

How to Enable HTTPS on EKI-152x & EKI-122x Series

For Firmware Version: • EKI-1521/2/4: v1.21 or later • EKI-1221/2/4: v1.09 or later

Calvin Lin, PAE, Advantech

Edge Computing WISE-Paas WISE-Paas WISE-Marketplace WISE-Marketplace WISE-DeviceOn WISE-DeviceOn Design-in Solution Suite AIFS A XNavi InsightAPM & InsightAPM

Introduction

• HTTPS with Certificates:

- 1. The HTTPS is a more secure way to access a website, with the communication content encrypted. The encryption is done by using correct certificates.
- 2. For EKI-122x/152x series supports HTTPS function, but the certificates required are not built-in by default. Users will need to import corresponding certificate files to the device to correctly enable the HTTPS function.
- 3. Firmware Version:
 - · EKI-1521/2/4: v1.21 or later
 - · EKI-1221/2/4: v1.09 or later
 - * HTTPS function currently only on models with lower port numbers. For standard 8 & 16 port model, currently not supported.
 - **With Encryption by Certificates, the system would require around 80s to collect sufficient "entropy" to fully boot up after powered/rebooted.



Generate the Certificates by EKI Utility on Windows (1/5)

- Download OpenSSL for Windows
 - EKI Utility version should be v3.07 or later to support this function.
 - Go to website for the OpenSSL installation file, and install it to the computer:

https://slproweb.com/products/Win32OpenSSL.html

File	Туре	Description
Win64 OpenSSL v3.1.4 Light <u>EXE MSI</u>	5MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v3.1.4 (Recommended for users by the creators of <u>OpenSSL</u>). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v3.1.4 EXE <u>MSI</u>	140MB Installer	Installs Win64 OpenSSL v3.1.4 (Recommended for software developers by the creators of <u>OpenSSL</u>). Only installs on 64-bit versions of Windows and targets Intel x64 chipsets. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.1.4 Light <u>EXE</u> <u>MSI</u>	4MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v3.1.4 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v3.1.4 EXE <u>MSI</u>	I I 6MB Installer	Installs Win32 OpenSSL v3.1.4 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

Generate the Certificates by EKI Utility on Windows (2/5)

Check System Settings

• Right click on "This PC" to find option "Properties".

(This Step is to open up System page in the Control Panel. Other approach would also do.)





Generate the Certificates by EKI Utility on Windows (3/5)

Advanced System Settings

- In System page, click on the Advanced System Settings to check it.
- Go to tab "Advanced", and click the button "Environment Variables..." for further editing.

System		
🗧 🔶 🕤 🛧 🖳 > Contr	rol Panel	
Control Panel Home	System Properties	×
 Device Manager Remote settings 	Computer Name Hardware Advanced System Protection Remote You must be logged on as an Administrator to make most of these changes Advanced System Protection Remote	2
 System protection Advanced system settings 	Performance Visual effects, processor scheduling, memory usage, and virtual memory Settings	1
	User Profiles Desktop settings related to your sign-in Settings	_
	Startup and Recovery System startup, system failure, and debugging information Settings	
	Environment Variables]
	OK Cancel Apply	



Generate the Certificates by EKI Utility on Windows (4/5)

• Modify Environment Variable

• Select "Path" in the System Variables for Edit, and click "New" to add path inside.

Path adding: C:\Program Files\OpenSSL-Win64\bin

			-
		C:\Program Files\Eclipse Adoptium\jdk-8.0.362.9-hotspot\bin	New
ser variables for Audrev.Wa	na	C:\TwinCAT\Common64	1
		C:\TwinCAT\Common32	Edit
Variable	Value	%SystemRoot%\system32	
OneDrive	C:\Users\	%SystemRoot%	Browse
OneDriveConsumer	C:\Users\	%SystemRoot%\System32\Wbem	
Path	C:\Users\	%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\	Delete
TEMP	C:\Users\	%SYSTEMROOT%\System32\OpenSSH\	
TMP	C:\Users\	C:\Program Files (x86)\nodejs\	
	and the second second	C:\Program Files\dotnet\	Move Up
		C:\Program Files\Microsoft SQL Server\130\Tools\Binn\	
ystem variables			Edit text
ariable	Value		
NUMBER OF PROCESSOR	\$ 8		
OS	Windows		
Path	C:\Progr		
PATHEXT	.COM;.EX		
PROCESSOR_ARCHITECTU	JRE AMD64		
PROCESSOR_IDENTIFIER	Intel64 Fa	ОК	Cancel
PROCESSOR LEVEL	6		
		New Edit Delete	



Generate the Certificates by EKI Utility on Windows (5/5)

• Generate the Certificates by EKI Utility

- After adding the Environment Variable, start EKI Utility and go to Create CA under Tools.
- Select the folder to store the generated certificate files.

File View Management	Tools Help		
🔊 🔼 🐋 💽 🔍	Simple Serial Test		
	Create CA	瀏覽資料夾	\times
🖃 📑 EKI Device		<u>a</u>	
RootCA			
Create new RootCA	L	> 3D Models	1
	Select PEM	> Calvin	
	Select KEY	✓ Cert-test_Calvin	
		→ 20210421_解決EKI-6333無法認證問題	
Server —		> 20210510_ClientCerts	
Create new Server (CA	20210909_ValidDateLonger	
Name server		> 20211004_CA-BitLength4096	
		20211021_FromTablet	
Client		20230830_Cert新建	
Create new Client C	CA	20231117_Certs_for_EKIUtility	
Name client		< >>	
		建立新資料夾(M) 確定 取消	
	OK Cancel		

AD\AN'

Generate the Certificates by VCOM-Driver on Ubuntu

• VCOM Driver with OpenSSL embedded

- VCOM Driver version should be v2.2.3 or later to support this function.
- Using command below to create related certificates:

#sudo adv-eki-tls-create -n eki1234abcd

Certificate File Name

- Default RootCA file will be created during the process, if it was not there before.
- Sample as the screenshot on the right. Users will need to input some information during the creating of the certificate files, such as Country Name, Organization Name, password, etc.
- Users can edit the /usr/local/advtty/ssl.json to customize the files:
 - Password, file path of the RootCA public key, and the key pair can be customized in this file.

	root@calvin-VirtualBox:/home/calvin# adv-eki-tls-create -n eki1234abcd
	public key /usr/local/advtty/rootCA.pem found.
	private key /usr/local/advtty/rootCA.key found.
	serial /usr/local/advtty/rootCA.srl found.
	Generating DH parameters, 1024 bit long safe prime, generator 2
	This is going to take a long time
	+
	+.
	+
	Can't load /root/.rnd into RNG
ate	140351476867520:error:2406F079:random number generator:RAND_load_file:Cannot ope
ne	n rile:/crypto/rand/randrile.c:88:rilename=/root/.rnd
	into your certificate request.
	What you are about to enter is what is called a Distinguished Name or a DN.
	There are quite a few fields but you can leave some blank
	For some fields there will be a default value,
	If you enter '.', the field will be left blank.
	Country Name (2 letter code) [AU]:TW
	State or Province Name (full name) [Some-State]:Taipei
、 <i>,</i>	Locally Name (eg, clly) []:Talpel Organization Name (eg. company) [Internet Widgits Pty Ltd]:Advantech
У	Organizational Unit Name (eq. section) []:ICG
	Common Name (e.g. server FODN or YOUR name) []:calvin
	Email Address []:calvin.lin@advantech.com
	Please enter the following 'extra' attributes
	to be sent with your certificate request
	A challenge password []:whatever
	An optional company name []:
	Writing FC key
	Copy the following files to the corresponding EKI device server
	the second s

Certificate File for HTTPS

key-pair(pub/priv): eki1234abcd.pem diffi-hellman: eki1234abcd_dh1024.pem rootCA: /usr/local/advtty/rootCA.pem

Upload the Certificates to EKI Device

- Service / Web Server
 - 1. Change the HTTPS support option to Enable. This enable the HTTPS function on EKI, while the HTTP still available.
 - 2. Select the created certificate file and upload. File should be used: *.pem
 - Use the same file for **both**, ex. client.pem, and upload it to both "Certificate" and "Private Key".
 - 3. Click the Save button below to store the configuration, and reboot.





Co-Creating the Future of the IoT World

