SANGFOR

NGAF

Removing certificate warning on VPN login page by using self-built CA configuration guide

Version 8.0.13

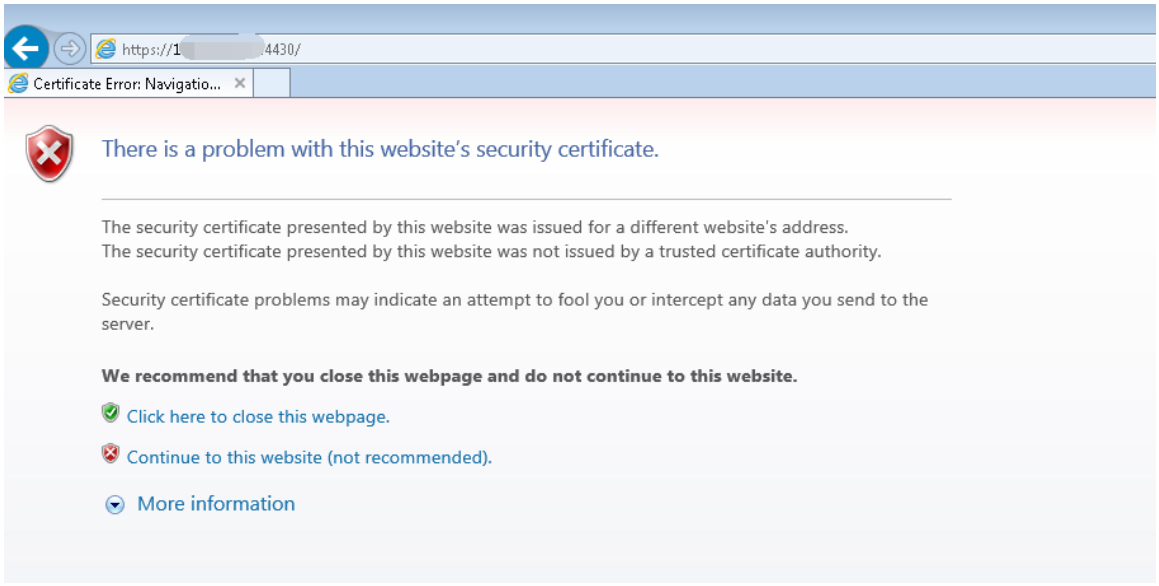
Contents

1. Function Introduction

The method of removing the certificate warning helps users to solve the problem of removing the warning by using a third-party certificate of SSL VPN, and can quickly grasp the method of removing the certificate warning by a third party certificate. The places marked in red in the document are some operations that require special attention or will cause the service to be restarted. Therefore, the operations that are specifically described are expected to pay special attention to the reader.

2. Principle Introduction

2.1 Why is There a Certificate Warning?



Everyone knows that when accessing the VPN login page is using the https protocol. Normally if accessing to device and the device cetificate is not trusted, means that endpoint fails to verify the server certificate. The endpoint will think that the connection to this server is an insecure connection, so this warning box will pop up. Sangfor device usually uses the method of updating the device certificate to remove the warning.

2.2 Principle of Removing the Certificate Warning

The warning box is a measure taken by Microsoft for security reasons. If you ignore these prompts, you can still visit the website smoothly. Normally after installing Windows, more than 100 certificates will be built into the system. These certificates are the root certificates of world-renowned companies, enterprises, or institutions. When we visit certain websites that are encrypted by the certificates issued by these certificate authorities, the error message will not appear. This is because the root certificates in the trusted root certificate authority in this machine are equivalent to the certificates issued by the root certificate authority in the machine.

For example, the certificate issuing authority is equivalent to the Ministry of Public Security, and each person's ID card is equivalent to his own unique certificate. In many circumstances, in order to prove your identity, you need to show your ID card, because it contains some of our very basic information, which is sufficient to prove that I am myself. When the other party checks the ID card, it is similar to the browser checking whether a certain certificate is legal, because we all know that the ID card is issued by the authoritative department of the Ministry of Public Security, and the ID card issued by this department must be real and valid, so it is naturalt hink you are who you are. Similarly, more than 100 trusted root certificate authorities pre-installed in this machine are equivalent to the Ministry of Public Security. When the browser detects a new certificate, it goes back to see if the issuer of the certificate is in its own trust organization. If it is, it will trust the certificate, otherwise it will not trust it, and this prompt will pop up. Tell you that the certificate detected by the browser is not a trusted root certificate authority.

In summary, to remove the certificate warning box during login, the following two conditions must be meet:

1. The device proves its own certificate, that is, the device certificate is issued to the device.
2. The issuing authority of the device certificate is trusted by the local browser, and the Trusted Root Certificate authority in the client's browser has a root certificate that issues the device certificate.

3.3 How to Remove the Certificate Alert

Based on the above principles, we can conclude that there are two ways to remove the certificate warning box:

1. Issue a device certificate to itself by Sangfor VPN device.
2. Remove the certificate warning by issue us a trusted device certificate through a third-party certificate authority.

Note: This document only describes how to remove the alarm box through the self-built CA.

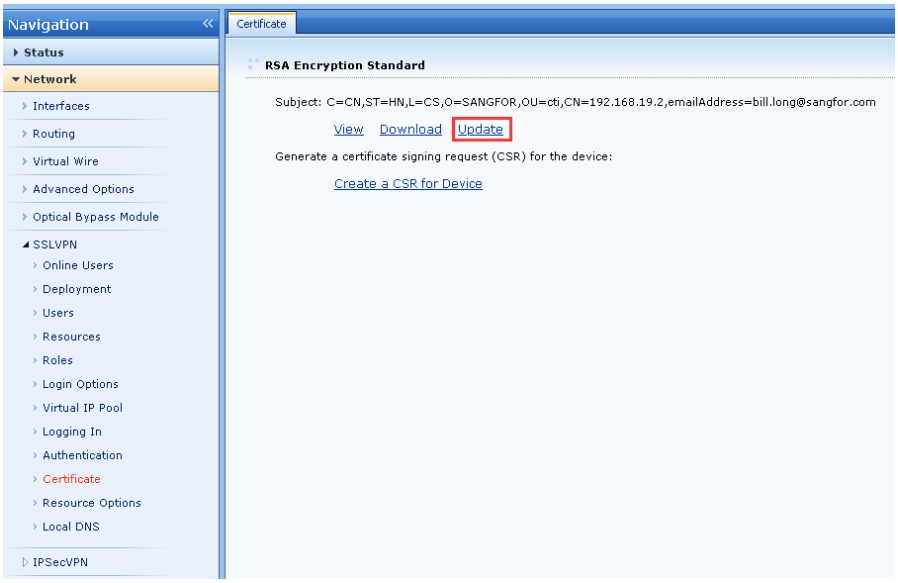
4. Configuration Method and Screenshot

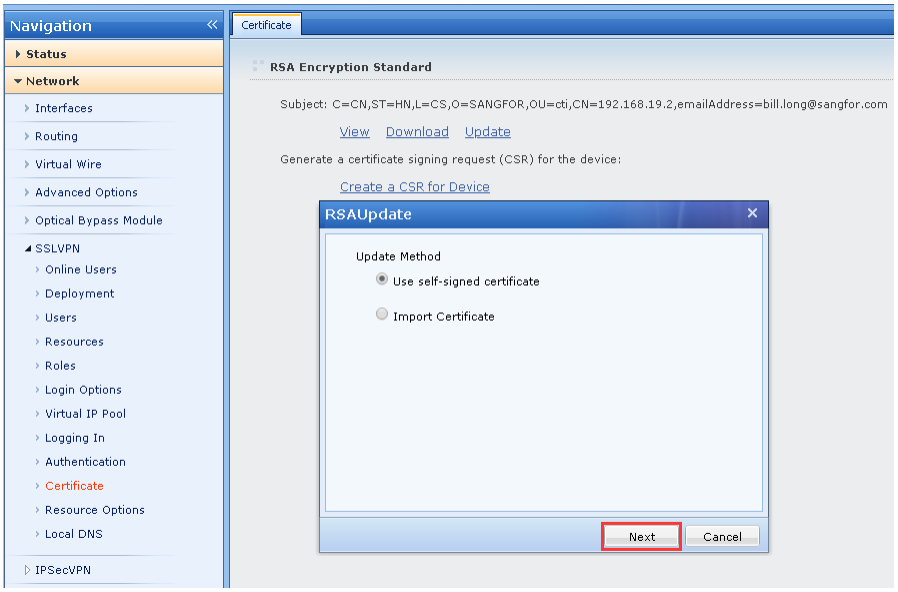
Implementation of self-built CA removing certificate alarm box:

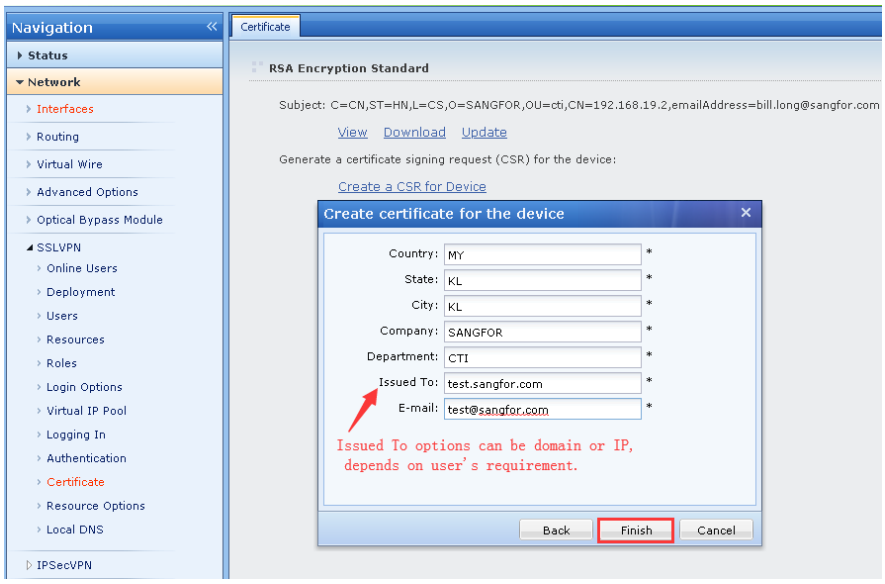
The principle of the self-built CA removing the certificate alarm box is to manually import the device self-signed device certificate into the browser's trusted root certificate authority, thereby removing the certificate alarm box.

4.1 Configuration on the NGAF device

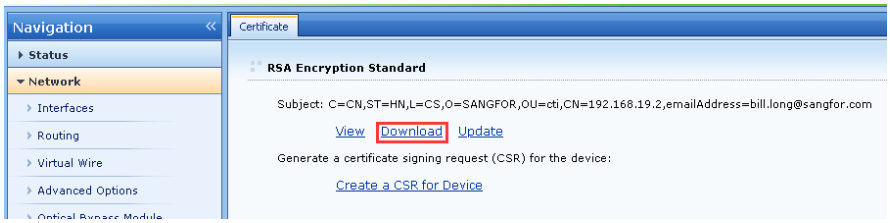
1. On NGAF device, go to **Network > SSLVPN > Certificate**, then choose the **Update > Use self-signed certificate** and configure as figures below:



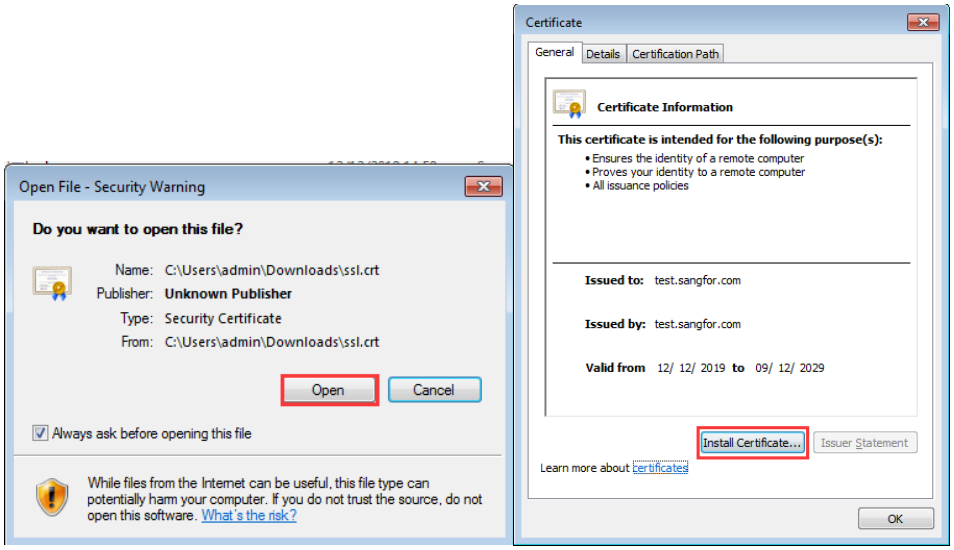


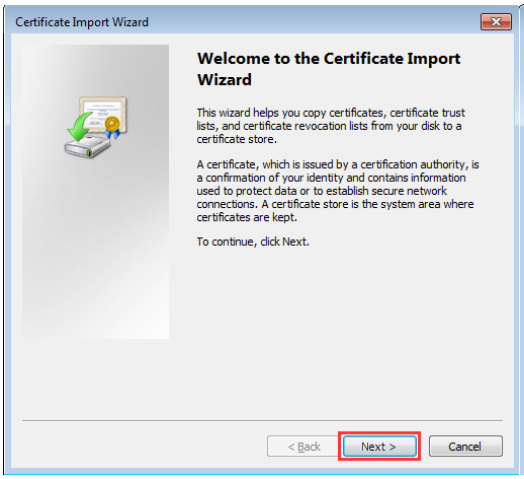


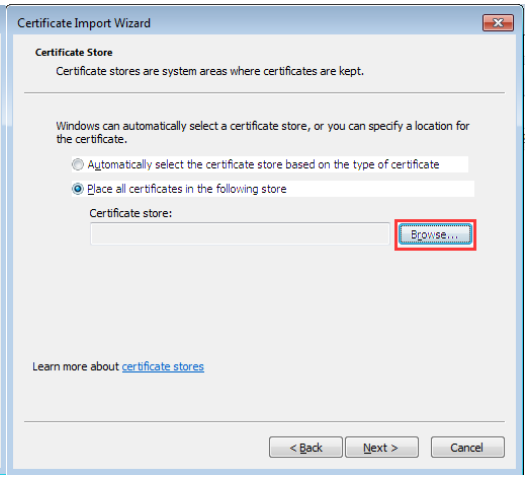
2. On **Certificate,** press on **Download** button to download the certificate as figure below:

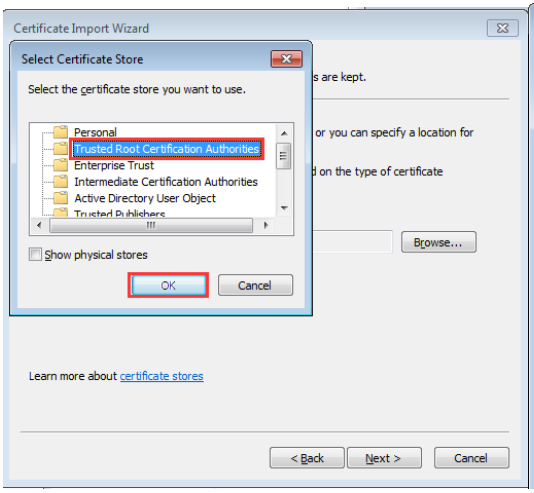


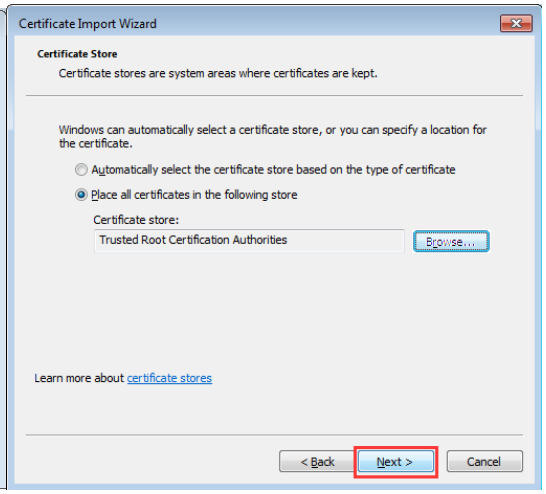
3. Double click on downloaded certificate, then press on the open button to install the certificate as figures below:

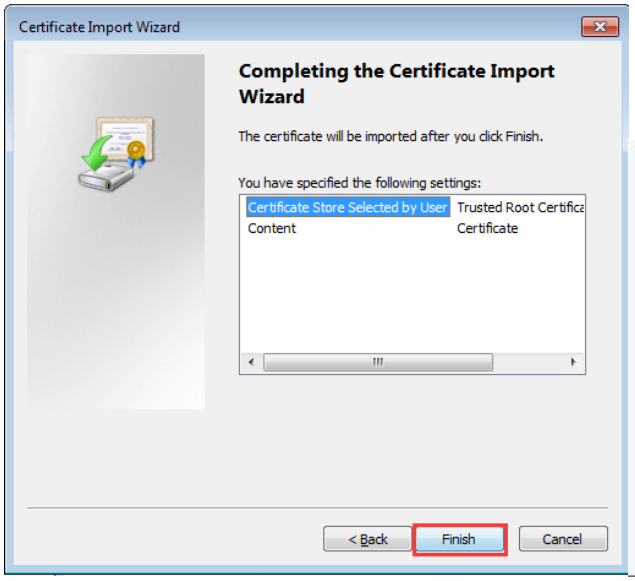


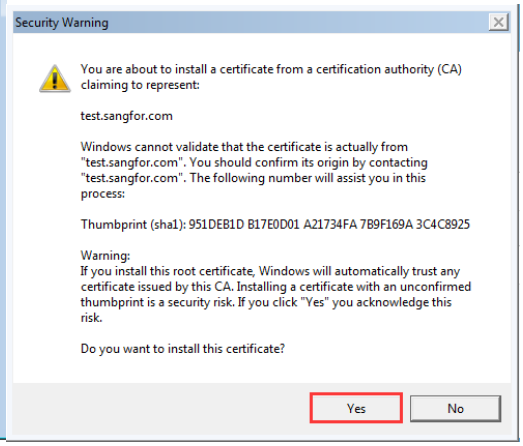

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

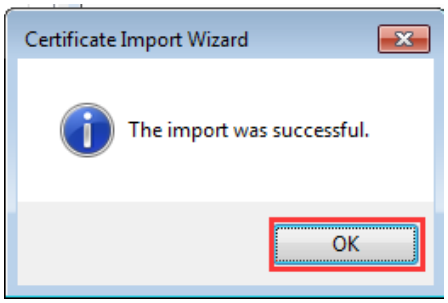

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Learn more about certificate stores
< Back
Next >
Cancel


Certificate Import Wizard
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Show physical stores
OK
Cancel
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

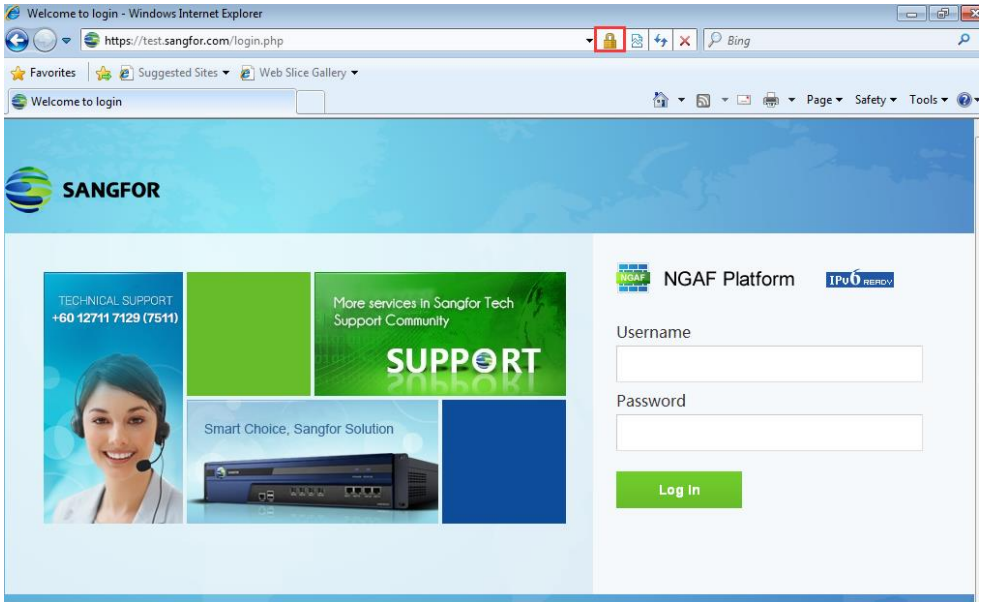

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

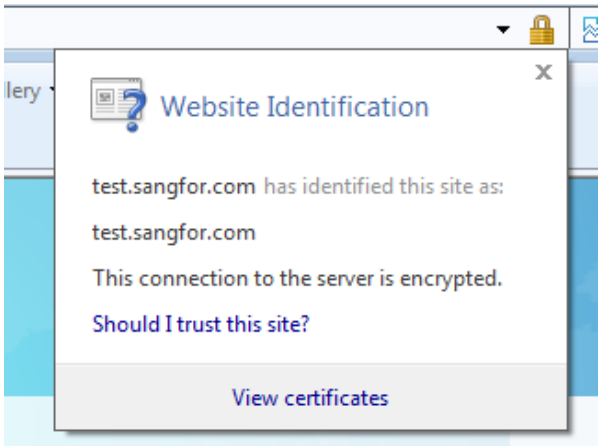

Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certifica
Content
Certificate
< Back
Finish
Cancel


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
test.sangfor.com
Windows cannot validate that the certificate is actually from "test.sangfor.com". You should confirm its origin by contacting "test.sangfor.com". The following number will assist you in this process:
Thumbprint (sha1): 951DEB1D B17E0D01 A21734FA 7B9F169A 3C4C8925
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No



4. After installed the certificate, try access to the web console using Internet Explorer. The certificate in this warning box shows a gold lock, indicating that the current login link is considered secure as figure below:





5. Precautions

1. In the cluster mode, you can update the device certificate and update the distributor. The distributor will synchronize the configuration to the real server.
2. Updating the device certificate requires restarting the SSL VPN service, which will cause online users to be disconnected.
3. In order to ensure that other exceptions will occur after updating the device certificate, it is recommended to back up the global configuration before updating the device certificate.

SANGFOR