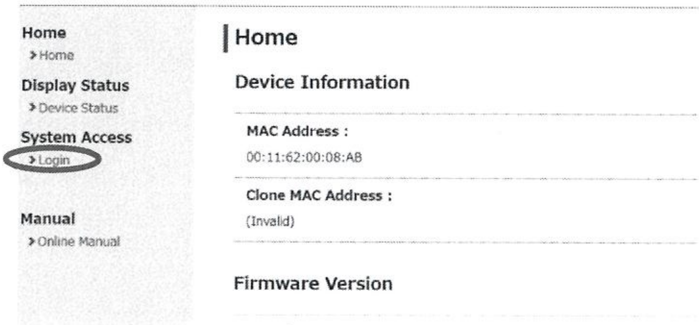
16.3. Example procedures for registration of SSL/TLS certificates

To use SSL/TLS communications (HTTPS), you must configure settings for the use of either a self-signed certificate or CA-signed certificate beforehand. The following shows the procedure for each.

16.3.1. Using a self-signed certificate

1. Create a certificate for the printer.
   Access the printer's IP address from the browser (in this procedure: http://192.168.1.81), and then log in with root privileges.



Home

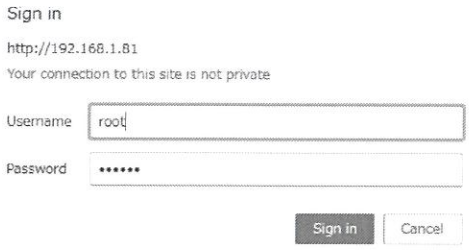
Device Information

MAC Address :
00:11:62:00:08:AB

Clone MAC Address :
(Invalid)

Firmware Version

Enter the following user name and password, and then click [OK].
User name: "root", password: "public" (factory-set)

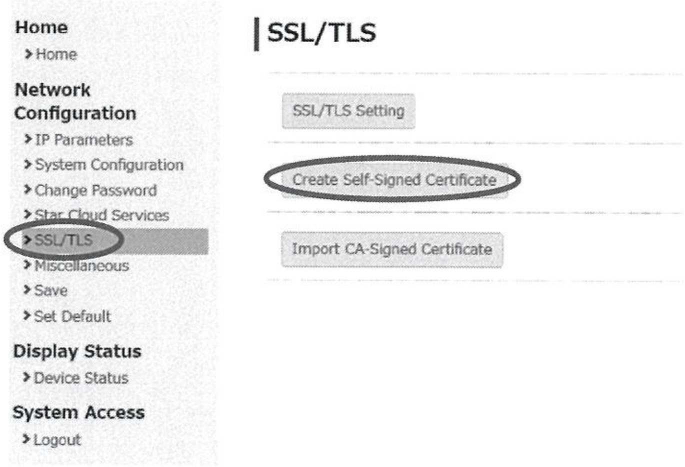

Sign in

http://192.168.1.81
Your connection to this site is not private

Username root
Password ••••••

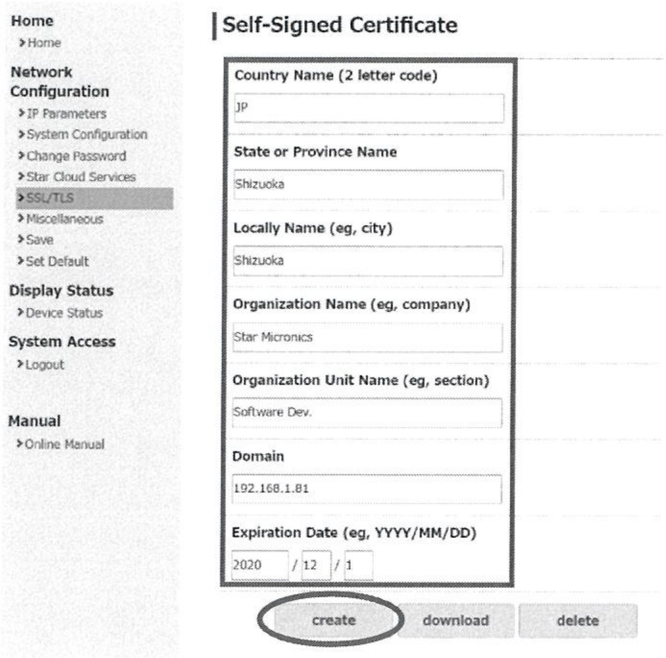
Click [SSL/TLS].

Click [Create Self-Signed Certificate].



SSL/TLS

After entering each item in the "Self-Signed Certificate" fields and clicking [Create], a certificate is created in the printer. For "Domain", enter the printer IP address (static value).* The screen below shows an example of input.



Self-Signed Certificate

Country Name (2 letter code): JP

State or Province Name: Shizuoka

Locally Name (eg, city): Shizuoka

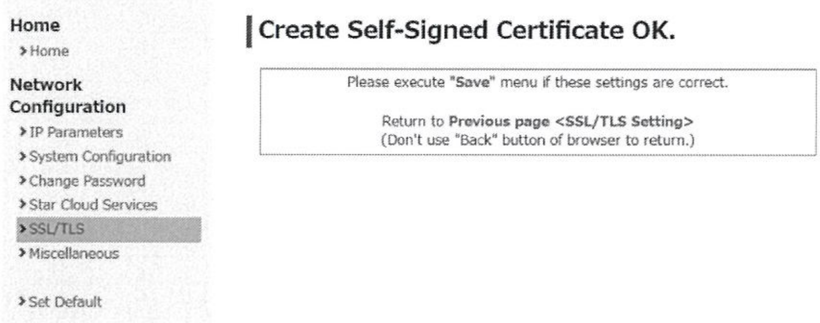
Organization Name (eg, company): Star Micronics

Organization Unit Name (eg, section): Software Dev.

Domain: 192.168.1.81

Expiration Date (eg, YYYY/MM/DD): 2020 / 12 / 1

The following screen appears when you successfully create a certificate.

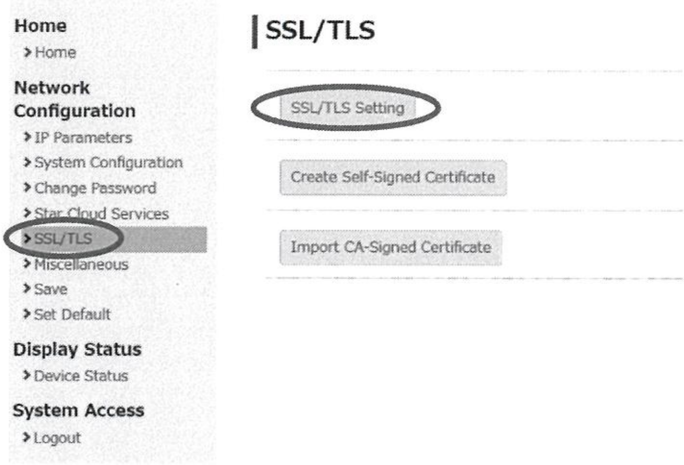


Create Self-Signed Certificate OK.

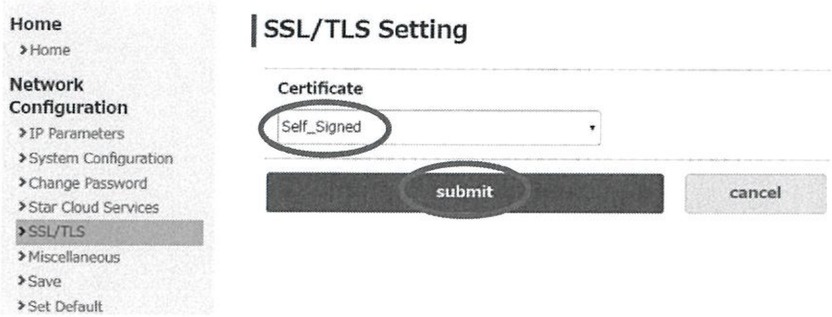
Please execute "**Save**" menu if these settings are correct.

Return to **Previous page <SSL/TLS Setting>**
(Don't use "Back" button of browser to return.)

2. Enable the printer self-signed certificate setting.
   Click [SSL/TLS]. Click [SSL/TLS Setting].



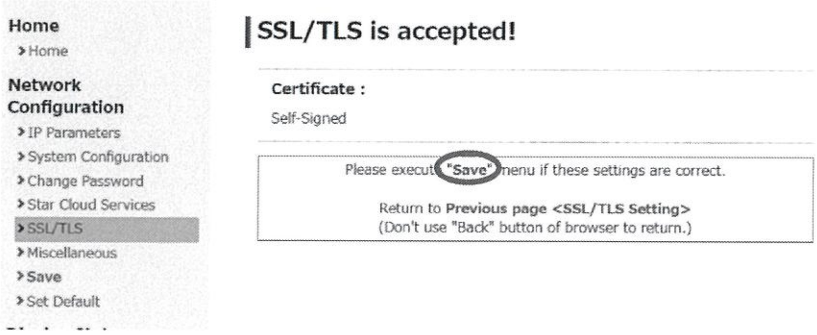
For "Certificate", select "Self-Signed" and click [Submit].



SSL/TLS Setting

Certificate: Self_Signed

The following information is displayed. Check that "Certificate" is "Self-Signed".



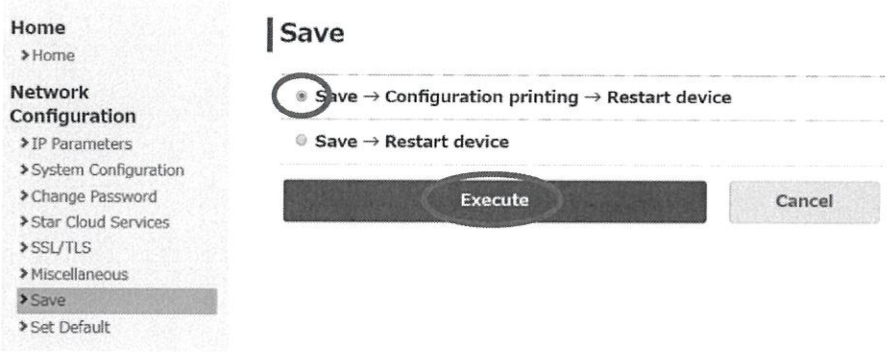
SSL/TLS is accepted!

Certificate :
Self-Signed

Please execute "Save" menu if these settings are correct.

Return to **Previous page <SSL/TLS Setting>**
(Don't use "Back" button of browser to return.)

Click [Save]. On the save screen, select "Save → Configuration printing → Restart device" and then click [Execute]. The printer prints the settings information. Check that the settings are those shown below.
- Self-Signed Certificate: Exist
- Certificate: Self-Signed



Save

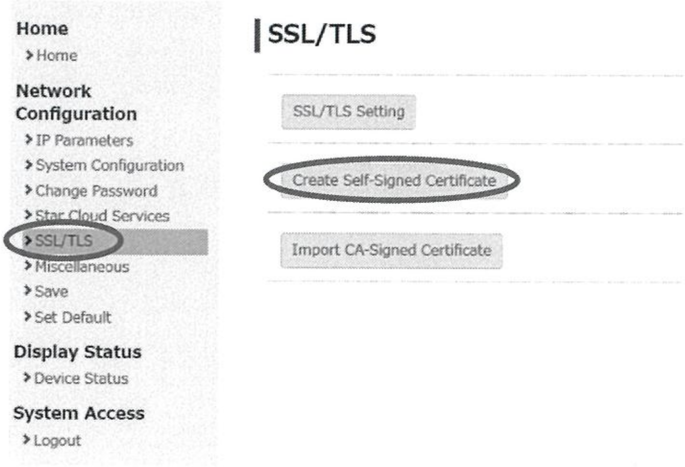
● **Save → Configuration printing → Restart device**
○ **Save → Restart device**

Creation of the printer self-signed certificates is completed.

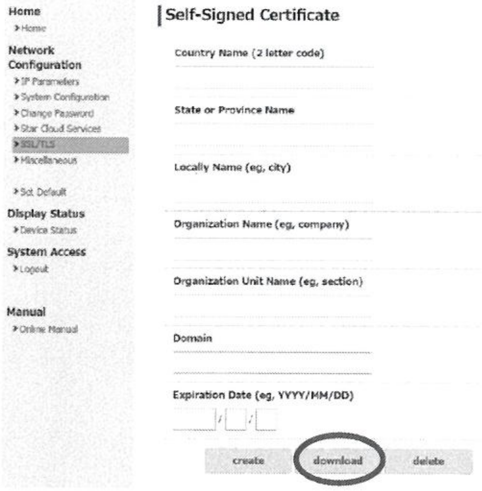
3. Importing a certificate to the web browser
   Import the certificate that was created in NIC to the web browser of the client device.

- Windows device (example shows Windows 7)

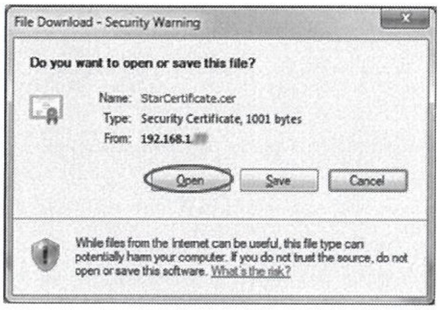
Click [SSL/TLS]. Click [Create Self-Signed Certificate].



Click [Download] and save a certificate file (name is not prescribed) to any place in Windows.
(In this example procedure, the file is saved with the name "StarCertificate.cer".



On the client device, double-click the saved certificate file and click [Open].


File Download - Security Warning

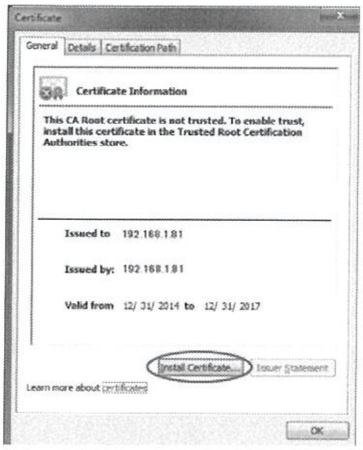
Do you want to open or save this file?

Name: StarCertificate.cer
Type: Security Certificate, 1001 bytes
From: 192.168.1.[redacted]

Open | Save | Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Click [Install Certificate…].



Certificate

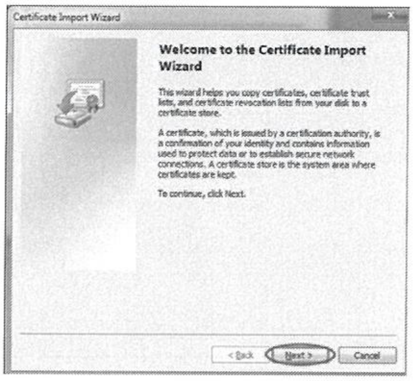
Certificate Information

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

Issued to 192.168.1.81

Issued by: 192.168.1.81

Valid from 12/ 31/ 2014 to 12/ 31/ 2017



Certificate Import Wizard

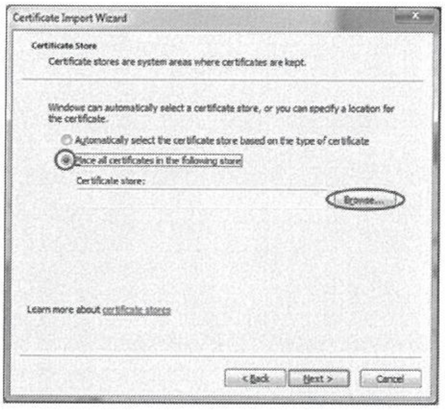
Welcome to the Certificate Import Wizard

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.

Select "Place all certificates in the following store" and then click [Browse…].



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

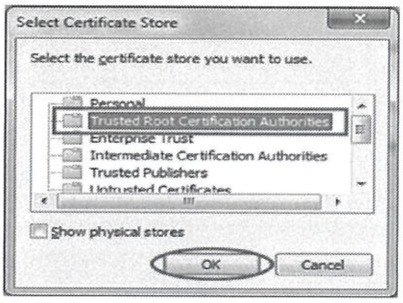
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

● Place all certificates in the following store

Certificate store:

Select "Trusted Root Certification Authorities" and then click [OK].



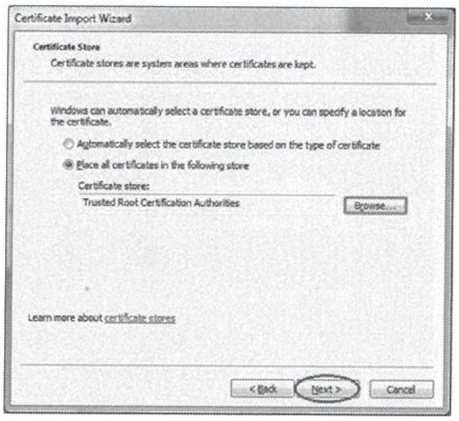
Select Certificate Store

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

Click [Next].



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.

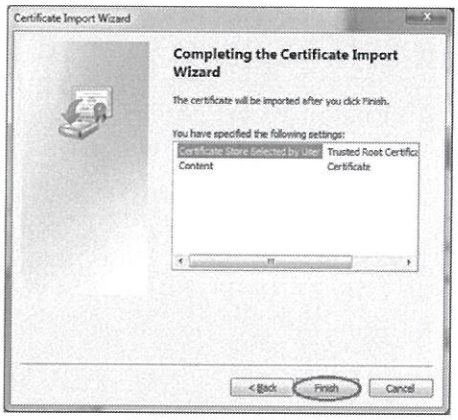
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

Learn more about certificate stores

Click [Finish].



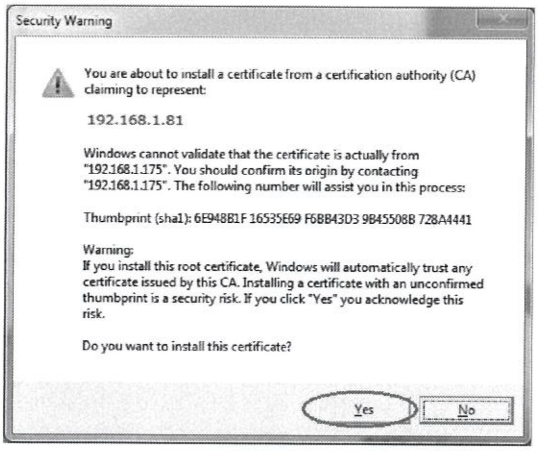
Completing the Certificate Import Wizard

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

Click [Yes] when the following message appears.



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

192.168.1.81

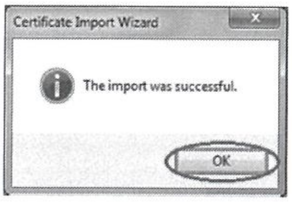
Windows cannot validate that the certificate is actually from "192.168.1.175". You should confirm its origin by contacting "192.168.1.175". The following number will assist you in this process:

Thumbprint (sha1): 6E948B1F 16535E69 F6BB43D3 9B45508B 728A4441

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.

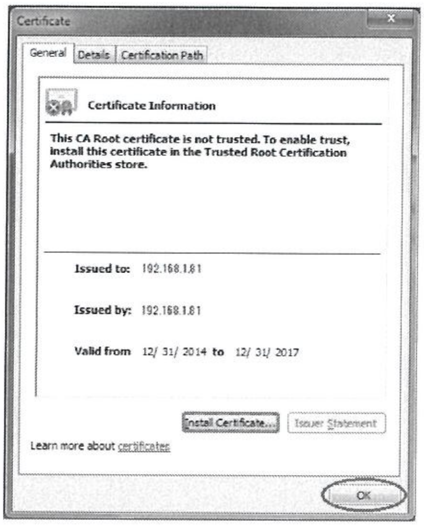
Do you want to install this certificate?

Click [OK].



The import was successful.

Click [OK] to close. The procedure is completed.



Certificate Information

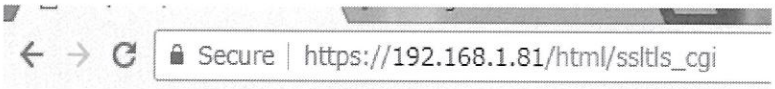
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: 192.168.1.81

Issued by: 192.168.1.81

Valid from 12/ 31/ 2014 to 12/ 31/ 2017

Turn the printer power ON again. It is now possible to access the printer web screen using an address starting with "https://".



Secure | https://192.168.1.81/html/ssltls_cgi

However, depending on the client device environment, you may need to add the address as a "Trusted sites". (For example, combination of Windows 10 + Microsoft Edge)

→ See "16.3.3. Additional information".

[Reference information]

When importing a certificate file to the web browser with Windows 8/8.1/10, you must activate certificate manager, "certmgr.msc" in Windows administrative tools, and then perform the following procedure.

- Select "Trusted Root Certification Authorities" and then [Certificate].
- Select [All tasks] and then [Import] from the "Operation Menu".
- Import a self-signed certificate using the import certificate wizard.
- Make sure you import the certificate by referring to "Trusted Root Certification Authorities" and then [Certificate].