

How to Create a Self Signed SSL Certificate with Windows Server

132438 2 Aug 2018 2 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article describes the steps to generate a Self Signed Certificate using IIS in Windows Server 2012.

The following sections are covered:

- [What to do](#)
 - [Create the SSL Certificate](#)
 - [How to Bind the Self Signed Certificate](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions:

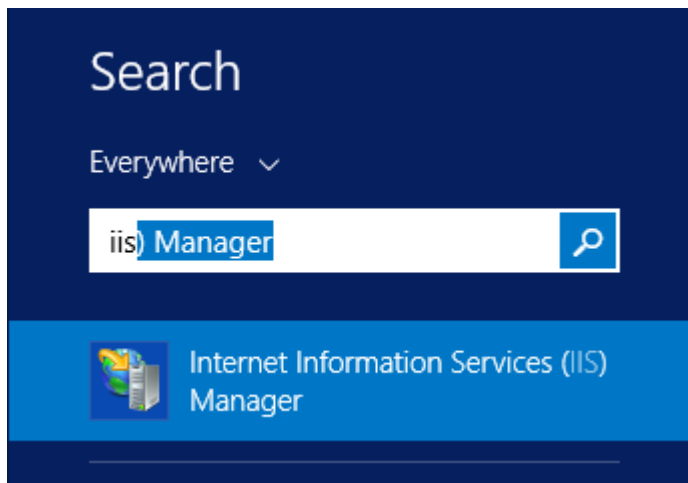
Windows Server 2012+

What to do

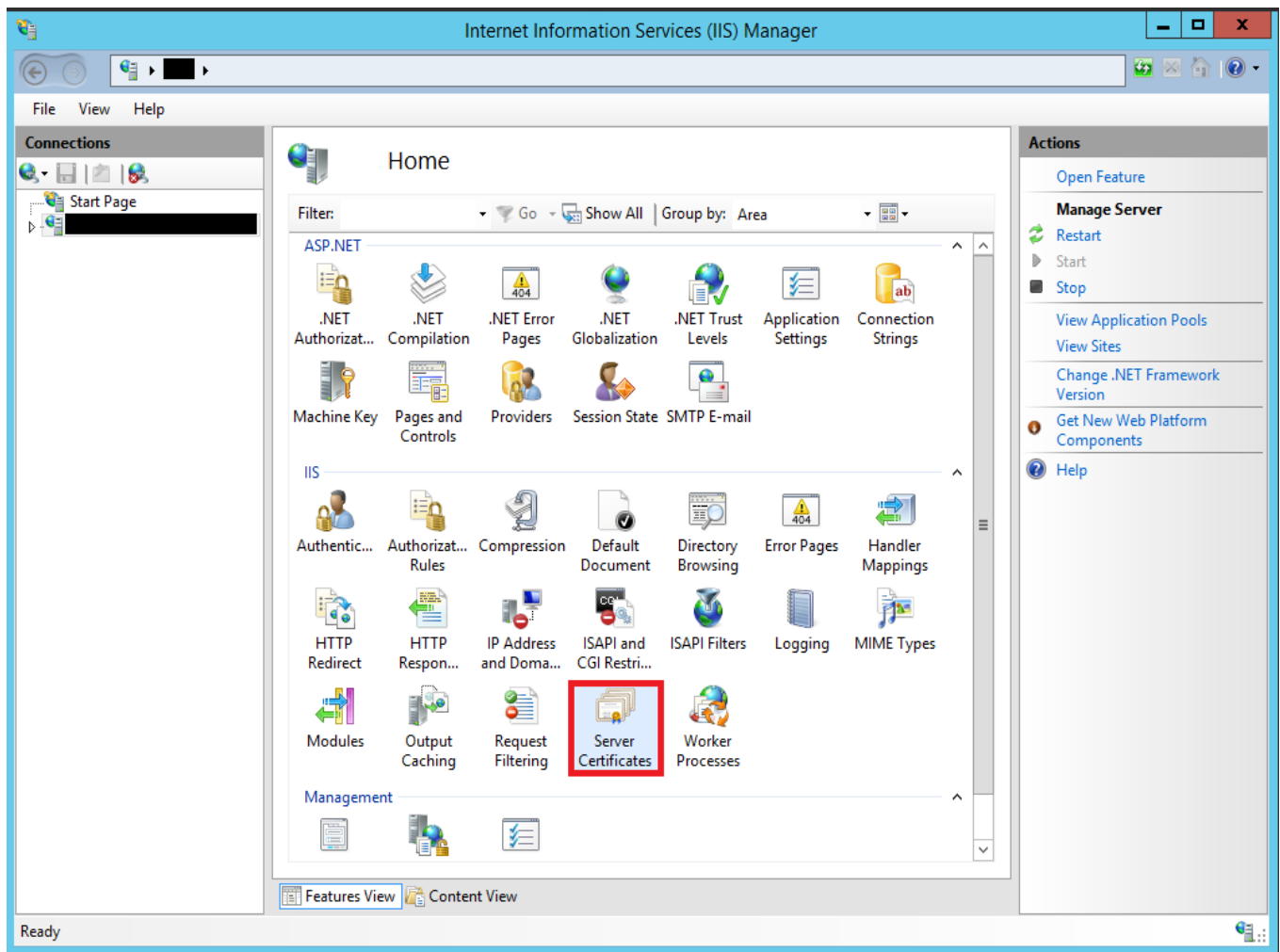
These steps will cover how to create and bind an SSL certificate using Windows Server.

Create the SSL Certificate

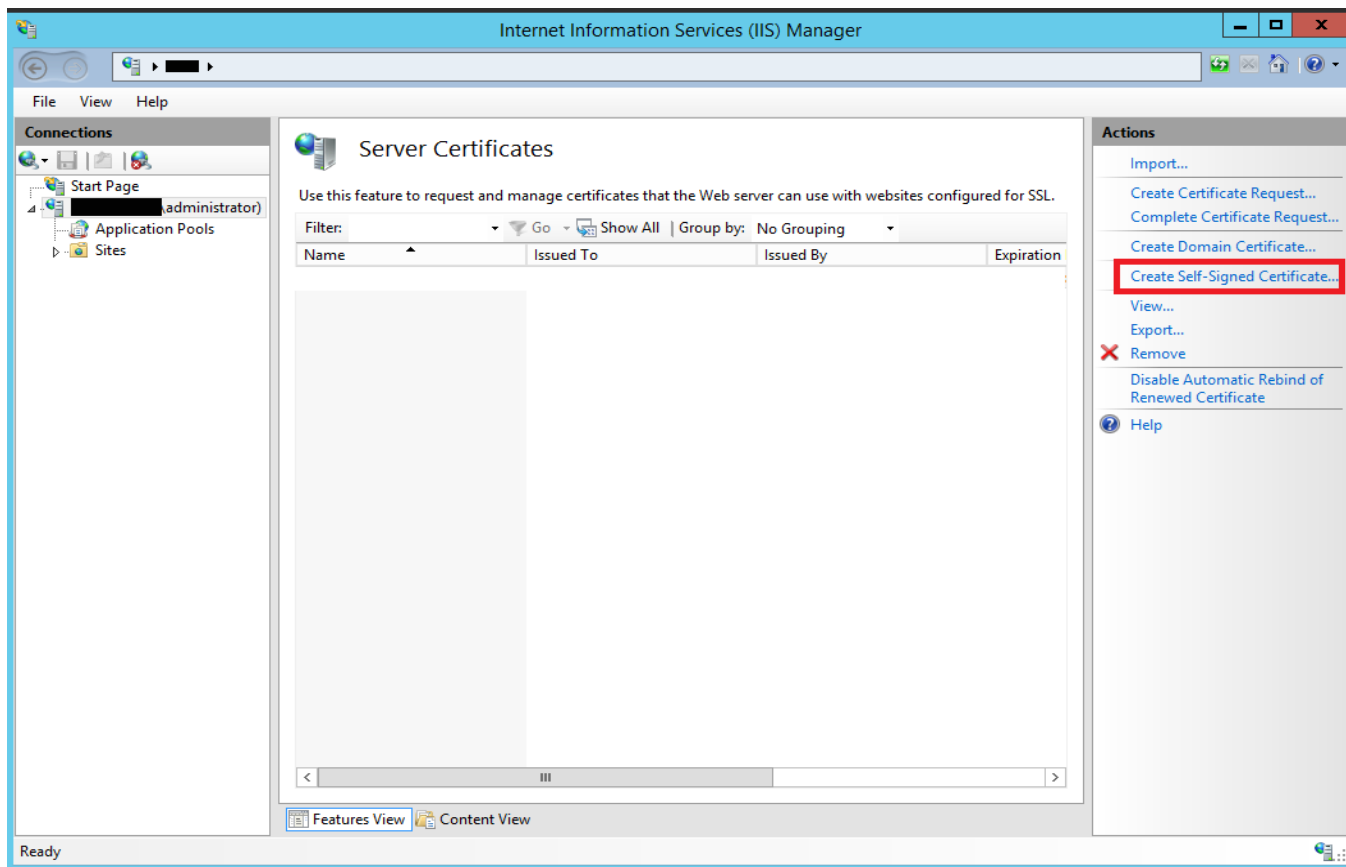
1. Click on the Windows icon in the taskbar, Search for IIS, and open Internet Information Services (IIS) Manager.



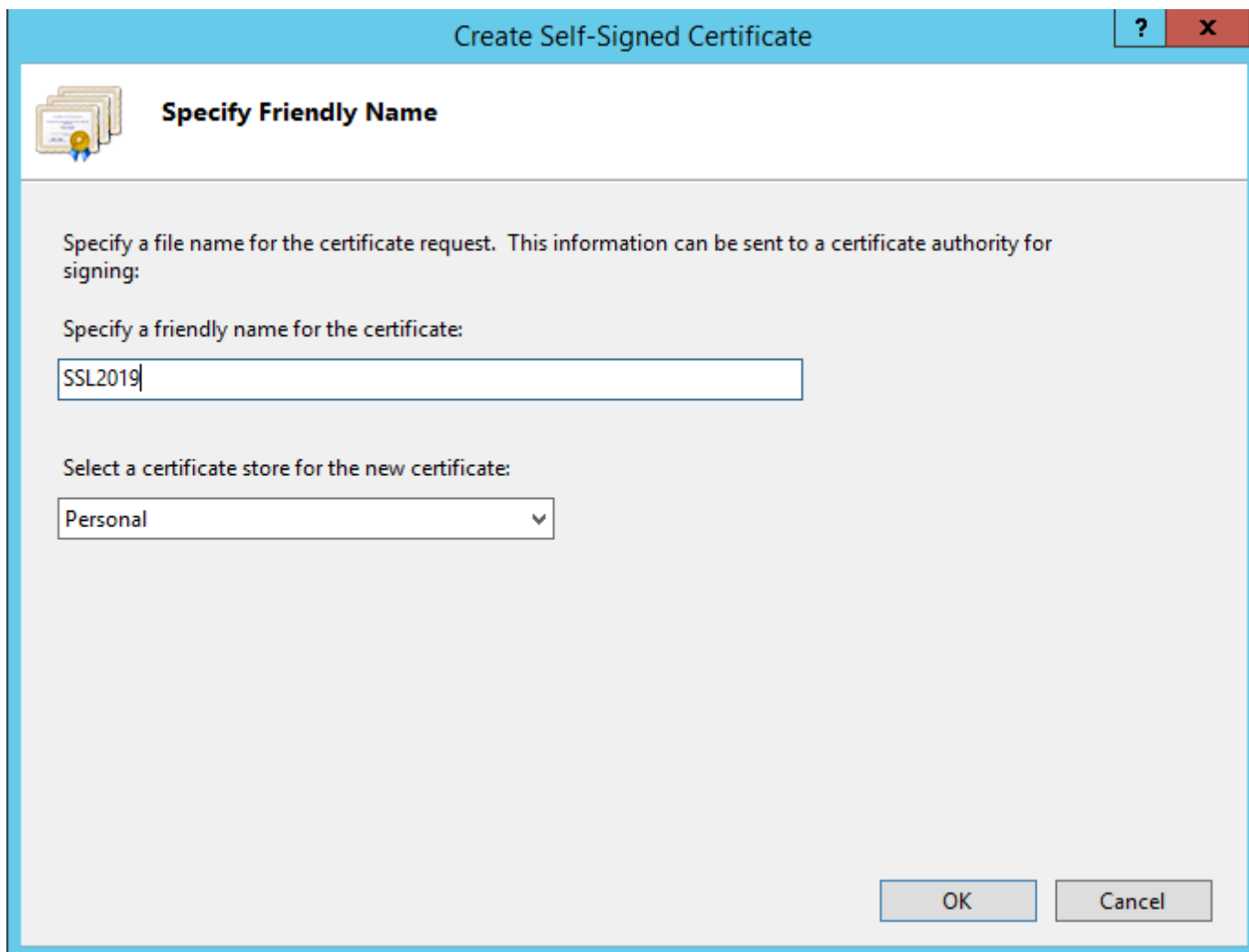
2. Click on the name of the server in the **Connections** column on the left. Double click the **Server Certificates** icon.



3. In the **Actions** column on the right hand side, click on **Create Self Signed Certificate**.



4. Enter the friendly name you wish to use to identify the certificate, and then click **OK**.



Create Self-Signed Certificate

Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

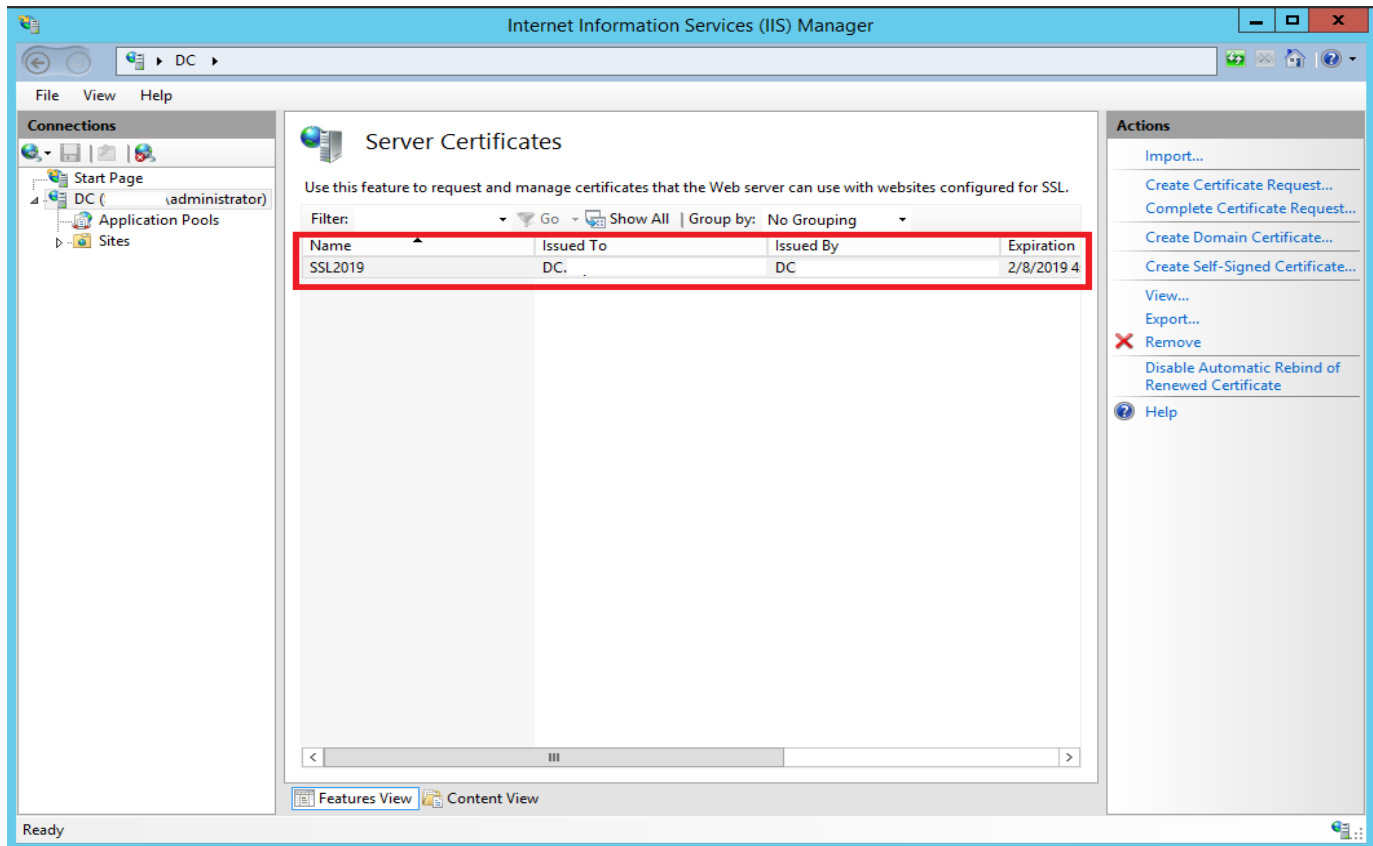
SSL2019

Select a certificate store for the new certificate:

Personal

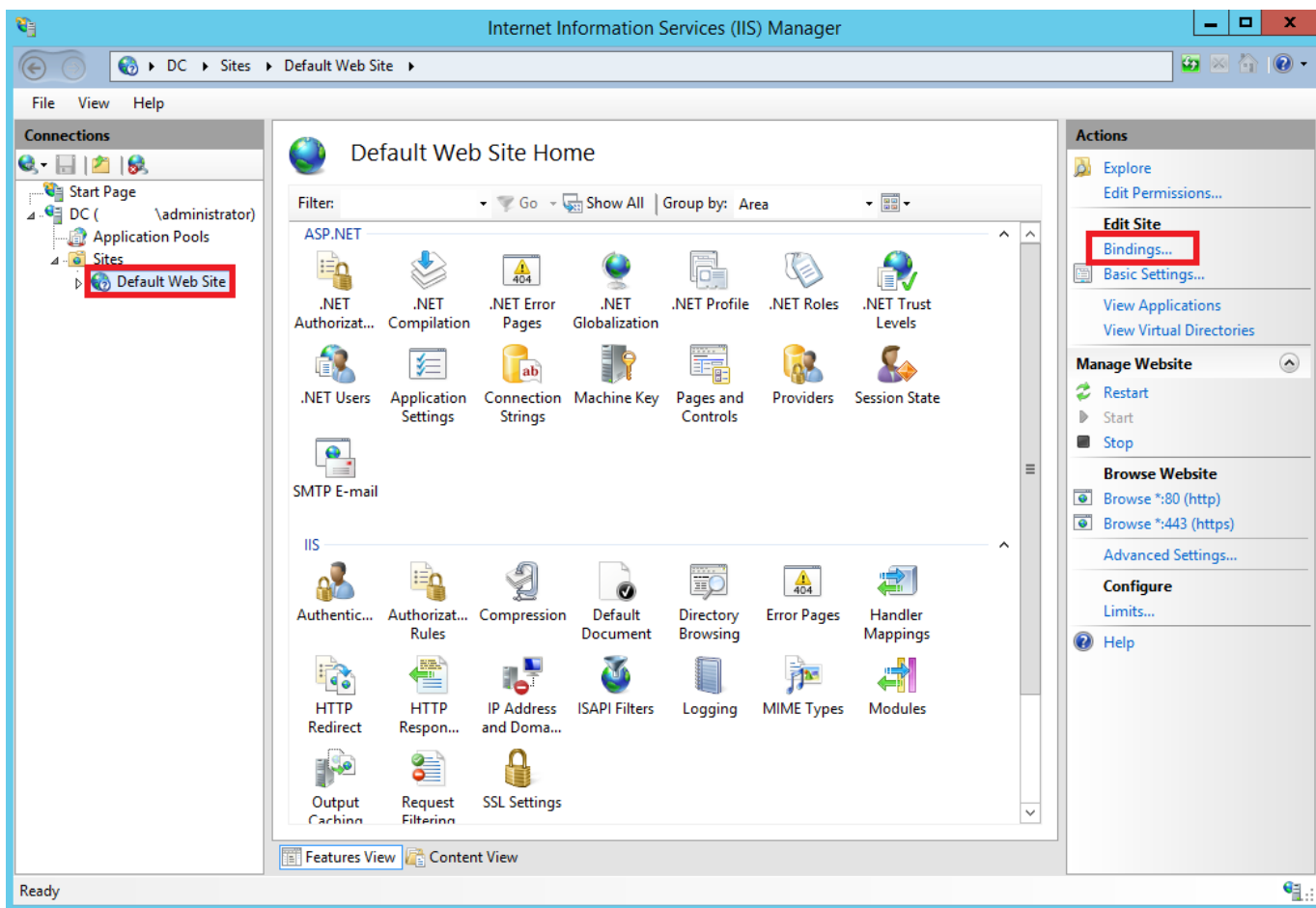
OK Cancel

5. You now have an IIS Self Signed Certificate, valid for one year, which will be listed under Server Certificates. The common name, is the server name.

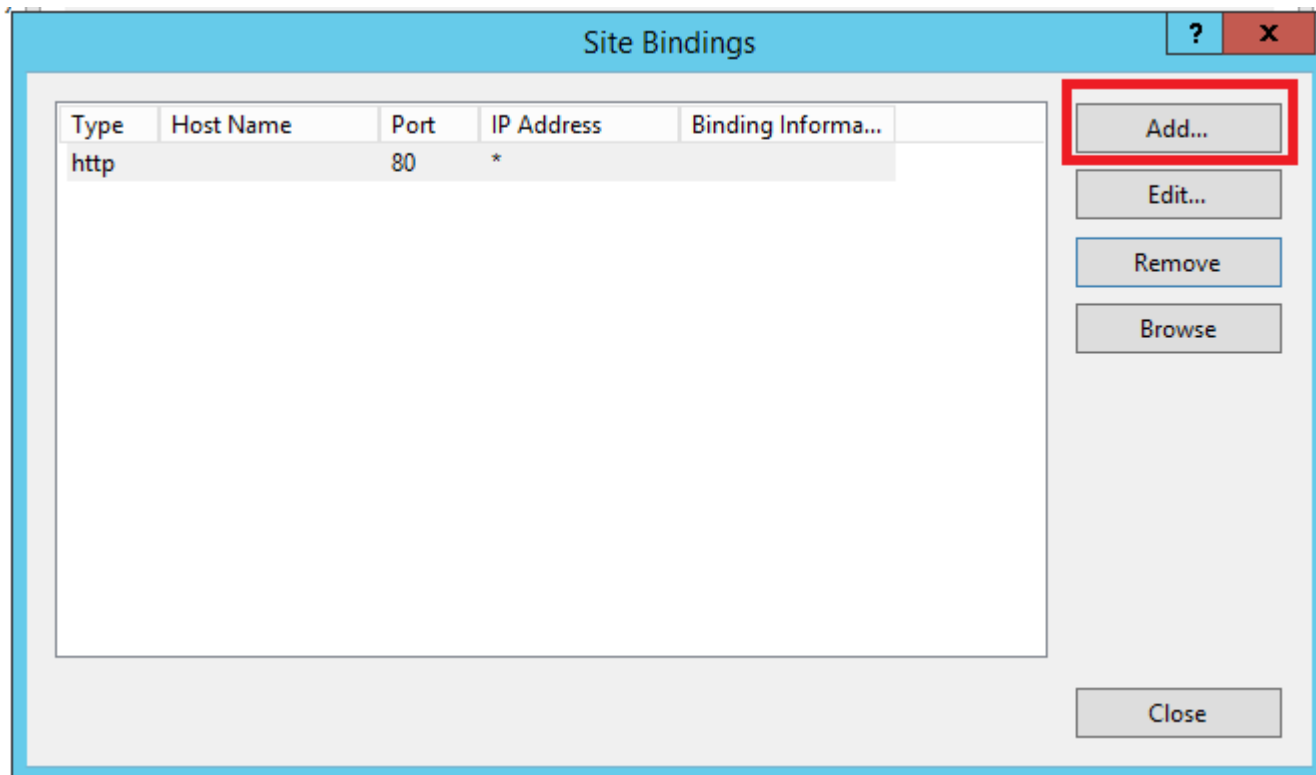


How to Bind the Self Signed Certificate

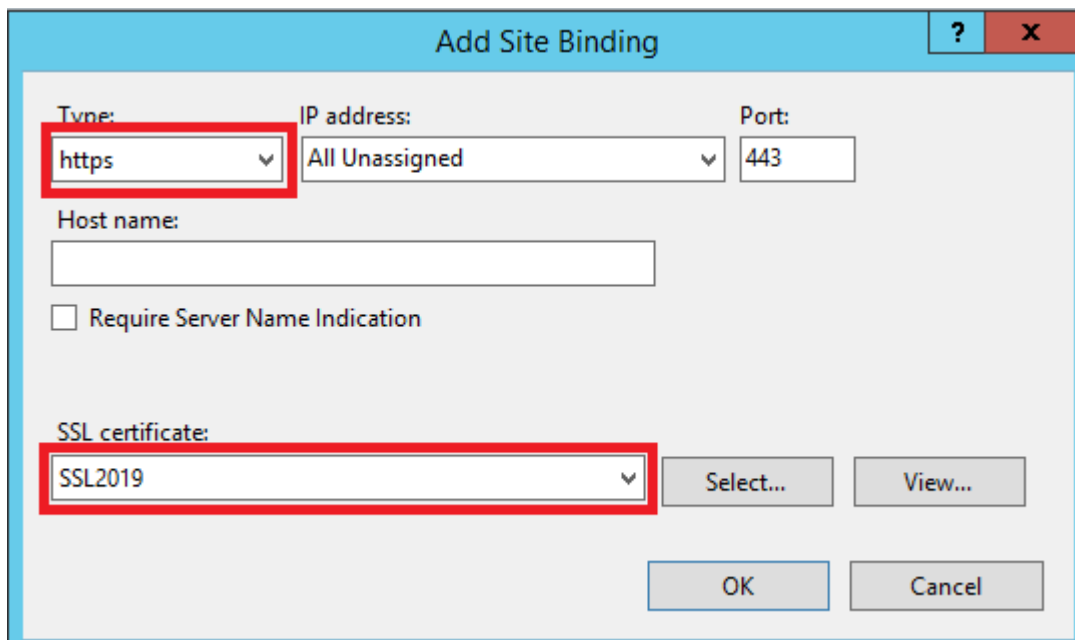
1. Browse to the connections column on the left hand side, expand the sites folder and click on the website you wish to bind the SSL certificate to. Once you've done that, on the right hand side, click on **Bindings** in the Actions column.



2. Click the **Add..** button.



3. Click the **Type** drop down menu. Select **https** . Click on the SSL Certificate drop down, choose the newly created SSL certificate. Click **OK**.



The 'Add Site Binding' dialog box is shown. It has a title bar with a question mark and a close button. The 'Type' dropdown is set to 'https' and is highlighted with a red box. The 'IP address' dropdown is set to 'All Unassigned'. The 'Port' field is set to '443'. The 'Host name' field is empty. The 'Require Server Name Indication' checkbox is unchecked. The 'SSL certificate' dropdown is set to 'SSL2019' and is highlighted with a red box. There are 'Select...' and 'View...' buttons next to the 'SSL certificate' dropdown. At the bottom are 'OK' and 'Cancel' buttons.

Type: **https** IP address: All Unassigned Port: 443

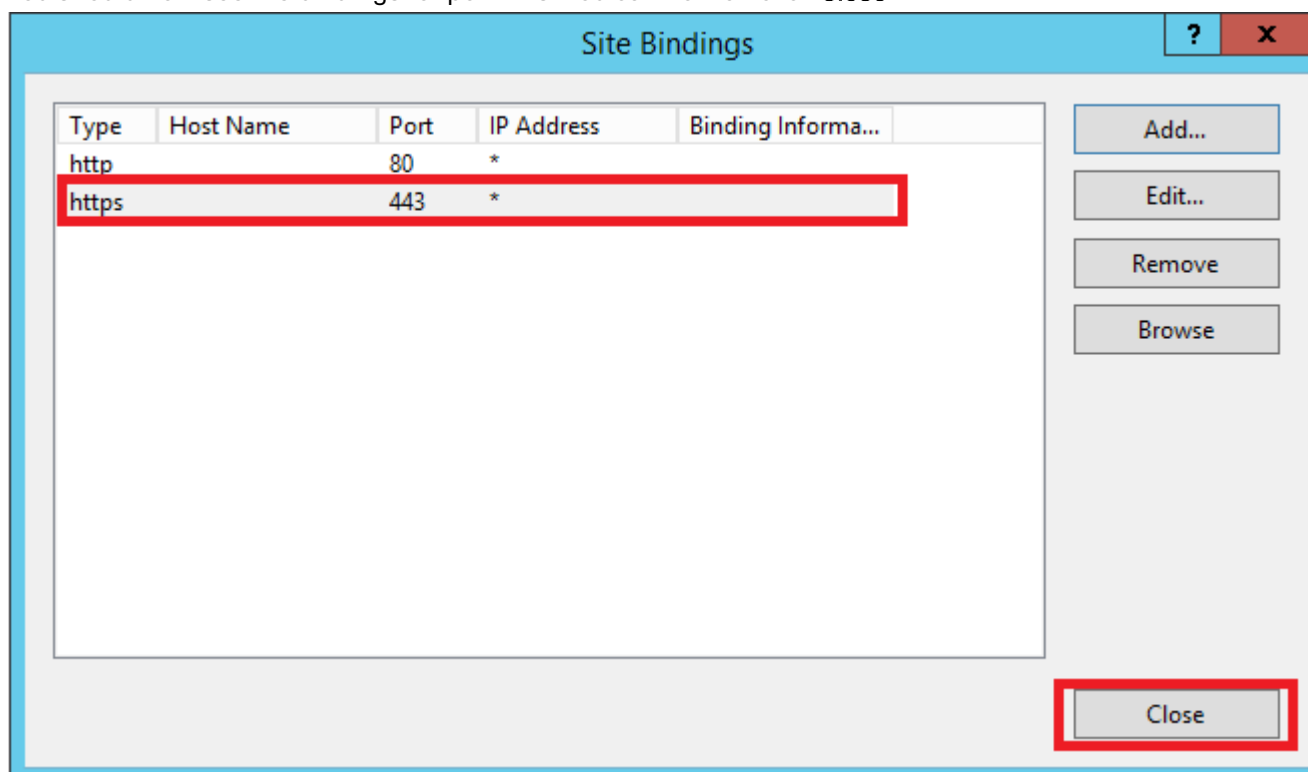
Host name:

☐ Require Server Name Indication

SSL certificate: **SSL2019** Select... View...

OK Cancel

4. You should now see the bindings for port 443. You can now on click **Close**.



The 'Site Bindings' dialog box is shown. It has a title bar with a question mark and a close button. It contains a table with the following data:

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

The 'https' row is highlighted with a red box. To the right of the table are buttons: 'Add...', 'Edit...', 'Remove', and 'Browse'. At the bottom right is a 'Close' button, which is highlighted with a red box.

Site Bindings

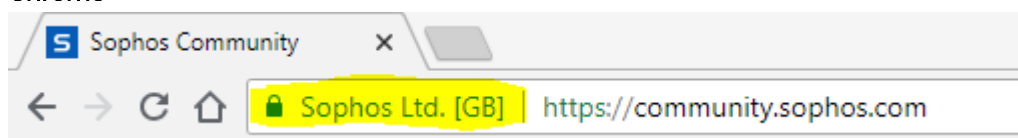
Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Add... Edit... Remove Browse

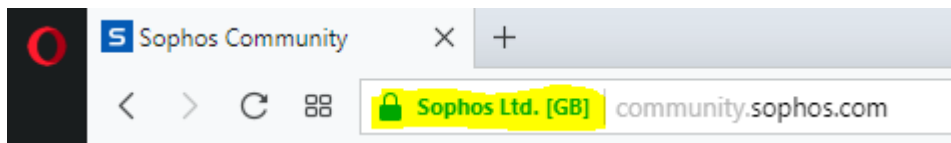
Close

5. To test the new Self Signed SSL Certificate, open up a browser, and go to the website. If the certificate has been installed and created correctly, depending on the browser you are using, you will see a green lock icon next to the URL, or it will say **Secure**. This is an example of how it would look in Google Chrome.

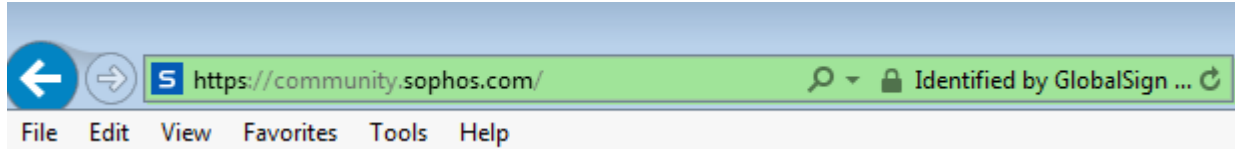
- **Chrome**



- **Opera**



- Internet Explorer



Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[General](#)

[SafeGuard encryption](#) > [Sophos SafeGuard Disk Encryption](#)

[SafeGuard encryption](#) > [Enterprise](#)

[SafeGuard encryption](#) > [General](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for **paid/licensed** products [open a support ticket](#).