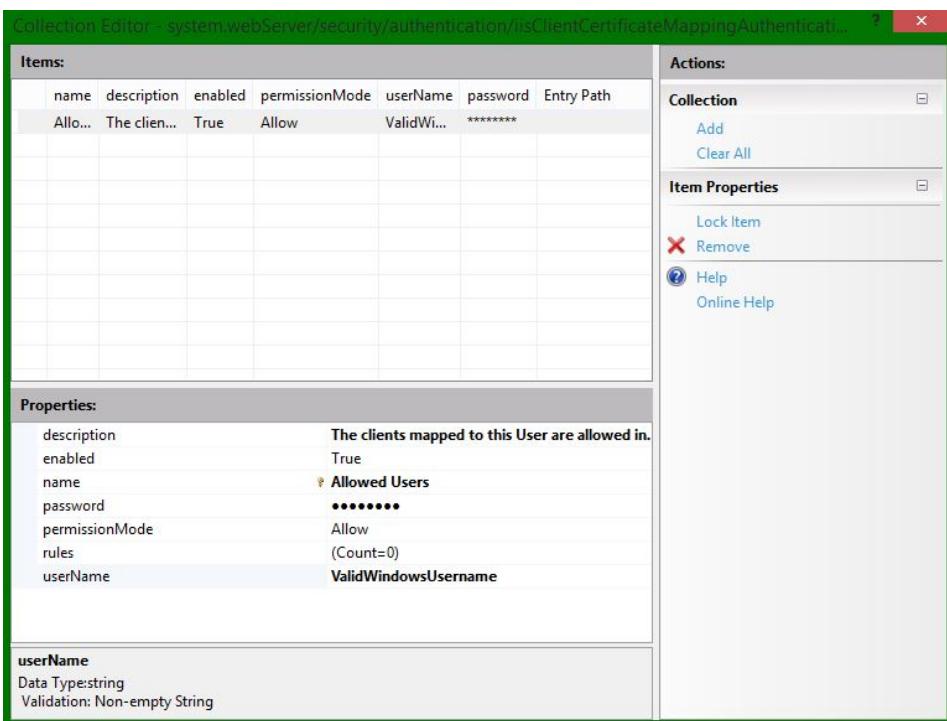
Paolo Longato  
<https://blog.jayway.com/au/thor/paolo-longatojayway-com/>(2)

Here you add the users that you want to grant access.



(<http://blog.jayway.com/wp-content/uploads/2014/10/27-add-new-mapping.jpg>)

Fill out the properties for a mapping and repeat for each user you want to configure for access or denial. **Remember** that you need the client certificate and root CA certificate installed on all the user's mmc.



(<http://blog.jayway.com/wp-content/uploads/2014/10/28-manytoone-mapping.jpg>)

Pär Sikö

(<https://blog.jayway.com/author/parsiko/>) (1)

Patrik Nordwall

(<https://blog.jayway.com/author/patriknordwall/>) (1)

Per Böckman

(<https://blog.jayway.com/author/perbockman/>) (4)

Per Ökvist

(<https://blog.jayway.com/author/perokvist/>) (20)

Per Wendel

(<https://blog.jayway.com/author/perwendel/>) (1)

Per-Erik Bergman

(<https://blog.jayway.com/author/pererikbergman/>) (14)

Per-Olof Bondesson

(<https://blog.jayway.com/author/perolofbondesson/>),

(10)

Petar Mataic

(<https://blog.jayway.com/author/petar-mataic/>) (5)

Peter Neubauer

(<https://blog.jayway.com/author/peterneubauer/>) (7)

Peter von Lochow

(<https://blog.jayway.com/author/petervonlochow/>) (18)

Peter Winzell

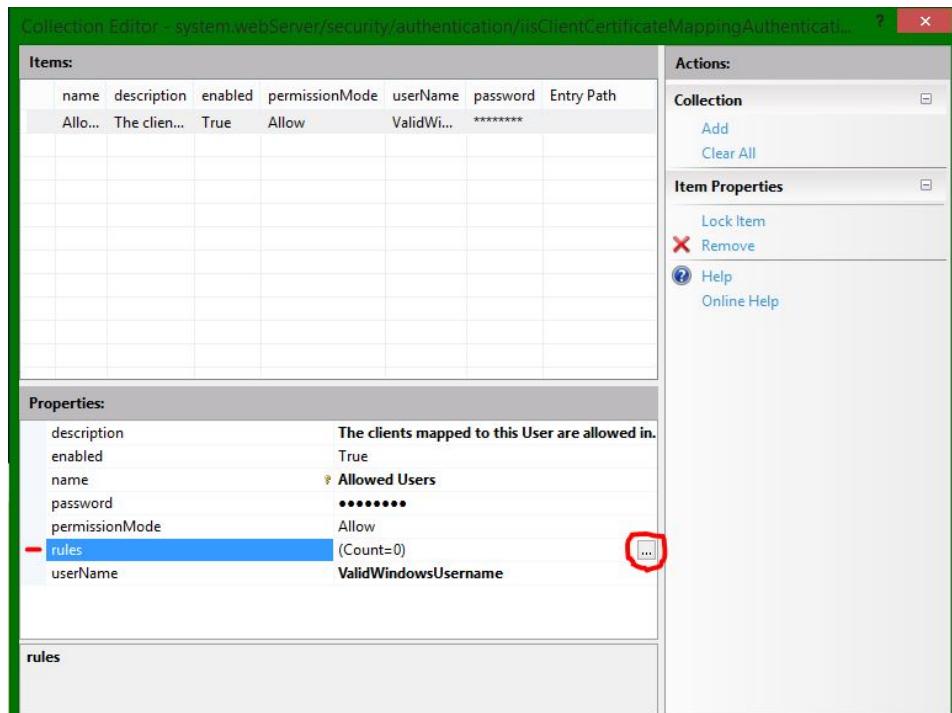
(<https://blog.jayway.com/author/peterwinzell/>) (2)

Philip Nilsson

(<https://blog.jayway.com/author/philipnilsson/>)

**IMPORTANT:** In order for this to work you need to enter a valid username and password and since my computer is the server, the credentials will be my Windows username and password.

Now we need to create some rules to go with this mapping so the server can determine if a client is allowed in or not. It's a so click on the rules property and the ... button



(<http://blog.jayway.com/wp-content/uploads/2014/10/29-add-rule.jpg>)

I will add one rule as an example where the server will check the client certificate to see if it's signed by the correct CA root. Go ahead and add more rules for more safety, please visit the [IIS Many-To-One Mapping](http://www.iis.net/configreference/system.webserver/security/authentication/iisclientcertificatemappingauthentication/manytoonemappings).

(<http://www.iis.net/configreference/system.webserver/security/authentication/iisclientcertificatemappingauthentication/manytoonemappings>)

reference for more documentation.

- [thor/philipnilsson/](#) (2)
- [Rena Reda](#)  
(<https://blog.jayway.com/author/renasreda/>) (4)
- [Rickard Nilsson](#)  
(<https://blog.jayway.com/author/rickardnilsson/>) (2)
- [Rickard Öberg](#)  
(<https://blog.jayway.com/author/rickardoberg/>) (7)
- [Rikard Ottosson](#)  
(<https://blog.jayway.com/author/rikardottosson/>) (2)
- [Robert Hedgate](#)  
(<https://blog.jayway.com/author/roberthedlegate/>) (21)
- [Sebastian Potter](#)  
(<https://blog.jayway.com/author/sebastian-potterjayway-com/>) (1)
- [Sergii Nezdolii](#)  
(<https://blog.jayway.com/author/sergiinezdolii/>) (1)
- [Sigurdur Birgisson](#)  
(<https://blog.jayway.com/author/sigurdurbirgisson/>) (11)
- [Silvia Man](#)  
(<https://blog.jayway.com/author/silvia-manjayway-com/>) (3)
- [Sladjan Trajkovic](#)  
(<https://blog.jayway.com/author/sladan-trajkovic/>) (1)
- [Stefan Li](#)  
(<https://blog.jayway.com/author/stefanli/>) (1)

The screenshot shows the 'Collection' section of the Collection Editor. It contains a single item with the following properties:

certificateField	certificateSubField	matchCriteria	compareCaseSensitive	Entry Path
Issuer	CN	CARoot	True	

**Properties:**

certificateField	Issuer
certificateSubField	CN
compareCaseSensitive	True
matchCriteria	CARoot

**matchCriteria**  
Data Type:string

(<http://blog.jayway.com/wp-content/uploads/2014/10/31-rule.jpg>)

Remember to apply the changes in the IIS Manager, so close the rules and mappings windows and click Apply

The screenshot shows the IIS Manager's Configuration Editor. The 'Actions' pane on the right has the 'Apply' button highlighted with a red circle.

**Configuration Editor**  
Section: system.webServer/security > From: ApplicationHost.config <|

Deepest Path: MACHINE/WEBROOT/APPHOST/IISWithCertificatesSample

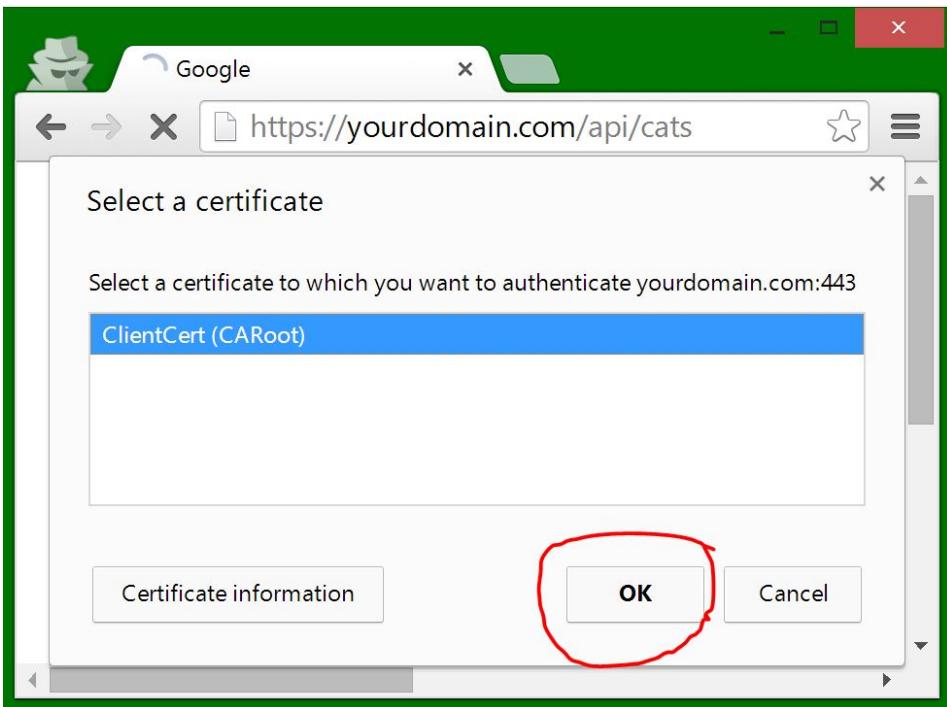
defaultLogonDomain	True
enabled	True
logonMethod	ClearText
manyToOneCertificateMappingsEnabled	True
manyToOneMappings	(Count=1)
oneToOneCertificateMappingsEnabled	True
oneToOneMappings	(Count=0)

**manyToOneMappings**

(<http://blog.jayway.com/wp-content/uploads/2014/10/32-apply-changes.jpg>)

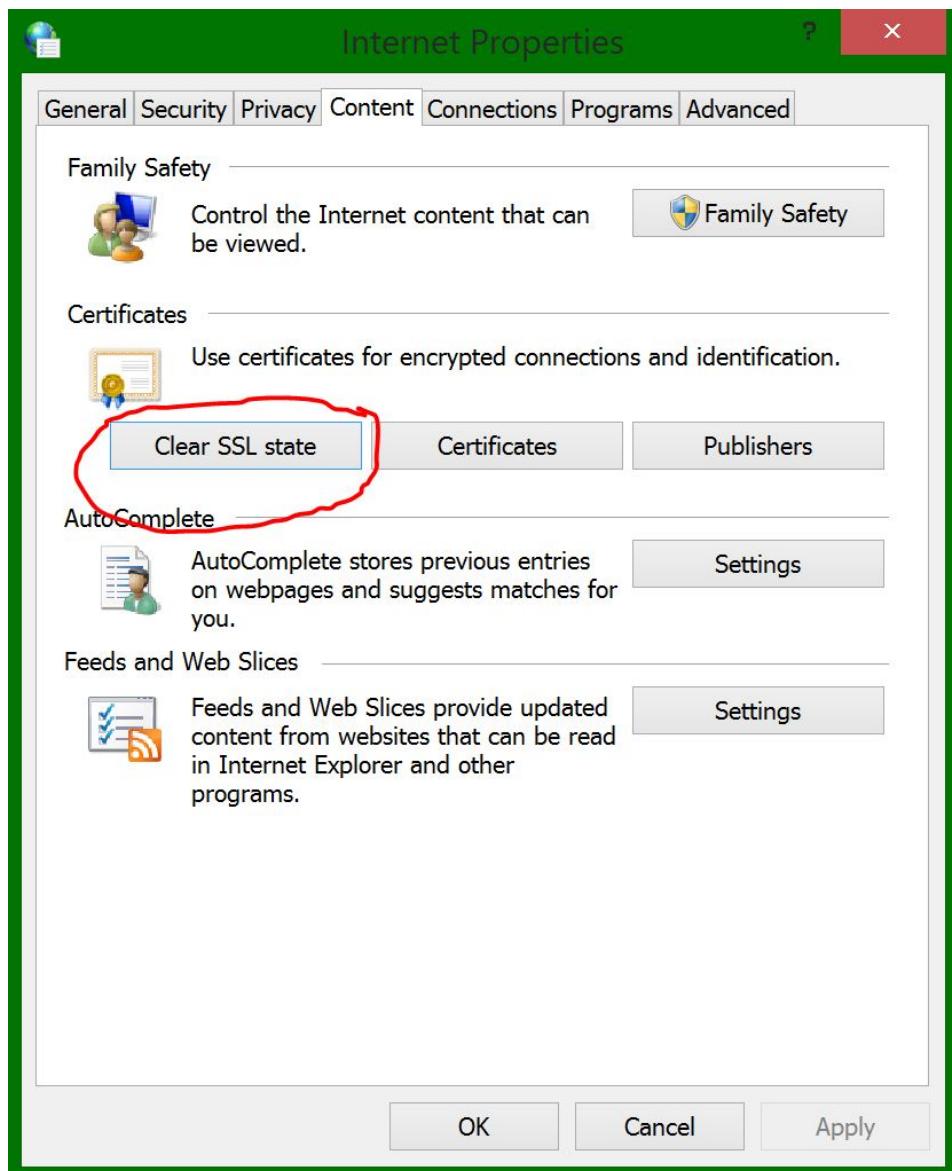
Open a new incognito browser window to make sure to start from a clean slate cache and cookie-wise and enter your url with the /api/cats and see the browser prompting you for a certificate. Choose the ClientCert and click ok to gain access to the cats.

- Stefan Severin  
(<https://blog.jayway.com/author/stefanseverin/>) (2)
- Steve Widinghoff  
(<https://blog.jayway.com/author/steve-widinghoffjayway-com/>) (6)
- Stuart McCulloch  
(<https://blog.jayway.com/author/stuartmcculloch/>) (1)
- Sune Simonsen  
(<https://blog.jayway.com/author/sunesimonsen/>) (1)
- Thomas Hansson  
(<https://blog.jayway.com/author/thomas-hanssonjayway-com/>) (2)
- Tobias Södergren  
(<https://blog.jayway.com/author/tobiassodergren/>) (17)
- Tomas Aschan  
(<https://blog.jayway.com/author/tomas-aschanjayway-com/>) (9)
- Tomas Nilsson  
(<https://blog.jayway.com/author/tomasnilsson/>) (10)
- Ulrik Sandberg  
(<https://blog.jayway.com/author/ulriksandberg/>) (30)
- Uzi Landsmann  
(<https://blog.jayway.com/author/uzilandsmann/>) (1)
- Vlado Palczynski  
(<https://blog.jayway.com/author/vladopalczynski/>) (1)



(<http://blog.jayway.com/wp-content/uploads/2014/10/33-ok-client-cert.jpg>)

If this is not working make sure that your client certificate is in your CurrentUser/Personal store as well as in your browser's certificate store. If yes, then go to Control Panel → Internet Options → Content and click Clear SSL state.



(<http://blog.jayway.com/wp-content/uploads/2014/10/34-clear-ssl-state.jpg>)

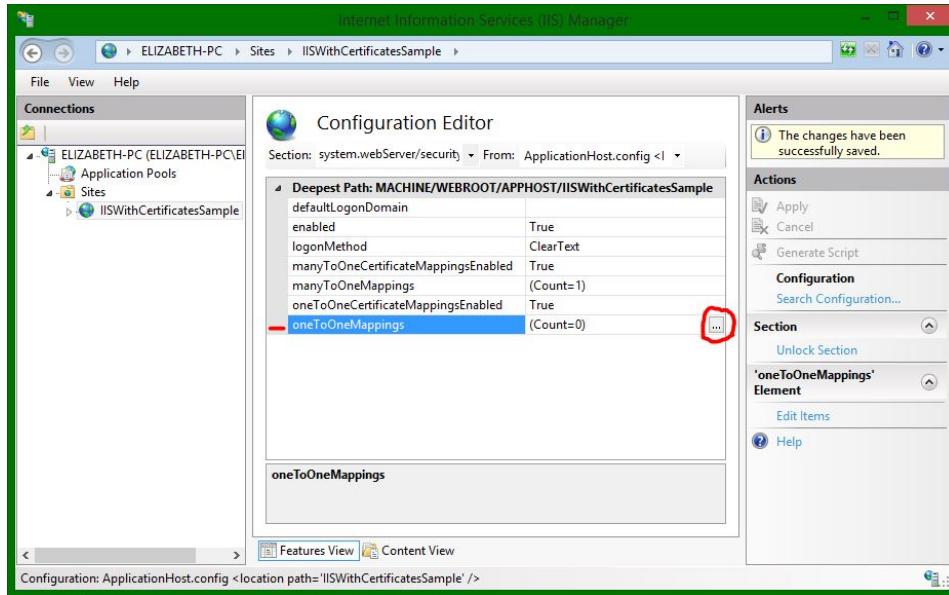
Open a new incognito windows and try again, your browser should now prompt you for the client certificate.

**NOTE:** Remember as I explained earlier on, Firefox has its own certificate store so you need to import the client certificate into "Your Certificates" in order to use this.

## One-To-One Mappings

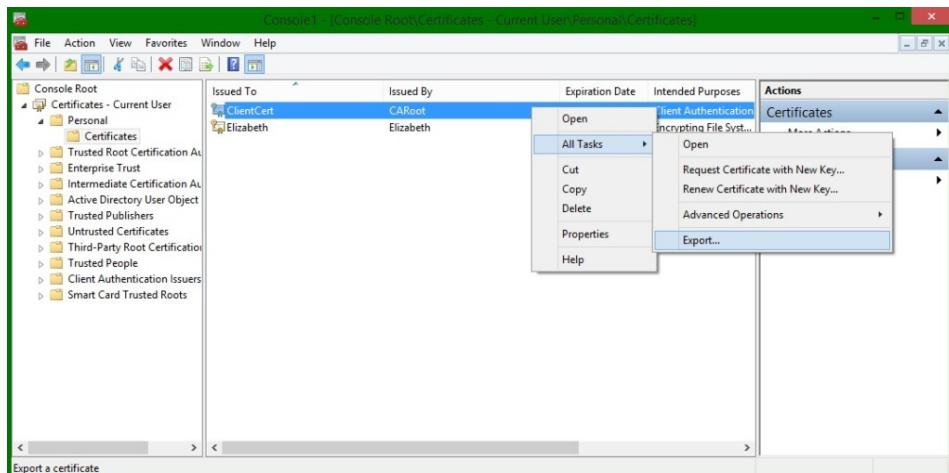
Let's walk through the one-to-one mappings as well. This approach means that we need an individual client certificate for each user mapping. You can either disable the many-to-one mapping and use the

same certificate and user or create new ones. Go back to the Configuration Editor and open the iisClientCertificateMappingAuthentication section again. Click the ... of the oneToOneMappings.

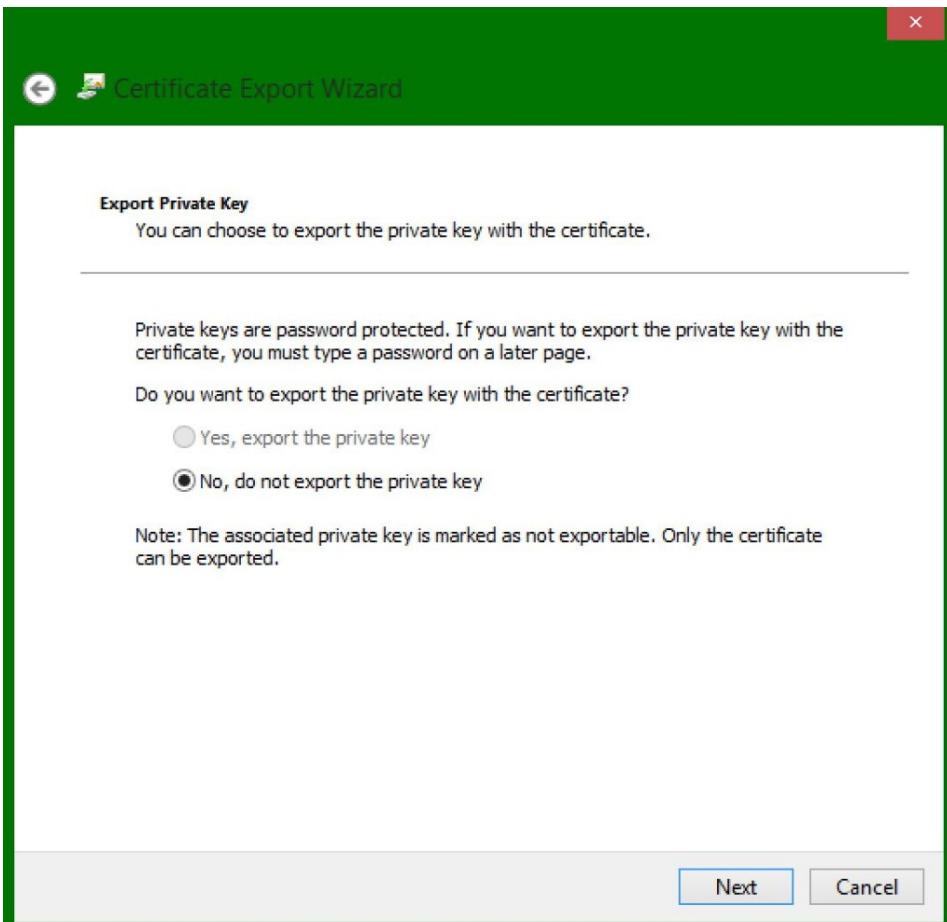


(<http://blog.jayway.com/wp-content/uploads/2014/10/35-enable-one-to-one-mappings.jpg>)

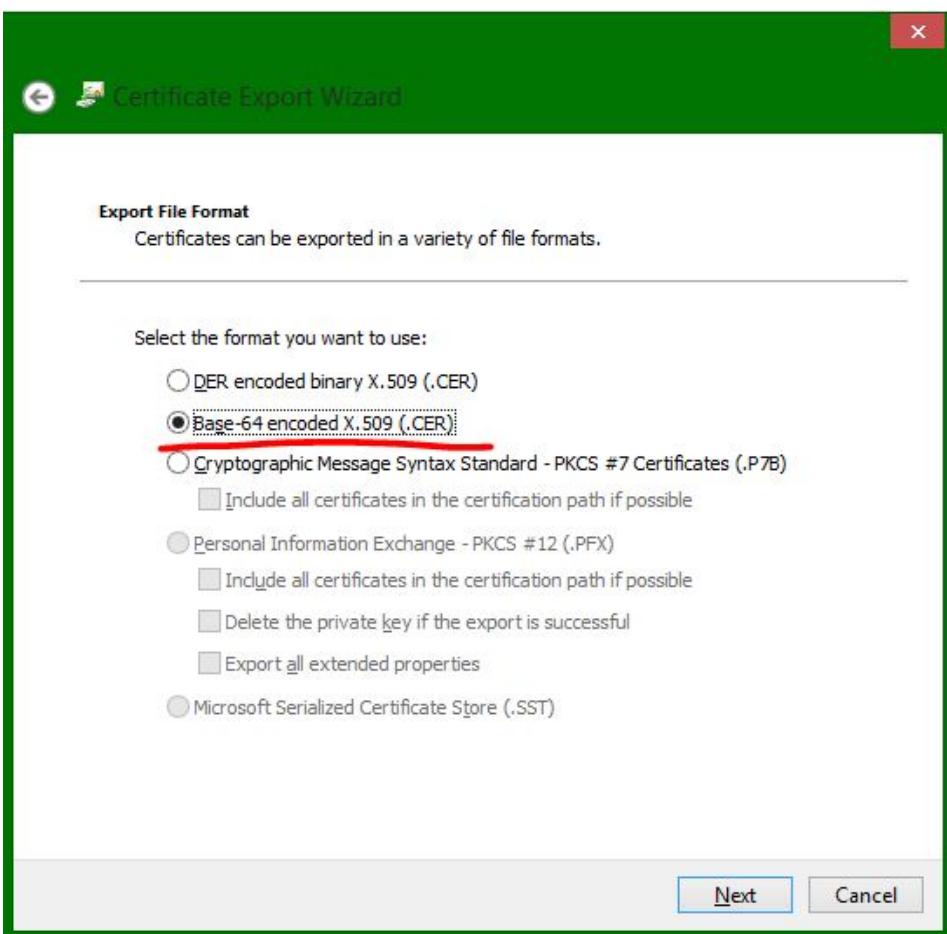
To add the mapping to the certificate we need to export the public key of the client certificate file. You can export this from your Machine Management Console (press the Windows button and search for mmc) Snap-in the Local Machine's Certificate's personal store and export the client ssl certificate you want to use without the private key in the base64 format.



(<http://blog.jayway.com/wp-content/uploads/2014/10/Export-client-cert.jpg>)



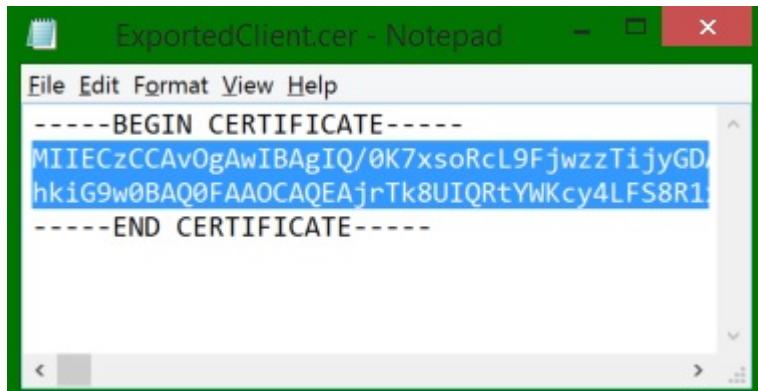
(<http://blog.jayway.com/wp-content/uploads/2014/10/Without-private-key.jpg>)



(<http://blog.jayway.com/wp-content/uploads/2014/10/base64-export.jpg>)

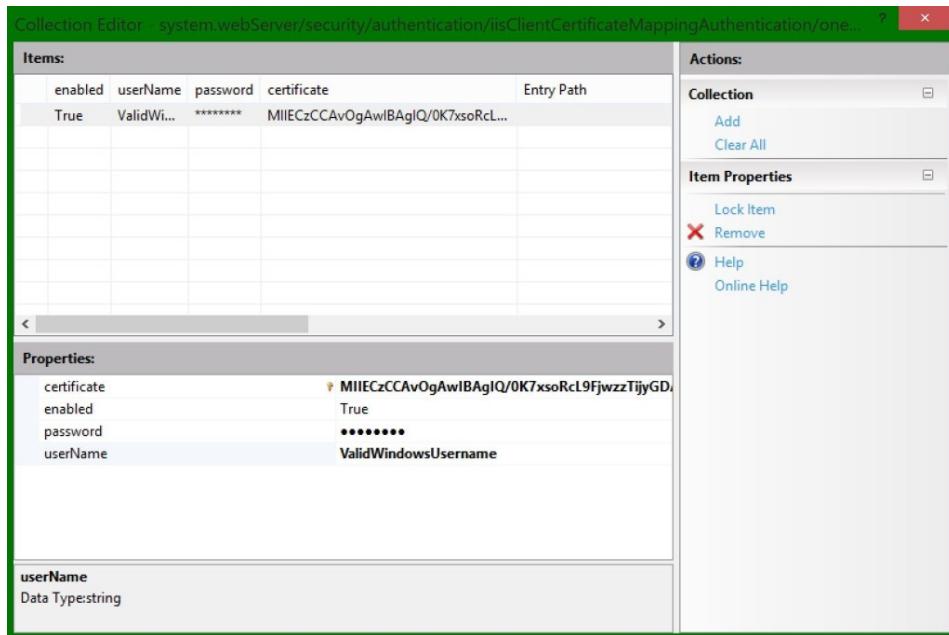
Right-click the newly exported certificate and open with notepad.

Remove all the line-breaks in the certificate itself.



(<http://blog.jayway.com/wp-content/uploads/2014/10/Remove-linebreaks.jpg>)

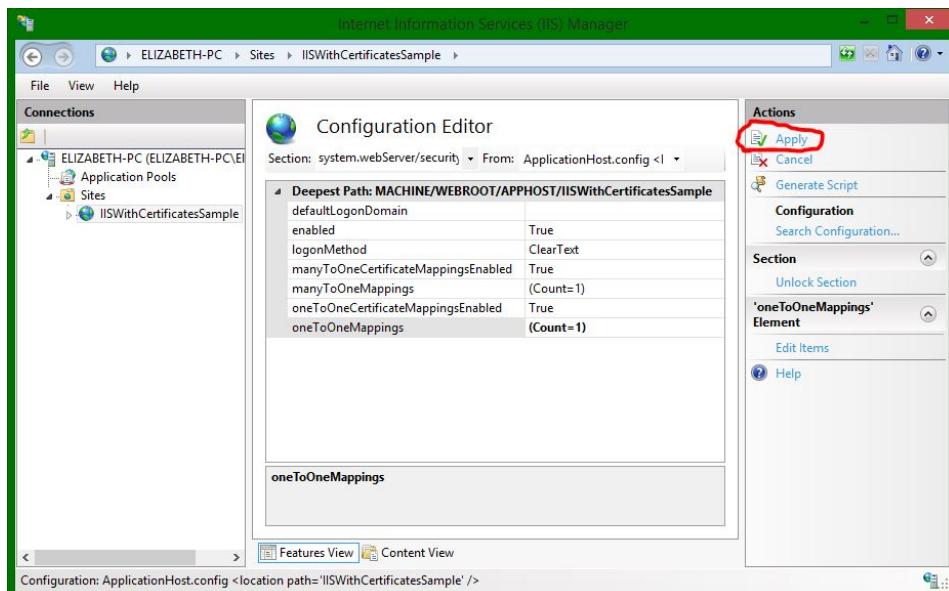
Now copy that into the certificate property field of the mapping and fill out the rest



(<http://blog.jayway.com/wp-content/uploads/2014/10/38-add-user-mapping1.jpg>)

**IMPORTANT:** In order for this to work you need to enter a valid username and password and since my computer is the server, the credentials will be a Windows username and password.

Again, remember to apply the changes.



(<http://blog.jayway.com/wp-content/uploads/2014/10/39-apply-changes.jpg>)

And there you go, try it out and when prompted choose the certificate you mapped to the user you just mapped.

I hope you found this post useful and for my next post I will be going through how to use self signed certificates together with Windows Azure and how to configure the IIS by C# code, take a look at it here:

<http://blog.jayway.com/2015/04/21/configure-a-windows-azure-cloud-service-to-use-your-self-signed-certificates-for-iis-client-certificate-mapping-authentication/>

<http://blog.jayway.com/2015/04/21/configure-a-windows-azure-cloud-service-to-use-your-self-signed-certificates-for-iis-client-certificate-mapping-authentication/>

Have a good one =)

TAGS: [.NET \(HTTPS://BLOG.JAYWAY.COM/TAG/.NET/\)](#), [GUIDE \(HTTPS://BLOG.JAYWAY.COM/TAG/GUIDE/\)](#), [IIS \(HTTPS://BLOG.JAYWAY.COM/TAG/IIS/\)](#), [IIS CLIENT CERTIFICATE MAPPING AUTHENTICATION \(HTTPS://BLOG.JAYWAY.COM/TAG/IIS-CLIENT-CERTIFICATE-MAPPING-AUTHENTICATION/\)](#), [PROGRAMMING \(HTTPS://BLOG.JAYWAY.COM/TAG/PROGRAMMING/\)](#), [SELF SIGNED CERTIFICATES \(HTTPS://BLOG.JAYWAY.COM/TAG/SELF-SIGNED-CERTIFICATES-2/\)](#), [SSL \(HTTPS://BLOG.JAYWAY.COM/TAG/SSL/\)](#), [TUTORIAL \(HTTPS://BLOG.JAYWAY.COM/TAG/TUTORIAL/\)](#), [WALK-THROUGH \(HTTPS://BLOG.JAYWAY.COM/TAG/WALK-THROUGH/\)](#), [WINDOWS 8.1](#)

← [Previous Post](#)

[Developing in F# impressions](#)  
(<https://blog.jayway.com/2014/10/24/developing-in-f-impressions/>)

[Next Post](#) →

[Microsoft OCR Library for Windows Runtime](#)  
(<https://blog.jayway.com/2014/12/09/microsoft-ocr-library-windows-runtime/>)

➤ THIS POST HAS 75 COMMENTS

Mohsan Hassan

4 FEB 2015 [REPLY](#)

Very helpful and detailed article. Thanks to the author :)

Tom Zuller

14 FEB 2015 [REPLY](#)

Thank you so much for your articles. Unlike a lot of articles and code snippets, your code and explanations worked correctly without errors. I learned more about certs and SSL from your articles than from any other sources I have come across.

[adventure saga \(<http://www.amazon.com/Aoleon-Martian-Girl-Science-Luminess-ebook/dp/B00S70U8NE/>\)](#)

2 MAR 2015 [REPLY](#)

Hi to every one, for the reason that I am genuinely eager of reading this website's post to be updated regularly.  
It carries nice information.

---

Kevin Barger

3 MAR 2015 [REPLY](#)

Kudos to Elizabeth! Thank goodness someone took the time to explain this for the rest of us. You could spend weeks trying to decipher those Microsoft “explanations”.

---

[matt vaughn \(<http://www.buildmotion.com>\)](#)

3 MAR 2015 [REPLY](#)

Awesome article on configuring IIS to use client certificates. Your explanations are clear and concise. Much appreciated.

---

[poptropica 2 \(](#)

4 MAR 2015 [REPLY](#)

I have read so many posts regarding the blogger except this article is truly a nice article, keep it up.

---

Kashif Ali

9 MAR 2015 [REPLY](#)

Hi , for the reason that I am genuinely eager of reading this website post to be updated regularly.  
It carries good Information.

---

Astrid

15 MAR 2015 [REPLY](#)

Hello, this is a very nice summary. I was looking for this information about client certification in IIS and I found it on various pages, but on none of them it was so nicely summarized.

I already have a working setup, I just can't find an answer to my question: client certificate needs to be located in Current User/Personal store. However, this means that the certificate is exclusive to the current user only. I need it to be available for all the users on that machine. So is there any way to make IIS and/or IE use the certificate that is located in Local Computer/Personal instead?

Thank you very much.

---

Elizabeth Andrews

14 APR 2015 [REPLY](#)

Hello Astrid

I'm glad to hear that you found my blog post useful =)

For IIS Client Certificate Mapping Authentication the browser looks in the CurrentUser store in order to prompt you to choose a client certificate so you will have to put them here for it to work. You can however use the many-to-one approach to map multiple certificates to a user account on the server, for example an "Allowed Users" account to represent a group in an organization. So it's the certificate rules you configure in the IIS manager that determines if the client is allowed or not. This means that you can install the client certificate (and your root CA, since we are making untrusted self-signed certificates) in whichever user on whichever machine you want in order to grant access.

I updated the part with the header called "Many-To-One Mappings" in this post in attempt to explain it more clearly, so please have a look.

Hope it helps! ^\_^

---

Astrid

18 MAY 2015 [REPLY](#)

Hello Elisabeth.

Just now I found your reply, thank you very much. I know that I can define a rule in the manyToOneMappings, which will fit to a group of users, such as Issuer's CN. I have it set like that already from the beginning. Our only concern is that the client certificates need to be in the Current User store, which is creating problems to the person that should distribute the certificates. We were hoping that there will be a way to avoid this (so that IE will read it from the Local Machine store), however it looks like there is no other way... they need to be in the Current User store.

I also wanted to ask you another question, but in the meantime I found a solution:

I have manyToOne setting in my IIS. Now I want to disable it. I mean, I don't want IIS to check any specific rule for the client certificates. It is enough if it checks if the client certificate's CA is in the server's Trusted Root Certification Authorities (which it is checking anyway).

I was not sure how to do this, because setting disabled for both manyToOne, oneToOne and the overall feature did not work.

What finally worked was to create a manyToOne mapping without any rule (rules count=0). If you find this information useful, you may update your article with this information.

With best regards,

Astrid

---

[Vikram \(<http://www.vss-tech.com>\)](#)

18 APR 2015 [REPLY](#)

The whole article is awesome.

I am faced with requirement for testing website by secure way. And we were not required to buy certificate for same.

Your article help a great. You wrote so nicely that there was no doubt. Just to follow steps and achieve goal. Thanks for sharing your wisdom with us.

---

[Diabetes Free Supplement \(<http://xiopa11.bloggplatsen.se/gilla/?url=http://diabetesfrees.com/>\)](http://xiopa11.bloggplatsen.se/gilla/?url=http://diabetesfrees.com/)

6 MAY 2015 [REPLY](#)

Have you ever thought about writing an e-book or guest authoring on other sites?

I have a blog centered on the same ideas you discuss and would love to have you share some stories/information. I know my readers would value your work. If you're even remotely interested, feel free to send me an e-mail.

---

[customized tee shirts \(<http://banksy-tshirt.org>\)](http://banksy-tshirt.org) 13 MAY 2015 [REPLY](#)

great points altogether, you simply won a emblem new reader.

What could you suggest about your post that you just made a few days ago? Any sure?

---

[Construction JB \(<http://sirrico.net/yourls/constructionjbc955867>\)](http://sirrico.net/yourls/constructionjbc955867)

13 MAY 2015 [REPLY](#)

An interesting discussion is worth comment. There's no doubt that that you should publish more on this subject, it might not be a taboo matter but usually folks don't

speak about such issues. To the next! Cheers!!

---

[Wifeward.com \(https://www.wifeward.com/hack-wpa-wifi-password/\)](https://www.wifeward.com/hack-wpa-wifi-password/)

13 MAY 2015 [REPLY](#)

Hi there! Extraordinary blog post, I actually enjoyed reading through it,  
many thanks!

I will be coming back to your blog to read more in the near future.

---

[tutorial clash of clans \(http://elmundodejosue.webgarden.com/section-1/blog/trucos-del-clash-of-clans\)](http://elmundodejosue.webgarden.com/section-1/blog/trucos-del-clash-of-clans)

22 MAY 2015 [REPLY](#)

An impressive share! I have just forwarded this onto  
a friend who has been conducting a little homework on this.  
And he in fact bought me breakfast simply because I discovered it for  
him...

lol. So allow me to reword this.... Thank YOU  
for the meal!! But yeah, thanks for spending some time to talk about this  
topic here on your site.

---

[kontakt lens nedir \(http://www.acuvue.com.tr\)](http://www.acuvue.com.tr)

25 MAY 2015 [REPLY](#)

Thanks a lot for sharing this with all of us you really know  
what you're speaking about! Bookmarked. Kindly also consult with my  
web site  
=). We will have a link alternate arrangement between us

---

The explanation is very clean and thank you very much.

But after following all the setting, when i select certificate in browser and click ok. I am getting

Server Error

401 – Unauthorized: Access is denied due to invalid credentials.

You do not have permission to view this directory or page using the credentials that you supplied.

I am not able to understand the problem, verified all the log files, no clue . could you please help.

---

I am struggling with this process and would appreciate a bit of guidance.

I have followed the guide for creating self signed certificates and am now trying to get my local IIS environment configured to use them. I am running IIS8 on a windows 8 machine.

The domain I am using is ‘angularjsauthenticationweb.com’ and I have modified the hosts file according to the sample. The non-https urls return as expected.

In IE both the angularjsauthenticationweb.com and

<http://www.angularjsauthenticationweb.com>

(<http://www.angularjsauthenticationweb.com>) sites return with HTTPS.

However, the lock does not appear in the URL bar until I press F5 to refresh the page. Once the page has been refreshed the locks appear and the cert appears to be correct (issued by CARoot and issued to matches my URL).

In Chrome I see some different behavior.

<https://angularjsauthenticationweb.com/>

(<https://angularjsauthenticationweb.com/>) opens up correctly with a

nice green lock. However, when I add www to make the URL

<https://www.angularjsauthenticationweb.com>

(<https://www.angularjsauthenticationweb.com>) I still see the green lock in the corner but the page does not return correctly and instead I receive an error message indicating:

'Your client certificate is either not trusted or is invalid.'

When I view the certificate it indicates it is issued by 'CARoot' and issued to the correct url 'www.angularjsauthenticationweb.com'

I also followed the instructions to add the CARoot cert to firefox:

Firefox Settings → Options → Advanced → View Certificates → Authorities → import your CARoot.cer file

However, when I try to open the secure URL's from firefox on my local PC where the site is hosted I receive the 'Secure Connection Failed' error with either the angularjsauthenticationweb.com or

<http://www.angularjsauthenticationweb.com>

(<http://www.angularjsauthenticationweb.com>) URL's.

I have been through the examples several times and have been unable to resolve the issues. I must be missing something here and could really use a nudge in the right direction. Thanks!

---

Q

17 JUN 2015 [REPLY](#)

You can open the about:config page via the location/address bar and use its search bar to locate this pref:

security.tls.insecure\_fallback\_hosts

You can double-click the line to modify the pref and add the domain (sso.iiaba.net) to this pref. If there are already websites (domains) in this list then add a comma and the new domain (no spaces). You should only see domains separated by a comma in the value column.

---

[lonut \(<http://-->\)](#)

9 JUN 2015 [REPLY](#)

Hello,

I have set up my IIS on Windows Server 2012 domain controller. How do I match your procedure on a Active Directory environment?

At the user field (manyToOne mappings) do I have to put domain\username?

In this moment I do get the error:

403 – Forbidden: Access is denied.

You do not have permission to view this directory or page using the credentials that you supplied.

Thanks

---

**Simi Sreedharan**

24 JUN 2015 [REPLY](#)

This is a wonderful post. Thankyou.

---

**Sophie**

8 SEP 2015 [REPLY](#)

This is a very nice article !

---

[Alex \(<https://yaplex.com>\)](#)

10 SEP 2015 [REPLY](#)

so complicated :)

you can do the same with Powershell command, details are there

<https://yaplex.com/blog/how-to-create-self-signed-certificate-for-domain> (<https://yaplex.com/blog/how-to-create-self-signed-certificate-for-domain>)

Excellent article – I'm trying to follow it – but I am blocked at getting IE/Chrome to actually allow me to select the Client certificate. It is in Current User\Personal\Certificates, it's the right purpose (proves your identity to a remote computer), has the key icon for 'You have a private key that corresponds to this certificate', the issue/expire dates are valid. The CA that this is issued from is in the Trusted Root Certificate Authority\Certificates folder. I'm feeling that it's just something foolish like one checkbox or another – any pointers?

---

Pingback: itemprop="name">[Configuring IIS hosted website for Https |](#)

[darren schwarz](#)

(<https://darrenschwarzdotcom.wordpress.com/2015/10/26/for-james-to-sully/>)

[Russ \(<http://NA>\)](#)

10 NOV 2015 [REPLY](#)

I seem to have found an interesting bug when following this guide. I can gain access to the website by passing in a certificate that should not grant access.

If I pass in a certificate that is in the hosting server's MMC, I get access to the web page. I made sure to enable client certificate mapping and enable only one to one mapping following this guide. I have disabled Many to one certificate mapping and I have no certificates in the "oneToOneMappings" section. Therefore, no certificate should provide access. I'm very confused as to how i am getting access to the website, any suggestions/tips?

Russ

---

Many thanks. Very good work and help.

---

Chad Cothorn

2 DEC 2015 [REPLY](#)

Going through this walkthrough, I got received a 503 error just after setting up my https bindings, and read: "Tadaa, you can now use <https://yourdomain.com/api/cats> and <https://www.yourdomain.com/api/cats>" (<https://www.yourdomain.com/api/cats>)"

My url worked fine with http, but not https. I tried a variety of google searches to find the problem and every one of them indicated that the Application Pool was not started or had an incorrect Identity. None of the recommendations helped until I came across a search result that said to do the following:

1. Open the Developer Command Prompt for VS (in my case, 2013)
2. Run : netsh http show urlacl url=https://+:443/
3. If something is there, then this is your problem. Port 443 is completely reserved and is blocking IIS.
  - If there is a need to reserve port 443 for an application running outside of IIS, it needs to be registered with an application path (i.e. <http://+:443/appPath>)
  - If there is nothing there, then ... this might not be the issue. No need to continue.
4. Run: netsh http delete urlacl <https://+:443/>
5. Try running your application again. It worked for me!

Here is the link to the page that helped me solve the problem:

<http://blogs.msdn.com/b/webtopics/archive/2010/02/17/a-not-so-common-root-cause-for-503-service-unavailable.aspx>

David L.

10 DEC 2015 [REPLY](#)

Thank you for the great post, it really helped me, but I have 1-2 things that I don't get.

The user (ValidWindowsUsername here) should be a single local user (like a service user), or do I really have to list all users who will user the certificate (many users sharing 1 client certificate)?

And if I do have to list them all, must I also provide the valid password?

Because that would be bad...

Also, do these users have to be local user on the server or can I use domain user, or maybe even groups?

Thank you in advance for your help!

David

---

A Tanner (<http://blog.jayway.com/2014/10/27/configure-iis-to-use-your-self-signed-certificates-with-your-application/>)

18 DEC 2015 [REPLY](#)

Can you please clear up my mis/understanding?

You mention that the CA root cert and the client cert should both be on the client PC (for client authentication). I assume from the user login screen shot that they will be presented to the server when the client wants to authenticate.

Does the server use the root cert presented by the client to verify the client cert or do you have to also install the root cert on the server as a trusted cert?

If the server uses the root cert presented by the client wouldn't this mean that anyone can act as a CA and produce their own root cert and client cert that will be accepted by the server?

thanks

---

Paniraj

30 DEC 2015 [REPLY](#)

Hi – Thanks for such a nice post, however it did not work me after following the exact steps which is mentioned. At this moment I am getting " HTTP Error 403.16 – Forbidden – Your client certificate is either not trusted or is invalid."

Kindly assist.

---

Pingback: itemprop="name">>[Using client certificates in .NET part 6: setting up client certificates for local test usage | Exercises in .NET with Andras Nemes \(<http://dotnetcodr.com/2016/01/28/using-client-certificates-in-net-part-6-setting-up-client-certificates-for-local-test-usage/>\)](#)

Chi

15 FEB 2016 [REPLY](#)

Thanks Elizabeth a lot for this. I am working with API like this. When i call API, it show a list of cerficates to choose. I have to choose a correct one. Do you know how to call a API like that.

Thanks in advance !

---

Bill

28 FEB 2016 [REPLY](#)

Just trying to go through this for “real” and you got pretty vague at: “Fill out the properties for a mapping and repeat for each user you want to configure for access or denial. Remember that you need the client certificate and root CA certificate installed on all the user’s mmc.”

---

Venkat

3 MAR 2016 [REPLY](#)

Thanks for the detailed post on certificate based authentication.  
Just one question: Why do I need a user name, if I am authenticating clients with certificates? Is this not enough, if the client public key is available on the server Trusted People store? basically I want to tell IIS that, which client certificates it can trust, and I don’t want to map certificate to user name.

Any comments or thoughts on this?

Thanks.

---

Eric Belair

9 MAR 2016 [REPLY](#)

This is the basic setup I have, but, when I try to apply Authorization Rules, it throws 401.2 errors. Any idea how to configure authorization correctly?

---

[Advan Star Note S5L \(<http://mukainternet.blogspot.com>\)](#) 6 APR 2016 [REPLY](#)

magnificent publish, very informative. I’m wondering why the opposite specialists of this sector don’t realize this.

You must proceed your writing. I’m sure, you’ve a great readers’ base already!

---

Excellent! I wish if I found this article earlier it would have saved my few days and some saved some hair ;-).

I have got everything working with Client Authentication using Many to One mapping for both external and self-signed certificates clients. But I am still unable to resolve the issue client certificates that have a wildcard in their subject names.

Any help would be appreciated.,

---

How i can bind certificate for localhost via  
netsh http add sslcert ipport=127.0.0.1:5000 certhash= appid={}?

---

This is an excellent article ; I implement my first Https site with the help of this article. Thanks for sharing this article.

---

This works great for me when installing everything (root CA, server & client certs) on the windows 2012 R2 server.

Use host name, with default 443 port, eg.

mydomain.com

After installing root CA & client certificate on to my local windows 7 pro PC, it doesn't have a clue what the domain is (not surprised).

So I removed hostname from IIS and I used ip address of server on my PC. Browser certificate warning, obviously. So how do I get domain to be seen on my PC?

---

steve

18 JUL 2016 [REPLY](#)

I can dour a GEt and Post using webapi and SSL Certificates but a Put fails with status code 405/ Any reason why this fails?

---

Pingback: itemprop="name">>[Bad Ssl Client Authentication Certificate | Home](#) (<http://mesotheliomaattorneyscalifornia.xyz/bad-ssl-client-authentication-certificate/>)

SK

9 AUG 2016 [REPLY](#)

Dear JAYWAY, Thank you very much for this article. It was very helpful.

---

[demisplurge.tumblr.com](#) (<http://demisplurge.tumblr.com>)

27 AUG 2016 [REPLY](#)

The SmartDNS alternative is faster but there you will not have your College gaming private due to the fact of no encryption involved.

---

Pingback: itemprop="name">>[Domain Ve Web Hosting Nedir | Great Value Webhosting](#) (<http://great-webhosting.xyz/domain-ve-web-hosting-nedir-2/>)

Geb

14 JAN 2017 [REPLY](#)

Still relevant..

Thanks for the details

---

Andy

19 JAN 2017 [REPLY](#)

Thanks for the tutorial!

I have followed your previous post to create the cert and configured IIS as above. But I've got "HTTP Error 401.2 – Unauthorized

You are not authorized to view this page due to invalid authentication headers." when I access it via browser. The browser has prompted me for client cert and I have selected the right one. Is there any way to debug such error?

I'm also confused on what to put for the username/password for the oneToOneMapping configuration. Is it my local computer domain account? As it never prompt me to enter a password from the browser.

---

Rafael

31 JAN 2017 [REPLY](#)

Hi Elizabeth

You have created a new site with a random domain name. I have my application below the default site.

Example: `http://localhost/MyApplication/Login.aspx`

I have questions about how I configure this type of url and I also do not have a domain.

---

[manish \(`http://asp.net%20website`\)](#)

16 FEB 2017 [REPLY](#)

I tried to make a ssl certificate but when i m added it on my demo website it shows me localhost instead of my url pls. help me to solve this problem.

Thanks in advance.

---

Wally Highsmith

23 FEB 2017 [REPLY](#)

Windows 2012 introduced stricter certificate store validations.

According to KB 2795828: Lync Server 2013 Front-End service cannot start in Windows Server 2012, the Trusted Root Certification Authorities (i.e. Root) store can only have certificates that are self-signed. If that store contains non-self-signed certificates, client certificate authentication under IIS returns with a 403.16 error code.

To solve the problem, you have to remove all non-self-signed certificates from the root store. This PowerShell command will identify non-self-signed certificates:

```
Get-Childitem cert:\LocalMachine\root -Recurse |
```

```
Where-Object {$_.Issuer -ne $_.Subject}
```

In my situation, we moved these non-self-signed certificates into the Intermediate Certification Authorities (i.e. CA) store:

```
Get-Childitem cert:\LocalMachine\root -Recurse |
```

```
Where-Object {$_.Issuer -ne $_.Subject} |
```

```
Move-Item -Destination Cert:\LocalMachine\CA
```

See: <http://stackoverflow.com/questions/26247462/http-error-403-16-client-certificate-trust-issue>

(<http://stackoverflow.com/questions/26247462/http-error-403-16-client-certificate-trust-issue>)

---

Adejumo

18 MAR 2017 [REPLY](#)

there is a software called jira which i have installed on my server – since this is not a microsoft program, will i be able to use IIS to publish this on the internet ?

---

[meilleure imprimante laser \(<http://unireptile.com>\)](#)

11 MAY 2017 [REPLY](#)

Great post. I was checking constantly this blog and I'm impressed!

Extremely helpful information specifically the closing part :

) I handle such info much. I was looking for this particular info for a long time.

Thank you and best of luck.

---

**tbs.User**

12 JUL 2017 [REPLY](#)

Awesome article. But I have issue with chrome, it shows my site unsecure.

Can you help me with that?

---

**Prashant Gorade**

21 SEP 2017 [REPLY](#)

Thanks for This. It's a very usefully for Us. Very good steps.

---

**Sema Uysal**

20 OCT 2017 [REPLY](#)

Hello,

This is a great article.

After I did all of the configuration, I realized that server is working with any valid client certificate which is valid for client and server machine.

To solve this problem :

Double click the Authentication icon and disable all the Authentication

method

Then you can connect with only client certificate which you created before for this site only.

Thank you.

---

Pingback: itemprop="name">>[Windows Docker \(part-4\) – Support](#)  
[\(https://mserversupport.wordpress.com/2017/12/12/windows-docker-part-4/\)](https://mserversupport.wordpress.com/2017/12/12/windows-docker-part-4/)

**Melinda Colliander**

12 DEC 2017 [REPLY](#)

Hi

Very informative article. Thank You so much for helping me out

---

**rodrigo**

25 JAN 2018 [REPLY](#)

beautiful and smart:)

---

[Scr888 Login \(http://wantoncraft.hol.es/scr8882018240977\)](#)

21 MAR 2018 [REPLY](#)

Hi, after reading this remaarkable piece of writing i am also delighted to share my experience here with friends.

---

[cong ty lap dat camera \(https://congtycamera.net\)](#) 1 APR 2018 [REPLY](#)

It's awesome in favor of me to have a site, which  
is valuable in support of my knowledge.  
thanks admin

---

### [Planet7 No Deposit \(<http://planet7nodeposit.wordpress.com>\)](http://planet7nodeposit.wordpress.com)

11 JUN 2018 [REPLY](#)

Hi, i read your blog occasionally andd i own a similar one and  
i was just curious if you get a lot of spam responses?  
If so how do you stop it, any plugin or anything you can suggest?  
I get so much lately it's driving me mad so any support is very much  
appreciated.

---

### [Allan \(<http://pelpago.com>\)](http://pelpago.com)

9 AUG 2018 [REPLY](#)

i have a problem  
Error HTTP 403.7 – Forbidden  
La página a la que está intentando obtener acceso requiere que el  
explorador tenga un certificado de cliente de Capa de sockets seguros  
(SSL) que reconozca el servidor web.

---

### [John Urrutia \(<http://www.johnurrutia.com>\)](http://www.johnurrutia.com)

14 SEP 2018 [REPLY](#)

Hi,  
I read your post and it is really clear.  
What I was wondering is if there is an alternative to have client  
authentication with IIS without mapping the certificate to a user

account.

My implementation scenario is a server to server communication using IIS on one end and php curl on the other. So the user is actually a server.

Thanks and regards,

Juan

---

Vikas

17 SEP 2018 [REPLY](#)

Amazing article.

---

### [Richard Dobeson Music & Film \(<https://richarddobeson.com>\)](#)

8 OCT 2018 [REPLY](#)

General Web Users with SSL Certificate Problems

Digital certificates provide security to websites by encrypting sensitive data and verifying the identity of the websites that are secured.

We provide these certificates as a service to website owners to ensure the security of online communications.

SSL problem messages and warnings are often displayed in an attempt to protect website users from potentially compromising situations.

However, an SSL error message may also indicate a problem that is entirely innocuous in nature. In this second case, there is often an issue either with the website you are connecting to or even possibly a misconfiguration on your own end.

---

### [clarke \(<http://www.rajasri.com/dotnet-web-development.php>\)](#)

2 JAN 2019 [REPLY](#)

I simply wanted to write down a quick word to say thanks to you for those wonderful information you are showing on this site.

---

Miguel

24 FEB 2019 [REPLY](#)

I've been reading your articles (while listening to Frantic Amber).

Lady you rock!

This is a great source of information, though I still have to re-read all mapping, which I didn't get to work yet. Maybe I have to clear the SSL cache first, but anyway. For the first time I see a spark of light when trying to deal with the certificates.

Cheers,

Miguel

---

David

12 APR 2019 [REPLY](#)

Seriously?

You didn't disabled anonymous authentication, without it IIS wont even look at mapping configuration and it will just authorize any request which have client certificate. This article doesn't show if mapping works or not. Not actually helpfull at all....

David

---

[Sarah's Blessing CBD Oil Review \(<https://sarahsblessingcbd.com/>\)](#)

13 APR 2019 [REPLY](#)

It's great that you are getting thoughts from this paragraph as well as from our argument made at this time.

[Akiv \(http://NA\)](http://NA)

22 APR 2019 [REPLY](#)

Hi,

A very good post indeed. It helped me to create and use certificates. But now it works with any client certificate. I configured one-to-one and also many-to-one, but in both case, it worked with whatever client certificate i choose. Can you help me with this?

---

[infiniteketo.com \(https://infiniteketo.com/\)](https://infiniteketo.com/)

2 MAY 2019 [REPLY](#)

I like this blog it's a master piece! Glad I discovered this on google.

---

[rajwap xyz \(https://sanitera.pl\)](https://sanitera.pl)

30 NOV 2019 [REPLY](#)

Just keep in mind that visitors will see a warning in their browsers (like the one below) when connecting to an IIS site that uses a self signed certificate until it is permanently stored in their certificate store. Never use a self signed certificate on an e-commerce site or any site that transfers valuable personal information like credit cards, social security numbers, etc.

---

[Install Iptv On Iphone](#)

([https://manuals.d12webdesign.com/Concern\\_Their\\_Reliability\\_Preparation\\_As\\_Well\\_As\\_Cleanliness](https://manuals.d12webdesign.com/Concern_Their_Reliability_Preparation_As_Well_As_Cleanliness))

18 FEB 2020 [REPLY](#)

Step 2: From the left menu, click on Services.

---

[Leave a Reply](#)

Your Comment Here...

Name (required)

Email (required)

Website



Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

Copyright - OceanWP Theme by Nick