User Guide

Configuring an SSL Certificate for Valerus

XX285-97-01

Document Number: 8009-8285-97-01 Rev: 8/21
Product specifications subject to change without notice

Vicon Industries Inc.
Tel: 631-952-2288) Fax: 631-951-2288
Toll Free: 800-645-9116
24-Hour Technical Support: 800-34-VICON
(800-348-4266)

General

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a web server and a client, creating a secure connection. An SSL certificate binds the domain owner and an organizational identity and, therefore, secures the connection between the web server and the web browser.

There are two types of SSL certificates, a self-signed certificate and a formal (trusted) CA certificate. Both certificates provide data encryption. The main difference is that a self-signed certificate is free and means the certificate is signed by the same individual whose identity it certifies; a CA certificate is issued by a trusted Certificate Authority that has verified the identity of the server, and there typically is a cost involved for it. Some trusted Certificate Authorities are DigiCert, GoDaddy, Verisign, but there are others as well. When a certificate is successfully installed on the server, the application protocol (HTTP) will allow changing to HTTPS, where the "S" stands for secure, and the web browser will show the secure session icon (this is different for each browser).

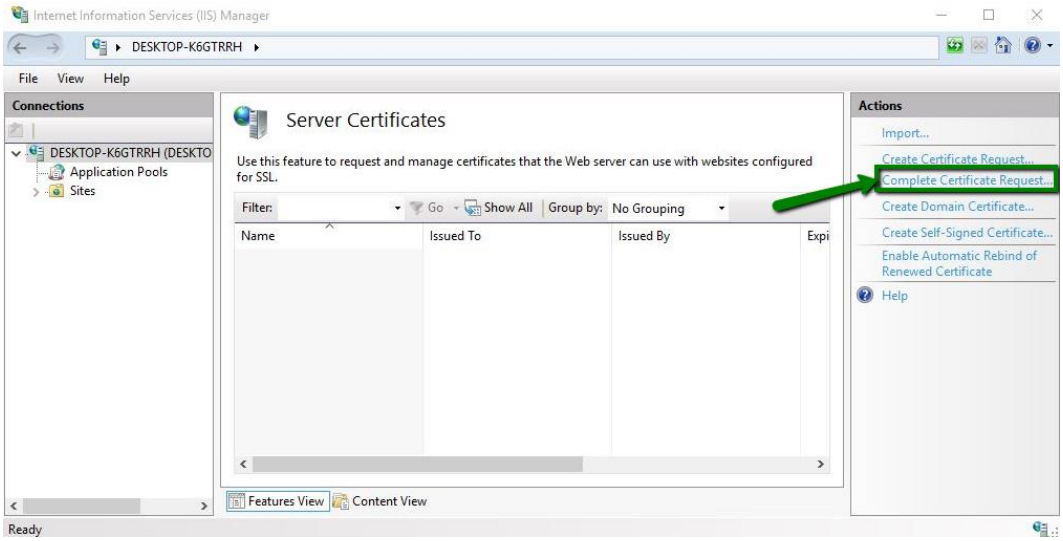
By default, Valerus installs a self-signed certificate. If a CA is necessary for your organization, it must be created as a Microsoft® IIS10 version. The steps to add a CA to an Application Server are below. If a CA is required for a Valerus Internet Gateway, follow the second set of steps.

Adding the SSL to the Valerus Application Server

After obtaining your own SSL Certificate, the Valerus web server that is running on the Application Server will need to be updated in order to stop using the default self-signed certificate and use this new one.

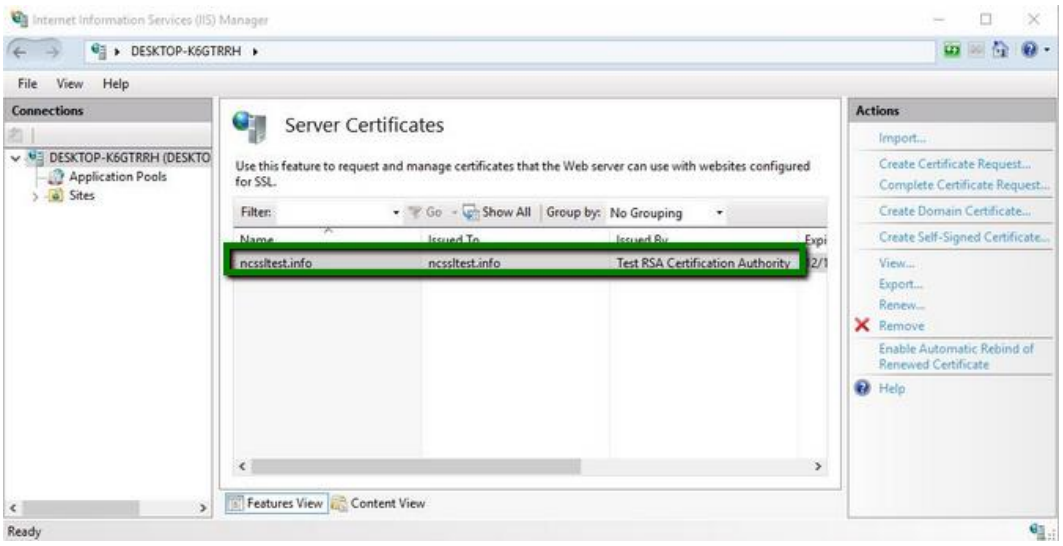
How to Upload Your SSL Certificate

1. Press **Win + R**; in the pop up window that displays, type in "***inetmgr***" to run the Internet Information Services (IIS) Manager.
2. On the IIS Manager home page, locate the **Server Certificates** icon and double-click it.
3. Locate the **Actions** panel on the right side and click **Complete Certificate Request**.



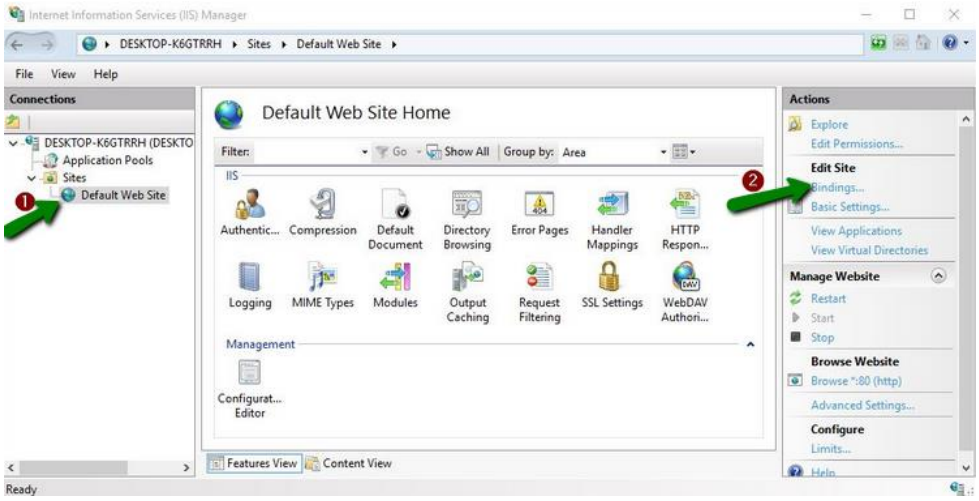
4. In the **Specify Certificate Authority Response** window, perform the actions below:
   a) In the **File name containing the certification authority's response** field, browse the file system to select the .p7b (or .cer) certificate you obtained.
   b) In the **Friendly name** field, specify any name that will help you to identify the certificate among other files. It is best to submit the actual domain name of the certificate.
   c) In the **Select a certificate store for the new certificate** field, leave the default value **Personal**.

5. Click **OK** to import the certificate to the server storage.
6. Once the import is complete, you will see a new entry associated with the imported certificate in the **Server Certificates** window.

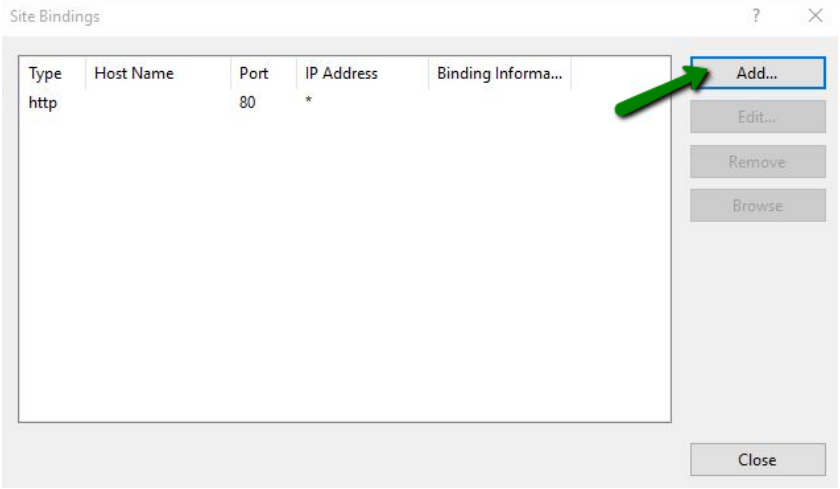


How to Bind the Certificate to the Valerus Website

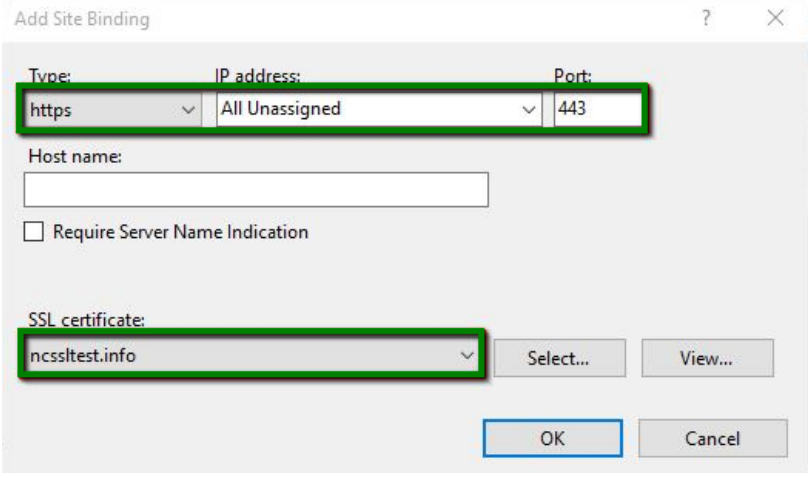
1. To assign the certificate to your Valerus website, continue to expand the **Sites** subsection in the **Connections** menu on the left and select the corresponding site. Then, in the **Actions** panel on the right side, locate the **Edit Site** menu and select the **Bindings** option.



2. On the right side of the **Site Bindings** window, click Add.

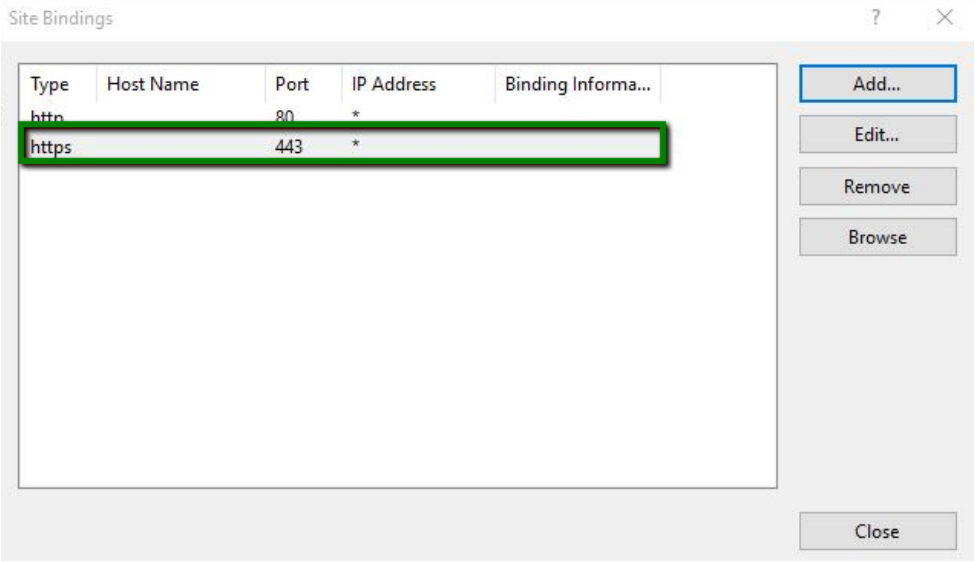


3. In the **Add Site Binding** window, modify the fields as below:
   a) In the **Type** field, select ***https***.
   b) In the **IP address** field, select your website's IP address or **All Unassigned**.
   c) In the **Port** field, specify ***443*** (default).
   d) In the **SSL certificate** field, select the previously imported certificate, which can be identified by the Friendly name.



Note: The **Require Server Name Indication** box needs to be checked if there are multiple SSL certificates on the server.

4. Click **OK** in order for the new **https** entry to appear in the **Site Bindings** window.



The certificate should now be installed, and the website should be accessible via HTTPS.

Installing the SSL on the Internet Gateway

If your system is using the Valerus Internet Gateway service in order to connect it to the Internet or another network, follow the additional steps below to allow browsing through the Internet Gateway using SSL.

This guide assumes the Valerus Internet Gateway has been set up and is working properly using the default ports as specified in the Internet Gateway manual. If the ports have been changed, make sure to use the new port numbers accordingly.

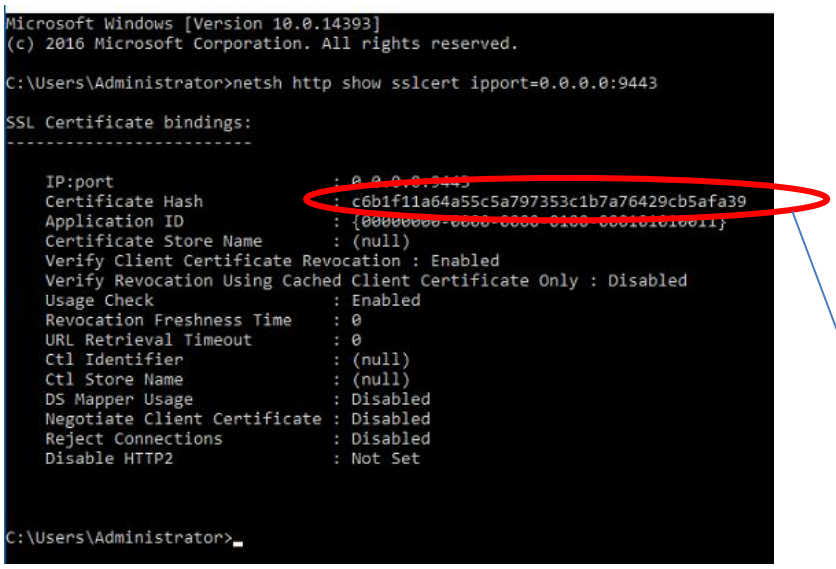
How to Bind the Internet Gateway

Once the SSL certificate is uploaded in the Application Server, user with admin rights must execute the commands below from an elevated command prompt on the Internet Gateway server (typically same server as the Application Server but may be on a separate one).

Show the existing SSL certificate associated with port number 9443:

```
Netsh http show sslcert ipport=0.0.0.0:9443
```

Take note of the certificate hash key, which will be entered in a later command. See example below:



Delete the existing SSL certificate associated with port number 9443.

Netsh http delete sslcert ipport=0.0.0.0:9443

Add/register the new SSL certificate associated with port number 9443

Netsh http add sslcert ipport=0.0.0.0:9443 certhash= "Insert Certificate Hash Key from the Show command here without quotes" appid={00000000-0000-0000-0100-000101010011} clientcertnegotiation=disable

VICON INDUSTRIES INC.

For office locations, visit the website: vicon-security.com