LOCAL CERTIFICATION AUTHORITY CREATOR

Model: LCA-SG

USERS MANUAL

Table of Contents

1. INTRODUCTION

Thank you for downloading our software program.

1.1 Overview

The SG6 supports HTTPS for enhancing secure communication.
This users manual describes how to create certificates indispensable for using HTTPS.

1.2 Applicable Versions

The contents of this users manual are applicable to the versions below.

MODEL	VERSION
LCA-SG	1.0.0
SG6	1.0.8

For details of the SG6, refer to the users manual (EM-8591-B) which is downloadable at our web site.

2. SERVER AUTHENTICATION

This section describes the purpose of web server certificates and how they are used.

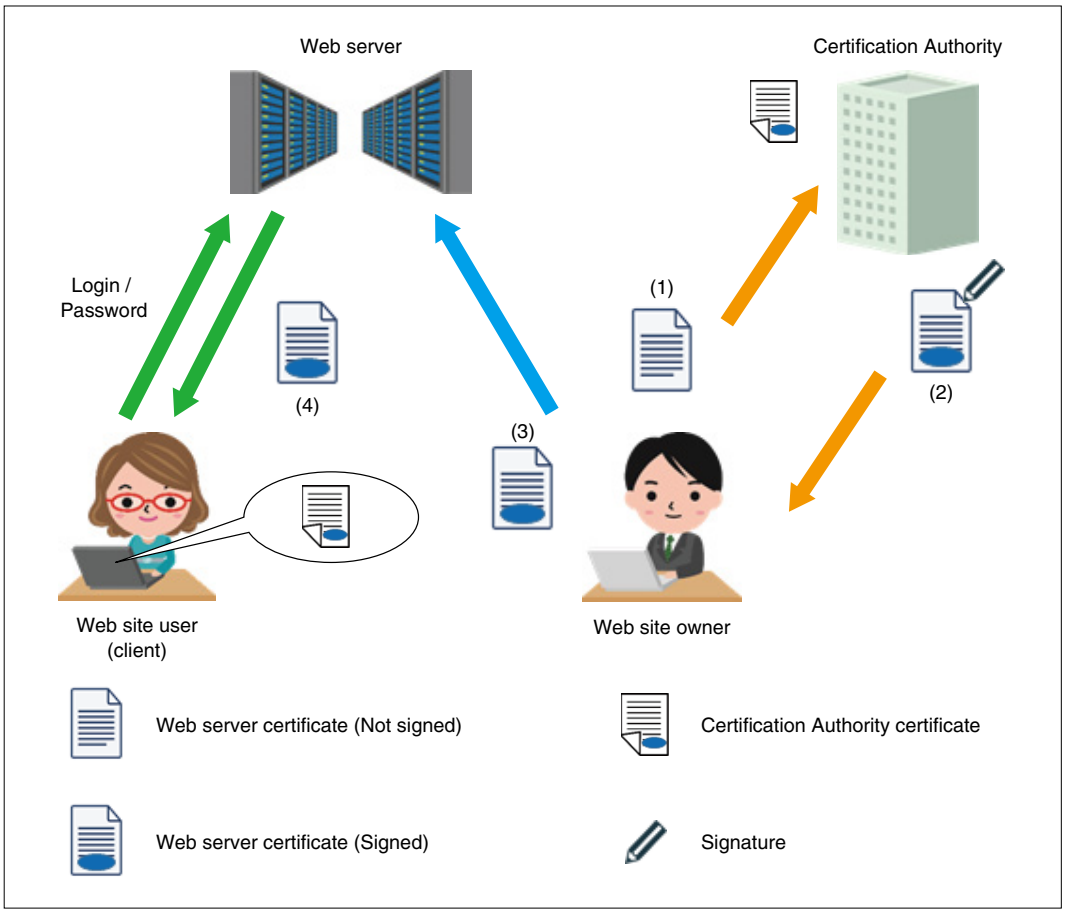
For further understanding, refer to relevant web sites or tutorial documents for terminologies such as 'root CA', 'intermediate CA', 'electronic signature', 'SSL/TLS', etc.

Below is a typical procedure to open a web site supporting HTTPS.

(1) The web site owner creates a web server certificate and requests a certification authority (CA) for its signature.

(2) The CA, after verifying the identity of the owner and the server, signs and returns it.

(3) The web site owner installs the certificate on the web server.



As a web site user accesses the web server via a browser over HTTPS, the web server certificate signed by the certification authority is downloaded ((4) in the above figure).

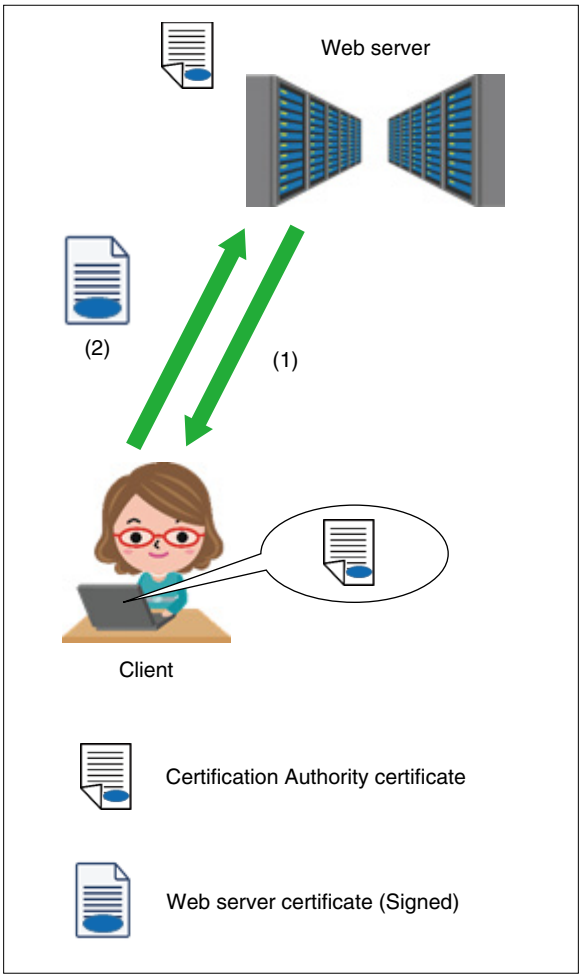
Then a second certificate by the CA that has signed the first one is needed to prove the authenticity of the signature.
For prompt verification, major CA certificates are pre-installed in browsers.
Once the authenticity is verified, the user can assure that the web site he/she is accessing is not a spoofed one.

The web server certificate also enables encrypted communication between the web server and the user, preventing eavesdropping and alteration of communication data.

As described above, HTTPS ensures the communication security. In this case, the web site user (client) authenticates the server by using the server certificate. On the other hand, the web server authenticates the user by his/her login name and password ((5) in the above figure). This transmission of login name and password is encrypted, which reduces the chance of eavesdropping. However, risks of being illegally logged in by conjecture, brute force attack, etc. remain.

3. CLIENT AUTHENTICATION

In contrast to the server authentication described in the previous section, TLS allows the server to request a certificate of the client ((1) in the following figure).
The client sends the signed client certificate to the server ((2) in the following figure), and the server that receives it permits the connection of the client.
Therefore, the certificate must be signed by a certification authority that the server approves.

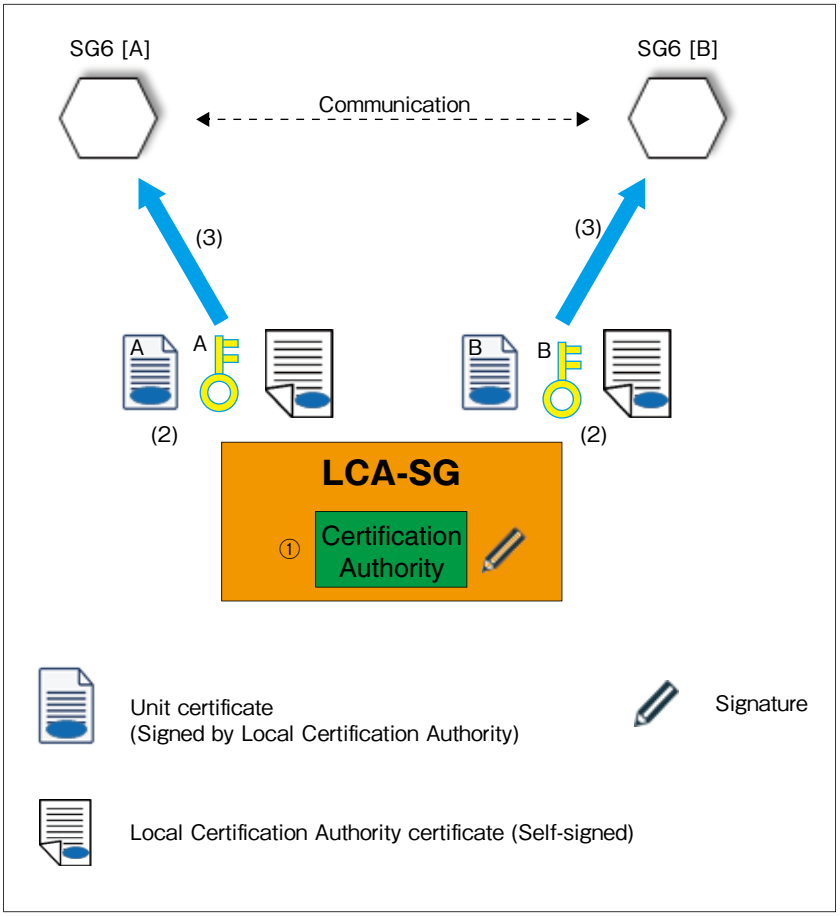


4. LOCAL CERTIFICATION AUTHORITY

The SG6 certifies devices in communication by mutual authentication using both server certification and client certification. This mutual authentication is possible because these are not widely publicized like a web server. In this case, building your own certification authority in a local environment makes it easier to use the system. Local Certification Authority Creator (Model: LCA-SG) is provided to help you.

The LCA-SG...

1) Builds a local certification authority (LCA) on the PC on which the program is installed. LCA certificate is also created at this time.
2) Creates a unit certificate and private key for each device. This certificate is signed by the LCA and commonly used for the server certificate and the client certificate.
3) Transfers the following items to the devices: the LCA certificate created in 1), unit certificate and private key created in 2).



All SG6s must have the certificates signed by the same LCA. When adding the SG6 to the communication network after the LCA-SG is reinstalled or the LCA is rebuilt, new certificates signed by the new LCA must be transferred to all SG6 units.

NOTES

- Files generated by the LCA-SG are critical in terms of security. Please handle them with utmost caution.
- Using the SG6 and the LCA-SG does not necessarily guarantee perfect security. You must run the system on your own risk and responsibility.

5. HOW TO USE LCA-SG

5.1 System Requirements

■ **SYSTEM REQUIREMENTS**

HARDWARE	REQUIREMENT
PC	IBM PC/AT or compatible
Operating System	Windows 10 Home, Professional, Enterprise editions (32-bit / 64-bit)
Other than OS	DOT.NET Framework 4 or later
RAM	2 GB or more
Hard disk area	60 MB or more (Separately secure hard disk space for user data)
Display resolution	XGA (1024 x 768) or more
Language	English / Japanese

5.2 Installing LCA-SG

Store the downloaded files in single folder, and execute 'Setup.exe'.
Follow instructions on the Windows installer.

A security warning message may appear during the installation.
Confirm the relevant files are the ones downloaded from our HTTPS site before resuming installation.

5.3 Creating Local Certification Authority

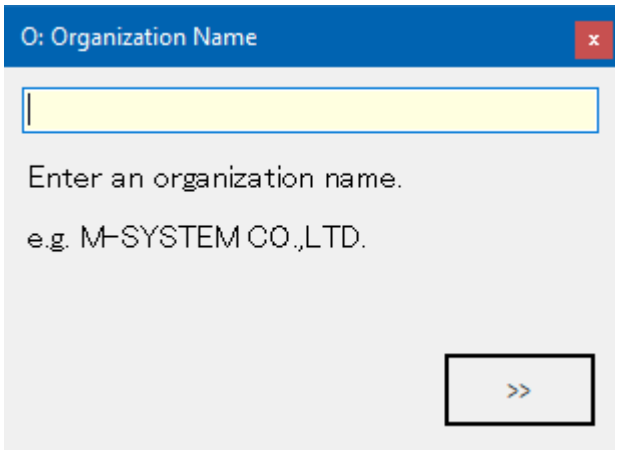
The LCA-SG, at the initial startup, asks you to specify your organization name and validity period of the certificate.

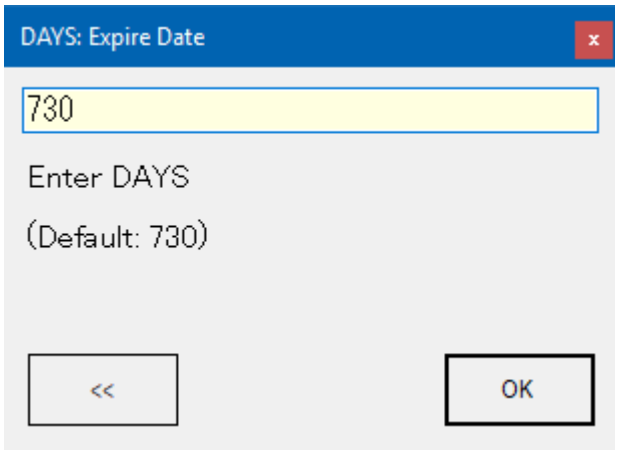
Enter the name of your company or organization, to represent the Local Certification Authority.

In the next dialog, set period of validity in days between 30 and 3563.

The confirmation dialog will appear after entering the all contents.

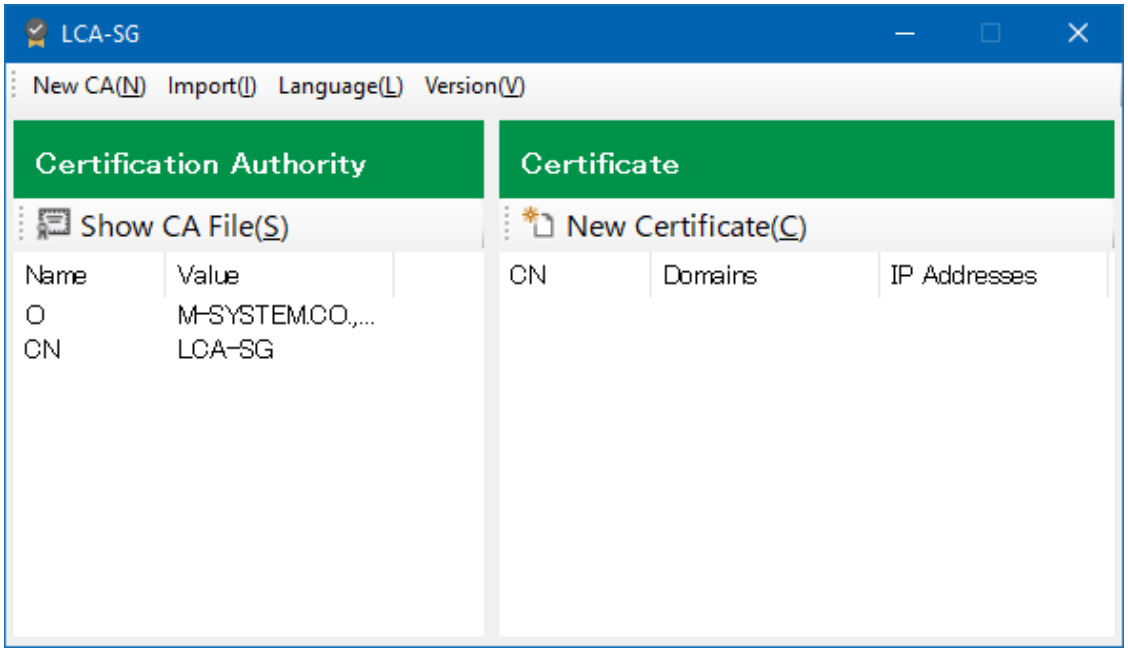
Confirm that the registered organization name and validity period are indicated after "O=" and click [OK].





PARAMETER ITEM	DESCRIPTION
Organization Name	Enter your company/organization name. Useable characters First character : A-Z, a-z, " _ (underscore)" Second and following characters: A-Z, a-z, 0-9, " _ (underscore)", " , (comma)", " . (period)", " - (hyphen)", " (blank)"
Expire Date	Enter a number of days (of validity) between 30 and 3653.

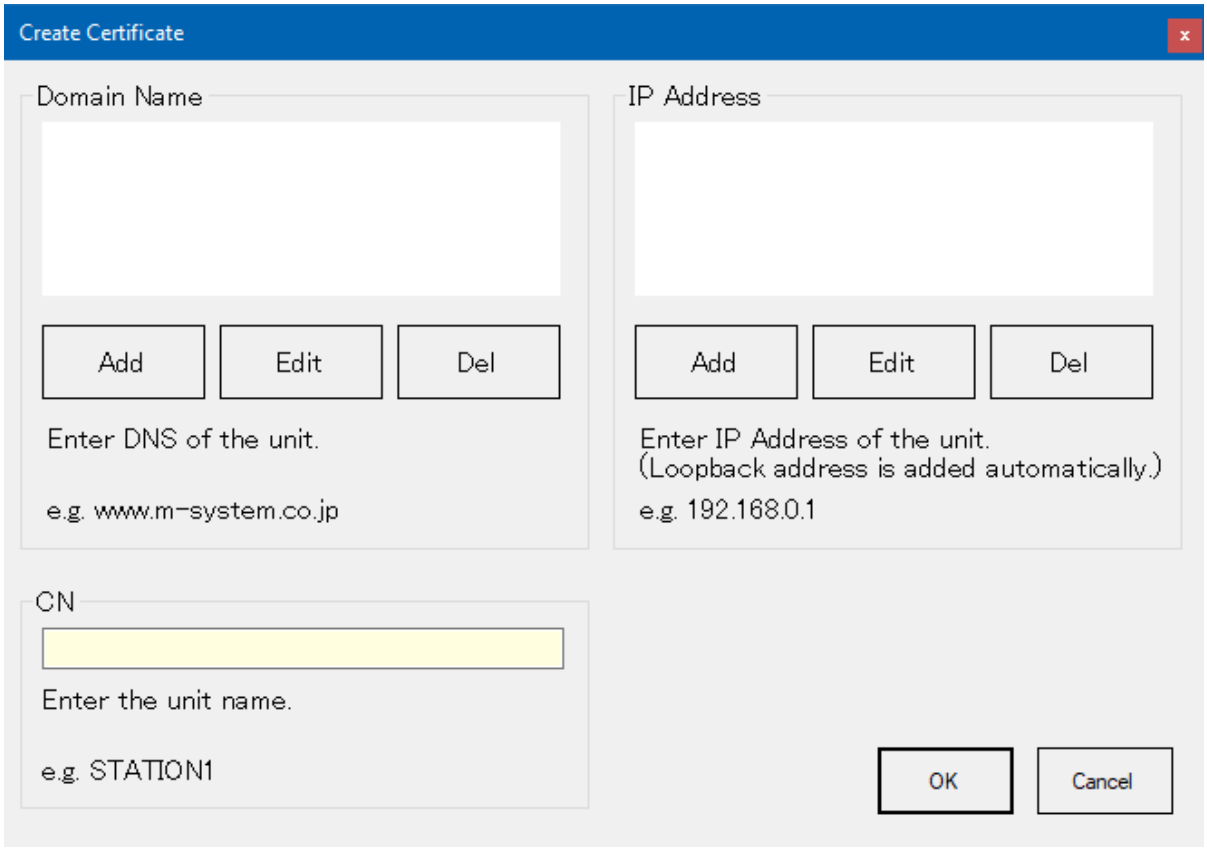
(3) After the Local Certification Authority has been created, the LCA-SG main screen as shown below appears.



5.4 Creating and Transferring Unit Certificate and Private Key

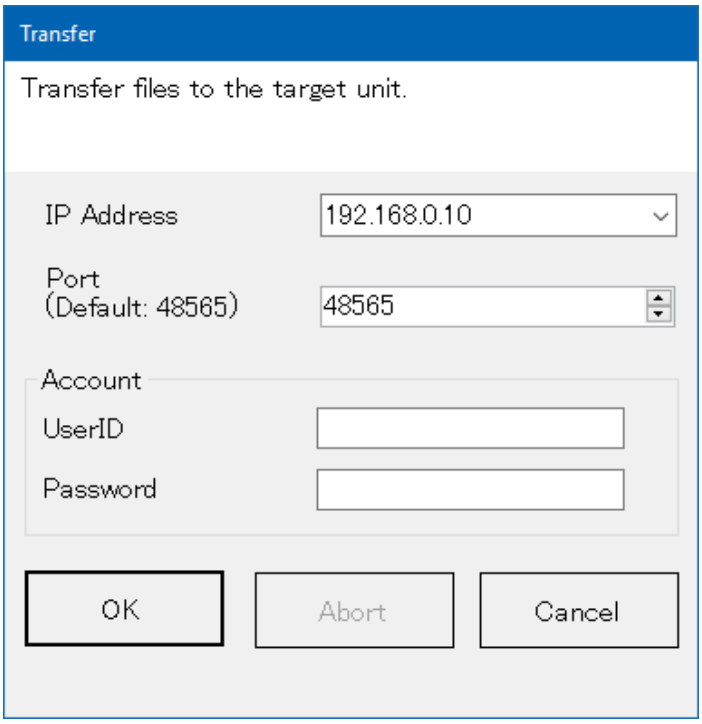
Next, you can create the SG6 unit certificate and transfer it to the device.

Click "New Certificate(C)" to open the dialog below. Set up information necessary to access to the SG6.



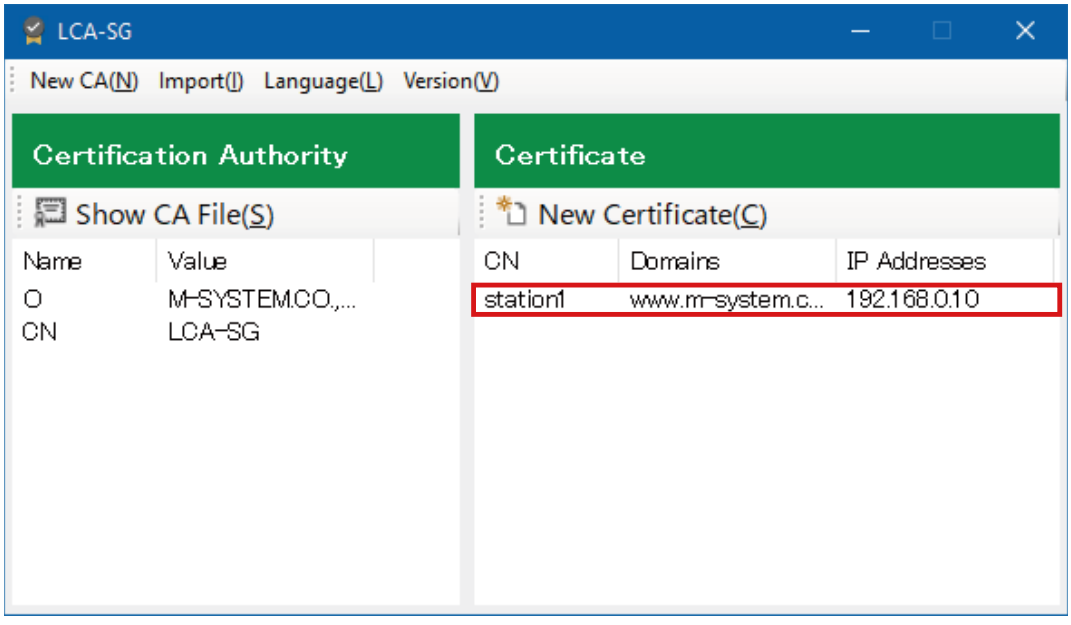
PARAMETER ITEM	DESCRIPTION
Domain Name	Enter the domain name of the SG6 for connecting to it through the internet. Use only alpha-numeric characters (Japanese characters are invalid). Up to 16 domain names can be registered. Usable characters: First character : A-Z, a-z, " _ (underscore)" Second and following characters: A-Z, a-z, 0-9, " _ (underscore)", " , (comma)", " . (period)", " - (hyphen)", " (blank)"
IP Address	Enter the IP address of both SG6 server and client for accessing the devices on a browser via a LAN or the internet. Use only alphanumeric characters. (Not compatible with IPv6) Up to 16 IP addresses can be registered. If you wish to reduce the number of IP addresses, you can set only one address as indicated below. Normal mode connection: SG6 server address Reverse mode connection: SG6 client address
CN	Enter the name to identify the SG6. Usable characters: First character: A-Z, a-z, " _ (underscore)" Second and following characters: A-Z, a-z, 0-9, " _ (underscore)", " , (comma)", " . (period)", " - (hyphen)", " (blank)"

(1) Click [OK] and the confirmation dialog appears. Click [Yes] to open the [Transfer] dialog.



(2) Confirm the target IP address and enter the user ID and password to login to the SG6.
Click [OK] to start the transfer of the certificate to the SG6.

(3) On the main screen, generated certificates are listed on the [Certificate] frame.
When two or more SG6 exists, repeat the same process for the number of units or right-click on the relevant certificate and select [Create / Transfer].
Transfer certificates to both SG6 server and SG6 client.
Reboot the SG6 after transferring.



NOTES

- File transfer must be executed only in a LAN environment.
- Please make sure to enter the domain name and IP address correctly.

5.5 Installing CA Certificate on Web Terminal

5.5.1 General Descriptions

In order to enable HTTPS through the SG6 when a web browser accesses a web server, the CA certificate as explained in "5.3 Creating Local Certification Authority" on page 8 must be installed on the terminal with browser.

This procedure must be performed on every terminal accessing the SG6 which has certificate signed by this Local Certification Authority.

If a terminal without the certificate accesses the SG6 over HTTPS, a security warning will appear on the browser.

The installation method varies depending on the software environment of the terminal.

5.5.2 Installing Certificate via LCA-SG

■ Windows (Chrome, Edge)

(1) Click [Show CA File(S)] on the LCA-SG main screen to display [Certificate] window.
Click [Install Certificate...] to start the [Certificate Import Wizard].

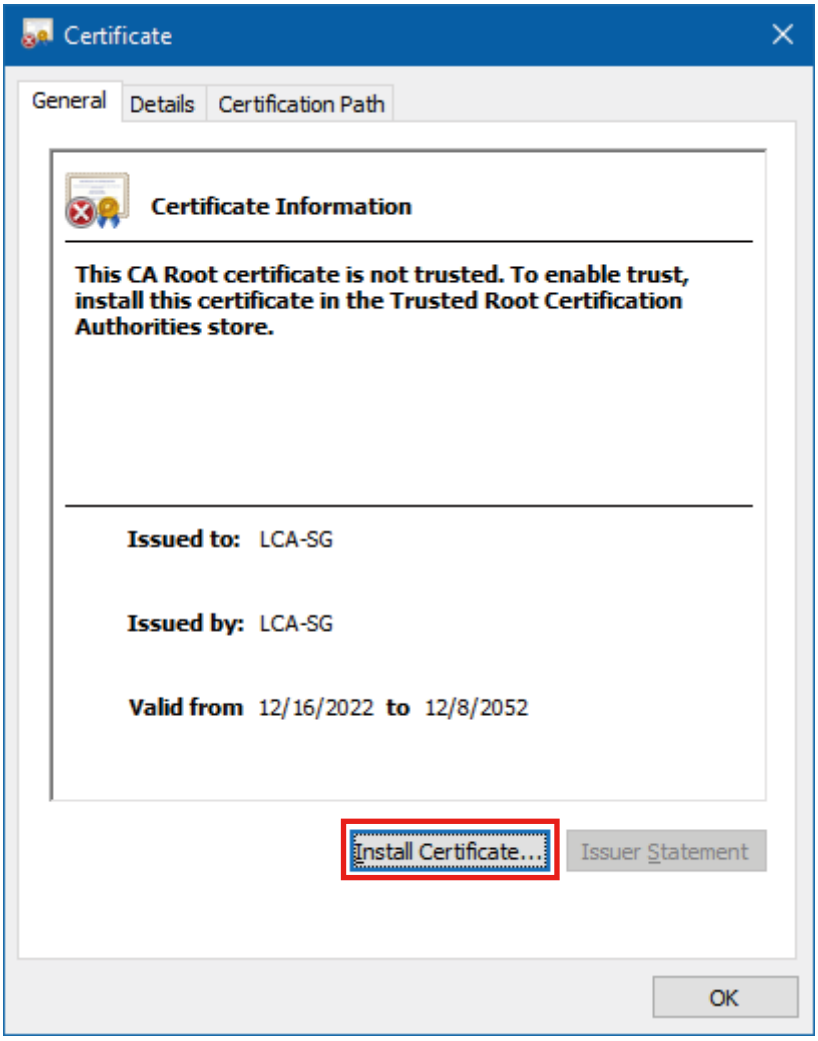


Figure. [Certificate] window when [General] tab is selected

(2) On the [Certificate Import Wizard] window, select [Current User] under Store Location and click [Next] button.

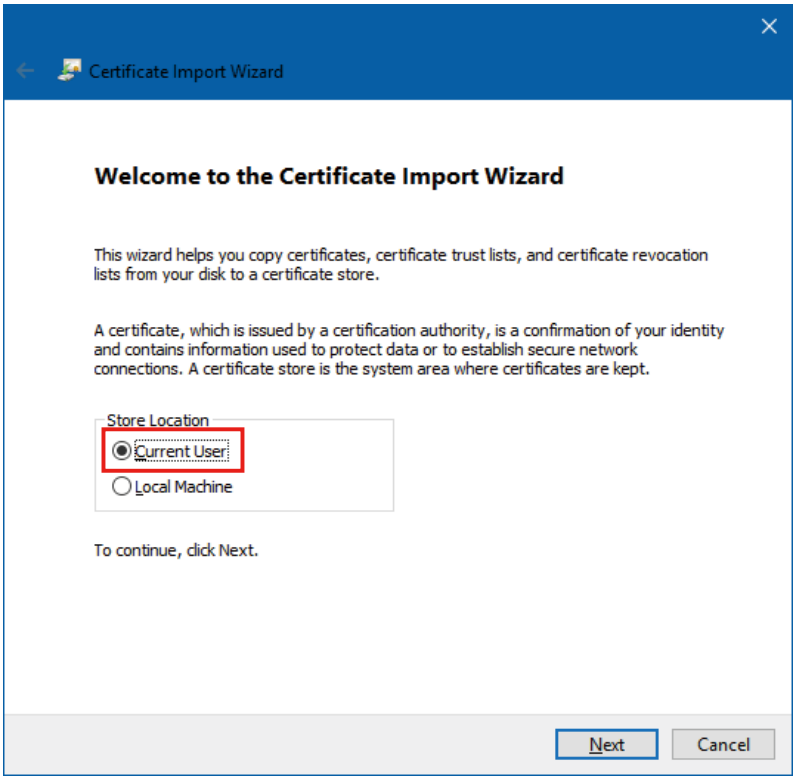


Figure. Initial View of [Certificate Import Wizard]

(3) On the [Certificate Store] window, select [Place all certificates in the following store], and click [Browse].

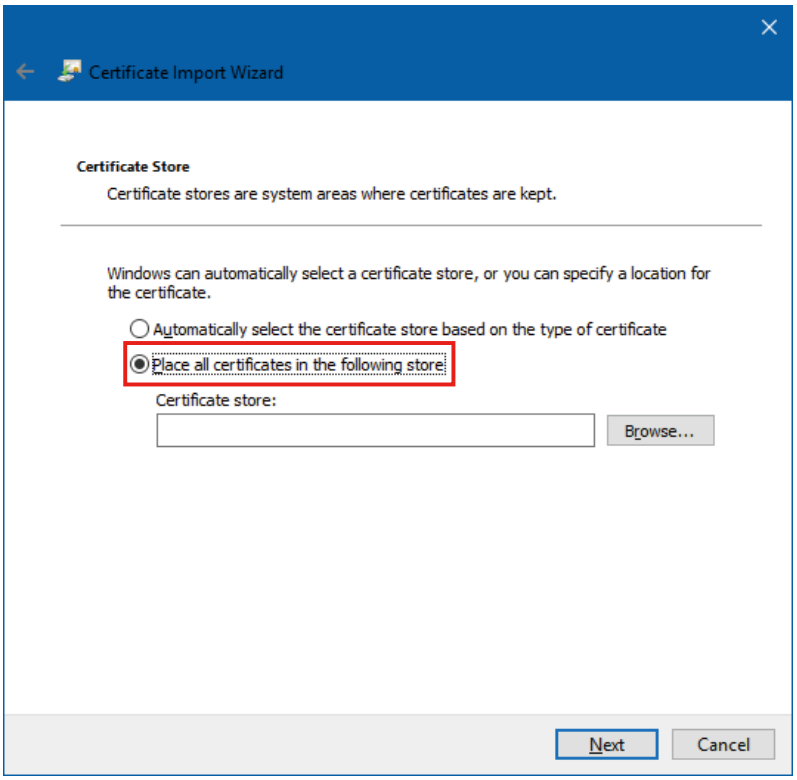


Figure. [Certificate Store] screen

(4) As the [Select Certificate Store] dialog appears, select the [Trusted Root Certification Authorities] folder, and click [OK].

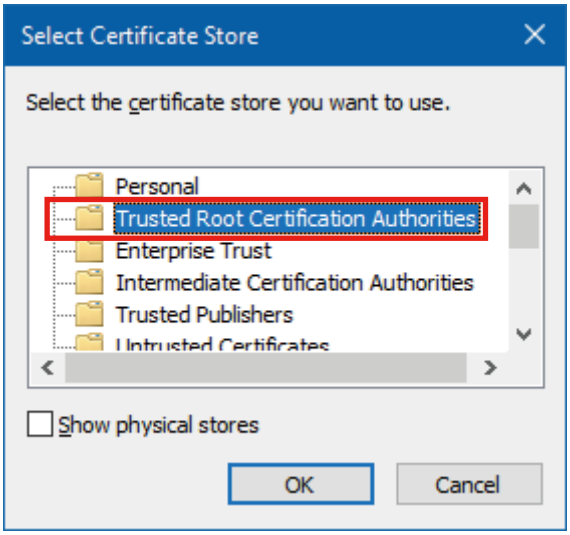


Figure. [Select Certificate Store] dialog

(5) A Windows security warning may appear during the import process.
The LCA-SG enables the user (yourself) to become a root certification authority. Read carefully the warning message before proceeding.

5.5.3 Using CA Certificate File

■ Windows (Chrome, Edge)

1) Save the certificate by following the procedure as in "5.6 Save CA Certificate File" on page 21.
2) Double-click the saved certificate to open the [Certificate] dialog.
   Click "Install Certificate...", then the [Certificate Import Wizard] starts.
   Follow the same procedure as in "5.5.2 Installing Certificate via LCA-SG" on page 11.
   The procedure is the same if the LCA-SG is not installed on the Windows terminal.

■ Windows (FireFox)

1) Save the certificate by following the procedure as in "5.6 Save CA Certificate File" on page 21
2) Start the FireFox browser, click menu at the right top and select Options.

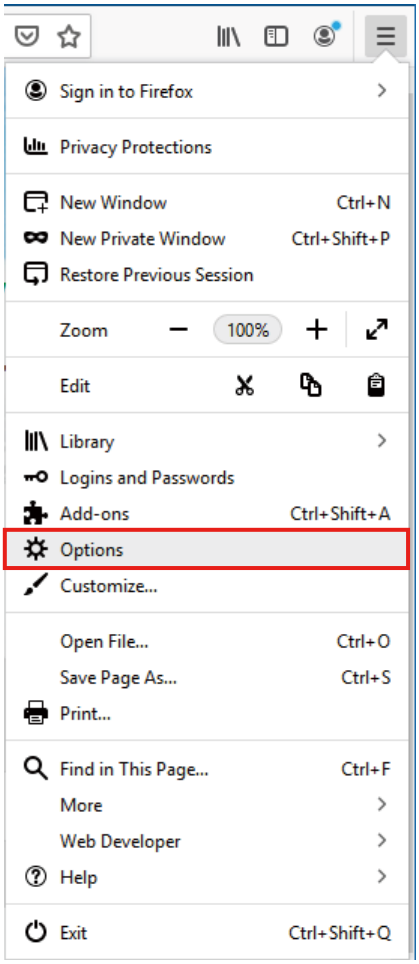


Figure. Firefox browser

3) Click "Privacy & Security".

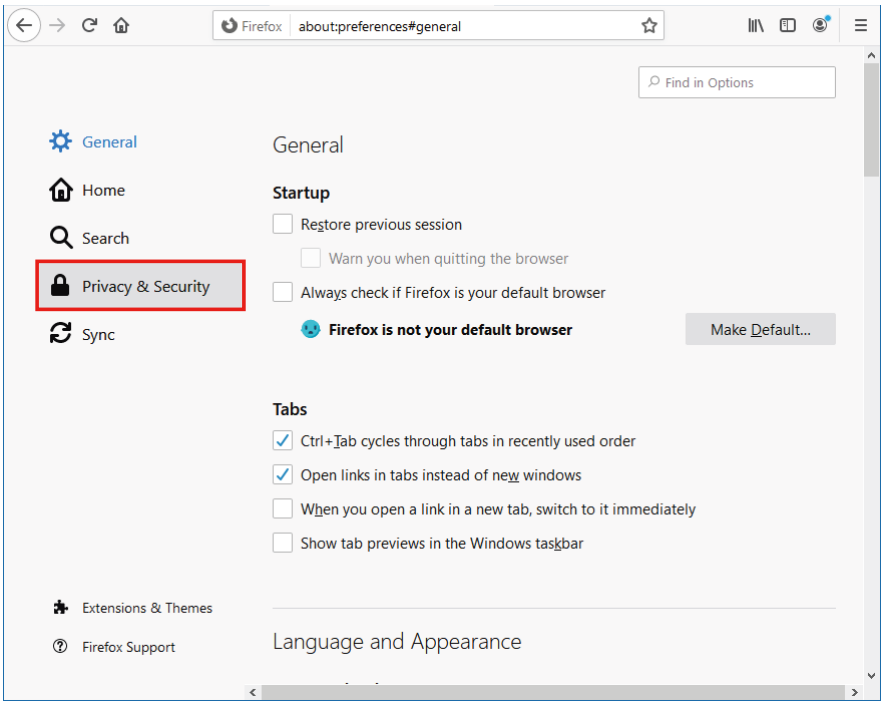


Figure. Firefox [Options] screen

4) Scroll down to Security and click "View Certificates...".

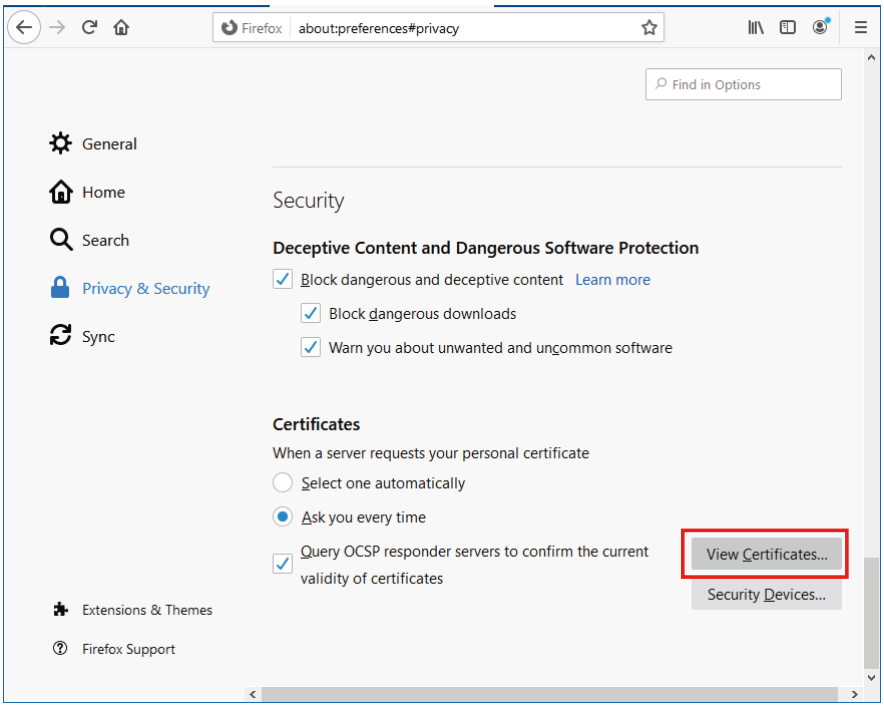


Figure. Firefox [Privacy & Security] screen

5) As the "Certificate Manager" appears, click "Import..." button.

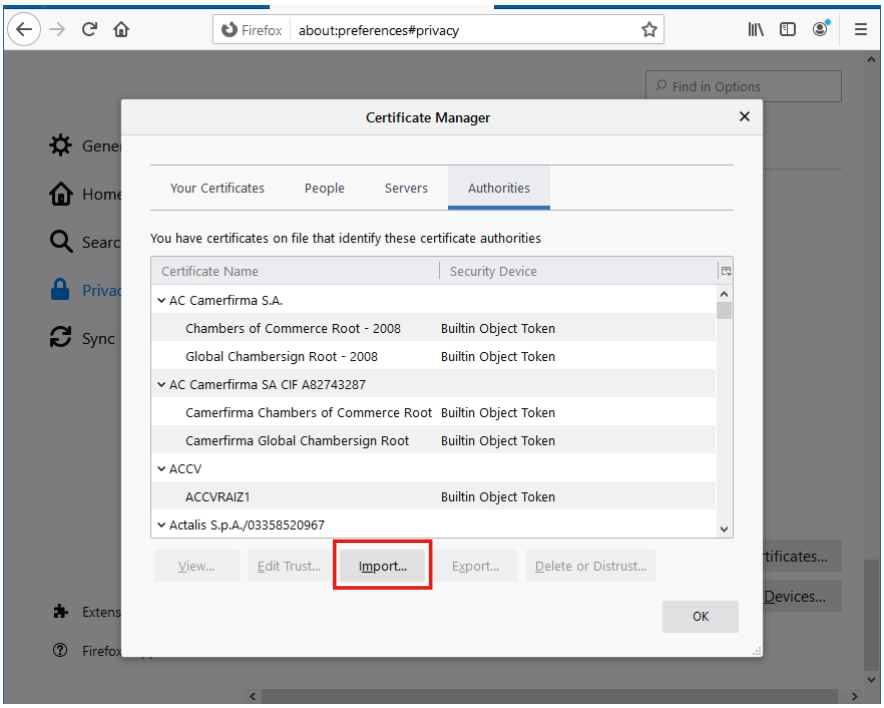


Figure. Firefox [Certificate Manager] window

6) As the [Select File...] window appears, select the file (cacert.crt) saved in Step 1.

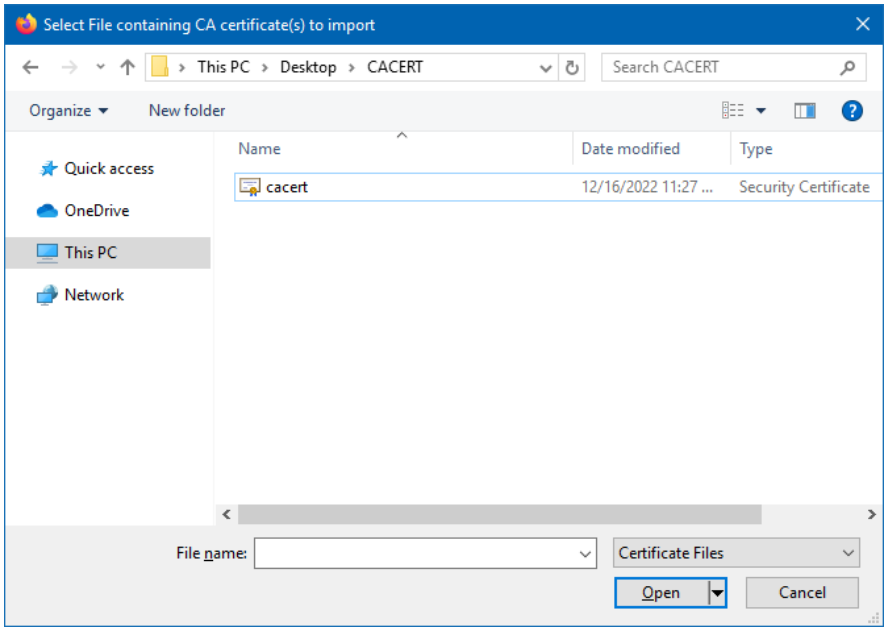


Figure. File Selector window

7) As the "Downloading Certificate" appears, check the box "Trust this CA to identify websites" and click OK.

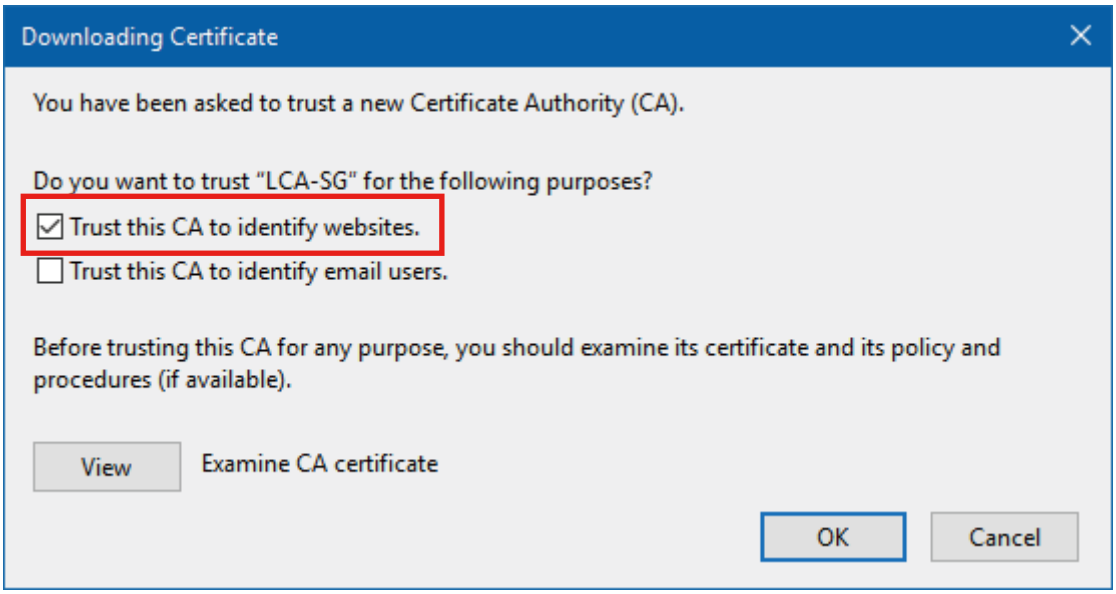


Figure. Firefox [Downloading Certificate] dialog

8) Close the Firefox browser.

5.5.4 Installing CA Certificate File from SG6

■ Windows (Chrome, Edge, FireFox)

1) Login to the SG6, then download the certificate from "Download CA Certificate File" in "Maintenance". Follow the same procedure as in "5.5.3 Using CA Certificate File" on page 14.

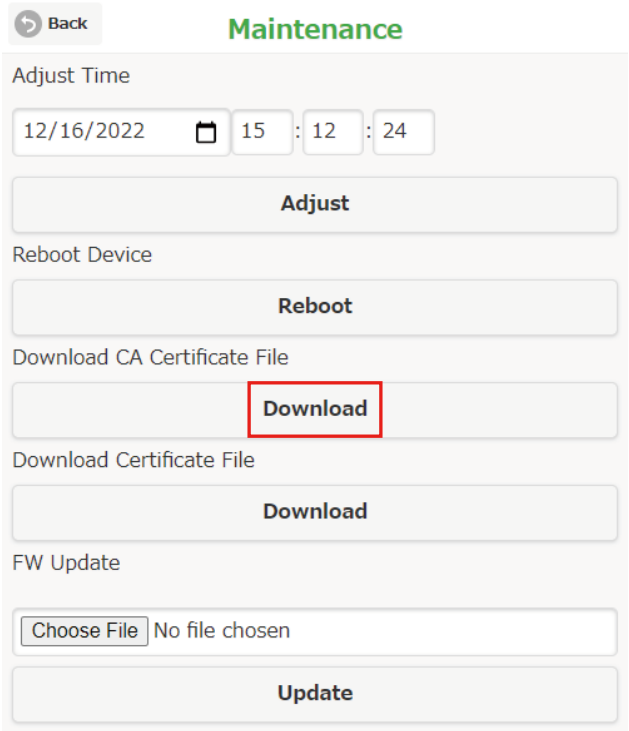


Figure. CA Certificate Download Screen

■ **IPadOS (Safari)**

1) Login to the SG6, then tap "Download CA Certificate File" in "Maintenance".
As the message window shown in the following figure appears, tap "Allow".

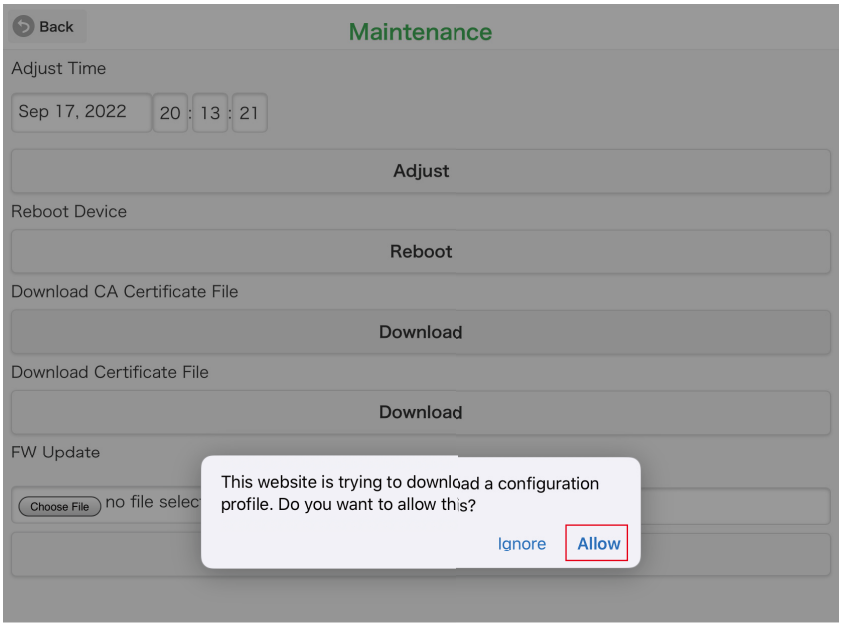


Figure. iPadOS Download confirmation dialog

2) After the file has been downloaded, go back to the Home screen, and tap Settings (gear icon).
Go to [Profile Downloaded].

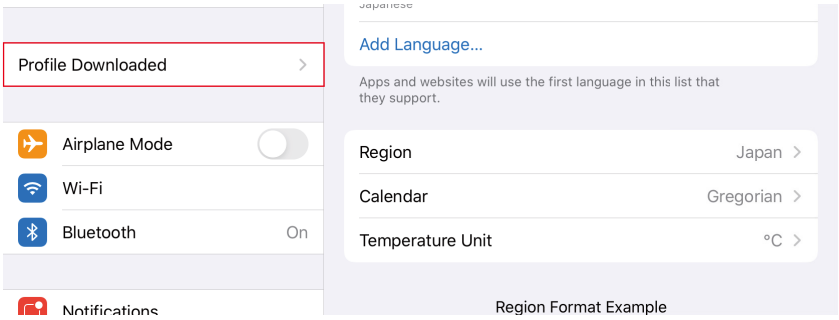


Figure. iPadOS Settings Screen

3) Tap the downloaded profile to display the [Install Profile] window.
Tap [Install] at the right top of the window to start installation of the profile on the terminal.
If a security warning appears during the installation, tap [Install] again to continue the installation.

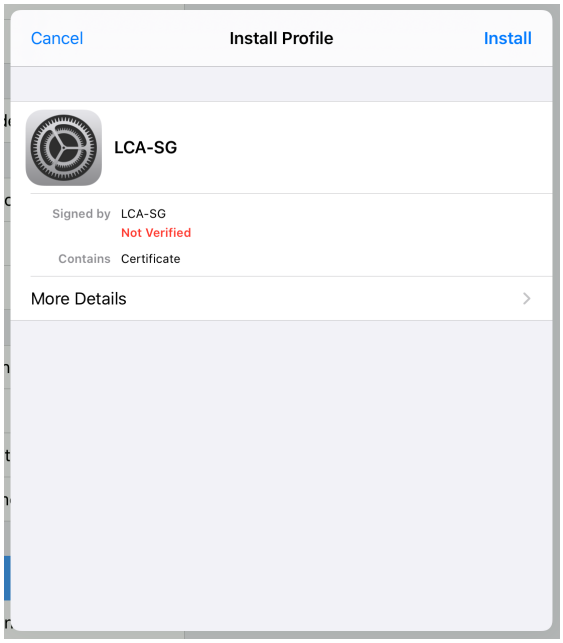


Figure. iPadOS [Install Profile] window

4) When the installation has been completed, tap [Settings] > [General] > [About] > [Certificate Trust Settings] to open the [Certificate Trust Settings] screen.
Under "Enable full trust for root certificates," turn on trust for the downloaded certificate.

■ **Android (Chrome)**

1) Login to the SG6, then tap "Download CA Certificate File" in "Maintenance".

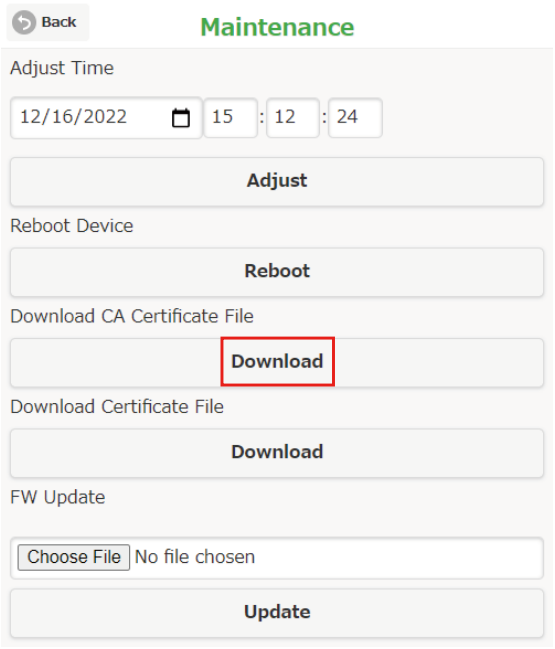


Figure. Android Maintenance Screen

2) Open Downloads from the menu on the right-top of the Chrome, and tap the saved certificate.

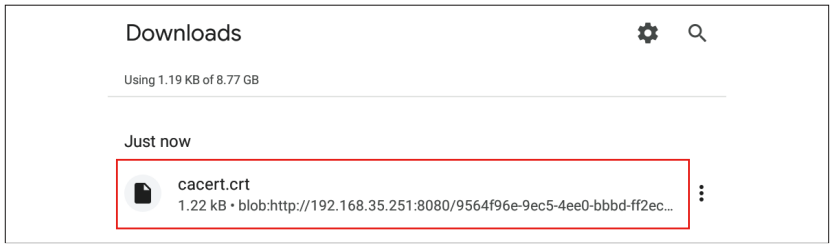


Figure. Download Screen

3) Enter any certificate name and tap OK to register the certificate.

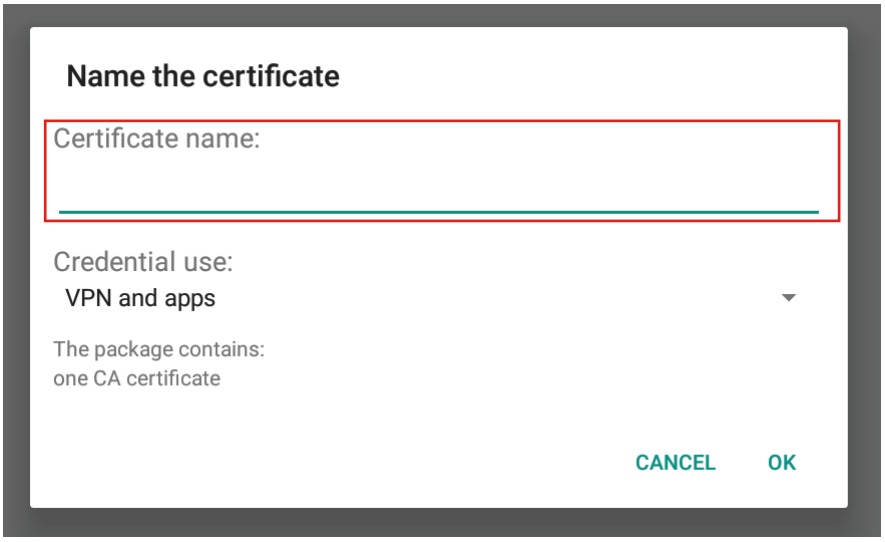
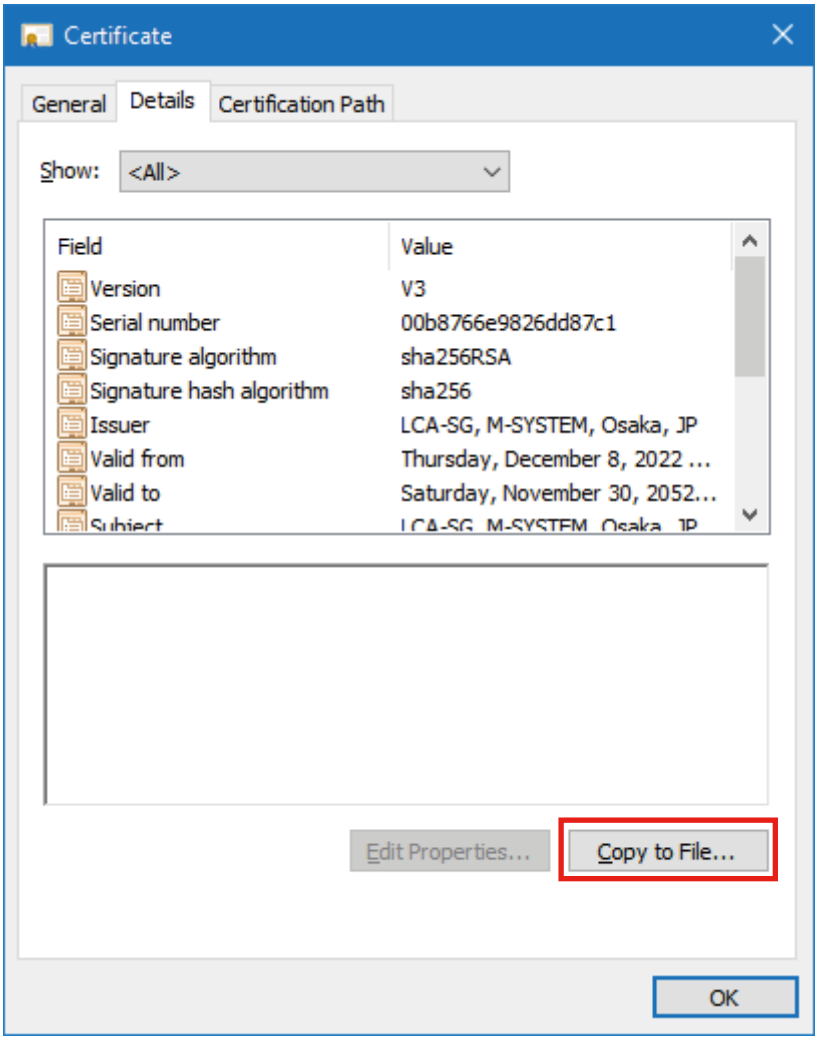


Figure. Android Certificate Installer Screen

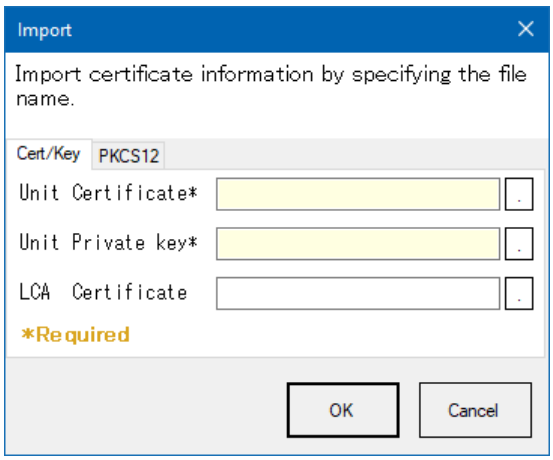
5.6 Save CA Certificate File

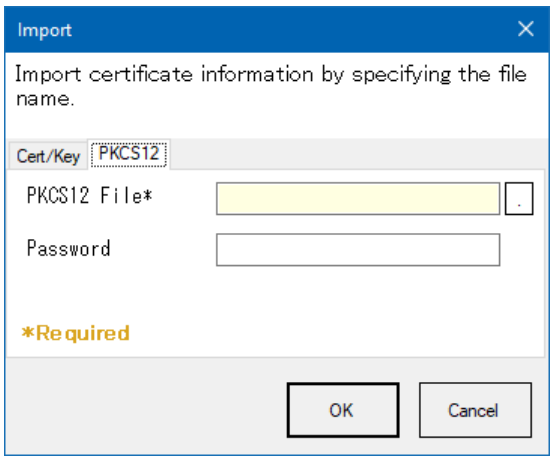
You can save to a device the certificate created as in "5.3 Creating Local Certification Authority" on page 8.
Click "Show CA File(S)" on the main screen, go to "Details" tab and click "Copy to FIle..."



5.7 Importing Third-party Certificate

You can use a third-party CA without using the LCA by the LCA-SG.
In this case, transfer the unit certificate, the private key and the CA certificate to the SG6 via the LCA-SG.





Compatible certificate formats are as follows: PEM (.crt, .key)
DER (.der)
PKCS12 (.pfx, .p12)

Select a file and click [OK] to start file transfer.

NOTES

- Please address any questions to the relevant third party CA regarding the import of third-party certificates.

5.8 Rebuilding Local Certification Authority

Normally, there is no need to rebuild the Local Certification Authority which was created at the initial startup of LCA-SG after its installation.
However, if need arises, rebuild the Local Certification Authority by clicking [New CA(N)] on the main screen.

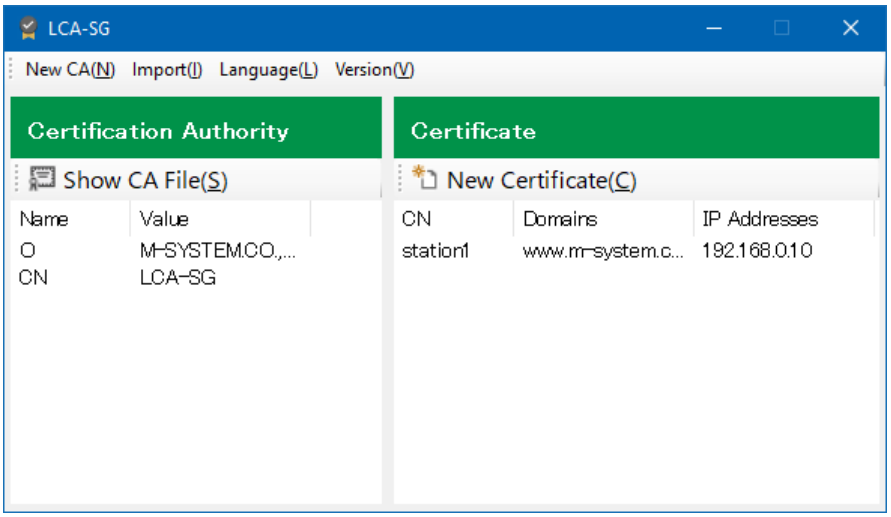


Figure 29 Rebuilding Local Certification Authority

In that case, the certificate for the new Local Certification Authority must be manually installed on the SG6 again.

5.9 Switching Display Language

The display language of LCA-SG is automatically selected by identifying your OS language.
Japanese is selected for Japanese OS and English is selected for non-Japanese OS.
In order to manually switch the display language, click [Language(L)] on the main screen to display Language.
Restart LCA-SG to apply the change.

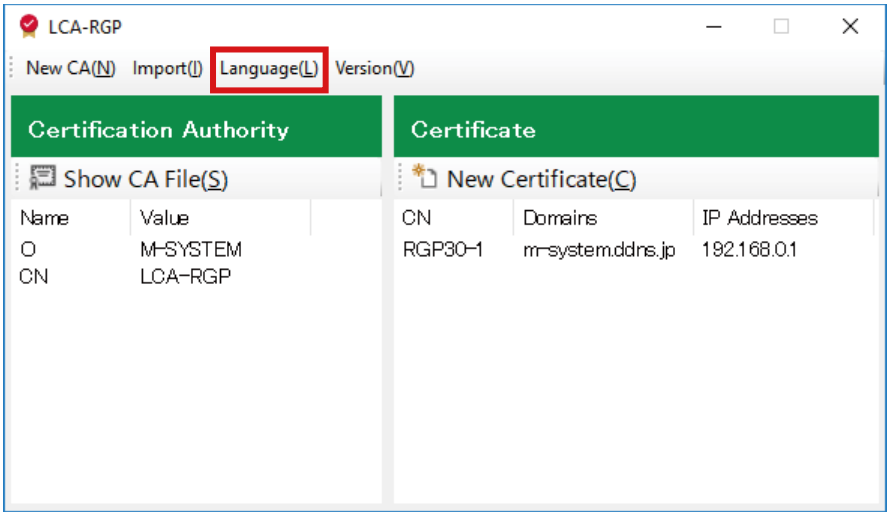


Figure 30 Switching Display Language

6. LICENSE

The LCA-SG uses OpenSSL v1.0.1r (dual license of OpenSSL and Original SSLeay).

The LCA-SG contains software to which the following Camellia license is applicable.

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)." The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].