Technical Information

Procedures for accessing cameras without Security Warning by browser through the self-signed root certificate

Panasonic i-PRO Sensing Solutions Co., Ltd,
As of January, 2020

Applicable models:

WV-SFV631L, WV-SFV611L, WV-SFN631L, WV-SFN611L, WV-SPN631, WV-SPN611, WV-SFV631LT, WV-SPW631L, WV-SPW631LT, WV-SFN480, WV-SFV481, WV-SFV781L, WV-SFN531, WV-SFR531, WV-SFV531, WV-SPV781L, WV-SPN531A, WV-SPW531AL, WV-SPW532L, WV-SFR611L, WV-SFR631L, WV-SPW611, WV-SPW611L, WV-SFN130, WV-SFN110, WV-SFV130, WV-SFV110, WV-SUD638, WV-S1131, WV-S1112, WV-S1111, WV-S1531LTN, WV-S1531LN, WV-S1511LN, WV-S1510, WV-S2531LTN, WV-S2531LN, WV-S2511LN, WV-S2131L, WV-S2130, WV-S2111L, WV-X6531N, WV-X6531NS, WV-S6511N, WV-S6131, WV-S6530N, WV-S6530NS, WV-S6110, WV-S6111, WV- S6130, WV-S4550LM, WV-S4550L, WV-S4150, WV-X4571LM, WV-X4571L, WV-X4171, WV-X4170, WV-X8570, WV-S8530, WV-X6533LN, WV-S6532LN

- Manufactured in April, 2016 and after
  Serial numbers: "PDxxxxxx", "PExxxxxx", "PFxxxxxx" and later. Also "Qxxxxxxx", "Rxxxxxxx" and later.

Concerning with the above cameras, you have to follow the procedures for each PC not to display the warning when you access the above cameras in https through the preinstalled self-signed root certificate.

Please note that this information is not guaranteed, but to provide our test results under out test environment.
Also please note that the following information is based on MS-Windows 7 (OS) and Internet Explorer 11 (Browser). So, another OS and/or another browser may need different procedure(s).

Here is the list of this document;

1. Install the Root Certification Authorities (CA)

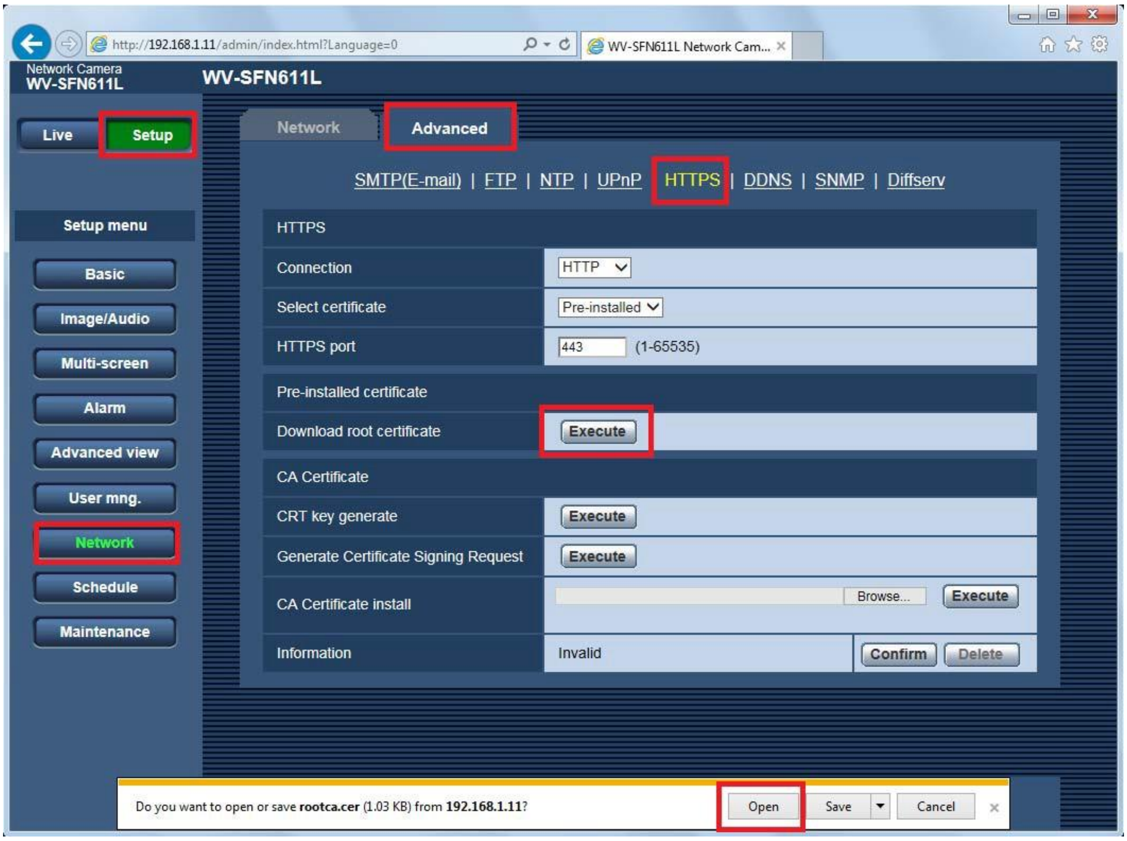
This procedure needs once per PC.

(1) Access the camera, the click “Set up” and “Network”.

(2) Click “Advanced”-tab and click “HTTPS”.

(3) Click “Execute” button at “Download root certificate”.

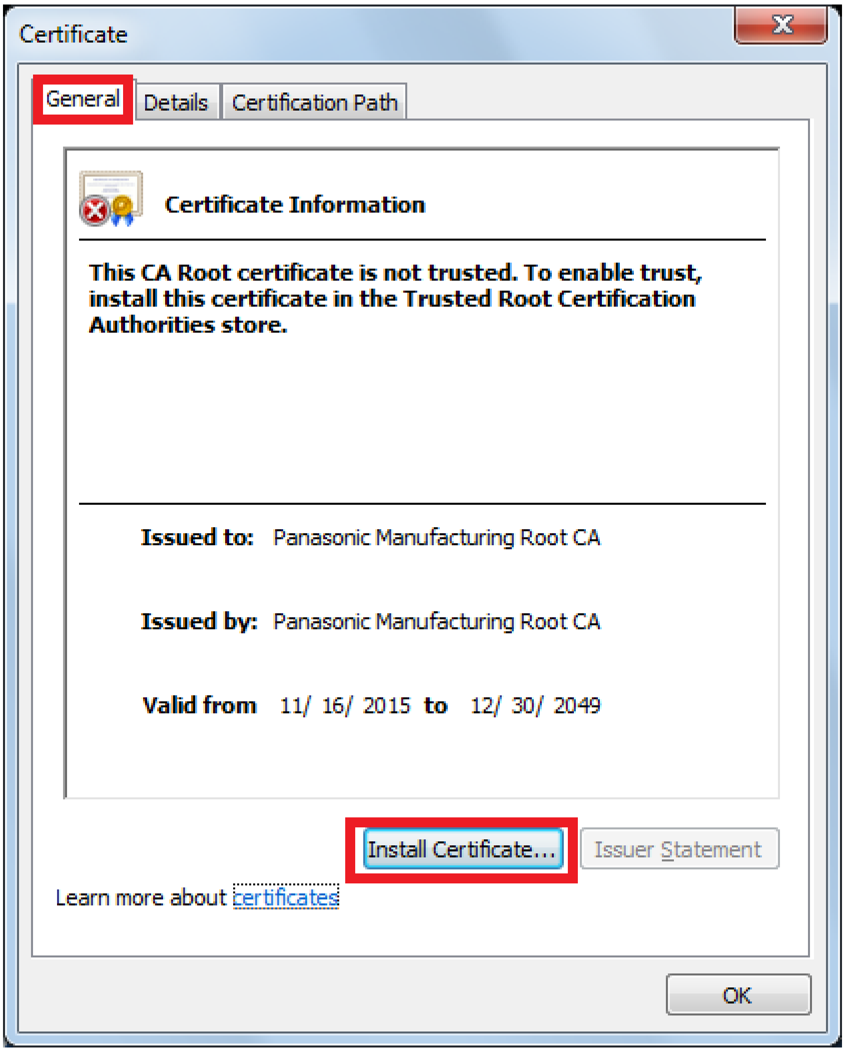
(4) Click “Open” at the bottom of the browser.



HTTPS	
Connection	HTTP
Select certificate	Pre-installed
HTTPS port	443 (1-65535)
Pre-installed certificate	
Download root certificate	Execute
CA Certificate	
CRT key generate	Execute
Generate Certificate Signing Request	Execute
CA Certificate install	Browse... Execute
Information	Invalid Confirm Delete

Do you want to open or save **rootca.cer** (1.03 KB) from **192.168.1.11**?

(5) You will see the “General”-tab, then click the “Install Certificate…” button.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Panasonic Manufacturing Root CA

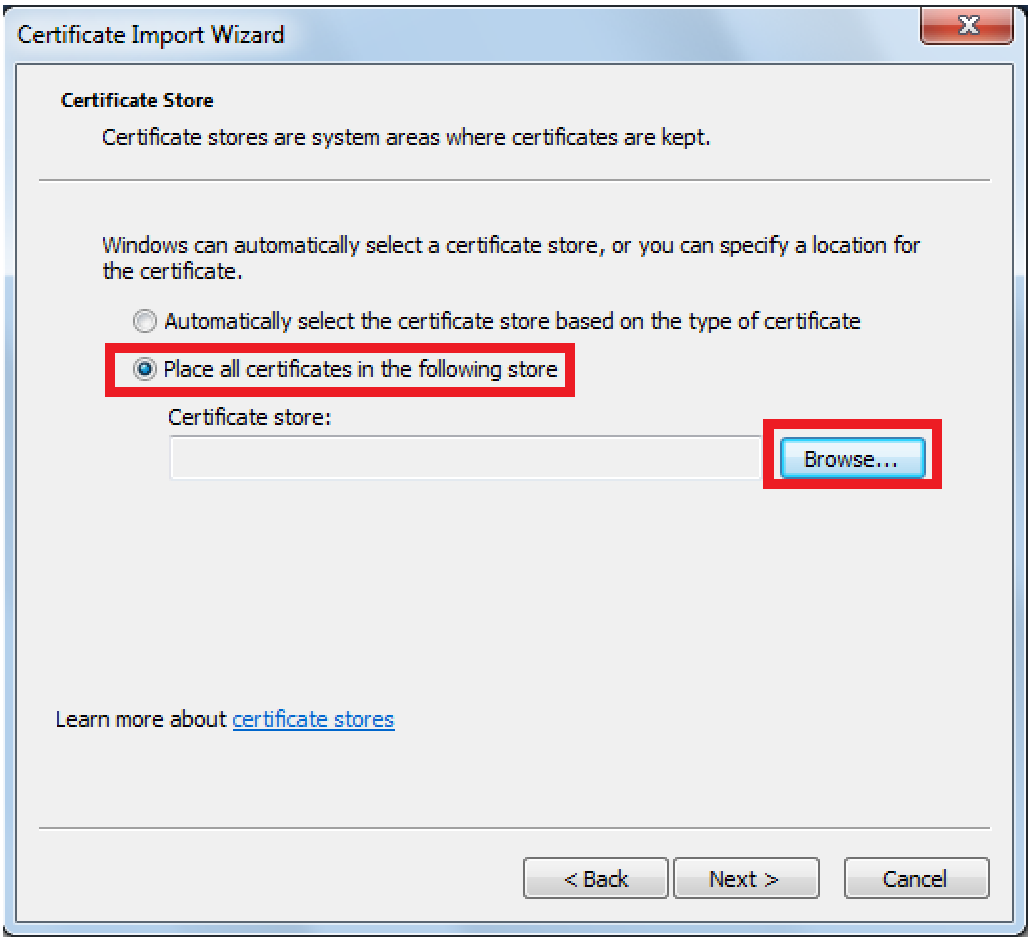
Issued by: Panasonic Manufacturing Root CA

Valid from 11/ 16/ 2015 **to** 12/ 30/ 2049

Learn more about certificates

(6) You will see the “Certificate Import Wizard”, then click “Next”.

(7) Select “Place all certificates in the following store”, then click “Browse…” button.



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.

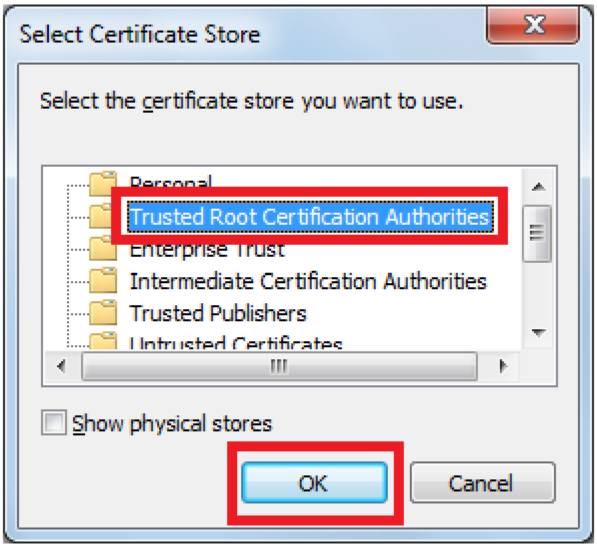
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Learn more about certificate stores

(8) Select “Trusted Root Certification Authorities” on the “Select Certificate Store” window, then click “OK” button.



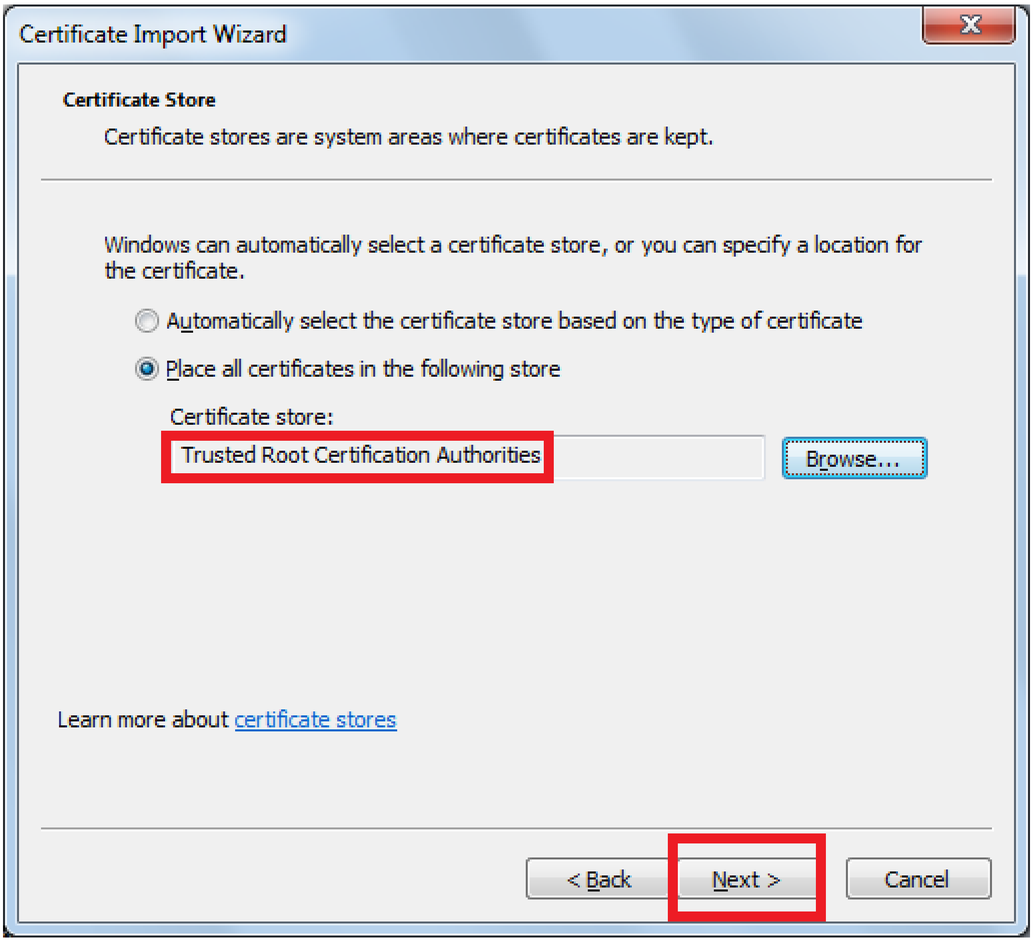
Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates

□ Show physical stores

(9) Make sure displaying “Trusted Root Certification Authorities” at “Certificate store”, then click the “Next” button.



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.

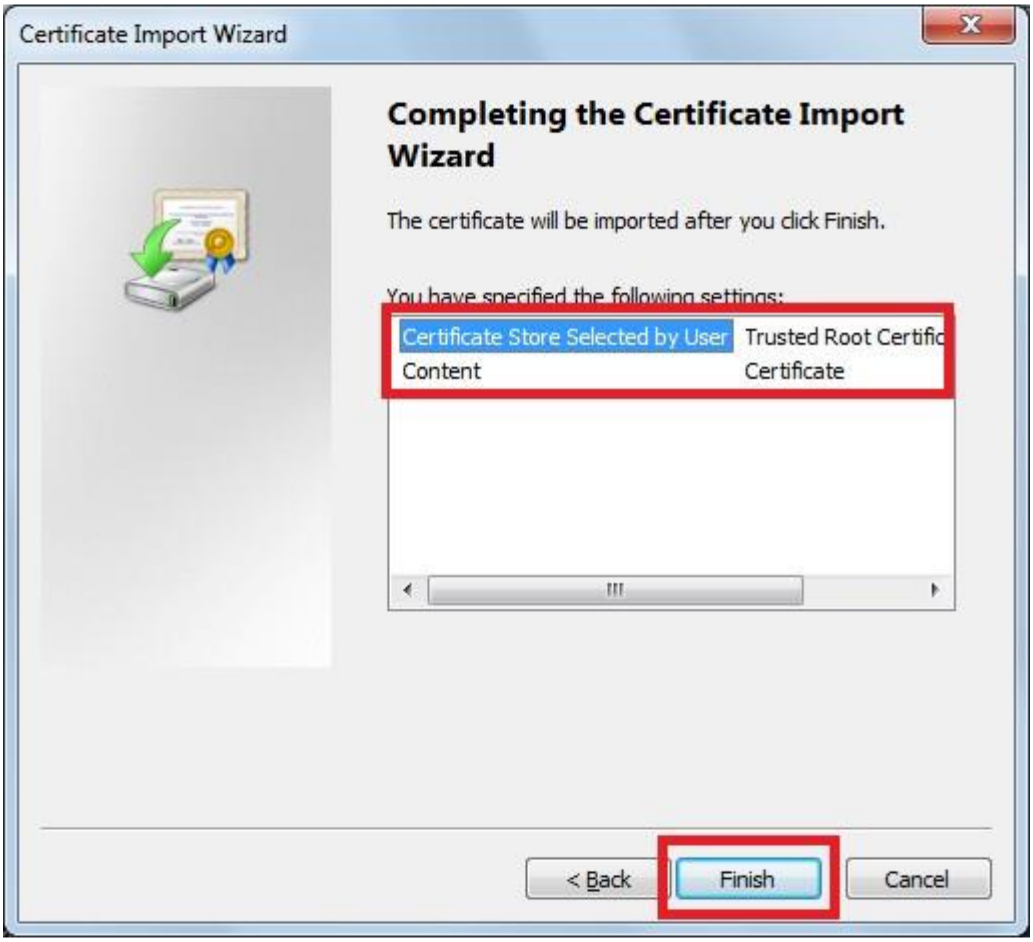
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

(10) Make sure “Trusted Root Certificate” at “Certificate Store Selected by User”, and make sure “Certificate” at “Content”, then click “Finish”.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

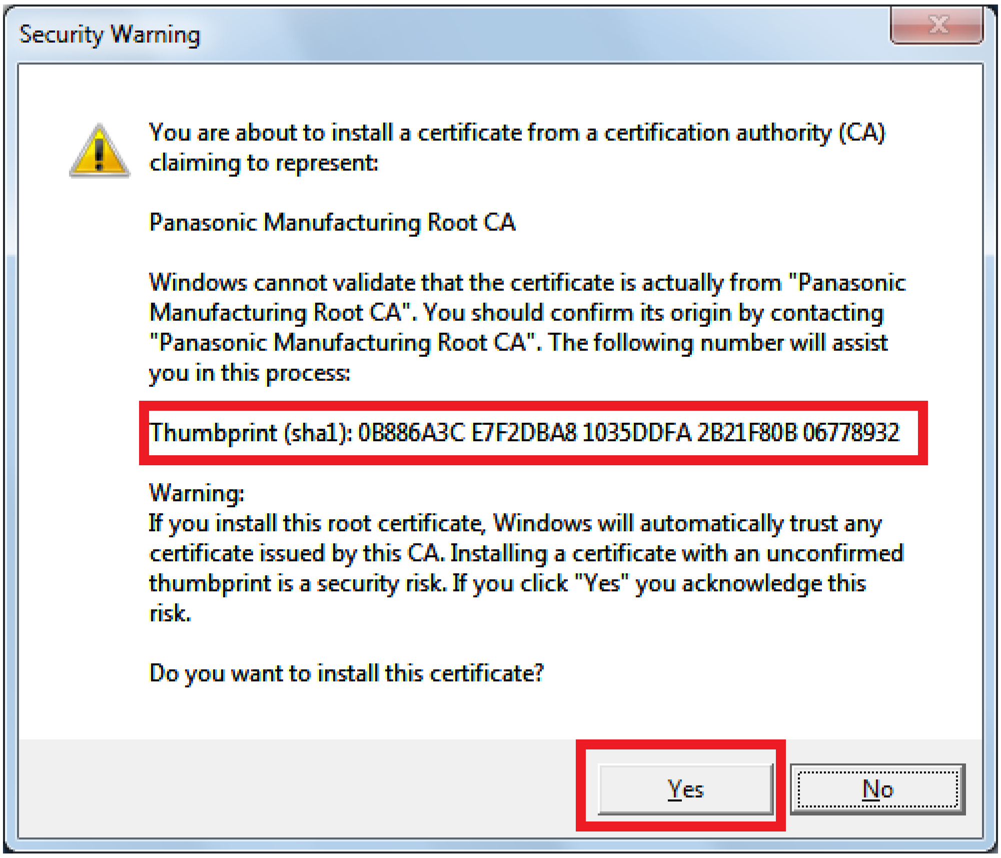
Certificate Store Selected by User	Trusted Root Certific
Content	Certificate

(11) Make sure the Thumbprint in the Security warning window shows same as follow, then click the “Yes” button.

- Thumbprint (sha1): 0B886A3C E7F2DBA8 1035DDFA 2B21F80B 06778932

Note:

Matching the thumbprint proves that it was taken out the correct root certificate from the target camera because others cannot create same thumbprint.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Panasonic Manufacturing Root CA

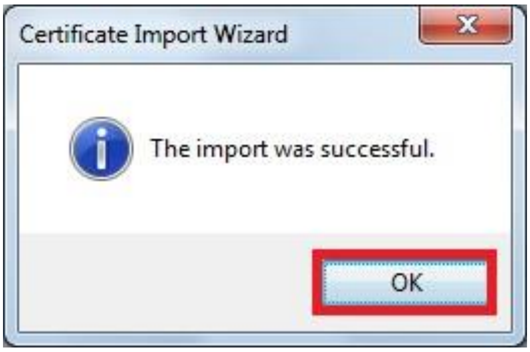
Windows cannot validate that the certificate is actually from "Panasonic Manufacturing Root CA". You should confirm its origin by contacting "Panasonic Manufacturing Root CA". The following number will assist you in this process:

Thumbprint (sha1): 0B886A3C E7F2DBA8 1035DDFA 2B21F80B 06778932

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.

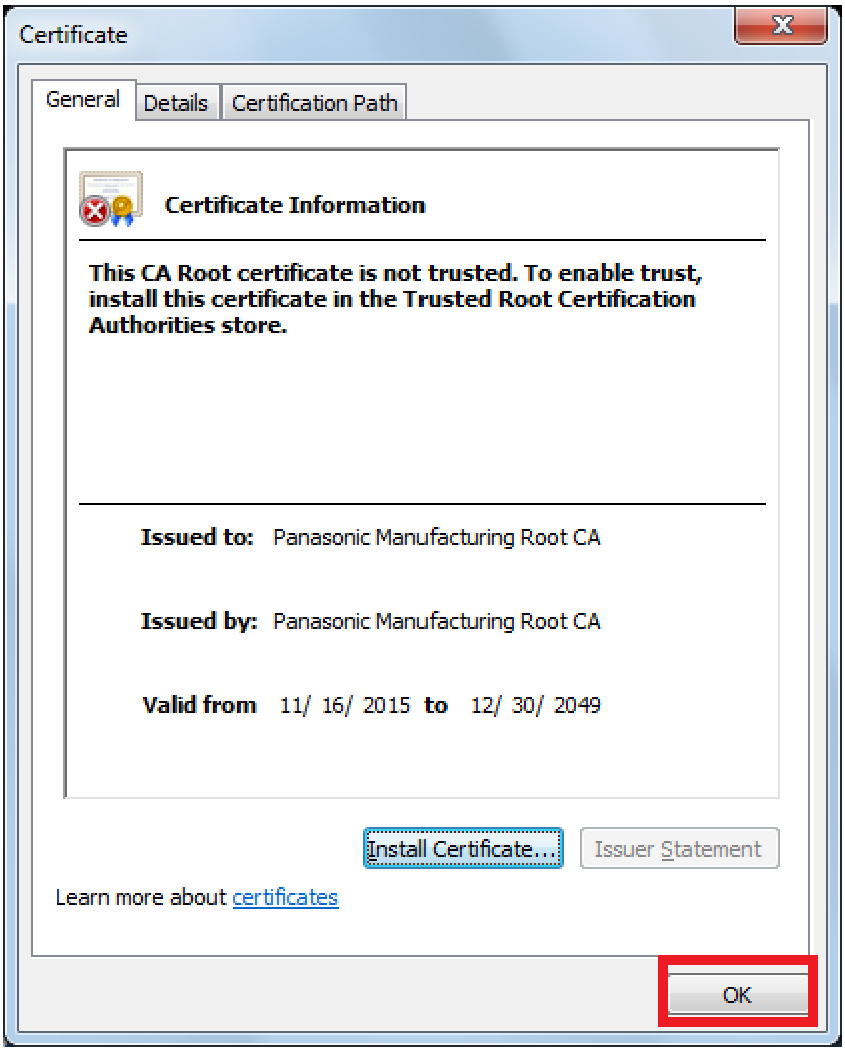
Do you want to install this certificate?

(12) Make sure the message “The import was successful.”, then click the “OK” button.



The import was successful.

(13) Click the “OK” button on the “Certificate” window to close.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Panasonic Manufacturing Root CA

Issued by: Panasonic Manufacturing Root CA

Valid from 11/ 16/ 2015 **to** 12/ 30/ 2049

(14) Restart the browser.

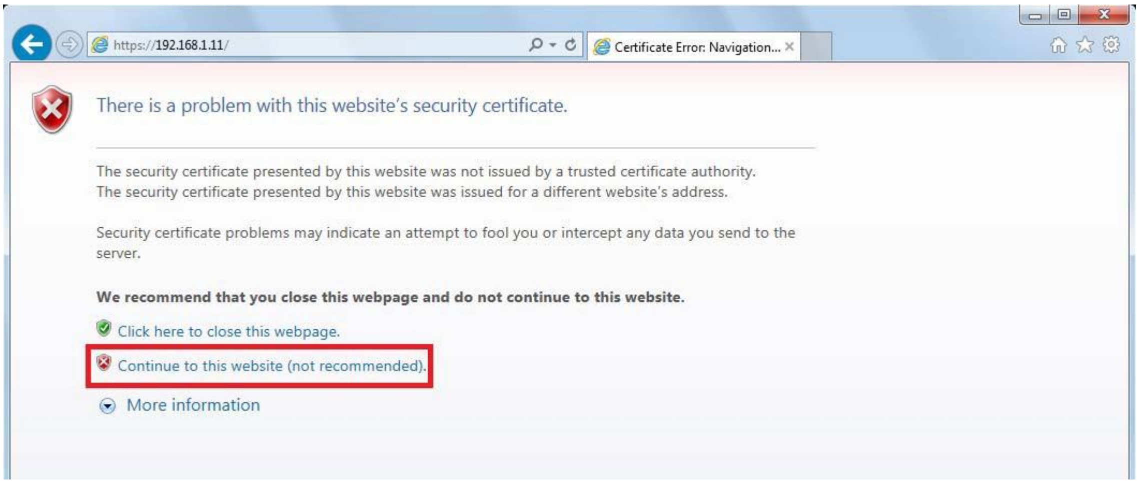
2. Editing the “hosts file”

This procedure needs for all PCs about all accessing cameras.

Note: The following are NOT for using with DNS service.

(1) Run a browser and access a camera in “https”. Please refer to the operating instruction manual how to access a camera in “https”.

(2) Click “Continue to this website (not recommended).” although you will see a warning “This is a problem with this website’s security certificate.”



There is a problem with this website’s security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website’s address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

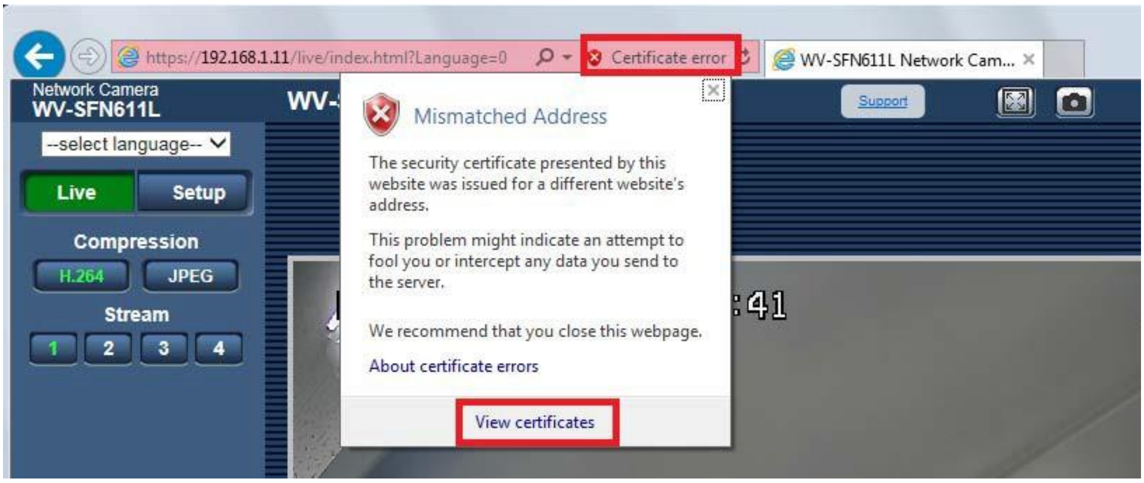
Note:

This warning is displayed for the string on the address-bar and the one at the subject on the certificate. Because the IP address or domain name that is assigned for the camera at creating the preinstalled certificate, is NOT finalized.

You do not need to worry about it because the Root CA at the STEP 1 certifies only for Panasonic devices.

(3) Click “Certificate error” at the right side of the address-bar on the browser.

(4) Click “View certificates” on the windows of the “Mismatched Address”.



Mismatched Address

The security certificate presented by this website was issued for a different website's address.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

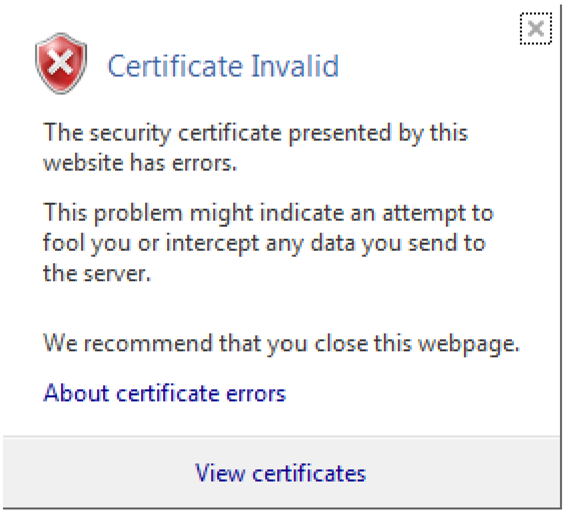
We recommend that you close this webpage.

About certificate errors

View certificates

Note:

Disconnect the camera if you see the warning of “Certificate Invalid” even if you set the STEP 1. Make sure if unknown devices are being connected because the camera is a possibility of spoofing.



Certificate Invalid

The security certificate presented by this website has errors.

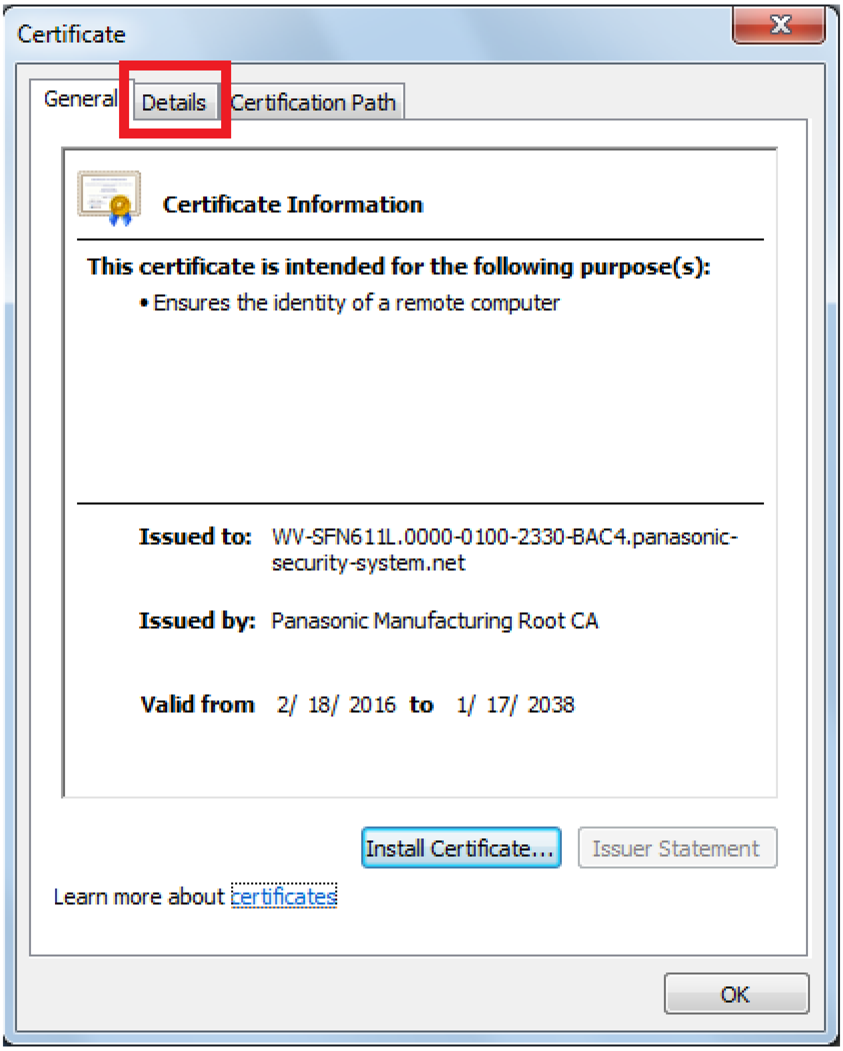
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

(5) Select “Details”-tab on the “Certificate” window, then click “Subject”-field.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

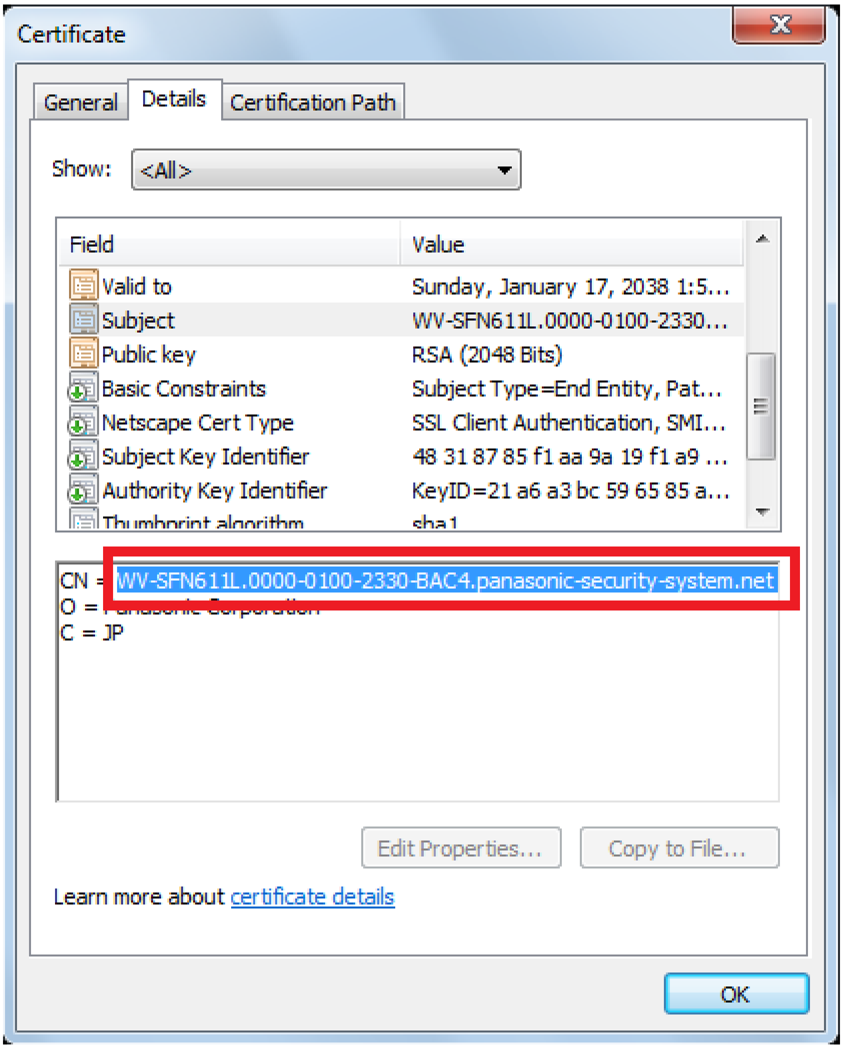
Issued to: WV-SFN611L.0000-0100-2330-BAC4.panasonic-security-system.net

Issued by: Panasonic Manufacturing Root CA

Valid from 2/ 18/ 2016 to 1/ 17/ 2038

Learn more about certificates

(6) Make sure selecting “<ALL>” at “Show:”, then click “Subject” in the field. Then copy the string after the “CN=”.



Show: <All>

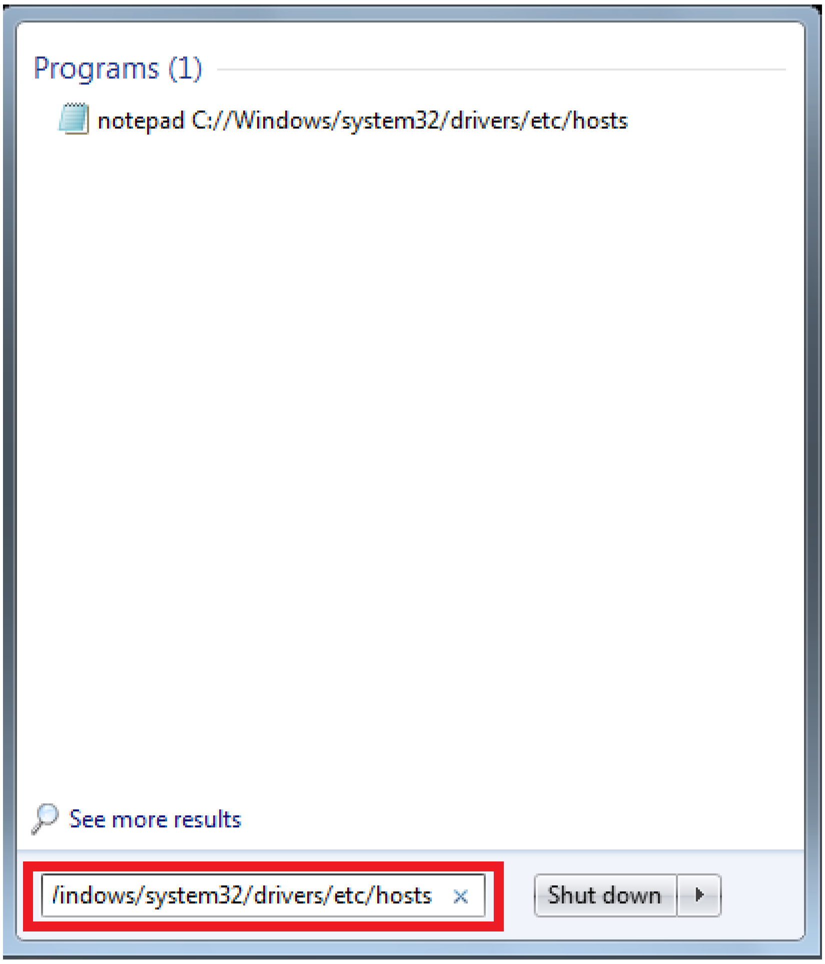
Field	Value
Valid to	Sunday, January 17, 2038 1:5...
Subject	WV-SFN611L.0000-0100-2330...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Netscape Cert Type	SSL Client Authentication, SMI...
Subject Key Identifier	48 31 87 85 f1 aa 9a 19 f1 a9 ...
Authority Key Identifier	KeyID=21 a6 a3 bc 59 65 85 a...
Thumbprint algorithm	sha1

CN = WV-SFN611L.0000-0100-2330-BAC4.panasonic-security-system.net
O = Panasonic Corporation
C = JP

Learn more about certificate details

(7) Open the Start menu of Windows, then input the string as follow into the input-field of “Search program and files”, then press “Ctrl” + “Shift” + “Enter” keys.

notepad C:¥Windows¥system32¥drivers¥etc¥hosts



Programs (1)

notepad C://Windows/system32/drivers/etc/hosts

(8) Click “Yes” when you see the window of “User Account Control”.

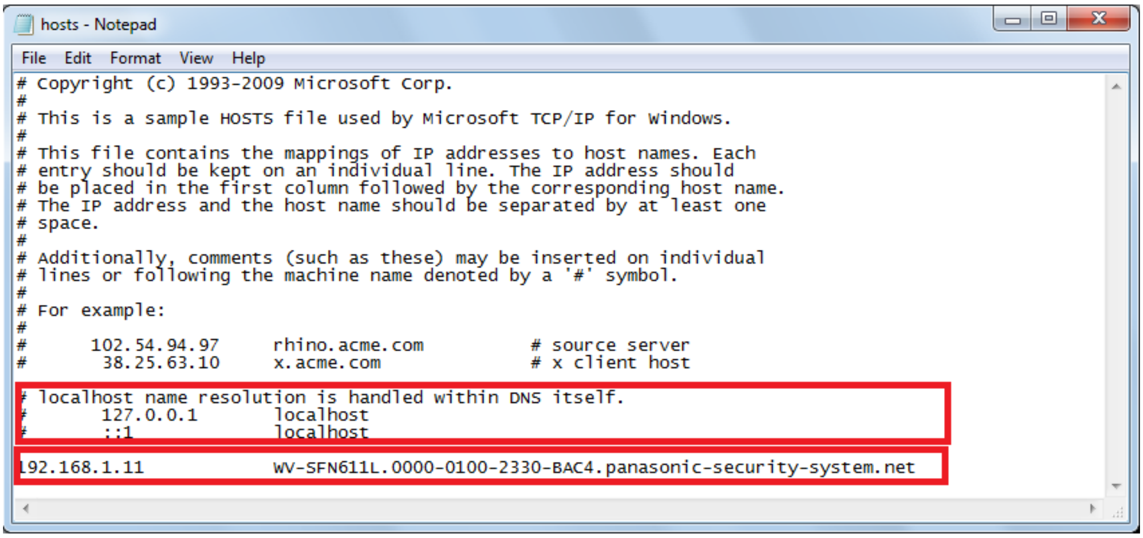
(9) You will see the window of “hosts – Notepad”, then add a string at the bottom of the text;

(IP address of the camera) (the copied string)

Example:

IP address of the camera is “192.168.0.10”

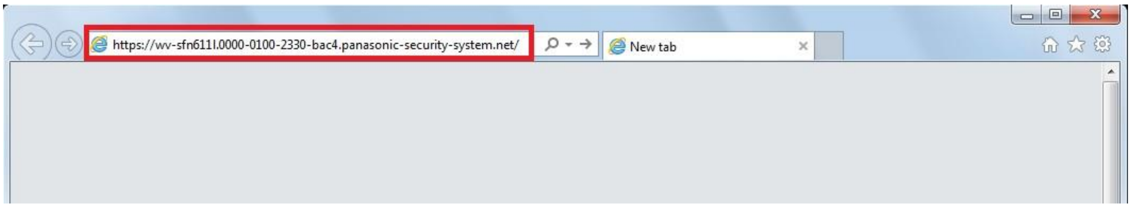
CN=WV-SFV631L.0000-0100-F0BA-77F0.panasonic-security-system.net



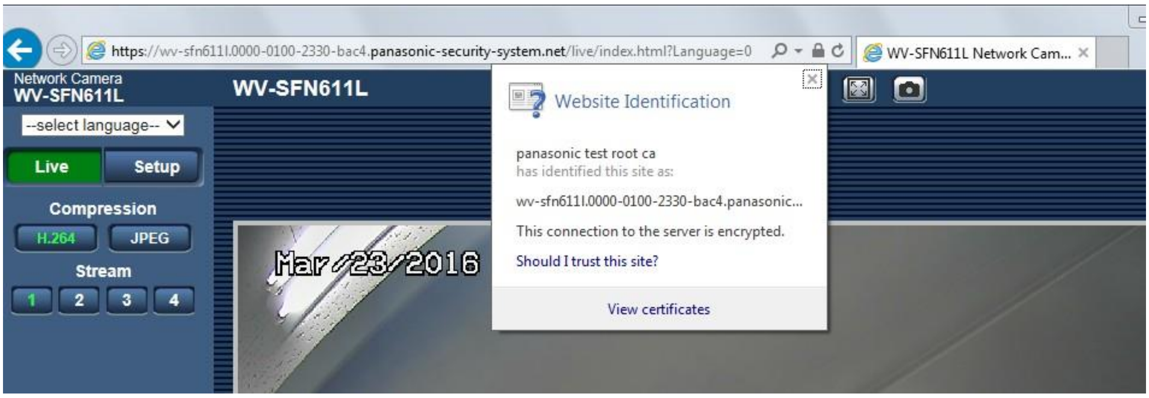
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.1.11            WV-SFN611L.0000-0100-2330-BAC4.panasonic-security-system.net
```

(10) Click “File”, select “Save” to save, then close.

(11) In a case access from a browser, input the string of the after “CN=” after the “https://” in the address-bar.


https://wv-sfn611l.0000-0100-2330-bac4.panasonic-security-system.net/

(12) You will see the background color of the address-bar in white after completion of the settings. Make sure the following display by clicking the lock icon in the address-bar.



https://wv-sfn611l.0000-0100-2330-bac4.panasonic-security-system.net/live/index.html?Language=0

Website Identification

panasonic test root ca
has identified this site as:

wv-sfn611l.0000-0100-2330-bac4.panasonic...

This connection to the server is encrypted.

Should I trust this site?

View certificates

Note:

If you cannot access successful, please ask the network administrator as the proxy server setting may be a cause of the problem.