

2012

Setup SSL in SharePoint 2013 Using Domain Certificate



Setup SSL in SharePoint 2013 Using Domain Certificate

Setup SSL in SharePoint 2013 Using Domain Certificate

In the previous articles, you learned how to setup SSL in SharePoint using a third party SSL certificate and a self-signed SSL certificate.

[Setup SSL In SharePoint 2013 Using Commercial Certificate](#)

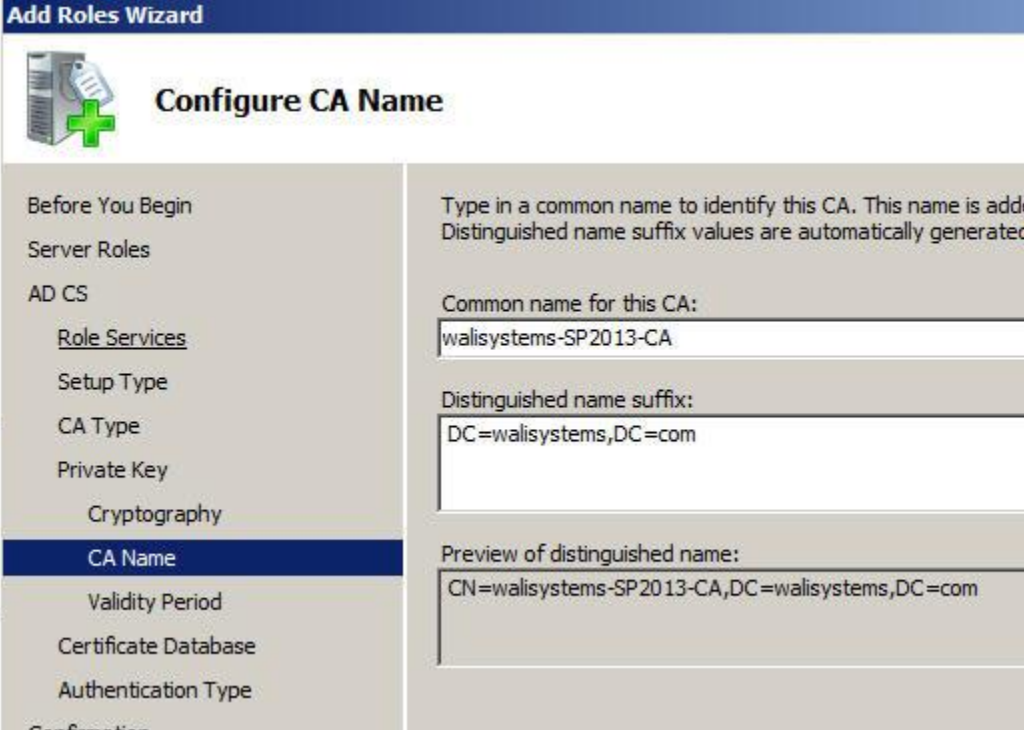
[Setup SSL In SharePoint 2013 Using Self-Signed Certificate](#)

In this article, you will learn how to setup SSL using a domain certificate. All steps are same as explained in the previous articles with the exception of creating domain certificate. I will repeat the steps again for your convenience.

1. To generate a domain certificate, you must have **Active Directory Certificate Services** running.
2. Open **Server Manager** (All Programs > Administrative Tools > Server Manager).
3. Expand **Roles** node and see if certificate services role is installed. If not, then install it first using the steps below.
4. Click **Roles**. Under **Roles Summary** header, you will see **Add Roles** link on the right, click it.
5. Click **Next**.
6. Check **Active Directory Certificate Services** role and click **Next**.
7. Click **Next** again.
8. **Certification Authority** will already be selected. Select the following services:
 - a. Certification Authority Web Enrollment
 - b. Online Responder
 - c. Certificate Enrollment Policy Web Service
9. Click **Next**.
10. Keep **Enterprise** selected and click **Next**.
11. Keep **Root CA** selected and click **Next**.
12. Keep **Create a new private key** selected and click **Next**.

Setup SSL in SharePoint 2013 Using Domain Certificate

13. Select **RSA#Microsoft Software Key Storage Provider** in the **cryptographic service provider (CSP)**. Change **key character length** from 2048 to 1024 unless this is production environment and you want to use strong keys. By default, **SHA1** is selected in **hash algorithm**, keep it selected and click **Next**.
14. Keep the default values selected and click **Next**. **Common name for CA** is the name that you will see in certification authority while generating domain certificate.



The screenshot shows the 'Add Roles Wizard' window with the 'Configure CA Name' step selected. The left-hand navigation pane includes options like 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name' (highlighted), 'Validity Period', 'Certificate Database', 'Authentication Type', and 'Confirmation'. The main area contains the following fields:

- Instruction: Type in a common name to identify this CA. This name is added to the distinguished name. Distinguished name suffix values are automatically generated.
- Field: Common name for this CA:
- Field: Distinguished name suffix:
- Field: Preview of distinguished name:

15. Keep default value selected and click **Next**. Default validity period is 5 years.
16. Keep default values selected and click **Next**. These are certificate database and log locations.
17. Keep default option **Windows Integrated Authentication** selected and click **Next**.
18. Click **Install**.
19. Now you have it installed, next step is to create a domain certificate but wait a minute. If your domain controller is on a separate machine then there is one step left. You have to import certificate to the SharePoint machine. The certificate is located in the following folder and has a .crt extension.

C:\Windows\System32\CertSrv\CertEnroll

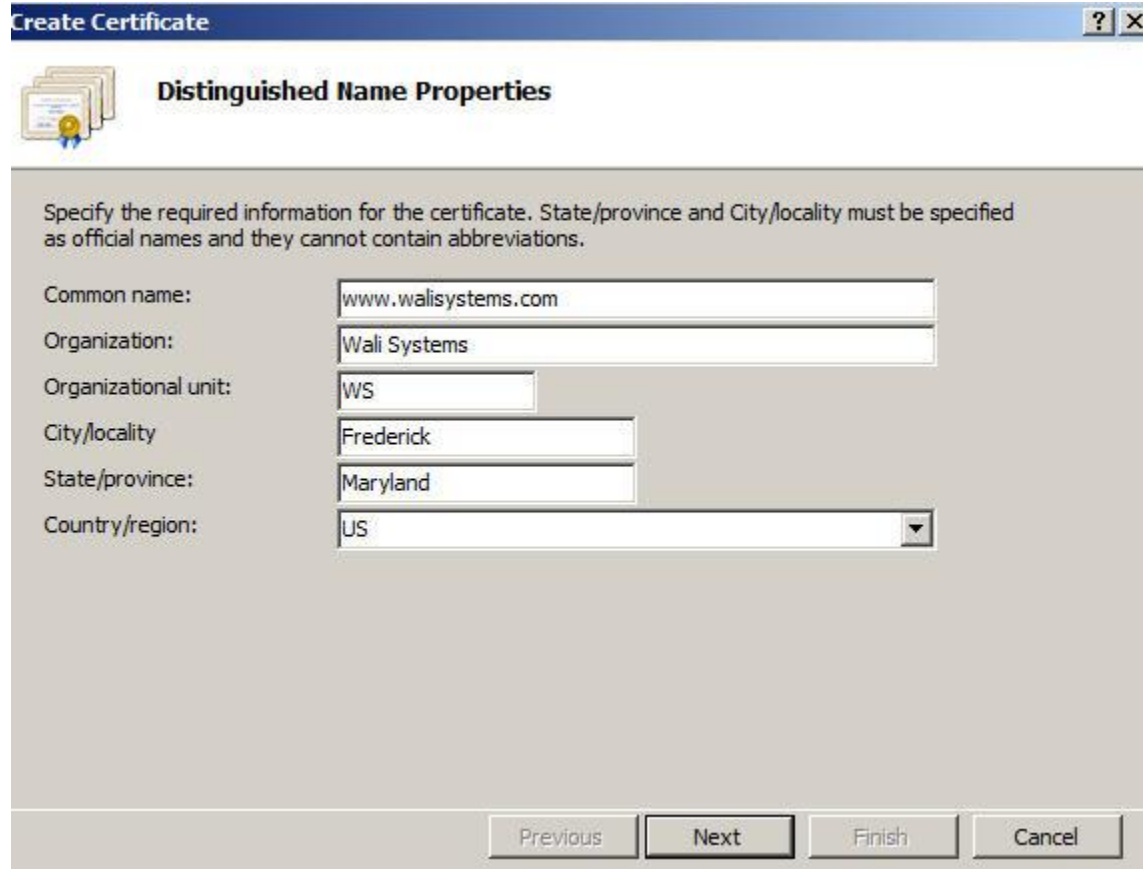
Setup SSL in SharePoint 2013 Using Domain Certificate

If you ever renamed your server, you will see multiple .crt files. Make sure you pick the one that is current. For example, if your server's FQDN is **walisystems.com** and server name is **SP2013** then the certificate file name will be **sp2013.walisystems.com_walisystems-SP2013-CA**.

Copy the file to the SharePoint machine and import it into **Trusted Root Certification Authorities**.

- a. Click Start > Run and type **mmc** and click **OK**. MMC console will open.
 - b. From **File**, select **Add/Remove Snap-in**.
 - c. Select **Certificates** from available snap-ins and click **Add >**.
 - d. Select third option **Computer account** and click **Next**.
 - e. Choose **Local Computer** and click **Finish**.
 - f. Click **Ok**.
 - g. Expand **Certificates (Local Computer)** node.
 - h. Expand **Trusted Root Certification Authorities** and click **Certificates** folder.
 - i. Right-click **Certificates** folder and select **All Tasks** then select **Import**.
 - j. Browse to the certificate (**.crt**) file that you copied from the DNS machine. Click **Next**.
 - k. Select **Automatically select the certificate store based on the type of certificate** and leave default store selected. Click **Next**.
 - l. Click **Finish**.
 - m. You will get **The import was successful** message. Click **Ok**.
20. Now, let's move to the next part which is creating a domain certificate. Open **IIS**.
21. Click on server name and under **Actions** on the right, click **Create Domain Certificate**.
22. Enter a friendly **Common name** for the certificate, for example, your server's FQDN. **Organization** should contain your organization's name or your server name. **Organization Unit** can be an abbreviation of your organization name or machine name. Enter **City**, **State** and select **Country**. Enter full state name, not the abbreviation. Click **Next**.

Setup SSL in SharePoint 2013 Using Domain Certificate



The screenshot shows a Windows-style dialog box titled "Create Certificate" with a subtitle "Distinguished Name Properties". The dialog contains a text area with the instruction: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." Below this are several input fields: "Common name:" with the value "www.walisystems.com"; "Organization:" with "Wali Systems"; "Organizational unit:" with "WS"; "City/locality" with "Frederick"; "State/province:" with "Maryland"; and "Country/region:" with a dropdown menu set to "US". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

23. Click Select button to select **Certificate Authority**. Select the one that you created above. If you are doing this first time then there will be only one authority listed there. Select it and click **OK**. Give a friendly name to the **Online Certificate Authority**, for example, WS_SP2013 and click **Finish**.

That's it. Next you will bind the certificate to your site.

Bind Certificate To Your Site

24. Open **IIS**.
25. Click server name. Expand **Sites** node.
26. Click site name that you will bind to the SSL certificate.
27. On the right, under **Actions**, click **Bindings**.

Setup SSL in SharePoint 2013 Using Domain Certificate

28. Click **Add**.
29. In **Type**, select **https**.
30. Keep 443 in the **Port**. This is default port used for SSL.
31. In **SSL Certificate**, select the certificate you just created. Look for the common name, for example, WS_SP2013. 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. In case you see error message, click **Certificate Error** (that appears instead of a golden lock). Click View Certificates. Click **Install Certificate** button to install the certificate. Click **Ok** to close the certificate window. Refresh your browser and now you will see a lock.

