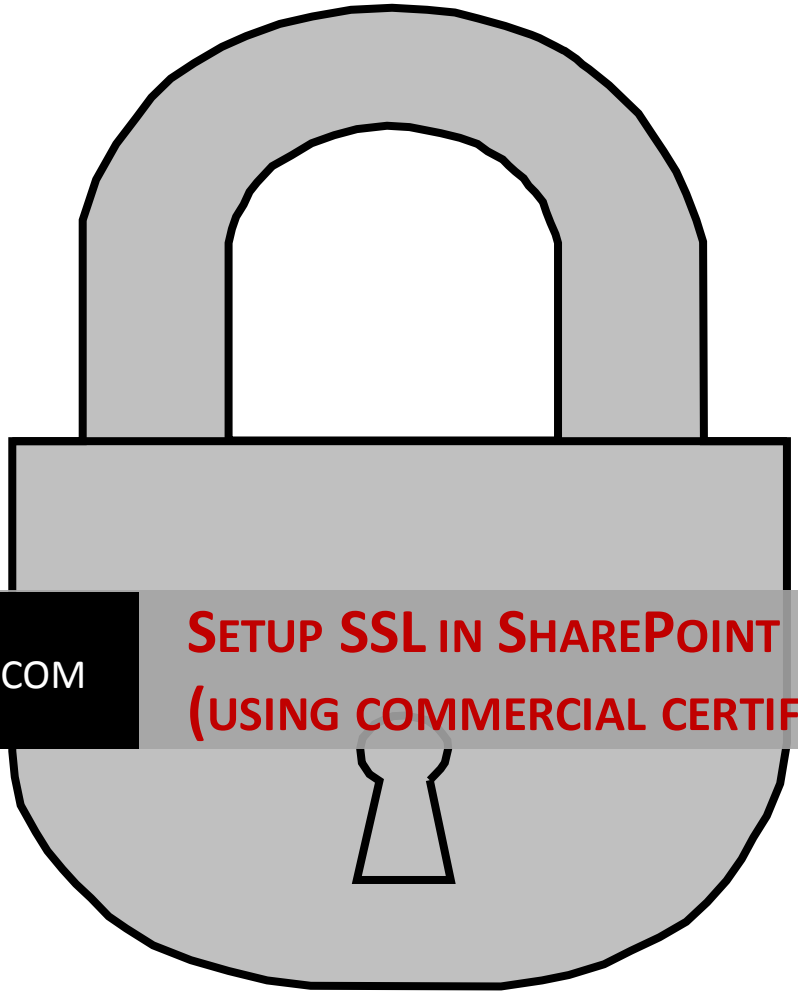
12/1/2012



WALISYSTEMSINC.COM

SETUP SSL IN SHAREPOINT 2013 (USING COMMERCIAL CERTIFICATES)

Setup SSL in SharePoint 2013

In this article you will learn how to setup SSL in SharePoint 2013. In my next article I will show you how to setup an Extranet in SharePoint 2013. Corporations usually setup SSL for Extranet sites. There are three ways to setup SSL.

1. One way is to use a commercial SSL certificate. There are many sites that sell SSL certificates. For learning purposes you can sign up for a trial version (30 days). This is what this article will focus on today.

2. Second way is to use a self-signed certificate that you create in IIS.

3. Third way is to set up your server to issue a certificate. This is what you need if you have custom DNS entries. Of course, you can also use first option (using commercial certificate) if you have DNS entries. If you use self-signed certificate and you have DNS entries, you get an error. More on this in another article!

So, let's start. In this article, I will show you how to use Verisign certificate. Verisign is one the most popular companies that issue SSL certificates. We will sign up for a trial version.

1. Before you sign up on Verisign site, we first need to create a certificate request. This will be needed when you sign up at Verisign.

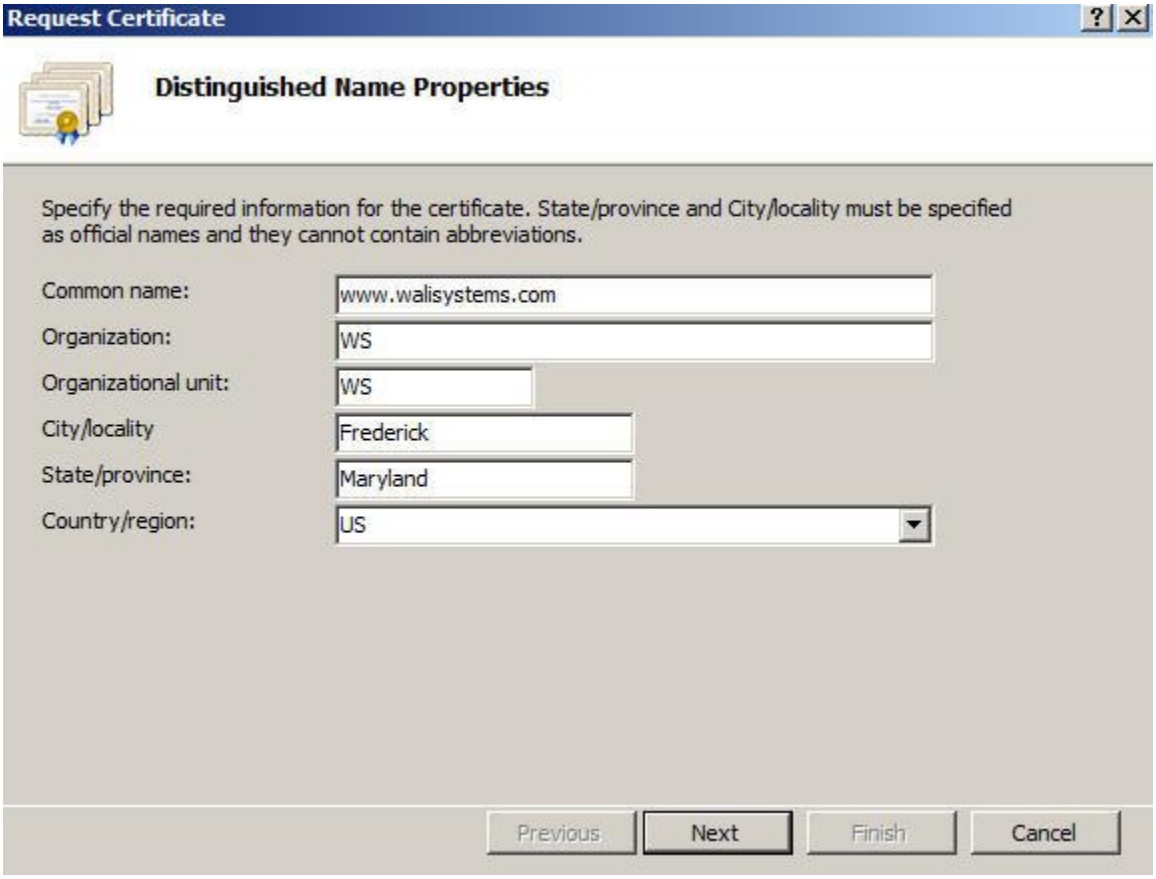
2. Open IIS 7.0 (Start > Administrative Tools > Internet Information Services (IIS) Manager).

3. Click on the server name.

4. In **IIS** section, double-click **Server Certificates**.

5. On the right side, under **Actions**, click **Create Certificate Request…** link.

6. **Request Certificate** form will open. Fill out the fields. Enter your site name or URL in the **Common Name** field. Enter your company name or abbreviation in **Organization** and **Organizational Unit** fields. Enter **City** and **State**. Enter full state name, abbreviation is not accepted. Select **Country/region** and click **Next.**



7. Keep the default values selected. **Cryptographic service provider** should have **Microsoft RSA SChannel Cryptographic Provider** selected. If it's a test or development environment, you can keep **Bit length** set to 1024. If it's a production environment and you are using a purchased SSL key, then select **Bit length** according to your needs. What kind of security is needed depends on what kind of site you have created and what kind of content it has. For confidential content or for government sites, you may want to select at least 2048 in **Bit length.** Remember, the greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

8. Browse to a folder that will store the request and give a name to the file, for example, sslrequest. Click **Finish.**

9. Go to Verisign site and sign up for a trial version. Here is the direct link for the signup page:

   https://trustcenter.websecurity.symantec.com/process/retail/trial_product_selector;jsessionid=5FD775036592747716 17C69ABB11A28D?uid=f0e5b79664a05e9b52b4844f12670f91&locale=VRSN_US

   Enter technical contact details and click **Continue.** On the next screen, you will be asked to enter CSR. Open the request file that you had created, copy it and paste it into the box on the site.

Once you have signed up, you will get an email with the key.

10. There will be three links in the email. Click the first link to download and install the Test Root CA Certificate. On the download page, there are different browsers listed. Select the browser that you will use for your site testing. Remember if you know you audience will use different browsers then you need to perform this step for every browser that your audience will be using. Steps for Internet Explorer are listed next.

11. Click the link **Download Secure Site Trial Root Certificate** link. From the box, copy the certificate and save it in a text file with a .cer extension.

12. Open Internet Explorer.

13. Go to Tools > Internet Options > Content > Certificates.

14. Click **Import…**. A wizard will open. Click Next.

15. Browse to the location of the recently stored .cer file (step 11 above).

16. Select the certificate and click **Open.**

17. Click **Next.**

18. Select **Automatically select the certificate store based on the type of the certificate.** Click **Ok.**

19. Click **Next** then **Finish.**

20. When prompted and asked if you wish to add the following certificate to the root store, click **Yes.**

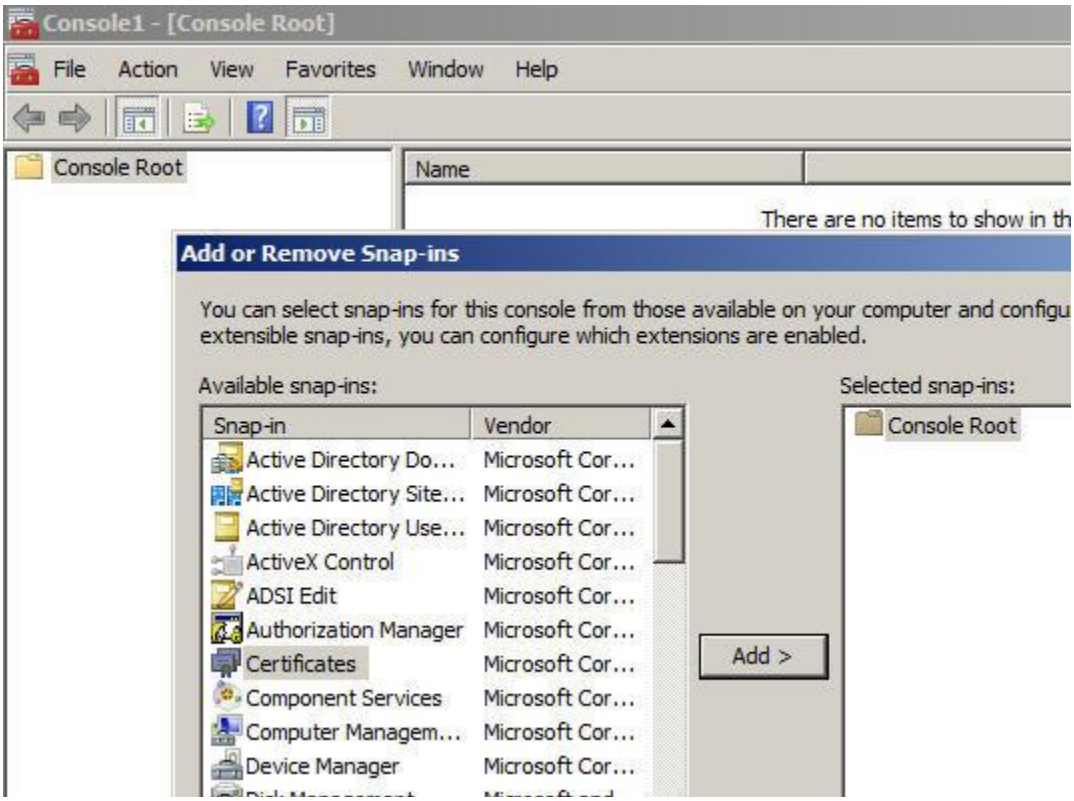
21. Second step listed in the email confuses many people. Basically this step is not required for latest IIS server. Users using IIS 5.0 or Higher servers do not need to download the intermediate CA as it is included with the SSL certificate upon issuance if they selected in the purchase as server vendor: Microsoft IIS 5.0 or higher. If you are not sure about the selection you made when requesting SSL certificate, go ahead and install it. It will not harm anything. To install it, perform same steps as listed above (Steps 11 – 19). Be sure to click second link in your email instead of first when performing step 11.

22. Just like the second step, third step in the email is equally confusing. Don't follow those steps, follow the ones listed below to install the certificate without hassles.

23. Copy the certificate from your email. It will be at the bottom of the email. Be careful when copying. Copy whole text including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- and paste it into Notepad. There should be no white spaces or extra line breaks. Save the file with **.p7b** extension. You can name the file as sslcert.p7b or whatever you prefer.

24. Click Start > Run and type **mmc** and click **OK**. MMC console will open.

25. From **File**, select **Add/Remove Snap-in**.



26. Select **Certificates** from available snap-ins and click **Add >.**

27. Select first option **My user account** and click **Finish.**

28. Click **OK**.

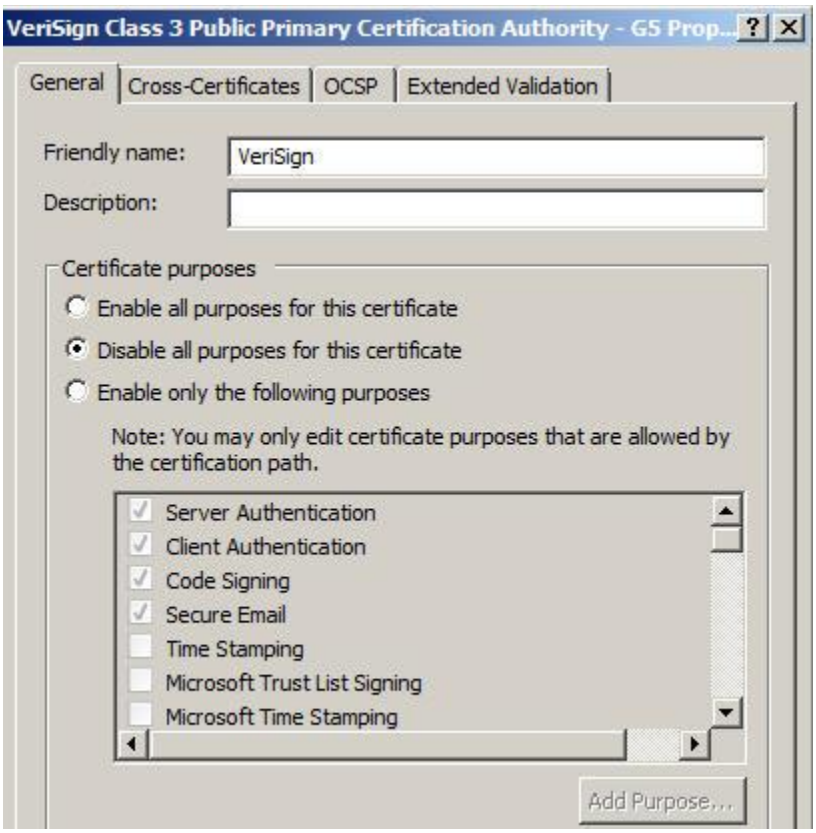
29. Expand **Certificates – Current User** node.

30. Expand the **Trusted Root Certification Authorities** folder on the left and select the **Certificates** subfolder.

31. Locate the following certificate:
    a. Issued To: **VeriSign Class 3 Public Primary Certification Authority - G5**

32. Right-click the certificate and select **Properties**.

33. In the **Certificate purposes** section, select **Disable all purposes for this certificate**. This is a pre-installed certificate and must be disabled before using new certificate from SSL.



34. Click **Apply** then **OK**.

Install Certificate

35. Finally, install the certificate. There are two ways to do it. One is through the IIS and the other is the MMC certificates console. I prefer the second way because you have to come to the MMC certificates console anyway to fix a problem if you opt to install the certificate through IIS. If you install the certificate through IIS, at the time of binding the certificate to your site, certificate will not show up in IIS and then you will have to come to the MMC certificates console to perform an additional step. So it's better to go with the MMC route from the beginning. There is another problem with the IIS method. You get the following error when you install the certificate through IIS.

Error Text: Cannot find the certificate request that is associated with this certificate file. A certificate request must be completed on the computer where the request was created.

36. Open MMC console (Start > Run > Type MMC > Click OK).

37. Certificates console will still be available because you added it in step 24 but if for some reason you had to restart your machine or log out of it then you will have to add the console again. Follow steps 24 – 28 to add **Certificates** console. Expand **Certificates – Current User** node on the left.

38. Expand **Trusted Root Certification Authorities** and click **Certificates** folder.

39. Right-click **Certificates** folder and select **All Tasks** then select **Import**.

40. Browse to the certificate (**.p7b**) file. Click **Next**.

41. Select **Place all certificates in the following store** and leave default store selected. Click **Next**.

42. Click **Finish**.

43. You will get **The import was successful** message. Click **Ok**. You may also get following security warning.

Error Description: You are about to install a certificate from a certification authority (CA) claiming to represent: Verisign Trial Secure Server Root CA – G2.

If you get this security warning, click **Yes** to install the certificate.

44. With MMC Certificates console still open, expand **Personal** folder on the left and right-click **Certificates** subfolder. Select **All Tasks** then select **Import**.

45. Browse to certificate file (.p7b) and Click **Next**.

46. Keep second option **Place all certificates in the following store** selected and keep **Personal** certificate selected as the default option. Click **Next**.

47. Click **Finish**. You will get **The import was successful** message. Click **Ok**.

Bind Certificate to your site

48. Finally, bind certificate to your site. Open **IIS**.

49. Click server name. Expand **Sites** node.

50. Click site name that you will bind to the SSL certificate.

51. On the right, under **Actions**, click **Bindings**.

52. Click **Add**.

53. In **Type**, select **https**.

54. Keep 443 in the **Port**. This is default port used for SSL.

55. In **SSL Certificate**, select the certificate you just installed. Please note that if you don't see new certificate in this drop down, then you probably missed steps 44 – 47 above. Click **OK**. That's it.

Alternate Access Mappings

56. Assuming you have a web application setup to work with SSL, configure Alternate Access Mappings to use site with SSL. Open **Central Admin Site** and click **Application Management**.

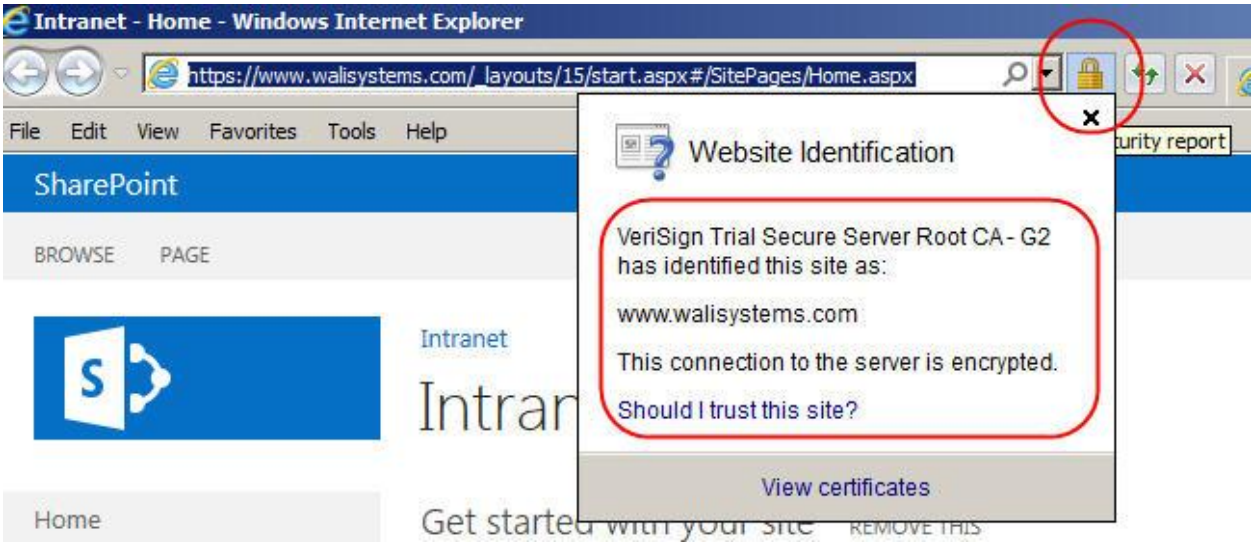
57. Under **Web Applications**, click **Configure alternate access mappings**.

58. You will notice you already have default site listed in the **Default** zone. To add new URL in the **Intranet** zone, click **Add Internet URLs**.

59. From the **Alternate Access Mapping Collection** drop down, select correct application that you want to use for the AAM setting and then add URL in the text box labeled **URL protocol, host and port**, for example, https://www.walisystems.com. From the **Zone** dropdown, select **Intranet**.

60. Click **Save**.

Now open site with https to test that everything works fine.



In the address bar, click the lock sign to check validity of the certificate. If you want to see the certificate, click **View Certificates** link at the bottom of the notification.