Source: C# Corner (www.c-sharpcorner.com)   PRINT

Article

Adding SSL Certificate To Azure Web Apps

By **Ramees** on **May 10 2017**

A SSL certificate is a digital certificate, which creates a secure link between the Website and then the visitor's Browser ensures that all the data that passes between the two remains private and secure, thus preventing hackers from stealing private information such as credit card numbers, passwords and the other user details.

In this article, let us see how to implement the same in Azure Web Apps as it is is highly recommended to have it these days as the search engines are promoting secure Websites only. By default, Azure used to provide a SSL certificate but to the *.azurewebsites.net* domain only. Let us learn how to implement the same for our custom domain also.

Here, I am continuing from the previous article, where we had already a custom domain mapped Website. You can see SSL section, which allows you to import or upload the certificate.
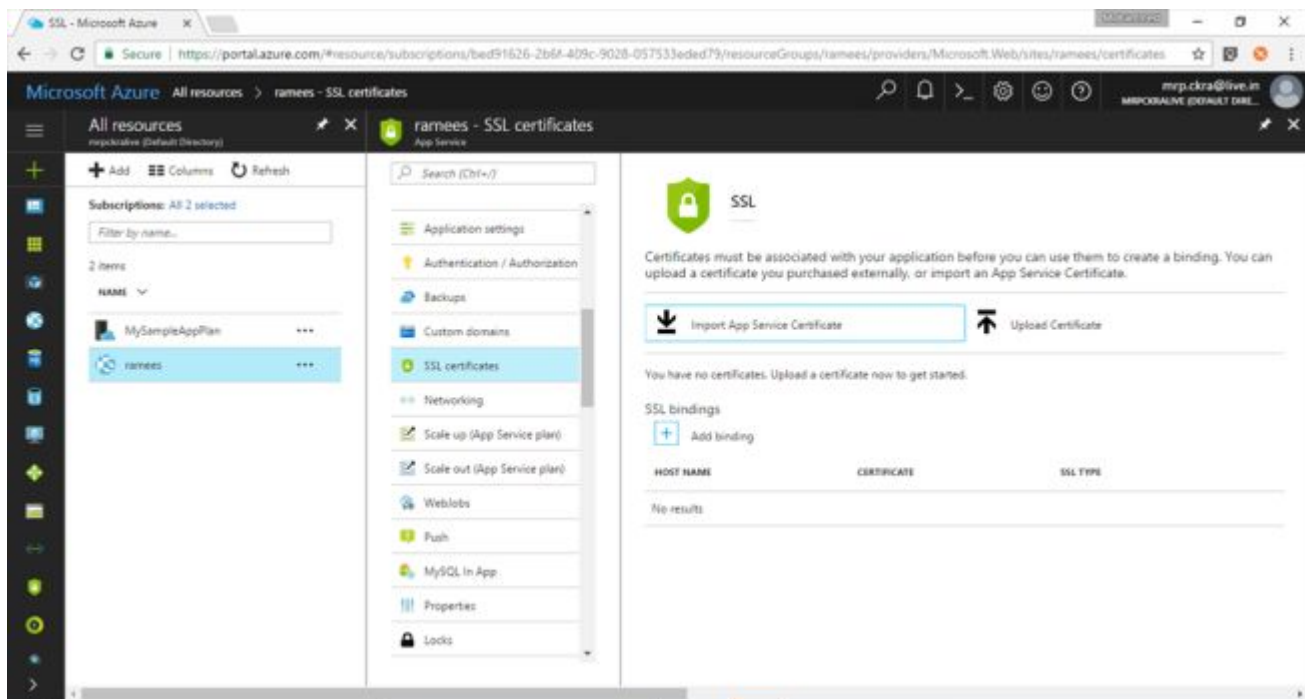

When you try to access the secure site now, you can see a warning state that the certificate was issued to a domain with *.azurewebsites.net*
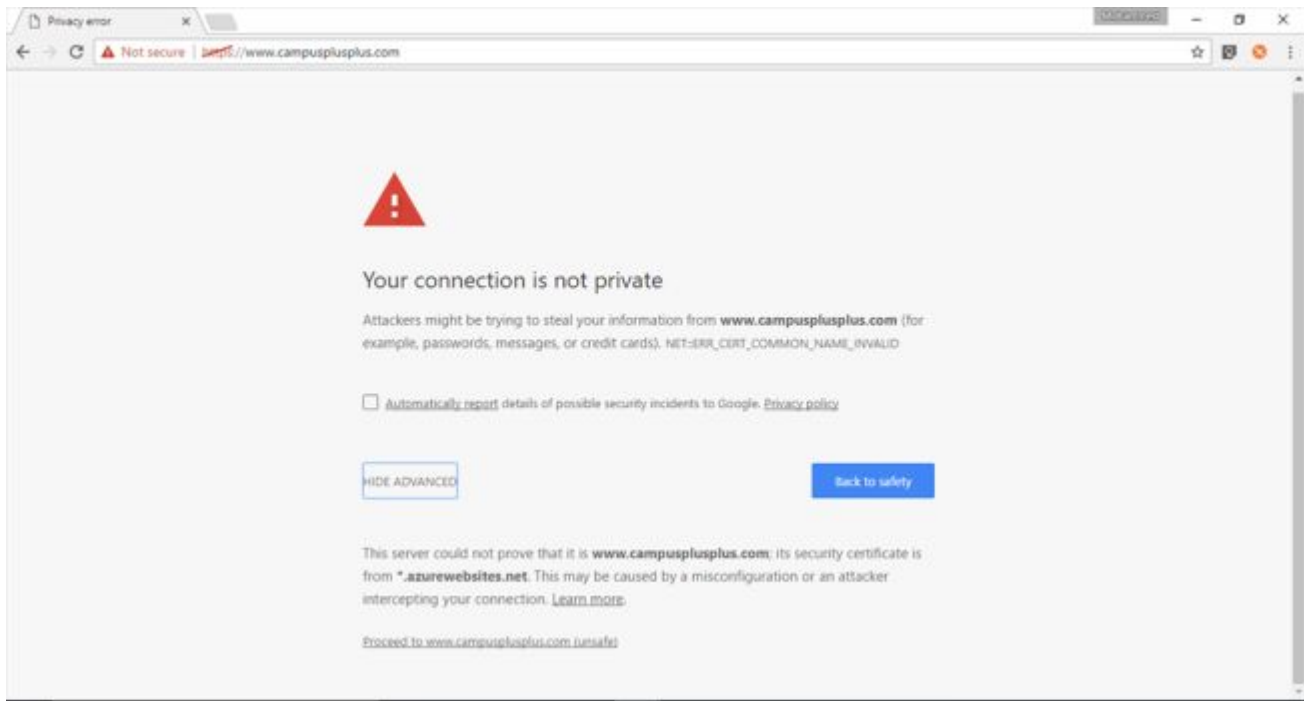
I have already acquired a certificate from a provider and you can also get one from any provider of your choice. You need to verify that you are the owner of the domain by adding some TXT values to your DNS settings. The certificate will be of .pfx extension with a private key integrated to it. Here, I am uploading it to the portal with the password.
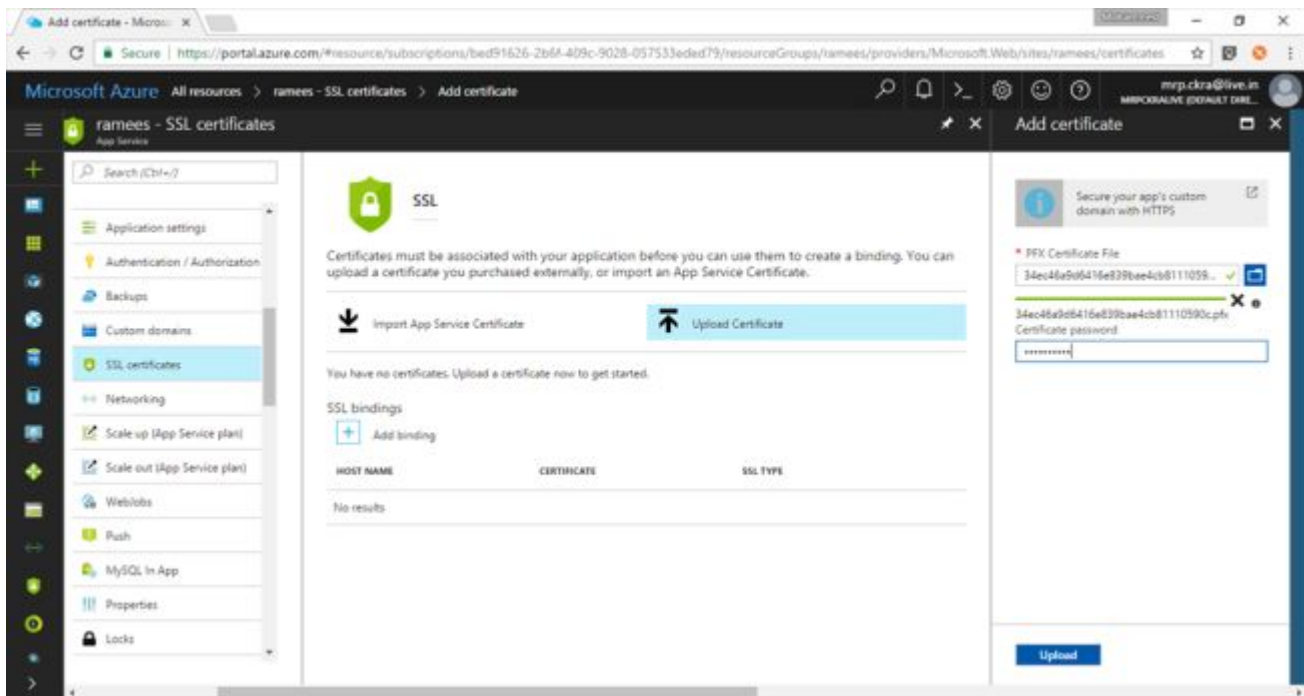

On uploading, you can see the certificate is added to your dashboard with the expiration date details.
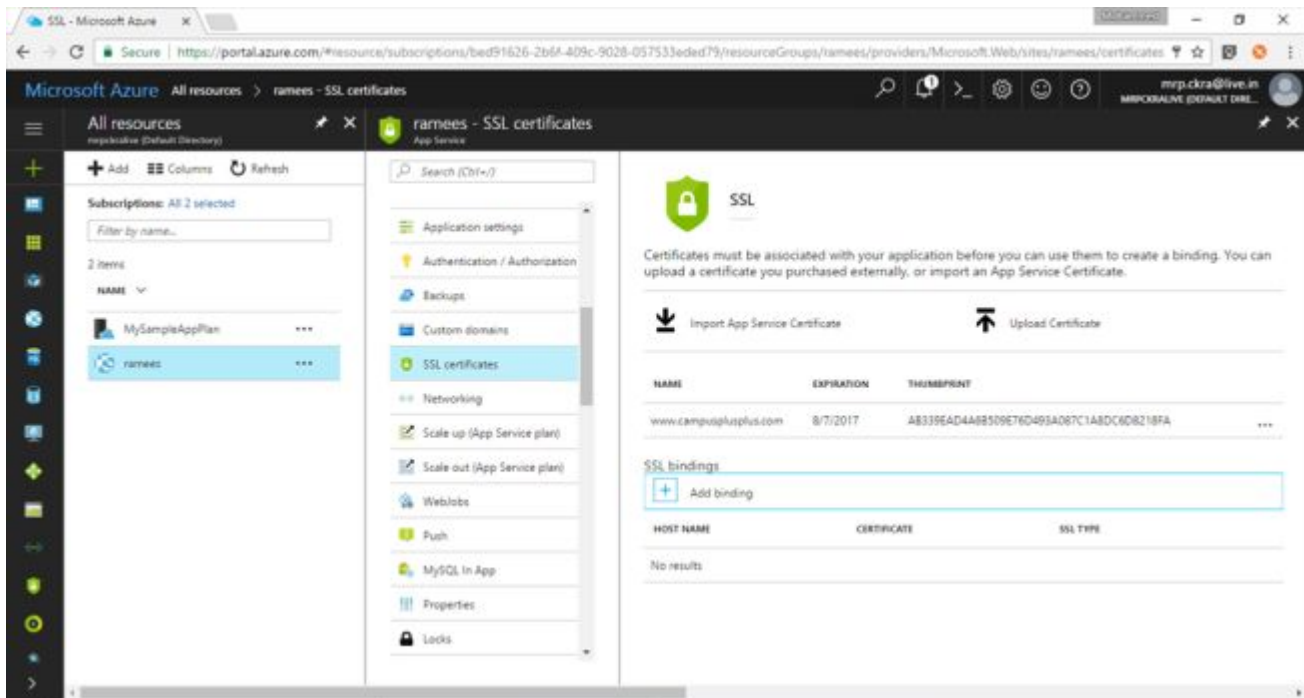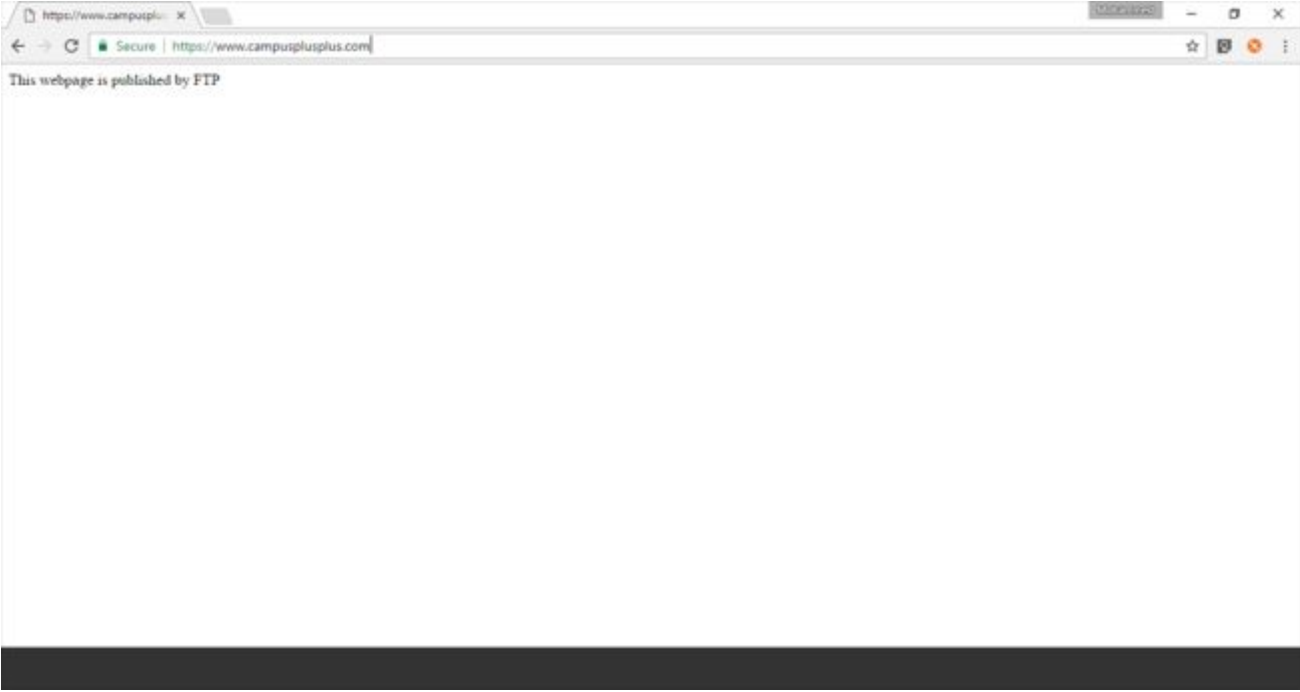
Now, we have to do the binding by providing the host name and selecting the certificate. Here, I am selecting it as SNI SSL and need to click Add binding.
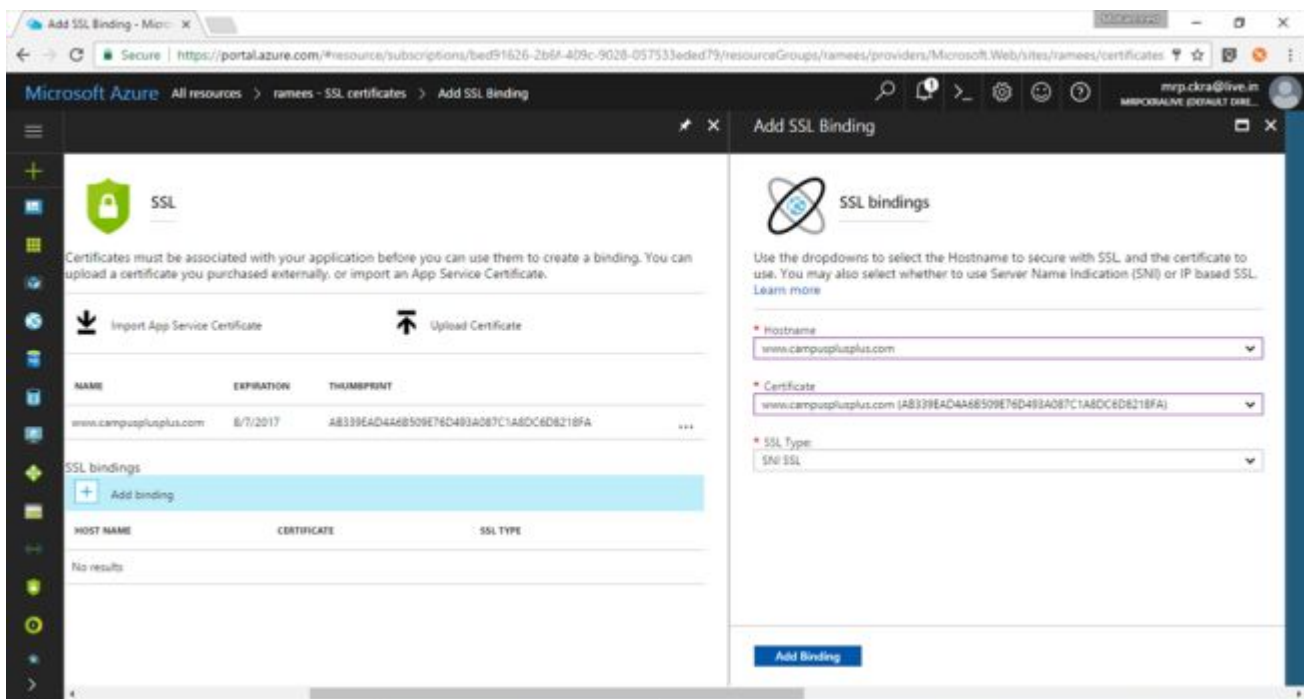
On binding, it will be listed in the dashboard. Adding SSL to a Web App may have a pricing impact as Microsoft may charge additionally for adding SSL certificate.
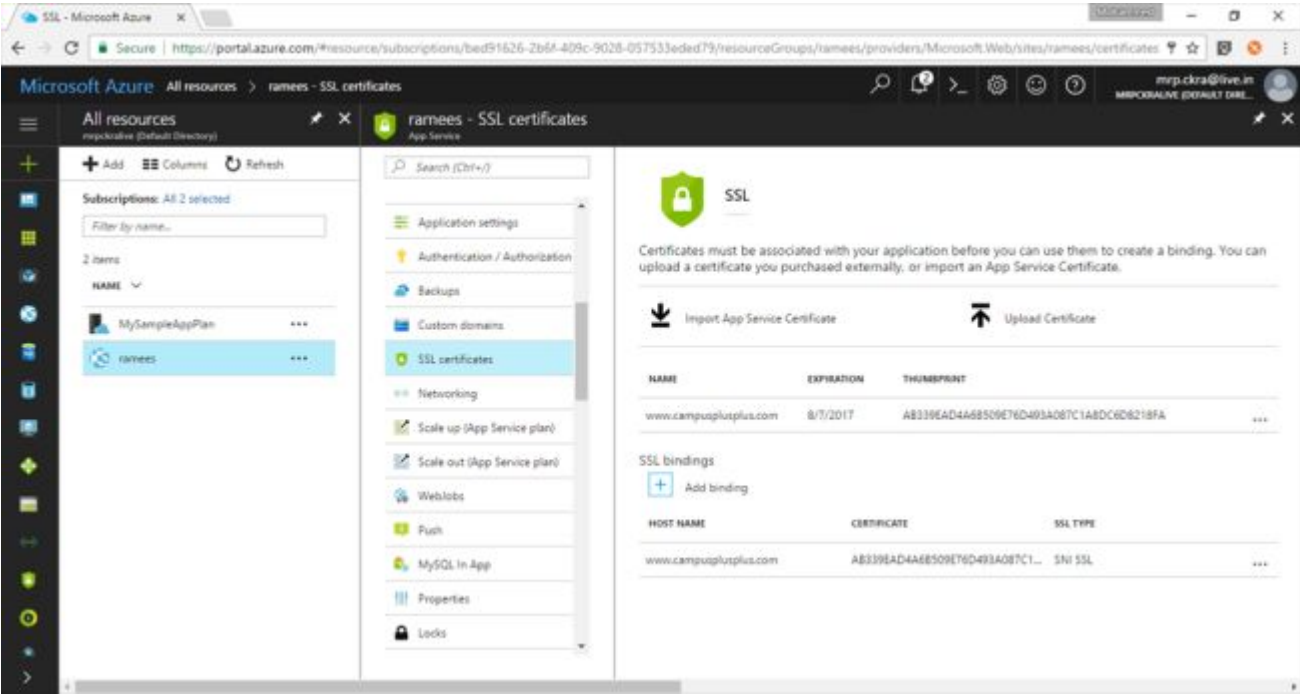
Now, if you visit the Website again with *https,* you can see that our Website is secured.

Thank you for using C# Corner