User Guide



Configuring an SSL Certificate for Valerus

XX285-97-01



Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.

Document Number: 8009-8285-97-01 Rev: 8/21 Product specifications subject to change without notice Copyright © 2021 Vicon Industries Inc. All rights reserved. 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

- 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.

internet Information Services (IIS) I	Manager				- 🗆 ×
C DESKTOP-K6GTF	≀RH ▶				🔯 🖂 🟠 🔞 -
File View Help					
Connections		rtificator			Actions
2	Server Ce	Import			
DESKTOP-K6GTRRH (DESKTO Application People	Use this feature to reque	Create Certificate Request			
> i Sites	for SSL.				Complete Certificate Request
	Filter:	🕶 🍸 Go 🕞 🙀 Show All 🛛 Group b	iy: No Grouping 🔹	-	Create Domain Certificate
	Name	Issued To	Issued By	Expi	Create Self-Signed Certificate
					Enable Automatic Rebind of Renewed Certificate
					🔮 Help
< >>	< Features View Cor	ntent View		>	
Keady					V <u>i</u> .:

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**.

complete a previously created certil esponse.	ficate request by retrieving	the file that contains the	certificate authority's	
ile name containing the certificatio	on authority's response:			
:\ncssItest_info.cer	32			
riendly name:	-			
cssitest.info				
elect a certificate store for the new	certificate:			
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.

File View Help					
onnections		ortificator		Actions	
	Server Certificates				time
DESKTOP-K6GTRRH (DESKTO Desktop Pools Stars	Use this feature to requise for SSL.	ured Create Comp	Certificate Request lete Certificate Request		
/ W Sites	Filter	🔹 🐨 Go 🕘 🖓 Show All 🛛 Gr	oup by: No Grouping 🔹	Create	Domain Certificate
	Name	Issued To	Jesuert Ru	Expi Create	Self-Signed Certificate
	ncssitest.info	ncssItest.info	Test RSA Certification Authorit	/1 View	Au
				Export.	
				Renew	here -
				× Remov	/e
				Enable Renew	Automatic Rebind of red Certificate
				😯 Help	
	٢.			>	
1	Concerning of the local division of the loca				

How to Bind the Certificate to the Valerus Website

 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.

Onnections Default Web Site Home DESERVOr-K6GTRRH (DESKTO	Actions Explore Edit Permissions
DEFAULT WED Site Home Desktop-k66TRRH (DESKTO Application Pools Sites	Explore Edit Permissions
DESKTOP-K6GTRRH (DESKTO Application Pools Sites IIS IS	Edit Permissions
Application Pools Sites IIS	
🕒 🔮 Default Web Site 🔣 🦿 🦓 👌 📅 🛕 📰 🐴	Edit Site Bindings Basic Settings
Authentic Compression Default Directory Error Pages Handler HTTP Document Browsing Mappings Respon	View Applications View Virtual Directories
Logging MIME Types Modules Output Request SSL Settings WebDAV Authori	Manage Website
Management	Browse Website Browse ":80 (http)
Editor	Advanced Settings Configure

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

ype	Host Name	Port	IP Address	Binding Informa	Add
ittp		80	^	-	Edit
					Remove
					Browse

- 3. In the **Add Site Binding** window, modify the fields as below:
 - a) In the **Type** field, select *https*.

Cian Disultanea

- 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.

nttps	~	All Unassigned	~ 443	1
lost name:				
20072102				
Denvine C	N	- I - I' - I'		
Require 3	erver Marr	ne indication		
) Require :	erver Nam	ne indication		
L certifica	erver Nam te: o	ne indication	Select	View

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.

/pe	Host Name	Port	IP Address	Binding Informa	Add
ttn		80	*		Edit
ttps		443	*		Cut
					Remove
					Browse

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:

C:\Users\Administrator>netsh htt	p show sslcert ipport=0.0.0.0:9443	
SSL Certificate bindings:		
IP:port	: A A C 0.0145	
Certificate Hash	: c6b1f11a64a55c5a797353c1b7a76429cb5afa39	
Application ID	: {0000000-0000-0000-0100-00010100011}	
Certificate Store Name	: (null)	
Verify Client Certificate Re	vocation : Enabled	
Verity Revocation Using Cach	t Emphlod	
Povocation Enachnoss Time	· A	
URL Retrieval Timeout	- 0	
Ctl Identifier	: (null)	
Ctl Store Name	: (null)	
DS Mapper Usage	: Disabled	
Negotiate Client Certificate	: Disabled	
Reject Connections	: Disabled	
Disable HTTP2	: Not Set	
Disable HTTP2	: Not Set	

- 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={00000000-0000-0100-00010101011} clientcertnegotiation=disable



VICON INDUSTRIES INC.

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

