12/15/2012

Walisystemsinc.com

Setup SSL in SharePoint 2013 (using self-signed certificate)

Setup SSL in SharePoint 2013

In the last article (link below), you learned how to setup SSL in SharePoint 2013 using commercial certificate.

Setup SSL in SharePoint 2013 using commercial certificates

In this article, you will learn how to setup SSL using self-signed certificate. This is useful if you are setting up a development environment or want to test SSL locally. It provides same level of protection as any other commercial certificate and you don't have to pay for it. Why then people use commercial certificates? It's a matter of trust. Basically you are asking your site users to trust you. It may work in some scenarios but might not work if your site is public facing (Internet). Why would people search you, they don't know you. So, you can use self-signed certificate locally for testing but for production you should use a reliable third party certificate issuing authority like Verisign, Thwarte, etc.

Follow the steps below to create a self-signed certificate for your site:

1. Open IIS 7.0.
2. Click on the server name in the navigation tree on the left.
3. On the right side, Under **IIS**, double-click **Server Certificates**.
4. On the extreme right, under **Actions** click **Create Self-Signed Certificate** link.
5. Enter a friendly name for the certificate, for example, I entered WS (for Wali Systems).
6. Double-click the newly created certificate.
7. Click on **Details** tab.
8. Click **Copy to File** button.
9. Certificate export wizard will start. Click **Next**.
10. By default second option **No, do not export the private key** is selected. Keep it selected and click **Next**.
11. Keep the default option **DER encoded binary X.509 (.CER)** selected and click **Next**.

12. Click **Browse** to go to the folder where you want the file to be saved. Enter file name and click **Save**.

13. Click **Next** and then **Finish**. Click **Ok** to close the success message box. Click **OK** to close the **Certificate** window.

The steps that follow are same as those demonstrated in the previous article. Certificates are issued to a computer, user. Or service. Administrators can add certificates to the **Trusted Root Certification Authorities Store** for a local computer or for a domain. Below, we will add certificate to the local computer store.

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

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

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

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

18. Click **OK**.

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

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

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

22. Browse to the certificate (**.cer**) file that you saved earlier. Click **Next**.

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

24. Click **Finish**.

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

If you share this server with others, then it's better to import the certificate using local computer account. Follow steps 14 – 25 again but this time in step 17, instead of selecting **My user account**, select **Computer account**. After you have imported certificate into **Trusted Root Certification Authorities**, import it into SharePoint Certificates as well. Expand **SharePoint** node, right-click **Certificates** node and import the certificate.

Manage Trust

26. This step is not required if you have a single server farm but if you are setting it up in a medium or large farm, then you should add certificate to the **Trust Relationships** in central administration site.

27. Open central administration site. Go to **Security** section (Click **Security** under **Central Administration** on the left).

28. In **General Security** section, click **Manage Trust**.

29. In the ribbon, click **New** button.

30. Add a name for this trust relationship.

31. Click **Browse** to import the certificate. This is mandatory regardless of whether you want to provide to or consume trust from the other farm.

32. Leave **Provide Trust Relationship** unchecked unless you want to provide trust to another farm. This is optional.

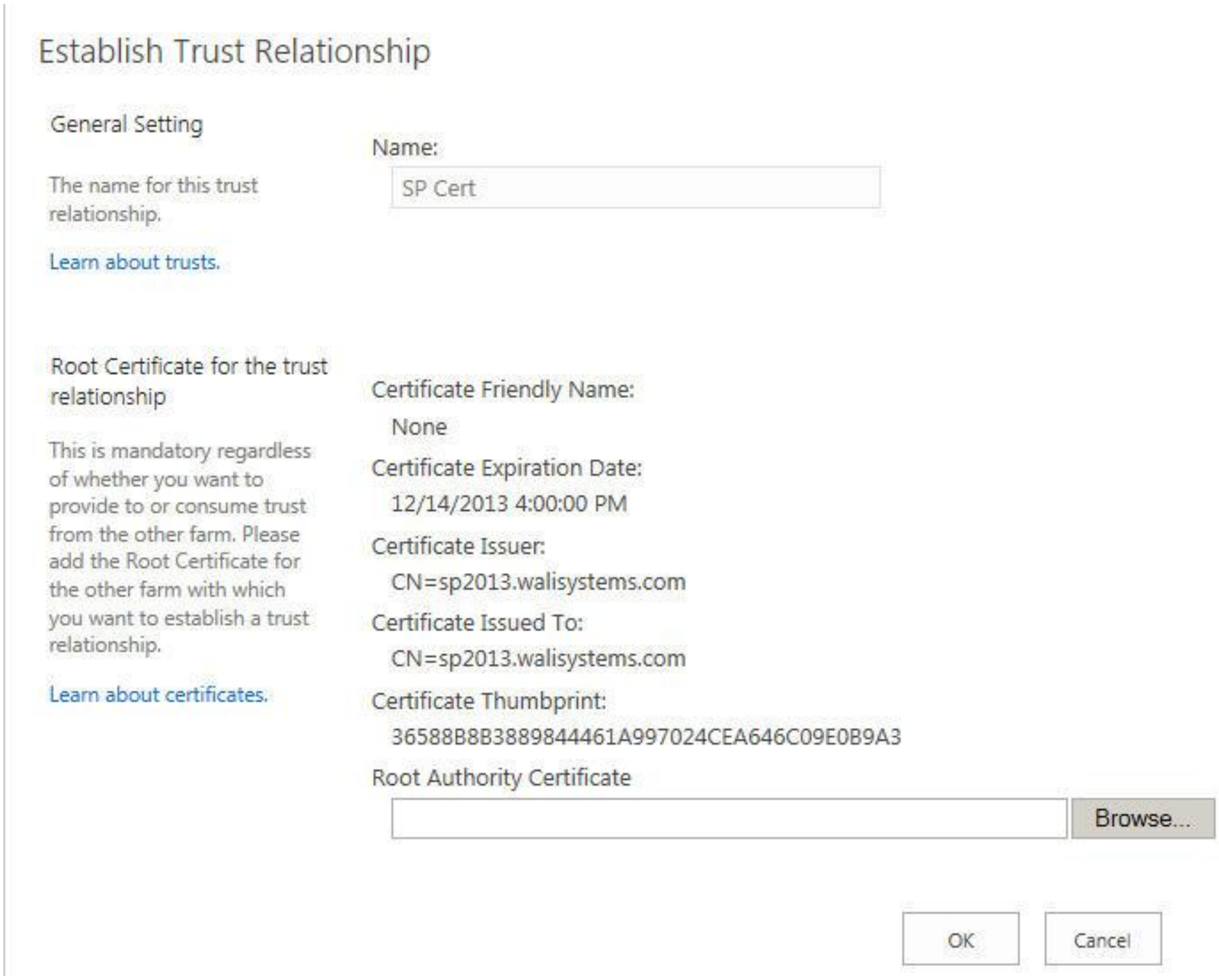
33. Click OK.

You can also add certificate using PowerShell. Open **SharePoint 2013 Management Shell** and run following command:

- $trustcert = new-object system.security.cryptography.x509certificates.x509certificate2(“**C:\\ws.cer**”)
- New-sptrustedrootauthority –name “**SP Cert**” –certificate $trustcert

** **C:\\ws.cer** is the path to the certificate file. Change it to the path on your machine.

** **SP Cert** is the name that you give to this trust relationship. This is what will appear in the **Manage Trust** interface in SharePoint Central Admin.



Establish Trust Relationship

General Setting

The name for this trust relationship.

Learn about trusts.

Name:

SP Cert

Root Certificate for the trust relationship

This is mandatory regardless of whether you want to provide to or consume trust from the other farm. Please add the Root Certificate for the other farm with which you want to establish a trust relationship.

Learn about certificates.

Certificate Friendly Name:

None

Certificate Expiration Date:

12/14/2013 4:00:00 PM

Certificate Issuer:

CN=sp2013.walisystems.com

Certificate Issued To:

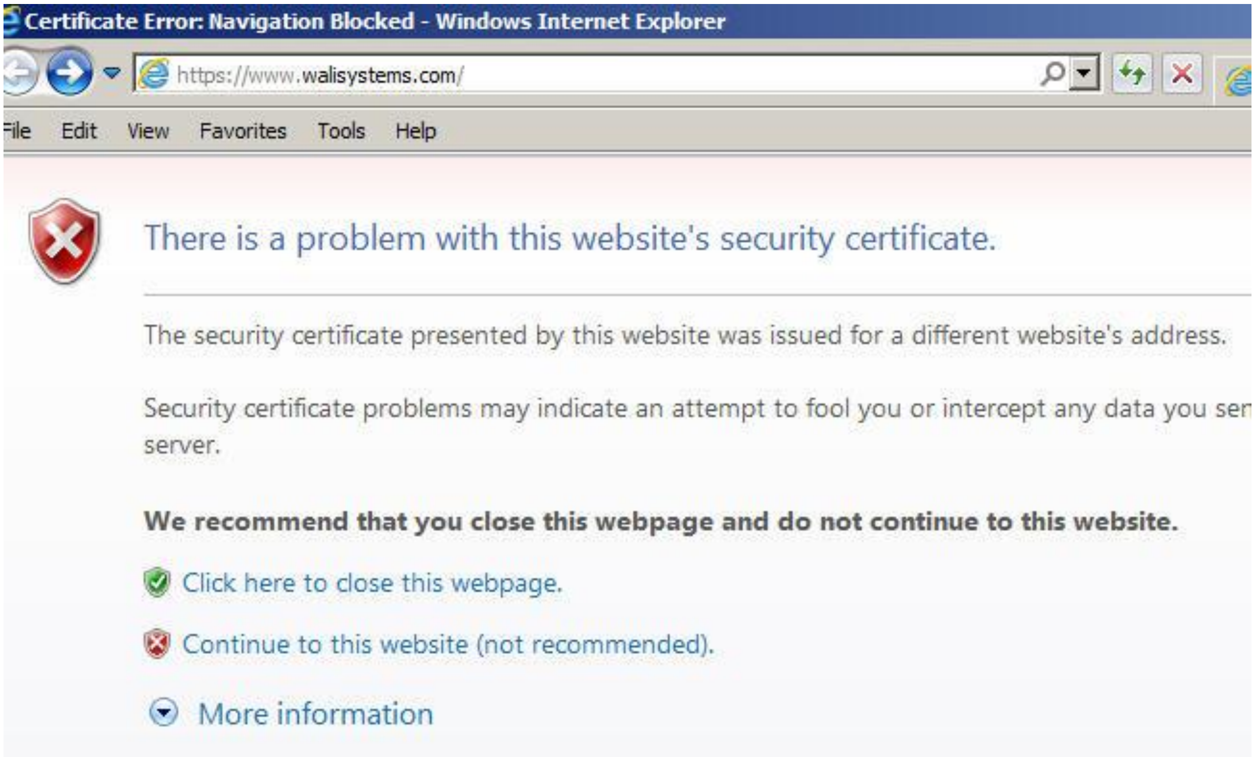
CN=sp2013.walisystems.com

Certificate Thumbprint:

36588B8B3889844461A997024CEA646C09E0B9A3

Root Authority Certificate

Your site should have correct host headers if you want this certificate to work correctly. For example, if you look at the figure above, you will notice that the certificate was issued to “sp2013.walisystems.com” so if your site does not have this host header, you will get an error. For example, when you try to open your site in the browser, you get this error:


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://www.walisystems.com/
File
Edit
View
Favorites
Tools
Help

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

The security certificate presented by this website was issued for a different website's address.

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

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

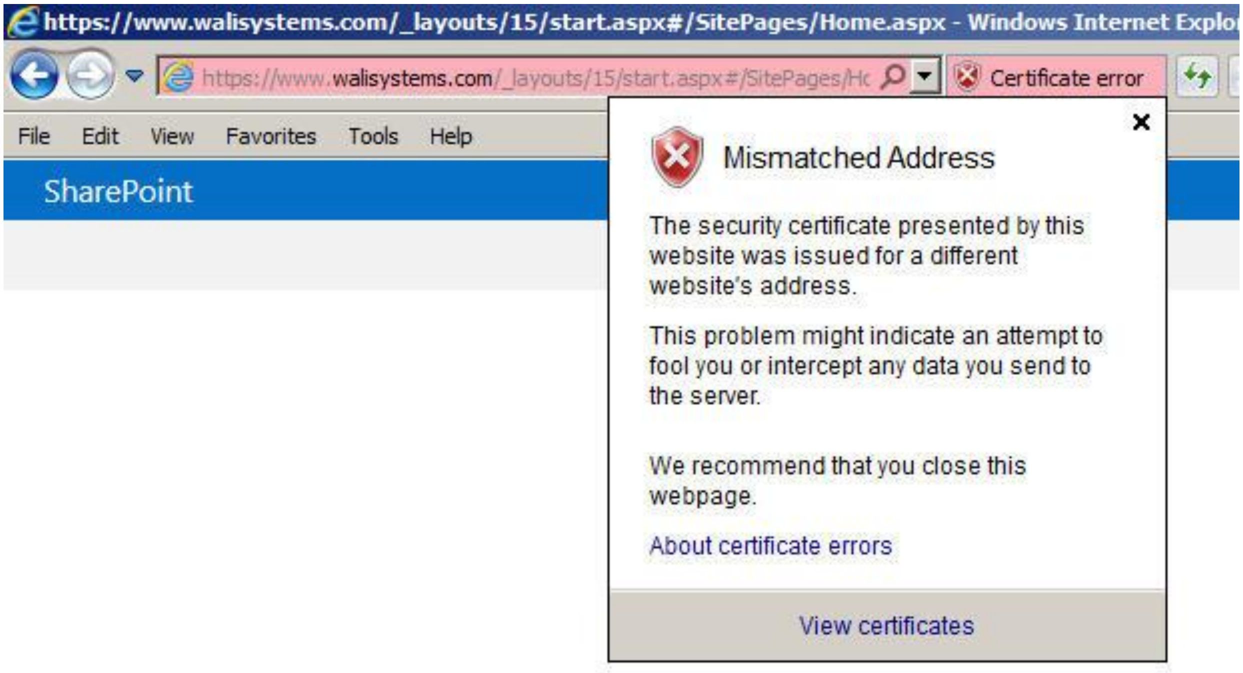
Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure: There is a problem with this website’s security certificate

Again, notice that I tried to open ” https://www.walisystems.com” but the certificate was issued to “sp2013.walisystems.com”. If you click **Continue to this website**, site will open but you will still get an error message.



https://www.walisystems.com/_layouts/15/start.aspx#/SitePages/Home.aspx - Windows Internet Explor
https://www.walisystems.com/_layouts/15/start.aspx#/SitePages/Hc
Certificate error
File
Edit
View
Favorites
Tools
Help
SharePoint

Mismatched Address

The security certificate presented by this website was issued for a different website's address.

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.

About certificate errors

View certificates

Figure: Mismatched Address

Error: The security certificate presented by this website was issued for a different website's address. This problem might indicate an attempt to fool you or intercept any data you send to the server.

To resolve the issue, create a new web application or extend an existing one. If you want to add https to your main site at port 80, then create a new web application with new host headers. Here are the steps:

Create New Web Application For SSL

34. Go to central administration. Click **Manage web applications**.

35. Click **New** button in the ribbon.

36. Select **Create a new IIS web site**. Change **Port** to **80**.

37. In the **Host Header**, enter the URL that want to use for this web application. For example, I wanted to use "sp2013.walisystems.com" because that was the URL for which the certificate was issued therefore I entered "sp2013.walisystems.com". Note: Do not add **HTTP** in the URL.

38. In **Security Configuration** section, select **Yes** in **Use Secure Sockets Layer (SSL)**.

39. Keep all other default options selected and click **OK**.

40. After web application is created, create a site collection at the root level.

Change Alternate Access Mappings

41. In Central Administration Site, go to **Application Management** section and click **Configure alternate access mappings**.

42. Change site collection in the drop down. Select the one that you just created. Click **Add Internal URLs**.

43. Enter complete URL that starts with **HTTPS**. For example, "https://sp2013.walisystems.com".

44. Change **Zone** to **Custom** or **Extranet**.

45. Click **Save**.

Bind Certificate To Your Site

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

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

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

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

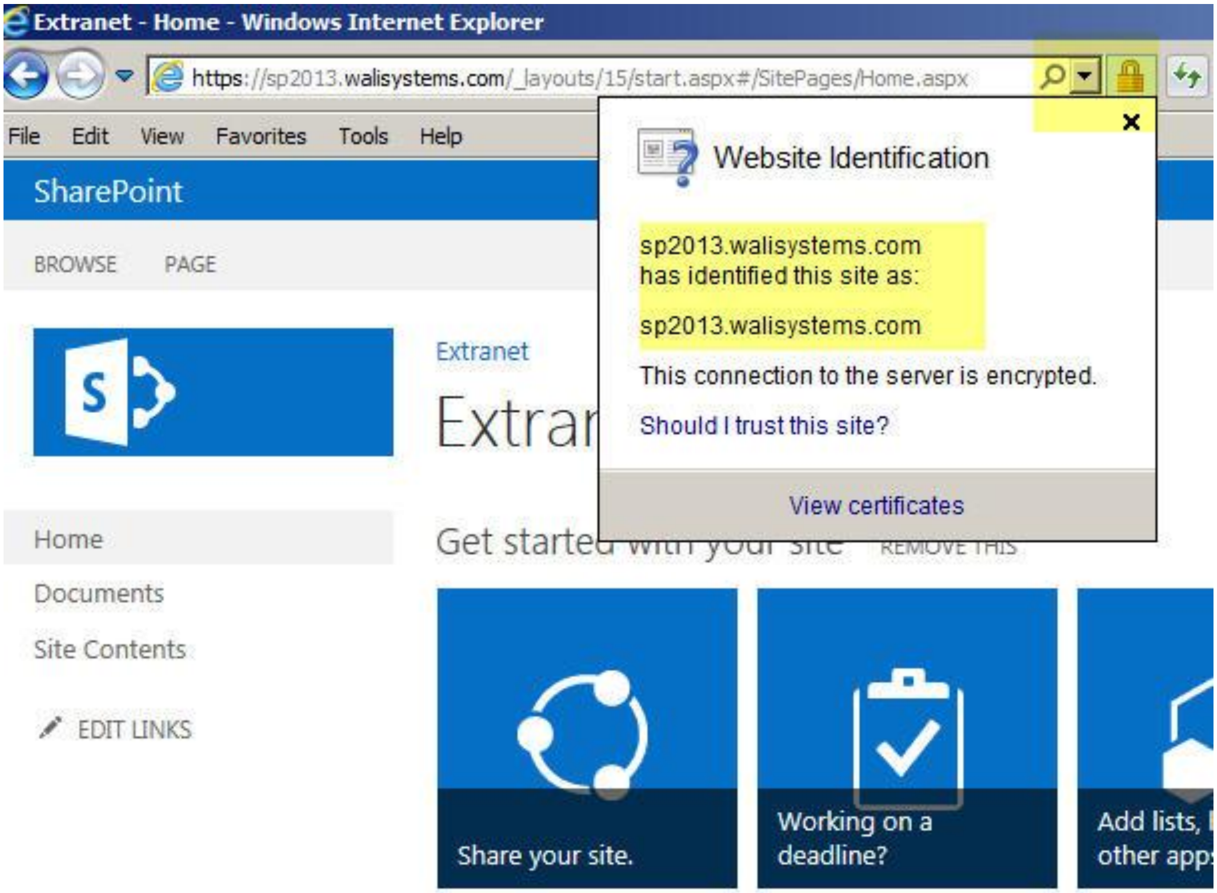
50. Click **Add**.

51. In **Type**, select **https**.

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

53. In **SSL Certificate**, select the certificate you just installed. Click **OK**. That's it.

To test SSL setup, open the site in browser. 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.



Website Identification

sp2013.walisystems.com has identified this site as:

sp2013.walisystems.com

This connection to the server is encrypted.

Should I trust this site?

View certificates