



# HTTPS Certificate Creation Manual

Version: 0.0.0  
Release date: February 7, 2014

© 2011 - 2014 Fanvil Co., Ltd.

This document contains information that is proprietary to Fanvil Co., Ltd (Abbreviated as Fanvil hereafter).  
Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

**Specifications are subject to change without notice.**

**Liability Disclaimer**

Fanvil may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked as reserved or undefined. Fanvil reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Fanvil sales office or your distributor to obtain the latest specification and before placing your product order.

fanvil file, forbidden to steal!

## Table of Contents

---

<b>Table of Contents</b> .....	<b>3</b>
<b>1 Revision History</b> .....	<b>4</b>
<b>2 Introduction</b> .....	<b>5</b>
2.1 Overview.....	5
2.2 Target Audience.....	5
<b>3 OpenVPN Server's Download And Installation</b> .....	<b>6</b>
<b>4 Server Configuration</b> .....	<b>7</b>
4.1 Initiation.....	7
4.2 Certificate Creation.....	7
<b>5 Generate HTTPS Certificate</b> .....	<b>10</b>
<b>6 Use HTTPS Certificate</b> .....	<b>11</b>
6.1 Upgrade HTTPS Certificate.....	11
6.2 Set HTTPS Web Type.....	11
6.3 Logon HTTPS Web Server.....	12

fanvil file, forbidden to steal!

## 1 Revision History

---

Revision history:

Revision	Author	Date	Description
0.0.0	Song Jupo	February 7, 2014	Initial version

## 2 Introduction

---

### 2.1 Overview

HTTPS is a secure transport protocol with ssl encryption, which supports data encryption and authentication, so it is more secure than HTTP Protocol. The protocol can establish a secure channel of information, all data submitted will be encrypted before submission, thus to ensure the security of data transmission.

Before using phone Web's HTTPS, you need to install HTTPS certificate.

Phone models that support HTTPS:

- ◆ C58/C60/C62/F66
- ◆ E01/E52/E58/ E62/E66
- ◆ F01/F52/F58/ F62/F66

### 2.2 Target Audience

This document's target audience are internal staffs and customers that want to use Web HTTPS.

## 3 OpenVPN Server's Download And Installation

---

Search and download the Windows version of the OpenVPN software on the Internet. Double click the downloaded software, and install it with default settings, the default install path is C:\Program Files\OpenVPN.

fanvil file, forbidden to steal!

## 4 Server Configuration

### 4.1 Initiation

Before using HTTPS, we should do some initialization work.

Open document C:\Program Files\OPENVPN\easy-rsa\vars.bat.sample, the following part need to be modified.

```
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=FortFunston
set KEY_EMAIL=mail@domain.com
```

(Please change settings according to your own situation):

```
set HOME=C:\Program Files\OPENVPN\easy-rsa
set KEY_COUNTRY=CN                #(Country)
set KEY_PROVINCE=BEIJING          #(Province)
set KEY_CITY=BEIJING              #(City)
set KEY_ORG=WINLINE               #(Organization)
set KEY_EMAIL=admin@winline.com.cn #(Email)
```

Everything after # are comments, please don't write file.

Then enter the command line (Start > Run - > CMD into DOS):

Enter directory of openvpn\easy-rsa.

Execute follow commands:

**init-config**

**vars**

**clean-all**

Note: The above is the initialization work, after the initialization, when you want to create certificate, you still need to initialize, but only need to enter the openvpn\easy-rsa directory, and run vars only, do not need run all of those steps. (If your server has been built, then make HTTPS certificate from this step).

### 4.2 Certificate Creation

#### Generate the root CA:

Input command "**build-ca**" and press Enter key.

```
Country Name (2 letter code) [CN]:                # (Can not fill)
State or Province Name (full name) [BEIJING]:      # (Can not fill)
Locality Name (eg, city) [BEIJING]:                # (Can not fill)
Organization Name (eg, company) [WINLINE]:         # (Fill your own info)
Organizational Unit Name (eg, section) []:unit1    # (Fill your own info)
Common Name (eg, your name or your server's hostname) []:admin # (Fill your own info)
Email Address [admin@winline.com.cn]:              #( Common Name@ Organization Name.com)
```





Organization Name (eg, company) [WINLINE]: # (Consistent with the root CA)  
 Organizational Unit Name (eg, section) []:unit1 # (Fill your own info)  
 Common Name (eg, your name or your server's hostname) []: adminServer # (Fill your own info)  
 Email Address [admin@winline.com.cn]: # (Can be different)  
 Please enter the following 'extra' attributes to be sent with your certificate request  
 A challenge password []:adminServer #(Fill your own info)  
 An optional company name []:winline #(Fill your own info)  
 Certificate is to be certified until Nov 24 06:24:34 2018 GMT (3650 days)  
 Sign the certificate? [y/n]:y #(Select 'y')  
 1 out of 1 certificate requests certified, commit? [y/n]y #(Select 'y')  
 The generated key stored in the openvpn\easy-rsa\keys directory.  
 As shown in Figure:

```

C:\Program Files\OpenVPN\easy-rsa>build-key-server server2
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\server2.key'
-----
You are about to be asked to enter information that will be incorporated
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) [CN]:
State or Province Name (full name) [BEIJING]:
Locality Name (eg, city) [BEIJING]:
Organization Name (eg, company) [WINLINE]:UOIP
Organizational Unit Name (eg, section) []:unit2
Common Name (eg, your name or your server's hostname) []:adminServer
Email Address [admin@winline.com.cn]:adminServer@UOIP.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:adminServer
An optional company name []:UOIP
Using configuration from openssl.cnf
Loading 'screen' into random state - done
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'BEIJING'
localityName      :PRINTABLE:'BEIJING'
organizationName  :PRINTABLE:'UOIP'
organizationalUnitName:PRINTABLE:'unit2'
commonName        :PRINTABLE:'adminServer'
emailAddress      :IA5STRING:'adminServer@UOIP.com'
Certificate is to be certified until Oct 28 06:19:55 2023 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
  
```

## 5 Generate HTTPS Certificate

---

Find server.key, server.crt files in the openvpn\easy-rsa\keys directory, then append server.key's content to the server.crt, after that you should rename server.crt to https.pem, https.pem is the HTTPS's certificate that we will use.

So far, HTTPS certificate is created.

## 6 Use HTTPS Certificate

### 6.1 Upgrade HTTPS Certificate

Logon the phone's Web, find SECURITY-SECURITY-Update Security File page, then click the Browse button and select the https.pem, click the Update button to upgrade.

As shown in Figure:

The screenshot shows the 'SECURITY' configuration page. The 'Update Security File' section contains a text input field for 'Select Security File', a 'Browse' button, and an 'Update' button. The 'Delete Security File' section contains a dropdown menu for 'Select Security File' with 'https.pem' selected and a 'Delete' button. Below these are sections for 'SIP TLS Files', 'HTTPS Files' (showing 'https.pem' with '(4576 Bytes)'), and 'OpenVPN Files'.

After the upgrade is complete, Delete Security File drop-down box and HTTPS FILES will show upgraded certificate file.

### 6.2 Set HTTPS Web Type

Find Webpage NETWORK-SERVICE PORT, then select Web Server Type to HTTPS and modify the HTTPS Port's value; After setting click the Apply button to submit and restart the phone.

As shown in Figure:

WAN	LAN	QoS&VLAN	SERVICE PORT	DHCP SERVICE	TIME&DATE
<b>Service Port Settings</b>					
Web Server Type		<input type="text" value="HTTPS"/>			
HTTP Port		<input type="text" value="80"/>			
HTTPS Port		<input type="text" value="443"/>			
Telnet Port		<input type="text" value="23"/>			
RTP Port Range Start		<input type="text" value="10000"/>			
RTP Port Quantity		<input type="text" value="200"/>			
<input type="button" value="Apply"/>					

If the phone is not restart, it will still use the original Web Server Type; HTTPS Web Server Type will take effect after phone restart.

### 6.3 Logon HTTPS Web Server

After the restart, the phone can use the new URL to logon. The new URL is https://Phone IP:HTTPS Port.