## Steps to follow to avoid certificate error when accessing Fortigate and firewall authentication using HTTPS.

You can avoid the Certificate Warning using the below mentioned procedure only for the HTTP to HTTPS Redirection Authentication Traffic. For this you can use the same *.example.com wildcard certificate which you had in your Local Certificate Store.

This example follows all the steps required to create and install a local certificate on the FortiGate unit, without using CA software.

**To generate a certificate request on the FortiGate unit - web-based manager**

**1.** Go to *System* > *Certificates* > *Local Certificates*.

**2.** Select *Generate*.

**3.** In the *Certificate Name* field, enter FGT.

---

Note:-

Do not include spaces in the certificate name. This will ensure compatibility of a signed certificate as a PKCS12 file to be exported later on if required.

---

Since the IP address is private, we will use the FQDN instead.

**4.** Select *Domain Name,* and enter fgt.example.com.

**5.** Enter values in the *Optional Information* area to further identify the FortiGate unit.

**Organization Unit -** Support

**Organization -** Example.com

**Locality (City) -** Bangalore

**State/Province -** Karnataka

**Country -** INDIA

**e-mail -** fgt@example.com

**6.** From the *Key Size* list, select *2048 Bit* or the most secure option available to you.

**7.** In *Enrollment Method*, select *File Based* to generate the certificate request

**8.** Select *OK*.

The request is generated and displayed in the *Local Certificates* list with a status of PENDING.

**9.** Select the *Download* button to download the request to the management computer.

**10.** In the *File Download* dialog box, select *Save* and save the Certificate Signing Request on the local file system of the management computer.

**11.** Name the file and save it on the local file system of the management computer.

**Generate and Import CA certificate using Microsoft CA**

**1.** Follow the below document for Active Directory Certificate Services Step-by-Step Guide

http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx

**2.** On AD server, open (https://servername/certsrv/) on browser.

**3.** Select "Request a Certificate" >> Advanced Certificate Request.

**4**. Edit and copy the csr file generated on Fortigate and paste it on "Base-64-encoded certificate request".

**5.** Select the Certificate Template as "Web Server" and select Submit.

**6.** Download the certificate.

**Import the SSL certificate into FortiOS To import the certificate to FortiOS- web-based manager**

**1.** Go to *System* > *Certificates* > *Local Certificates*.

**2.** Select *Import* > Local Certificate and choose the certificate file.

**3.** Select OK.

**On Fortigate CLI**

Configure Fortigate unit to use the newly imported certificate HTTPS admin access.

# config sys global
# set admin-server-cert <certificate_name>
# end

#config firewall policy
#edit <Authentication_Policy_ID>
#set auth-cert <certificate_name>
#set auth-redirect-addr "FGT.example.com"
#end

#config user setting
#set auth-cert <certificate_name>
#set auth-secure-http enable
#end

-- First you need to give the Hostname to your FortiGate unit on the Dashboard. For Example : FGT

-- After this you need to create a Host and Pointer Record in your Internal DNS Server for the full FQDN like FGT.example.com which should resolve IP Address of your FGT Internal Interface.

-- The DNS Resolution from Hostname FGT.example.com to IP (Internal Interface IP) should happen from all the Client Systems and FGT CLI.

-- Please make sure FGT is able to resolve ip to hostname and hostname to ip.

**On PC Browser**

Add the CA certificate on browser.

When you access Fortigate using HTTPS with domain name (https://fgt.example.com), the users will get the login prompt without certificate error.

You can avoid the Certificate Warning using the below mentioned procedure only for the HTTP to HTTPS Redirection Authentication Traffic. For this you can use the same *.example.com wildcard certificate which you had in your Local Certificate Store.

When identity based authentication is enabled, when user access HTTPS sites, Fortigate will redirect to https://fgt.example.com:1003 without Certificate Warning.