

# CITIZEN

## **IF5-EFX1**

# **Ethernet Interface Board User's Manual**

Ver.1.10

**CITIZEN SYSTEMS JAPAN CO., LTD.**

# Contents

<b>Contents .....</b>	<b>2</b>
<b>Read before using .....</b>	<b>4</b>
<b>1. Introduction .....</b>	<b>5</b>
1-1. Features .....	5
1-2. Specifications .....	6
1-3. Part Names and Functions .....	7
<b>2. Preparation .....</b>	<b>8</b>
2-1. Connecting LAN cable.....	8
<b>3. Network Settings and Operation .....</b>	<b>9</b>
3-1. Overview .....	9
3-2. Panel Button .....	11
3-3. Printing the Interface Board Configuration.....	12
3-4. Returning the Interface Board Configuration to Factory Default Settings.....	13
3-5. Display status by LED .....	14
3-6. Simple Setting Procedure Example for Wired LAN .....	15
<b>4. Web Manager .....</b>	<b>16</b>
4-1. Starting the Web Manager .....	16
4-1-1. Initial Setup (Board Firmware v1.19 and later) .....	17
4-2. HOME Window .....	18
4-3. STATUS Window .....	19
4-3-1. STATUS>>System Status Tab .....	20
4-3-2. STATUS>>Network Status Tab .....	21
4-3-3. STATUS>>Printer Status Tab.....	22
4-3-4. STATUS>>Service Status Tab.....	23
4-4. CONFIG Window.....	24
4-4-1. CONFIG>>General Tab .....	25
4-4-2. CONFIG>>User Account Tab .....	26
4-4-3. CONFIG>>Maintenance Tab .....	27
<b>5. NetToolK.....</b>	<b>28</b>
5-1. Installing the NetToolK .....	28
5-2. Information List Window.....	31
5-3. Setup Window .....	33
5-3-1. “General” Tab.....	33
5-3-2. “Wireless LAN” Tab.....	33
5-3-3. “Supported Protocols” Tab .....	34
5-4. “User Account” Tab.....	34
5-5. “Maintenance” Tab .....	35
<b>6. XML Function.....</b>	<b>37</b>
6-1. Overview .....	37
6-2. CONFIG>>Service Tab .....	38
6-2-1. XML Print.....	38

---

6-2-2.	XML Config.....	38
6-2-3.	XML Settings (Displayed only for firmware version V1.14 and later) .....	38
6-2-4.	Submit / Reset Button.....	39
<b>7.</b>	<b>SSL/TLS function .....</b>	<b>40</b>
7-1.	Overview .....	40
7-2.	CONFIG>>SSL/TLS Tab .....	42
7-2-1.	SSL/TLS tab .....	42
7-2-2.	Create Self-Signed Certificate .....	43
7-2-3.	Update Self-Signed Certificate.....	44
7-3.	To enable SSL/TLS communication using a self-signed certificate .....	45
7-3-1.	Generating and exporting self-signed certificates .....	45
7-3-2.	Example of importing a self-signed certificate in a browser (Chrome) .....	50
7-4.	SSL/TLS and certificate related specifications .....	54
7-4-1.	SSL/TLS communication specifications.....	54
7-4-2.	Self-signed certificate related specifications .....	56
7-4-3.	CA signed certificate related specifications.....	57
7-4-4.	Handling of saved certificates when restoring factory settings/updating firmware .....	57

## Read before using

Be sure to read this manual carefully before using the product. After you read it, store it in a safe place so that you can reread it when necessary.

- Contents of this manual may be changed without notice.
- Reproducing and/or copying the contents of this manual by any means without permission are prohibited.
- We will not be responsible for any adverse occurrence that results from the use of this manual, regardless if it contains omissions, errors/misprints, etc.
- Note that we will not be responsible for (a) loss caused by improper operation or mishandling of the device by the user, or (b) loss due to operational environment.
- Data etc. are basically impermanent; long time or permanent storing/saving of data by the device is not possible.
- Note that we will not be responsible for any loss or loss of profits owing to loss of data due to breakdown, repairs, inspections, etc.
- Please contact us if there are omissions, errors, ambiguities, etc. in this manual.
- Refer to this document along with the user manual of the printer.

### Trademarks

- Microsoft, Windows 7, Windows 8, Windows 10 and Windows 11 are registered trademarks of Microsoft Corporation U.S.A.
- CITIZEN is a registered trademark of Citizen Watch Co., Ltd.
- Other company names and product names mentioned here are trademarks or registered trademarks of those companies.

# 1. Introduction

Thank you for purchasing the Citizen IF5-EFX1 Ethernet (LAN) interface board.

By using the LAN interface board (hereinafter referred to as the interface board) with our label printers, you can connect printers directly to a network and use computers on the network to print to the printers. It also enables mutual communication between the PC and the printer, so that the printer's operating status and print settings can be checked from the PC. In addition, printing based on XML format data can be performed.

Please note that the following is supported only if the firmware of this board is of the compatible version or later.

For firmware version V1.19 and later, you will be prompted to set an administrator password during the initial setup.

Function	Supported Version
SSL/TLS Function (TLS1.3, ECDSA signature)	V1.14 and later
XML Config (version 2.0)	V1.14 and later
HTTP Keep Alive	V1.14 and later
Administrator Password Initial Setup Function	V1.19 and later

## 1-1. Features

- Support for DHCP, static IP, and ZeroConf methods of IP address acquisition
- Configuration through a browser or utility software
- Support for Raw 9100 port and LPR printing methods
- Panel button to print configuration information and change the configuration mode
- LED indicators for connection, operation, and error statuses
- Support for printing by XML data depending on the printer
- Secure communication with SSL/TLS function.
- XML Config function is available for configuration of the board.

## 2 Introduction

---

### 1-2. Specifications

#### Main board (Network)

Ethernet	Standards	100BASE-TX/10BASE-T, Full Duplex/Half Duplex auto negotiation
	Port	RJ-45
Network	IP Version	IPv4
	Protocols	TCP, UDP, HTTP, HTTPS, ICMP, DHCP, SNMP
	Port number for printing	RAW (port 9100 (Changeable)), LPR
	IP address setting	Manual, DHCP

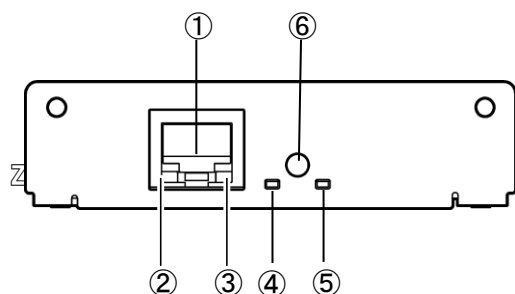
#### Hardware

Type name		IF5-EFX1
Hardware	Supported Models	CL-S5xx(II) / 6xx(II) / 70x(II) series
	Operation panel	LED: 4 (2 on panel, 2 on RJ45 connector), Button: 1

#### Software

Software	Setting methods	Browser, PC setting tool, Cloud
	Firmware upgrade	Browser, PC setting tool, Cloud
	Supported Platforms	Windows 7, Windows8, Windows10, Windows 11, HTML5 browser

### 1-3. Part Names and Functions



- ① RJ45 connector (compatible with 10Base-T/100Base-TX)  
Connection for LAN cable
- ② Ethernet transmission speed LED indicator (green)\*<sup>1</sup>  
Shows Ethernet transmission speed with steady/blinking light.
- ③ Ethernet status indicator LED (yellow)\*<sup>1</sup>  
Shows Ethernet connection status (disconnected, receiving data, etc.).
- ④ Ethernet status LED indicator (green)\*<sup>1</sup>
- ⑤ Ethernet status LED indicator (red)\*<sup>1</sup>  
Shows transmission, connection and error statuses with steady/blinking lights combinations.
- ⑥ Panel button\*<sup>2</sup>  
Used to operate the Interface board.

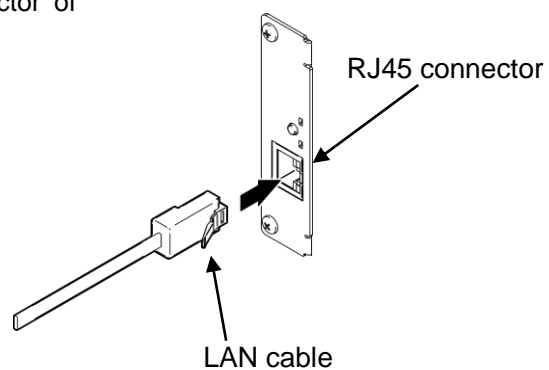
\*<sup>1</sup> See 3-5, Display status by LED (page 14) for indicator details.

\*<sup>2</sup> See 3-2, Panel Button (page 11) for panel button operations.

## 2. Preparation

### 2-1. Connecting LAN cable

Connect a LAN cable to the RJ45 connector of this interface board.



### 3. Network Settings and Operation

#### 3-1. Overview

To use this interface board connected to a network, you need to connect to the network and configure the settings for communication in addition to configuring the settings of the printer.

If the firmware version of this board is V1.19 or later, it is necessary to set the user password via Web Manager during the initial setup.

For making configuration changes for network connection after the initial setup, three methods are available.

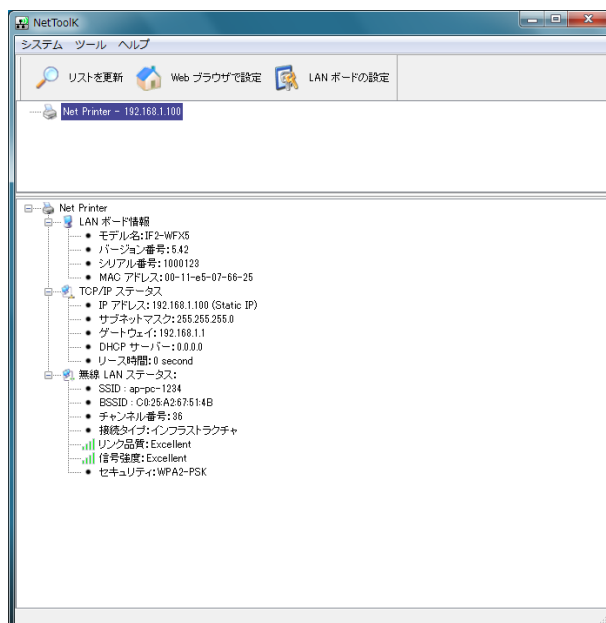
##### Web Manager

Connect to this interface board from a browser and then configure the settings on the dedicated settings screen.



##### NetToolK

Connect to this interface board from a dedicated tool for Windows and then configure the settings.



## 2 Network Settings and Operation

---

You can check the current state and restore the initial state by operating the panel button.

See the next page for an explanation of the panel button.

Furthermore, you can check the communication and other statuses from the LEDs on the interface.

See “3-5 Display status by LED” (page14).

### **XML Config**

By sending XML format data to this interface board, you can configure some of the board's functions.

Details are beyond the scope of this manual. Therefore, please refer to the manual of XML Config SDK for details.

JavaScript and Excel VBA macros are available as sample programs for this function.

The timeout setting for this function is present in the 6-2 CONFIG>>Service Tab.

### **Warning**

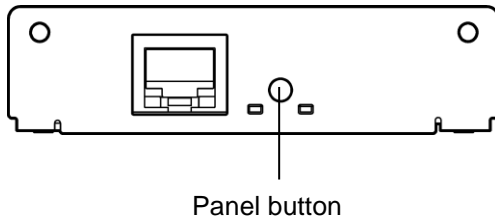
After the firmware upgrade starts, do not disconnect power or transmission to the printer until the upgrade is complete.

When updating the firmware, it is necessary to obtain the correct firmware data from us.

If the firmware is not updated correctly, this interface board may not boot.

### 3-2. Panel Button

The panel button on the operation panel is used to operate the Interface board. It allows you to print the setting information of this interface board and restore the initial state.



#### ■ Starting the Interface Board

Turn on the printer. The Interface board starts working approximately 20 seconds after the printer turns on.

#### ■ Printing the Interface Board Configuration

Press the panel button. See 3-3, Printing the Interface Board Configuration (page 12) for details.

#### ■ Switching to Setting Mode

Press and hold the panel button. The buzzer\* will sound once, signaling a switch to setting mode.

- Setting mode enables the reading of the factory default settings. See 0, (page 12) for details.
- If there is no activity for three seconds in the setting mode, the buzzer\* will sound once, signaling a return to normal mode.

- \* If the printer to which this interface board is connected is set to not buzz, the buzzer will not sound.

#### Warning

When the operation is complete, the interface board will restart automatically.

When automatically obtaining the IP address from the DHCP server is set, an IP address that differs from the previous one may be assigned.

### 3-3. Printing the Interface Board Configuration

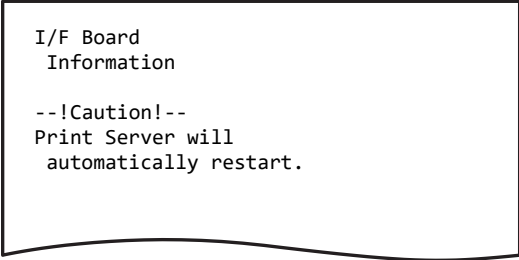
Press the panel button to print out the configuration of the interface board from the printer.

- ① Title of the printout.
- ② Model name, hardware revision, and firmware version of the interface board
- ③ System information of the interface board  
The LAN board name, serial number, and MAC address are printed.
- ④ Network information of the interface board
- ⑤ Ethernet information. Printed when connected by Ethernet.
- ⑥ Printer information. The name of the manufacturer and the model name of the printer connected to the interface board are printed.
- ⑦ Configuration information of the interface board. The information stored in the interface board is printed and may be different from the connection status of the current network. Check the connection status using the network information of ④.
- ⑧ Configuration information of SSL/TLS function

①	I/F Board Information
②	IF5-EFX1(Rev1.1.3): Ver 1.07
③	System LAN Board Name : Net Printer Serial Number : 100123 MAC Address : 00:01:02:0a:0b:0c
④	Current Network Status IP Address : 192.168.0.2 (DHCP) Subnet Mask : 255.255.255.0 Gateway : 192.168.0.1 DHCP Server : 192.168.0.1
⑤	Ethernet Status Speed & Duplex : Auto (100BaseTx Full)
⑥	Printer Status Manufacturer : CITIZEN Model : CL-S521
⑦	User Configuration DHCP : Enable IP Address : 192.168.0.10 Subnet Mask : 255.255.255.0 Gateway : 192.168.0.1 Print Port : 9100 Receive Timeout : 180
⑧	SSL/TLS Certificate : Disable Self-Signed : Not Exist CA-Signed : Not Exist

### 3-4. Returning the Interface Board Configuration to Factory Default Settings

- 1) Press and hold the panel button to switch to setting mode.
- 2) After the interface board has switched to setting mode, press and holds the panel button again within 3 seconds. The following message is printed, and the interface board returns to factory default settings.



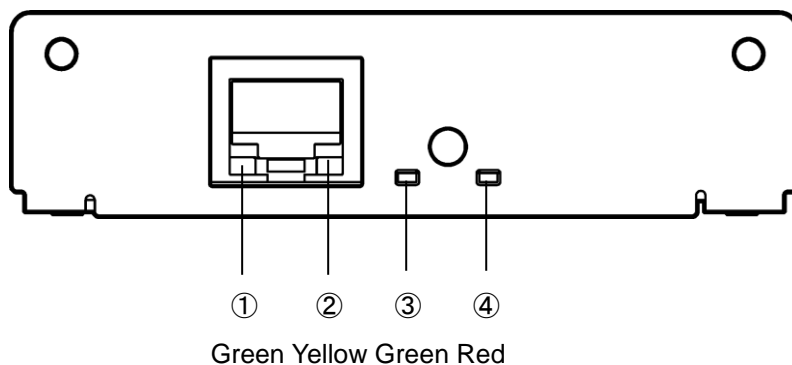
```
I/F Board  
Information  
  
--!Caution!--  
Print Server will  
automatically restart.
```

#### Warning

When the operation completes, this interface board restarts automatically.  
When automatically obtaining the IP address from the DHCP server is set, an IP address that differs from the previous one may be assigned.

### 3-5. Display status by LED

The meanings of each LED display are as follows.



#### ① Ethernet transmission speed indicator

Transmission speed	LED (green)
100 Mbps	On
10 Mbps / Disconnected	Off

#### ② Ethernet connection/transmission status indicator

Connection status	LED (yellow)
Connected	On
Disconnected	Off
Transmitting data	Flashing

#### ③ ④ LAN status indicator

Connection Status		LED (green)	LED (red)	Description
Printer disconnected		Off	-	Not connected to printer.
Printer connection	Network: disconnected	On	Off	Connected to printer.
	Ethernet connecting	On	Flashing (1-second cycle)	Seeking IP address from DHCP server via Ethernet.
	Ethernet working	On	On	Network operation via Ethernet.
Resource error		Alternating blinking (1-second cycle)		The interface board is malfunctioning.
System error		Alternating blinking (0.2-second cycle)		The interface board is malfunctioning.

### 3-6. Simple Setting Procedure Example for Wired LAN

If you do not know much about network settings, configure the settings about the corresponding procedure below.

However, the instructions in the procedure may not necessarily be appropriate for your network environment.

■ Configuration where an IP address is assigned from a DHCP server

- 1) Connect the LAN cable to the interface board. The LAN cable must be connected to, for example, an enabled network environment in which a DHCP server exists.
- 2) The IP address is automatically obtained from the DHCP server within 90 seconds after powering on the printer and starting up this interface board.

Press the panel button to print out the configuration information and check the assigned IP address. See 3-3, Printing the Interface Board Configuration (page 12) for details.

- 3) Once the conditions for the printer to join the network are in place, configure the wired LAN settings in Web Manager.

Connect to Web Manager of the printer from the browser of a PC connected to the same network.

See “4 Web Manager” (page 16) for details.

Instead of Web Manager, you can also use NetToolK, a network configuration tool for Windows.

See “5 NetToolK” (page 28) for details.

■ Configuration using a static IP address

The procedure differs for the part of step 2) above. Since the IP address assigned by the DHCP server is not used, the ZeroConf function assigns an IP address of 169.254.XX.YY (XX.YY varies depending on the environment). Press the panel button to print the setting information and then confirm the assigned IP address.

Adjust the IP address of your PC so that it can connect to the IP address of the printer.

The subsequent procedure is the same as step 3) above.

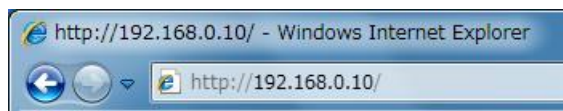
## 4. Web Manager

The Interface board is equipped with a Web manager function, which allows accessing the Interface board from a web browser and checking the status or change settings of the interface board.

### 4-1. Starting the Web Manager

In the address bar, enter the IP address and then press **Enter**.

If the SSL/TLS feature is enabled, you can also connect using “https”.



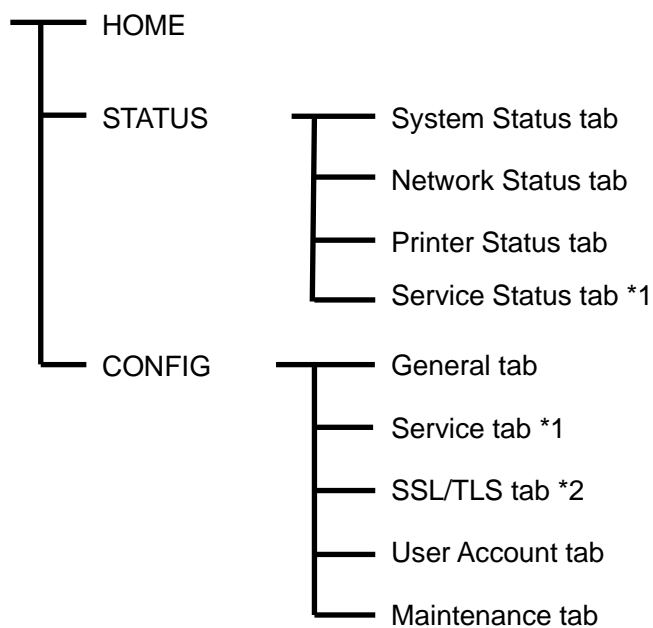
\* The image to the left is a sample. Enter the actual allocated value for the IP address.

#### Warning

- If the network settings of your PC and this interface board do not match, you will not be able to display the configuration screen of this interface board. Please match the IP address of the interface board to the network settings you are using.
- The IP address of this interface can be confirmed as described in “Printing the Interface Board Configuration”.

#### Web Manager Window Layout

The Web manager consists of the following windows and tabs.



\*1 If the XML function is available, the Service Status tab will appear on the STATUS windows and the Service tab will appear on the CONFIG windows.

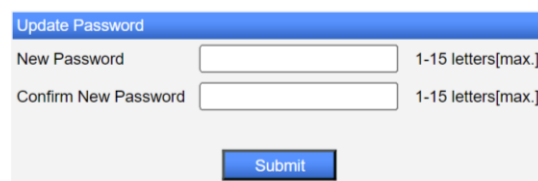
\*2 If the SSL/TLS function is available, the SSL/TLS tab will appear in the CONFIG window.

For details of XML function (Service tab) and SSL/TLS function, see “6 XML Function” (page 37) and “7 SSL/TLS function”(page 40).

#### 4-1-1. Initial Setup (Board Firmware v1.19 and later)

During the initial setup, it is necessary to set the administrator password in the CONFIG screen. After the password is set, the login screen will be displayed.

Update Password.  
You need to update LAN board password as this is your first time logging in!

The screenshot shows a web form titled "Update Password" with a blue header. It contains two input fields: "New Password" and "Confirm New Password". To the right of each field is the text "1-15 letters[max.]". Below the fields is a blue "Submit" button.

##### New Password / Confirm New Password

Enter the desired administrator password for this interface board. (1-15 characters, alphanumeric)

##### "Submit" button

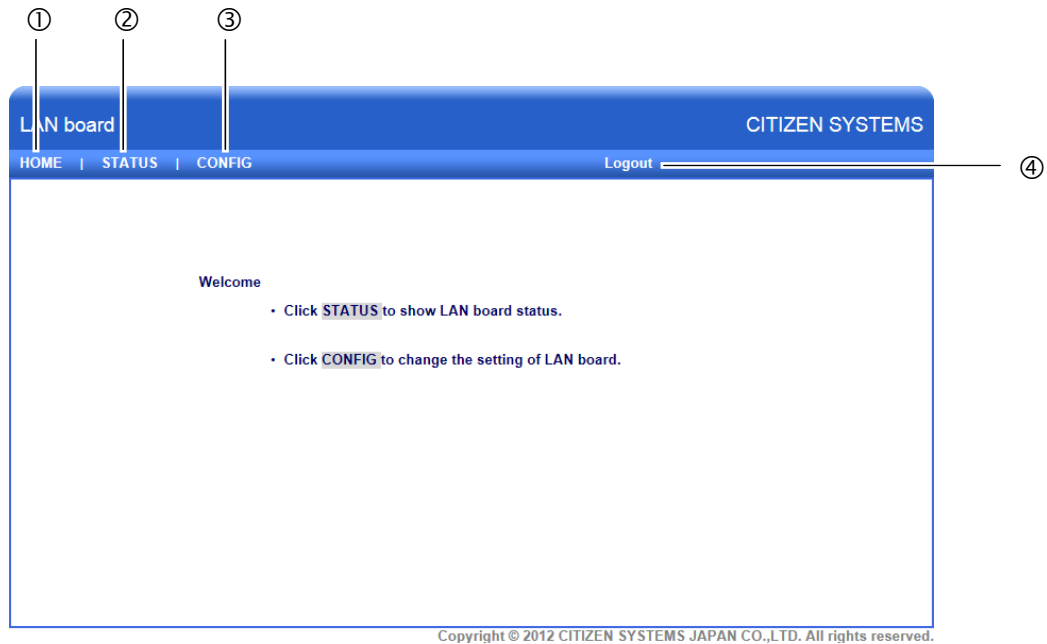
Enter the administrator password and click the "Submit" button. This will display the login screen.

##### Note

If you forget the set password, you will need to revert to the initial settings. Please refer to "3-4. Returning the Interface Board Configuration to Factory Default Settings" for details.

### 4-2. HOME Window

This is the Home window of the Web manager.



① HOME button

Display the Home window.

② STATUS button

Display the Status window. At the status window, you can check the status of the Interface board.

③ CONFIG button

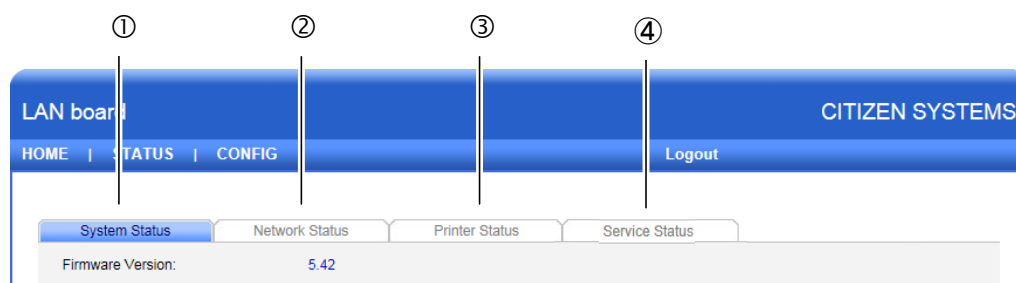
Display the CONFIG window. At the CONFIG window, you can configure the Interface board.

④ Logout button

Log out from the CONFIG window of the Interface board. Since the CONFIG screen cannot be accessed from multiple PCs at the same time, it is necessary to log out when configuring with another Web manager or "NetToolK".

### 4-3. STATUS Window

This screen displays the status of the Interface board.



① System Status tab

See 4-3-1, STATUS>>System Status Tab (page 20).

② Network Status tab

See 4-3-2, STATUS>>Network Status Tab (page 21).

③ Printer Status tab

See 4-3-3, STATUS>>Printer Status Tab (page 22).

④ Service Status tab

See 4-3-4, STATUS>>Service Status Tab (page 23).

### 4-3-1. STATUS>>System Status Tab

System Status	Network Status	Printer Status
Firmware Version:	5.42	①
Model Name:	IF2-EFX	②
Serial Number:	1000125	③
MAC Address:	00-11-E5-07-66-25	④
Print Settings		
Raw Port Number:	9100	⑤
Timeout for print data:	180	⑥
LPR Queue Name:	lp	⑦
UPnP:	Enable	⑧

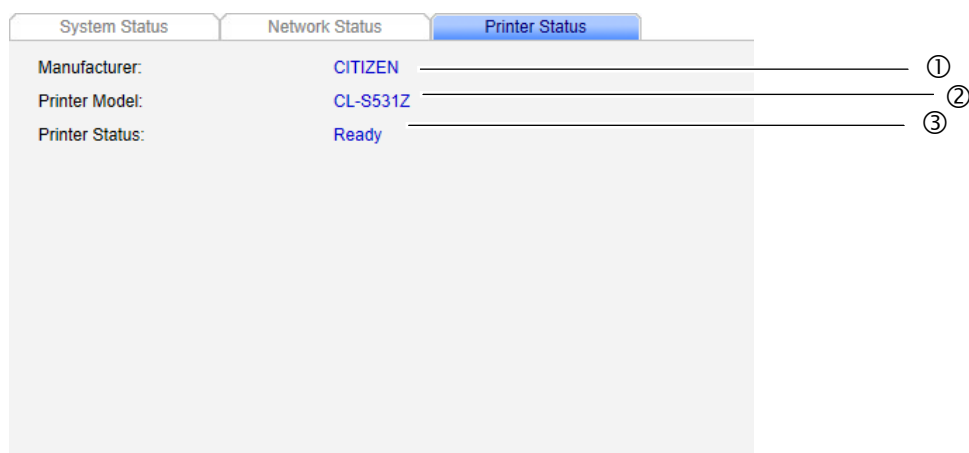
- ① Firmware Version  
displays the firmware version of the Interface board.
- ② Model Name  
displays the model name of the Interface board.
- ③ Serial Number  
displays the serial number of the Interface board.
- ④ MAC Address  
Displays the MAC address of the Interface board.
- ⑤ RAW Port Number  
Displays the TCP port number for RAW printing.
- ⑥ Timeout for print data  
Displays the socket timeout duration during printing. When the host and the TCP/IP socket are connected, and the host sends no data for this duration during printing, the socket is forced to close. When the setting is "0", the socket remains connected until a disconnection request is received from the host.
- ⑦ LPR Queue Name  
Displays the LPR queue name.
- ⑧ UPnP  
Displays the UPnP configuration status.

## 4-3-2. STATUS&gt;&gt;Network Status Tab

System Status	Network Status	Printer Status
LAN board name:	Net Printer	
IP Address:	192.168.1.101 (dhcp)	
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	
DHCP Server:	192.168.1.1	
Lease Time:	86400 seconds	
SSL/TLS:	Self-Signed	
Self-Signed:	Exist	
CA-Signed:	Exist	

- ① LAN board name  
displays the LAN board name of the Interface board.
- ② IP Address  
Displays the IP address of the Interface board.
- ③ Subnet Mask  
displays the subnet mask of the Interface board.
- ④ Default Gateway  
displays the default gateway of the Interface board.
- ⑤ DHCP Server  
Displays the IP address of the DHCP server from which the Interface board obtained its IP address.
- ⑥ Lease Time  
Displays the lease time of the IP address allocated by the DHCP server.
- ⑦ SSL/TLS  
Displays the status of SSL/TLS function  
 Disable: The function is disabled.  
 Self-Signed: The function is enabled by the self-signed certificate.  
 CA-Signed: The function is enabled by the certificate authenticated by CA
- ⑧ Self-Signed  
Displays the registration status of the self-signed certificate
- ⑨ CA-Signed  
Displays the registration status of the certificate authenticated by CA

### 4-3-3. STATUS>>Printer Status Tab



- ① Manufacturer  
Displays "CITIZEN".
- ② Printer Model  
displays the model of the printer to which the Interface board is connected.
- ③ Printer Status  
displays the operational status of the printer to which the Interface board is connected.  
Ready: Ready to print.  
Offline: Not ready to print.  
Paper Empty: Out of paper.  
Error: Error status.

(Note) If the bidirectional port of the Windows printer driver for the printer connected to this interface board is enabled, the printer status will not be displayed correctly. In such cases, confirm the printer status from the Windows spooler.

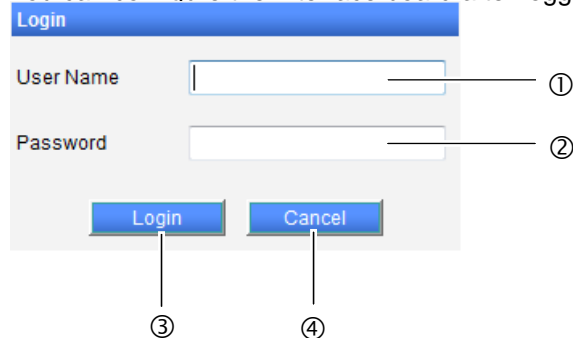
## 4-3-4. STATUS&gt;&gt;Service Status Tab

System Status	Network Status	Printer Status	Service Status
<b>XML Print</b>			
Service Version:		2.0	①
Port Number:		8080	②
<b>XML Config</b>			
Service Version:		1.0	③

- ① Service Version:  
Displays the service version of XML Print function.
- ② Port Number:  
Displays the TCP port used by XML Print function.
- ③ Service Version:  
Displays the service version of XML Config function

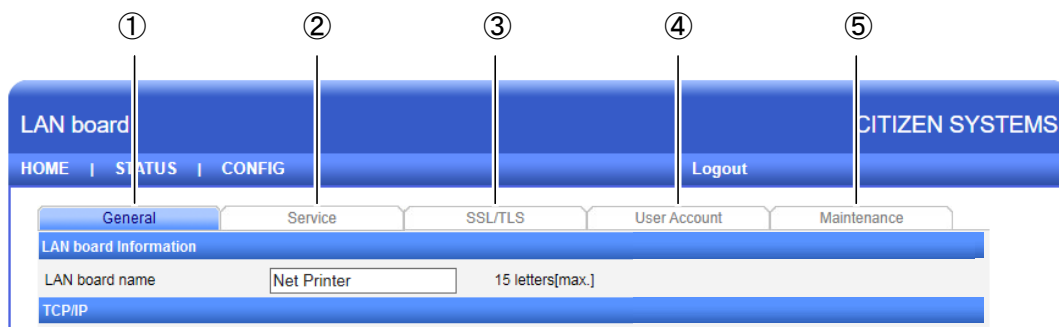
### 4-4. CONFIG Window

You can configure the Interface board after logging in as an administrator.



The diagram shows a 'Login' window with a blue header. Below the header are two input fields: 'User Name' and 'Password'. To the right of each field is a circled number: ① for User Name and ② for Password. At the bottom of the window are two buttons: 'Login' and 'Cancel'. Below each button is a circled number: ③ for Login and ④ for Cancel.

- ① User Name  
Enter the name of the Interface board administrator. (Initial setting: admin)
- ② Password  
Enter the administrator password. (Initial setting: admin. From version 1.19 and later, it is necessary for you to set your own password.)
- ③ Login button  
Enter the administrator name and password, and then click "Login". The CONFIG window appears.
- ④ Cancel button  
Cancel login.



The diagram shows the 'CONFIG' window. At the top is a blue header with 'LAN board' on the left and 'CITIZEN SYSTEMS' on the right. Below the header is a navigation bar with 'HOME | STATUS | CONFIG' and a 'Logout' button. Below the navigation bar are five tabs: 'General', 'Service', 'SSL/TLS', 'User Account', and 'Maintenance'. Below the tabs is a section titled 'LAN board Information' with a table containing 'LAN board name' and 'Net Printer' and '15 letters[max.]'. Below this is a section titled 'TCP/IP'.

- ① General tab  
See 4-4-1 CONFIG>>General Tab (page 25).
- ② Service tab  
See 6-2 CONFIG>>Service Tab (page 38)
- ③ SSL/TLS tab  
See 7-2 CONFIG>>SSL/TLS Tab (page 42)
- ④ User Account tab  
See 4-4-2 CONFIG>>User Tab (page 26).
- ⑤ Maintenance tab  
See 4-4-3 CONFIG>>Maintenance Tab (page 27).

## 4-4-1. CONFIG&gt;&gt;General Tab

**LAN board Information**

- LAN board name (factory default: Net Printer)

Set the ID of this Interface board.

**TCP/IP**

- Obtain an IP Address Automatically (factory default)  
Automatically obtain the IP address from the DHCP server.
- Use the following IP Address  
Set IP addresses in the IP Address, Subnet Mask, and Default Gateway fields.

**UPnP Setting**

- UPnP (factory default: Enable)

Set the UPnP setting.

**Print Settings**

Configure the printing functions of the printer.

- Raw Port Number (factory default: 9100)  
Set the TCP port number for RAW protocol printing.
- Timeout for print data  
Set the timeout duration for the connection to the host.
- Action at Timeout  
Select the action for other connections when a timeout occurs with the host. There are two selections: Close all connections and Move to next connection.

## 2 Web Manager

---

- TCP Keep Alive

Select whether the TCP Keep Alive feature is enabled or disabled.

### Submit button

Enter the changes.

### Reset button

Cancel the changes.

### 4-4-2. CONFIG>>User Account Tab

You must log in as an administrator to change the settings of the Interface board. At this screen, the administrator name and password can be changed.

The screenshot shows the 'Set User' configuration screen. At the top, there are three tabs: 'General', 'User Account' (which is selected and highlighted in blue), and 'Maintenance'. Below the tabs, the title 'Set User' is displayed in a blue header bar. The main area contains three input fields: 'New User name' with the value 'admin', 'New Password', and 'Confirm New Password'. Each field has a label to its right indicating a maximum of 15 letters. At the bottom of the form, there are two buttons: 'Submit' and 'Reset'.

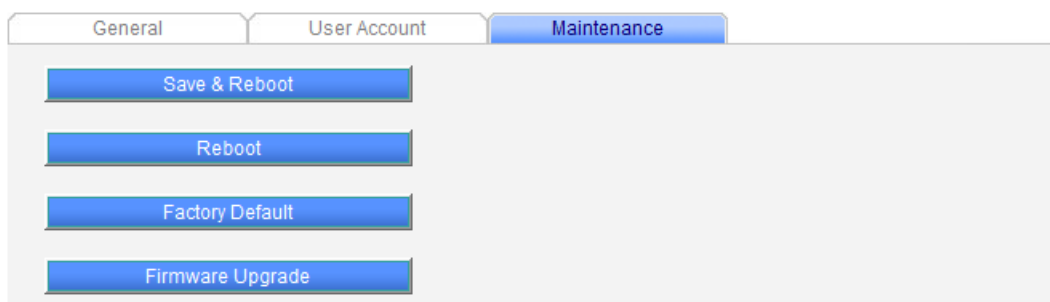
### Set User

- New User name (factory default: admin)  
Enter the new administrator name.
- New Password (factory default: admin. From version 2.57 and later, it is necessary for you to set your own password.)  
Enter the new password.
- Confirm New Password  
Enter the password again.

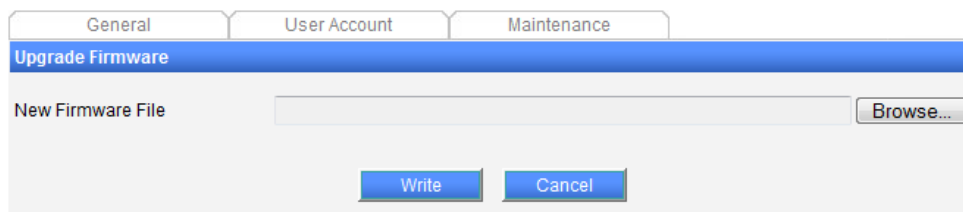
### Warning

If you forget the new username and password, settings must be returned to the factory default settings. (Please refer to "3-4. Returning the Interface Board Configuration to Factory Default Settings" for details.)

## 4-4-3. CONFIG&gt;&gt;Maintenance Tab



- Save & Restart button  
Save changes, and restart the Interface board.
- Restart button  
Restart the Interface board without saving changes.
- Factory Default button  
Return the Interface board to the factory default settings.
- Firmware Upgrade button  
Upgrade the firmware of the Interface board.

Firmware upgrade

- 1) Click "Browse" and select the firmware file.
- 2) Click "Write".

**Warning**

After the firmware upgrade starts, do not disconnect power or transmission to the printer until the upgrade is complete.

If you are performing a firmware update, it is important to obtain the correct firmware data from us.

If the firmware update is not performed correctly, there is a possibility that the interface board may not boot properly.

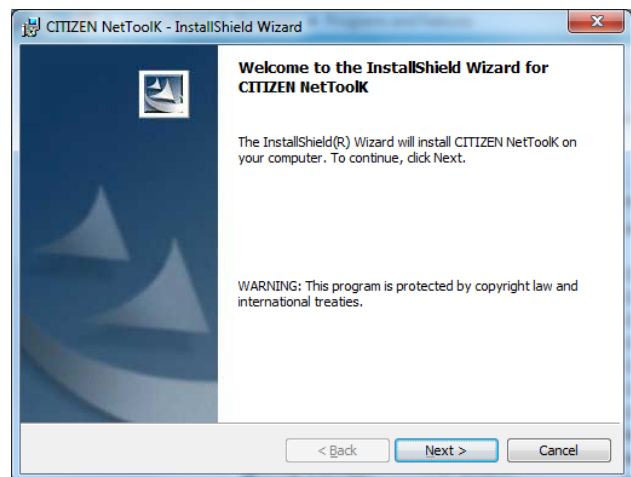
## 5. NetToolK

The “NetToolK” utility software runs on the Windows and can be used to change the settings of the Interface board. This tool can be used with both wired and wireless LAN interface boards.

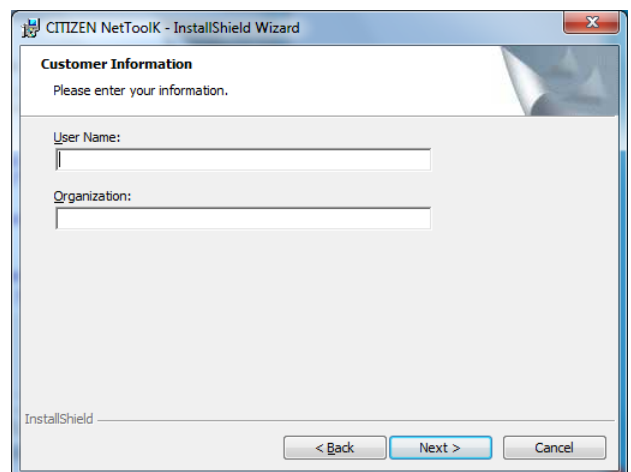
This interface board does not have anything to do with wireless LAN, but it includes a description of wireless LAN.

### 5-1. Installing the NetToolK

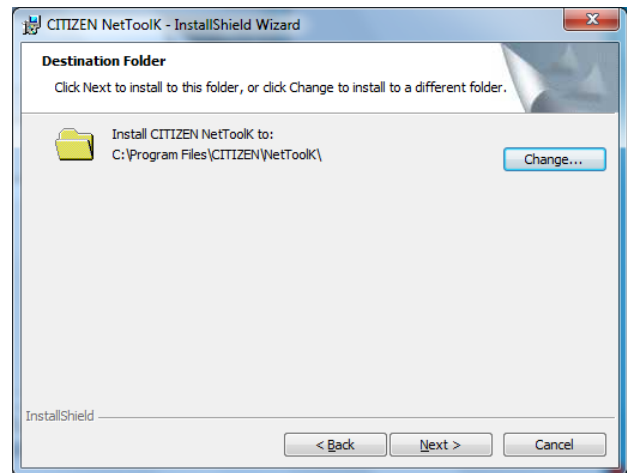
- 1) Acquire the file “NetToolKSetup.exe” from the CD-ROM or our website. Double click the file.
- 2) If the “User Account Control” screen appears, click “Continue.”
- 3) The screen shown on the right appears.  
Click “Next.”



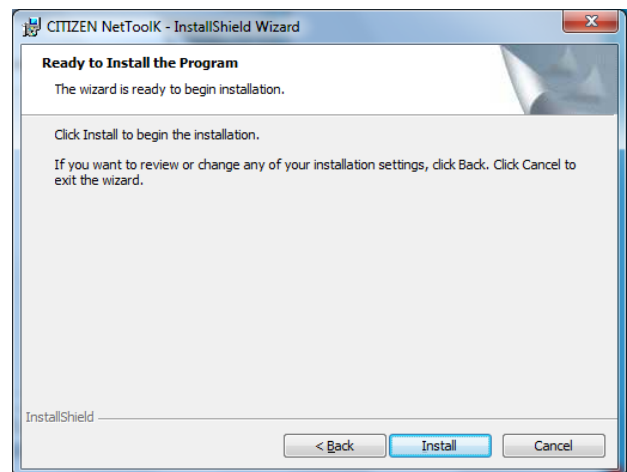
- 4) Enter a username and organization,  
and then click “Next.”



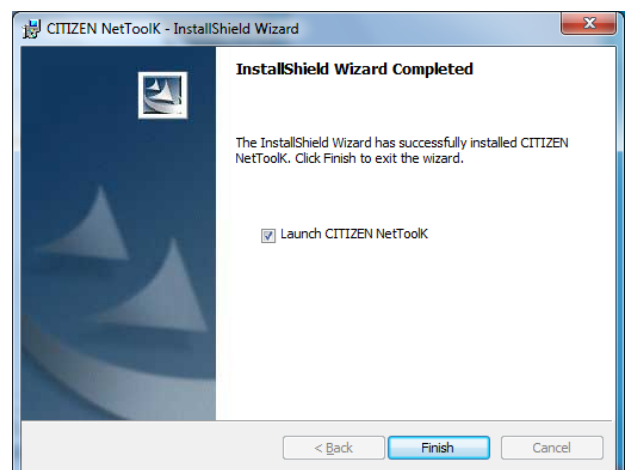
- 5) The screen shown on the right appears.  
Click “Next.”



- 6) The screen shown on the right appears.  
Click “Install.”



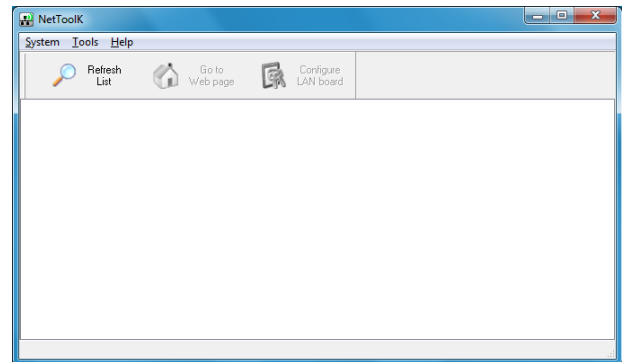
- 7) Click “Finish” to complete installation.



#### 4 NetToolK

---

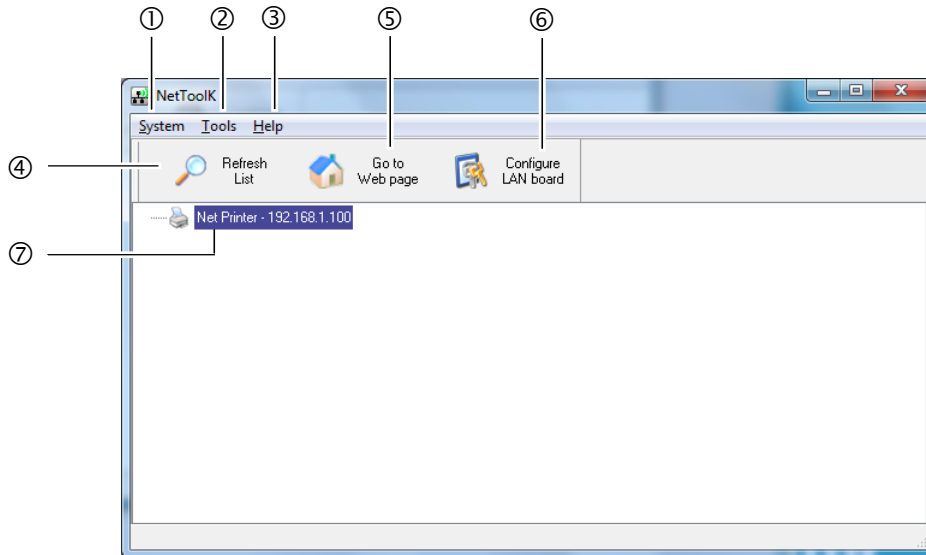
- 8) The PC setting tool starts. Select “Exit” from the “System” menu.



- 9) The icon on the right is placed on the desktop of the computer. You can now start program by double clicking this icon.



## 5-2. Information List Window

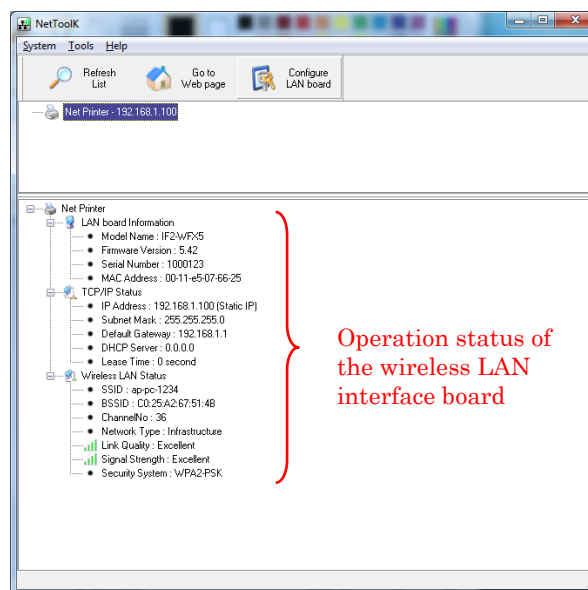
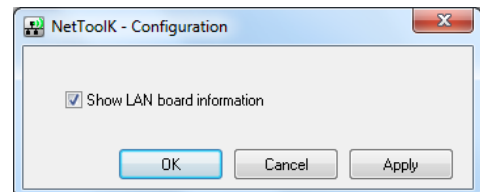


## ① "System"

Select "System" – "Exit" to exit the NetToolK.

## ② "Tools"

Select "Tools" – "Settings" to switch the display of the LAN interface board information. When the "Show LAN board information" check box is selected, the LAN interface board operation status can be displayed as shown below.



③ "Help" menu

Select "Help" – "About" to display the version information of the NetToolK.

④ "Refresh List" button

Refresh the list of the LAN interface board. The application periodically refreshes the list, but you can refresh the list manually by clicking this button.

⑤ "Go to Web Page" button

Select the LAN interface board you want to configure, and then click "Configure using a web browser". The browser starts and displays the Web manager.

⑥ "Configure the LAN Board" button

Select the LAN interface board you want to configure, and then click "Configure the LAN Board". See 5-3 Setup Window (page 33).

If the firmware version of this board is V1.19 or later, it is necessary to set the user password via Web Manager before performing any configuration.

⑦ LAN interface board list

The list displays the LAN interface boards connected to the network. The LAN interface boards connected to the same subnet are displayed.

### 5-3. Setup Window

You can configure the LAN interface board by selecting the LAN interface board from the list screen and clicking “Configure the LAN Board”.

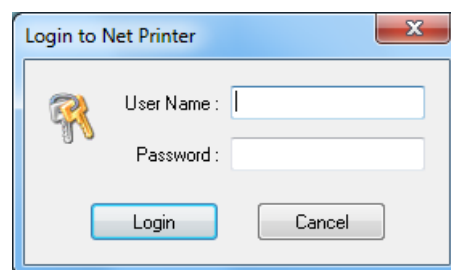
If the firmware version of this board is V1.19 or later, it is necessary to set the user password via Web Manager before performing any configuration.

To login at the login screen, enter a username and password.

Username: admin (factory default)

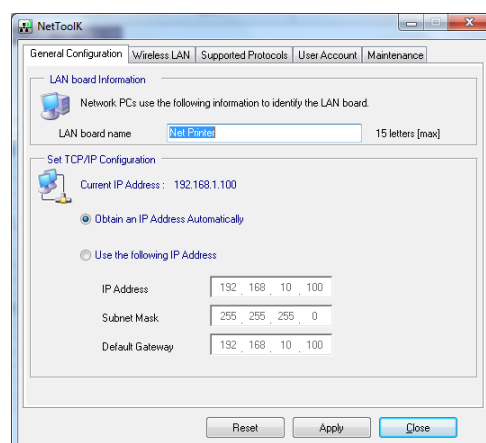
Password: admin: (factory default)

(From version 1.19 and later, it is necessary for you to set your own password.)



#### 5-3-1. “General” Tab

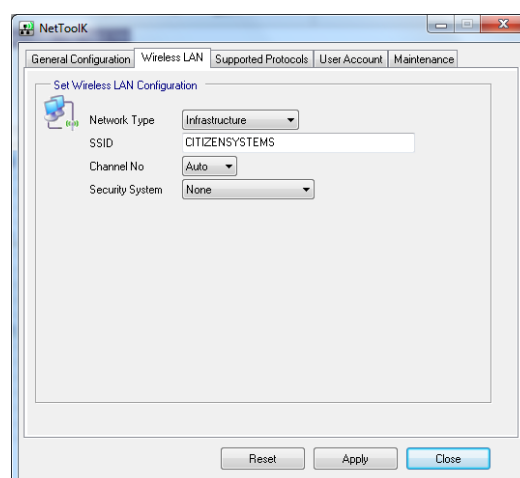
Use the “General” tab to configure the LAN board name and IP address



#### 5-3-2. “Wireless LAN” Tab

Use the “Wireless LAN” tab to configure the LAN.

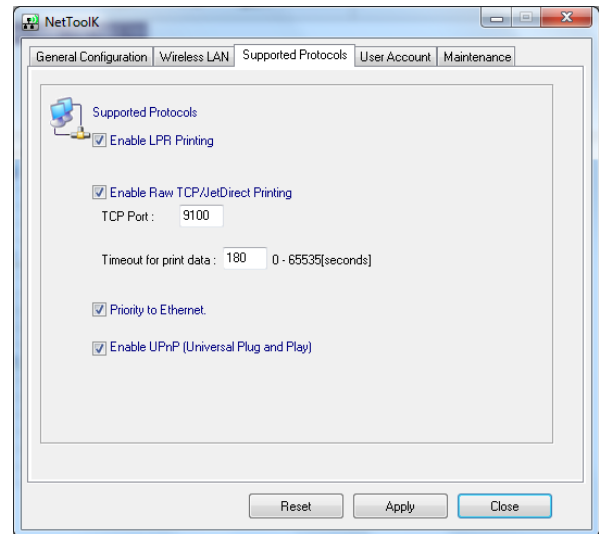
(This tab is not displayed for a wired LAN interface board.)



## 4 NetToolK

### 5-3-3. "Supported Protocols" Tab

Use the "Supported Protocols" tab to enable LPR and the RAW protocol, set the printer timeout duration, enable "Priority to Ethernet", and enable UPnP.



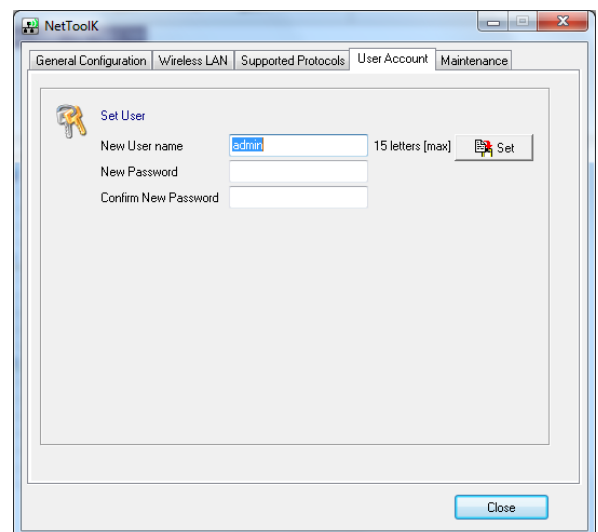
### 5-4. "User Account" Tab

Use the "User Account" tab to change the administrator name and password.

#### Warning

If you forget the new username and password, settings must be returned to the factory default settings.

(Please refer to "3-4. Returning the Interface Board Configuration to Factory Default Settings" for details.)



### 5-5. "Maintenance" Tab

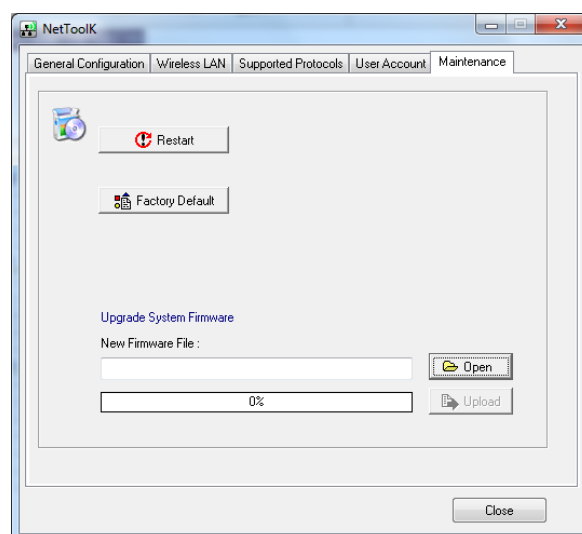
Use the "Maintenance" tab to restart the LAN interface board, return the settings to the factory default settings, and update the firmware.

#### Note

After the firmware upgrade starts, do not disconnect power or transmission to the printer until the upgrade is complete.

If you are performing a firmware update, it is important to obtain the correct firmware data from us.

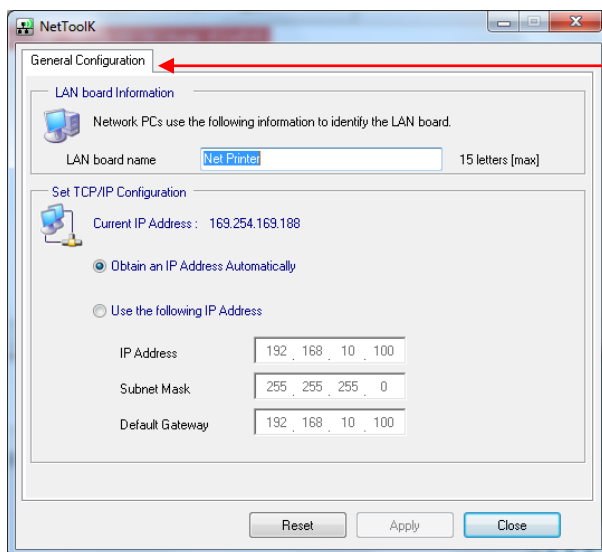
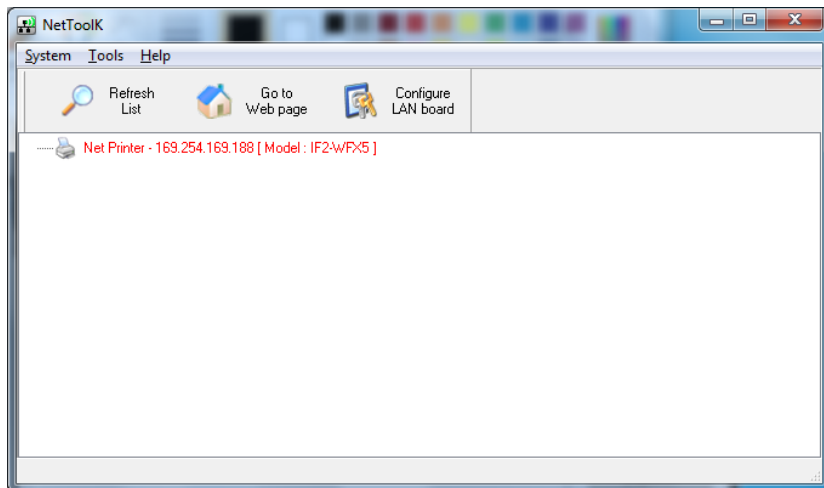
If the firmware update is not performed correctly, there is a possibility that the interface board may not boot properly.



## 4 NetToolK

---

Note: If the computer at which you are performing the configuration and the LAN interface board have different subnet values, a message like the one shown below appears in red letters. If this message appears, set the IP address using the “Configure the LAN Board” button before configuring the LAN interface board.



Only the board name and IP address can be configured. Configure the IP address correctly one time before configuring the wireless LAN interface board.

## 6. XML Function

### 6-1. Overview

The XML function is a function of this interface board that converts special data in the form of XML tags received into printer commands, etc., to achieve printing and other functions.

For more information about XML tag format data and the JavaScript library that generates XML data, please refer to the separate document on the CITIZEN XML Print service.

This function can be used when the following conditions are met.

Printer supports the XML function.

This interface is connected.

The firmware version of the printer and this interface board supports XML function.

If the conditions are met, the Service Status tab is displayed in the STATUS window and SSL/TLS tab is displayed in the CONFIG window.

When using these functions, the URL to which the XML tag format data is sent is as follows.

If you use the URL specification method by port number, the numeric part will change depending on the port number setting.

		URL
HTTP	XML Print service	http://IP address:8080/ http://IP address/xmlprint/
	XML Config service	http://IP address/xmlconfig/
HTTPS	XML Print service	https://IP address/xmlprint/
	XML Config service	https://IP address/xmlconfig/

## 4 XML Function

### 6-2. CONFIG>>Service Tab

The screenshot shows the 'CONFIG>>Service Tab' interface. It has five tabs: General, Service (selected), SSL/TLS, User Account, and Maintenance. Under the 'Service' tab, there are two sections: 'XML Print' and 'XML Config'. The 'XML Print' section contains three input fields: 'Port Number' with the value '8080', 'Timeout for connect' with the value '10', and 'Timeout for print' with the value '60'. To the right of these fields are their respective ranges: '5-60[Seconds]' for connect and '10-600[Seconds]' for print. The 'XML Config' section contains one input field: 'Timeout for connect' with the value '10', with a range of '5-180[Seconds]' to its right. At the bottom of the form are two buttons: 'Submit' and 'Reset'.

#### 6-2-1. XML Print

Item	Initial value	Configurable range	Description
Port Number	8080	1025 - 65535	Connection port number
Timeout for connect	10	5 - 60	Timeout period waiting for printing to start
Timeout for print	60	10 - 600	Timeout period waiting for completion of printing

#### 6-2-2. XML Config

This function allows you to set some configuration items at once. For details, please refer to "CITIZEN XML Config Service JavaScript Config SDK Programming Manual".

Item	Initial value	Configurable range	Description
Timeout for connect	10	5 - 180	Timeout period waiting for processing to start

#### 6-2-3. XML Settings (Displayed only for firmware version V1.14 and later)

Item	Default	Setting Range	Explanation
HTTP Keep Alive	Disable	Enable Disable	Enables HTTP Keep Alive when using each XML service.
HTTP Keep Alive Timeout	5	5-30	Timeout period when HTTP Keep Alive is enabled.
HTTP Keep Alive Max Requests	100	1-100	Maximum number of requests that can be sent within the same connection when HTTP Keep Alive is enabled.

#### 6-2-4. Submit / Reset Button

After changing the settings, press the “Submit” button and then press the “Save & Reboot” button in the Maintenance menu. The settings will be enabled after the board reboots.

## 7. SSL/TLS function

### 7-1. Overview

#### Necessity of SSL/TLS support

Encrypted communication is necessary to prevent third parties from eavesdropping on, altering, or spoofing the communication data flowing over the network. The SSL/TLS protocol has become the standard for encrypted communication infrastructure.

The http protocol is used to send and receive web data and XML data, and https is the SSL/TLS-compatible version of it. If https is used for communication between the host and the printer, the printer must also support SSL/TLS.

#### Overview of SSL/TLS support

A digitally signed certificate (hereafter referred to as a signed certificate) is required for SSL/TLS encrypted communication. The server stores the signed certificate, and the client side must confirm or approve the certificate as trustworthy to enable SSL/TLS encrypted communication.

There are two types of signing certificates: those signed by a public certification authority (CA) and self-signed certificates signed by the private CA.

In the case of self-signed certificates, the client side must certify that the certificate is trustworthy so that it can communicate without warning. For this purpose, this board has a function to export a file that contains the unique information for certification.

This board also allows importing a certificate signed by a public CA for more secure communication.

#### Differences in procedures for preparing signed certificates between this board and a normal server

For SSL/TLS communication, you will need a signed certificate file and a private key file. The general procedure for preparing these on a normal server is as follows.

1. The applicant requesting the certificate generates a private key.
2. Applicant creates a certificate signing request (CSR) by entering the applicant's identification information and adding a signature with the applicant's private key.
3. The applicant submits the CSR to either a self-certification authority prepared by the applicant or an external public CA.
4. The signing authority generates a certificate with its own private key signature attached to the CSR and returns it to the applicant. (Depending on the submitted certification authority, the certification becomes either a self-signed certificate or a public CA signed certificate).
5. The applicant stores and places the signed certificate file and his private key file.

This board has an internal private key and self-certification authority, and if you want to use a self-signed certificate, you only need to enter the identification information in step 2 above. (For the detailed procedure, refer to 7-3-1 Creating and exporting a self-signed certificate.

On the other hand, to use a public CA signed certificate on this board, the user must perform steps 1 through 4 above, and then import the certificate file (which has signature by public CA) and the applicant's private key file to this board (as step5).

It is also possible to import self-signed a certificate prepared by the user (not generated by this board) into this board in the same way as public CA signed certificate.

#### Certificate Expiration

Signed certificate have expiration date and must be updated to the new expiration date before they expire. A window to update the expiration date is also provided, or you can use the XML Config function to send an XML file to the printer for updating expiration date.

#### Types of Certificates and Descriptions in Subsequent Chapters

The certification authority that issues the certificate and the way the certificate is handled on this board are as follows

- A. Internal certificate: A self-signed certificate generated and stored inside the printer.
- B. Local certificate: A certificate signed by a private certification authority (CA) on the local network and imported into the board.
- C. Public certificate: A certificate 子 signed by a public certification authority (CA) on the Internet and imported into the board.

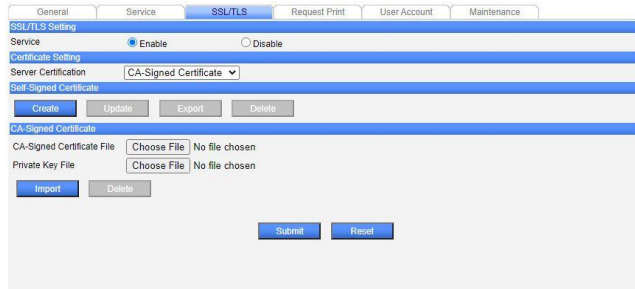
The descriptions in the following chapters correspond to certificate A, B, or C as follows.

Chapter	A. Internal certificate	B. Local certificate	C. Public certificate
7-2-1	Applicable	Applicable	Applicable
7-2-2	Applicable		
7-2-3	Applicable		
7-3-1	Applicable		
7-3-2	Applicable	Applicable	
7-4-1	Applicable	Applicable	Applicable
7-4-2	Applicable		
7-4-3		Applicable	Applicable
7-4-4	Applicable	Applicable	Applicable

There are two types of local certificates: those with the same certification server and certification authority, and those with a different certification server and certification authority. The differences do not affect whether the explanations in each chapter are applicable or not, so they are not separated. However, depending on the browser you use and other factors, there may be differences between these two conditions.

### 7-2. CONFIG>>SSL/TLS Tab

#### 7-2-1. SSL/TLS tab



#### SSL/TLS Setting

- Service  
Select whether the SSL/TLS function is enabled or disabled.
- Protocol (Displayed only on firmware version V1.14 and later)  
Select the version of TLS to be used during communication.

#### Certificate Setting

- Server Certification  
Select the server certificate type used for SSL/TLS communication from either Self-Signed Certificate or CA-signed certificate.

#### Self-Signed Certificate

- “Create” button  
Move to “Create Self-Signed Certificate” page. See “7-2-2 Create Self-Signed Certificate”.
- “Update” button  
Move to “Update Self-Signed Certificate” page. See “7-2-3 Update Self-Signed Certificate”.
- “Export” button  
Export a certificate to install the server information to the client.  
No need to reinstall for certificate renewal.
- “Delete” button  
Deletes the self-signed certificate that was created.

#### CA-Signed Certificate

- CA-Signed Certificate File  
Select the public CA signed certificate file to import.
- Private Key File  
Select the private key file to import.
- “Import” button  
Import the selected certificate and private key into the printer.
- “Delete” button  
Delete the imported certificate and private key.

## 7-2-2. Create Self-Signed Certificate

The screenshot shows a web interface for creating a self-signed certificate. The 'SSL/TLS' tab is selected. The form is titled 'Create Self-Signed Certificate'. It contains the following fields:

- Issuer:**
  - Common Name: 192.168.1.100
  - Organization Unit: (empty)
  - Organization: CITIZEN SYSTEMS JAPAN
  - Locate: (empty)
  - State: (empty)
  - Country: JP (with a note '2 characters')
- Validity (Not Before):** 2020/04/01 (with a note 'YYYY/MM/DD')
- Validity (Not After):** 2021/04/01 (with a note 'YYYY/MM/DD')
- Internal Certification Authority:**
  - Validity (Not Before): 2020/04/01 (with a note 'YYYY/MM/DD')
  - Validity (Not After): 2049/12/31 (with a note 'YYYY/MM/DD' and a red asterisk indicating it is a mandatory field)

At the bottom of the form are 'Create' and 'Cancel' buttons. A red asterisk at the bottom right indicates that the 'Validity (Not After)' field is mandatory.

**Create Self-Signed Certificate (Items and meanings for CA-Signed Certificate are the same.)**

- **Issuer**
  - About the organization (administrator) operating the server.
- **Key Type**
  - Select the signing algorithm used when creating the certificate.
- **Common Name**
  - Enter the IP address or FQDN of the print server.
- **Organization Unit**
  - Enter the name of the department of the operating organization.
- **Organization**
  - Enter the name of the operating organization.
- **Locate**
  - Enter the location (city, ward, town, village, etc.) of the Operator.
- **State**
  - Enter the location of the Operator (State/Prefecture).
- **Country**
  - Enter the country code where the Operator is located using two letters of the alphabet.
- **Validity (Not Before) (Default: Entry Date)**
  - Enter the start date of the certificate validity period.
- **Validity (Not After) (Default: 1 year after the entry date)**
  - Enter the end date of the certificate validity period.
- **Internal Certification Authority**
  - This field is for entering information about certificate renewal.
- **Validity (Not Before) (Default value: Entry date)**
  - Enter the start date of the period for which you wish to renew the certificate. Enter the Specify a date before the certificate validity period.
- **Validity (Not After) (Default: 12/31/2049)**
  - Enter the end date of the period for which you wish to renew the certificate. Specify the date after the certificate validity period.

## 4 SSL/TLS function

### 7-2-3. Update Self-Signed Certificate

General Service **SSL/TLS** User Account Maintenance

Update Self-Signed Certificate

Issuer

Common Name \* 192.168.1.100

Organization Unit

Organization \* CITIZEN SYSTEMS JAPAN

Locate

State

Country \* JP 2 characters

Validity (Not Before) \* 2021/05/01 YYYY/MM/DD

Validity (Not After) \* 2022/05/01 YYYY/MM/DD

Internal Certification Authority

Validity (Not Before) \* 2020/04/01 YYYY/MM/DD

Validity (Not After) \* 2049/12/31 YYYY/MM/DD

\* mandatory field

Update Cancel

#### Update Self-Signed Certificate

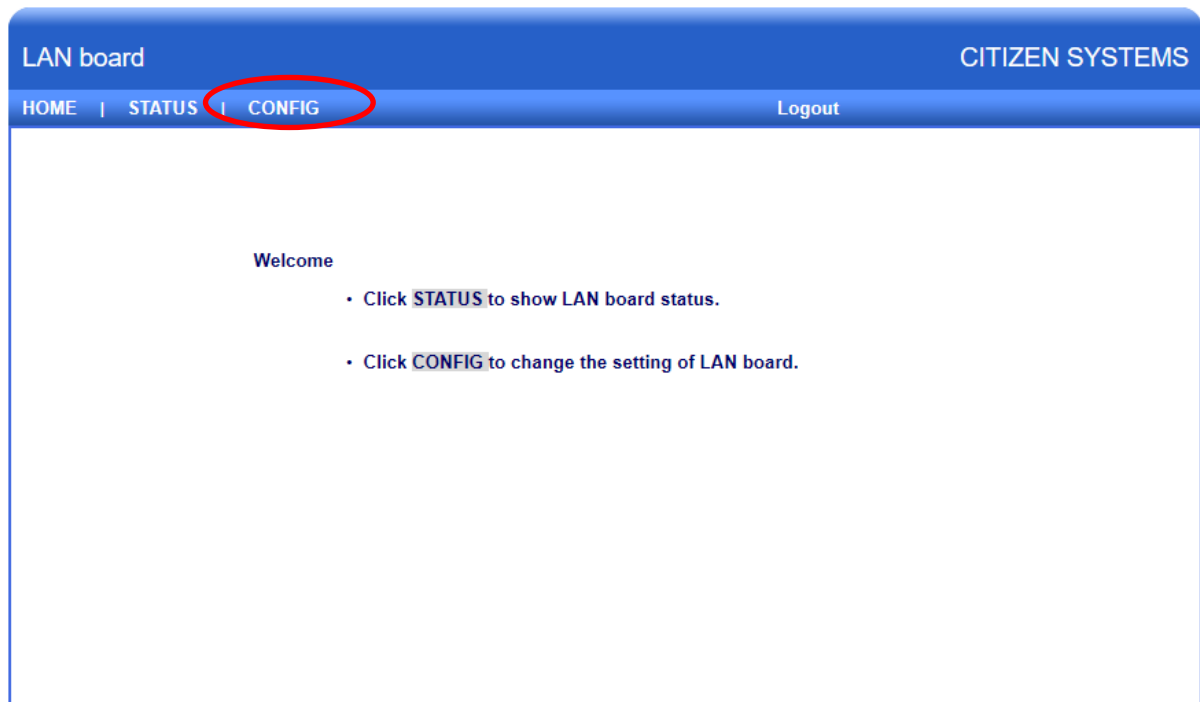
(If you select CA-Signed Certificate in Certificate Settings, the screen will still be the same.)

- Issuer  
Enter the information about the organization that operates the server (administrator).
- Common Name  
Enter the IP address or FQDN of the print server.
- Organization Unit  
Enter the name of the department of the operating organization.
- Organization  
Enter the name of the operating organization.
- Locate  
Enter the location (city, ward, town, village, etc.) of the Operator.
- State  
Enter the location of the Operator (State/Prefecture).
- Country  
Enter the country code where the Operator is located using two letters of the alphabet.
- Validity (Not Before) (Default value: Entry date)  
Enter the start date of the certificate validity period within the period for which the certificate can be renewed.
- Validity (Not After) (Default: 1 year after the entry date)  
Enter the end date of the certificate validity period within the period for certificate renewal.
- Internal Certification Authority  
Displays information on certificate renewal.
- Validity (Not Before)  
displays the start date of the period during which certificate renewal is possible.
- Validity (Not After)  
displays the end date of the period for which the certificate can be renewed.

### 7-3. To enable SSL/TLS communication using a self-signed certificate

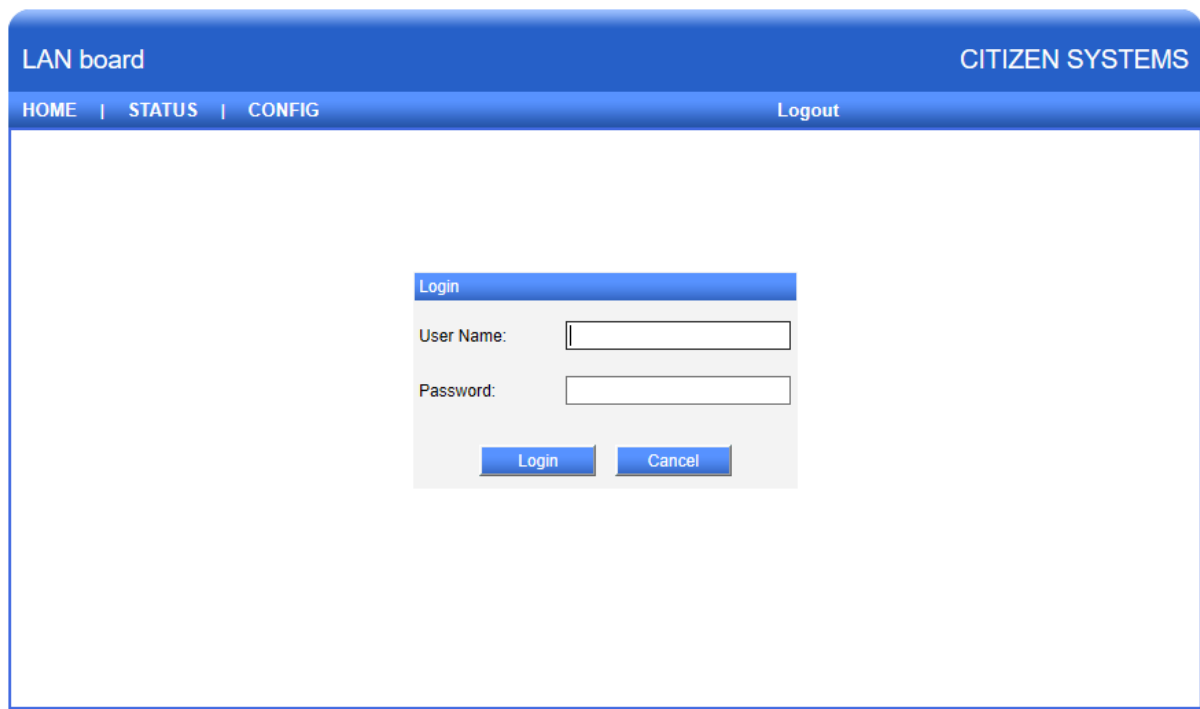
#### 7-3-1. Generating and exporting self-signed certificates

1) Access the IP address of the board from your browser. 2) Select the "CONFIG" tab.



3) Enter User Name and Password to enter the configuration screen.

(Default: admin / admin. From version 1.19 and later, it is necessary for you to set your own password.)



#### 4 SSL/TLS function

4) Set a static IP and select the "Submit" button.

The screenshot shows the 'LAN board' configuration page for 'CITIZEN SYSTEMS'. The 'CONFIG' tab is active, and the 'SSL/TLS' sub-tab is selected. Under the 'TCP/IP' section, the 'Use the following IP Address' option is selected. The IP Address is set to '192.168.1.30', Subnet Mask to '255.255.255.0', and Default Gateway to '192.168.1.1'. These three input fields are circled in red. Below this, the 'UPnP Setting' shows 'UPnP' as 'Enable'. The 'Print Settings' section includes 'Raw Port Number' (9100), 'Timeout for print data' (180), and 'Action at Timeout' set to 'Close all connections'. The 'Submit' button is circled in red.

5) Select the "SSL/TLS" tab and go to the SSL/TLS setting window.

6) Click the "Create" button to enter the self-certification windows.

The screenshot shows the 'SSL/TLS' configuration page. The 'SSL/TLS' tab is circled in red. Under the 'Certificate Setting' section, 'Server Certification' is set to 'Self-Signed Certificate'. Below this, the 'Self-Signed Certificate' section has a 'Create' button circled in red. Other buttons like 'Update', 'Export', and 'Delete' are also visible. At the bottom, there are 'Submit' and 'Reset' buttons.

7) Enter a static IP in Common Name,.

For Validity, the first one is the validity period of the certificate stored on the board, and the second one is the validity period of the file to be exported. Basically, there is no need to change it.

An error will occur if the first Validity is set outside the period of the second Validity.

8) Click the "Create" button.

LAN board CITIZEN SYSTEMS

HOME | STATUS | CONFIG Logout

General Service **SSL/TLS** Request Print User Account Maintenance

Create Self-Signed Certificate

Issuer

Common Name \* 192.168.3.42

Organization Unit

Organization\* CITIZEN SYSTEMS JAPAN

Locate

State

Country \* JP 2 characters

Validity (Not Before) \* 2020/05/19 YYYY/MM/DD

Validity (Not After) \* 2021/05/19 YYYY/MM/DD

Internal Certification Authority

Validity (Not Before) \* 2020/05/19 YYYY/MM/DD

Validity (Not After) \* 2049/12/31 YYYY/MM/DD

\* mandatory field

Create Cancel

#### 4 SSL/TLS function

9) Press the "OK" button.

LAN board CITIZEN SYSTEMS

HOME | STATUS | CONFIG Logout

General | Wireless LAN | Service | **SSL/TLS** | Request Print | User Account | Maintenance

Create Self-Signed Certificate

Create Self-Signed Certificate success.

Change settings will be not effective unless "Save & Reboot" button in "Maintenance" tab is pressed.

**OK**

Copyright © 2012 CITIZEN SYSTEMS JAPAN CO.,LTD. All rights reserved.

10) Select "Enable" for Service and CA-Signed Certificate for Server Certification in SSL/TLS Setting.

11) Click the "Export" button to save the self-certificate file. The file will be used for importing into your browser.

12) Press the "Submit" button.

LAN board CITIZEN SYSTEMS

HOME | STATUS | CONFIG Logout

General | Wireless LAN | Service | **SSL/TLS** | Request Print | User Account | Maintenance

SSL/TLS Setting

Service ☒ **Enable** ☐ Disable

Protocol ☒ TLS 1.2 ☐ TLS 1.3

Certificate Setting

Server Certification Self-Signed Certificate ▾

Self-Signed Certificate

Create Update **Export** Delete

CA-Signed Certificate

CA-Signed Certificate File ファイルを選択 選択されていません

Private Key File ファイルを選択 選択されていません

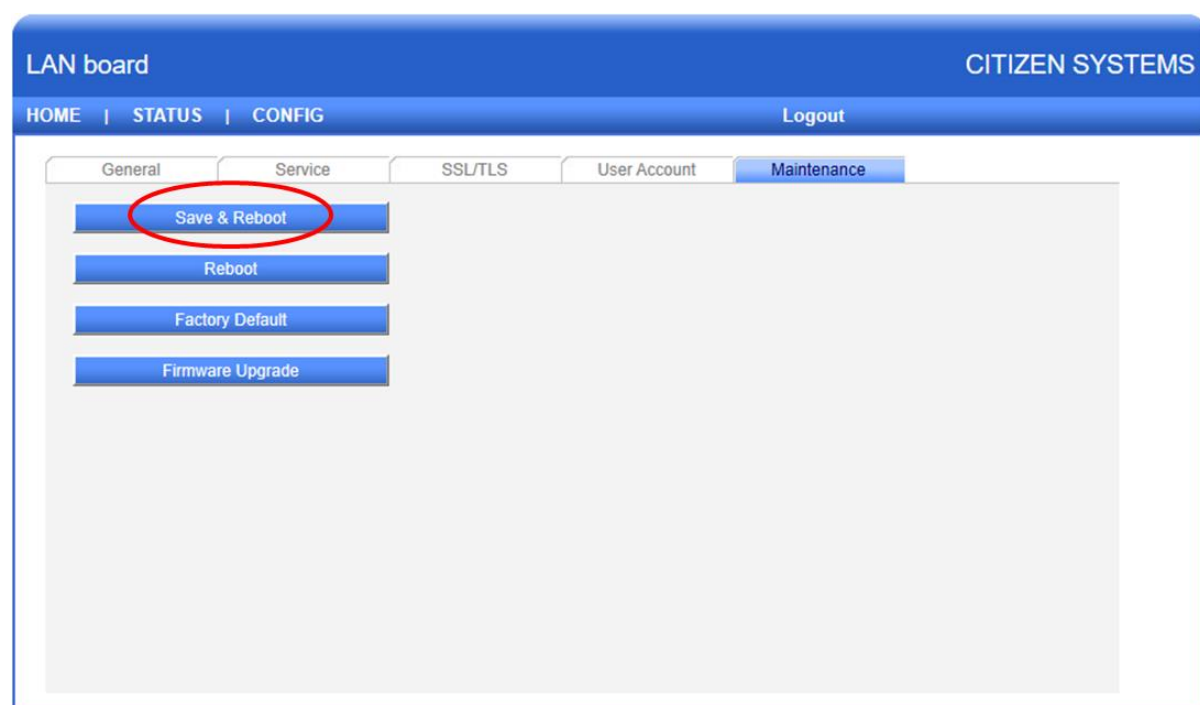
Note: Only unencrypted files are supported.

Import Delete

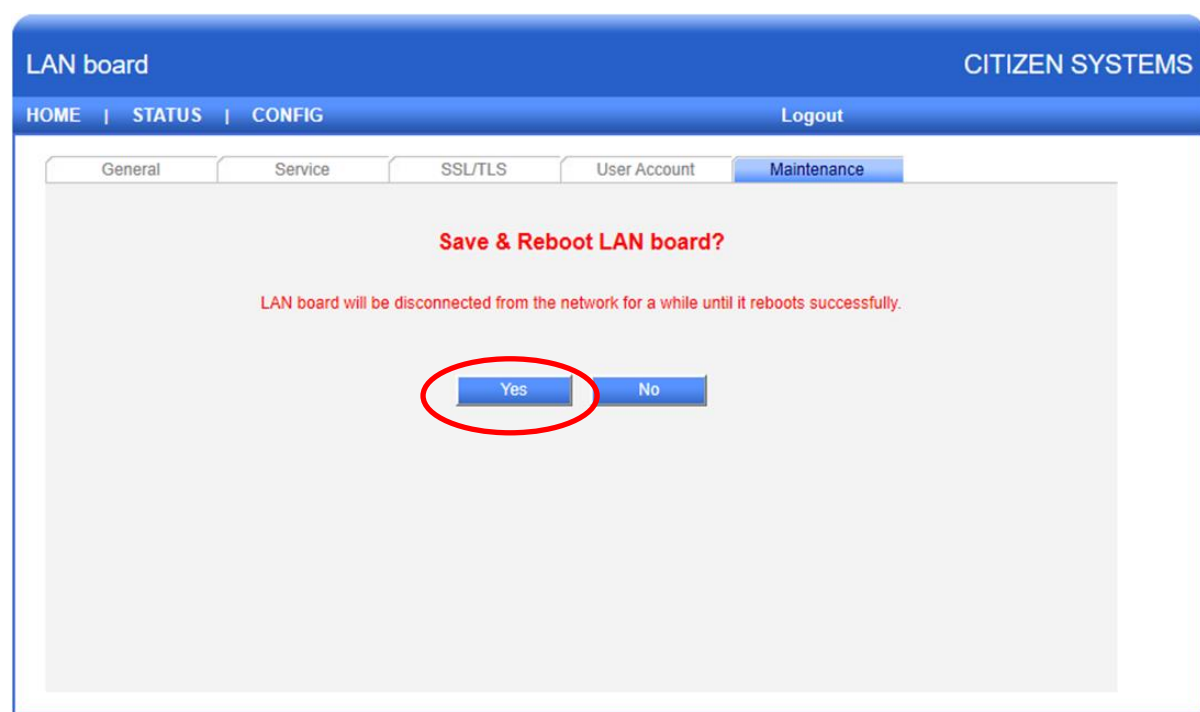
**Submit** Reset

Copyright © 2012 CITIZEN SYSTEMS JAPAN CO.,LTD. All rights reserved.

13) Press "Save & Reboot".



14) Click the "Yes" button to save & reboot.

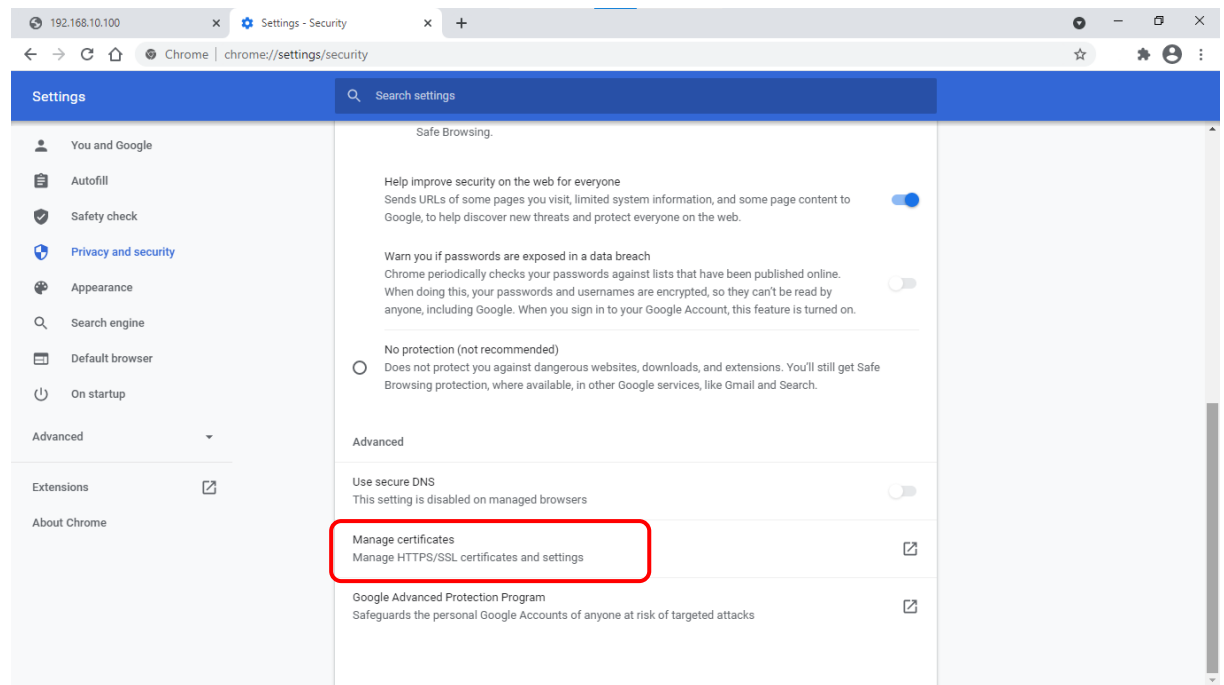


Please wait until the board reboots. The configuration changes will be reflected after the reboot.

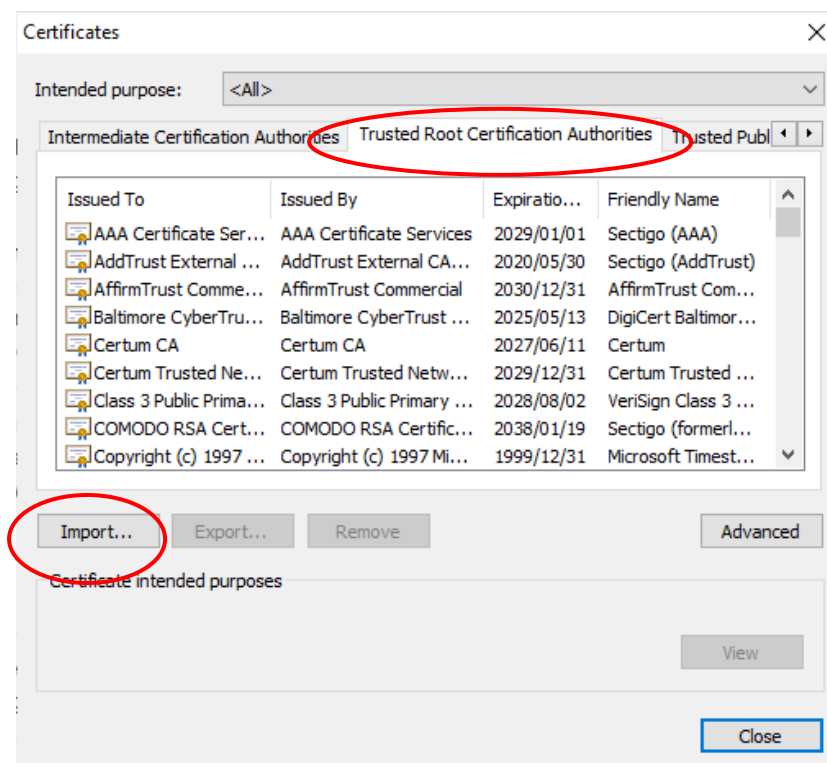
## 4 SSL/TLS function

### 7-3-2. Example of importing a self-signed certificate in a browser (Chrome)

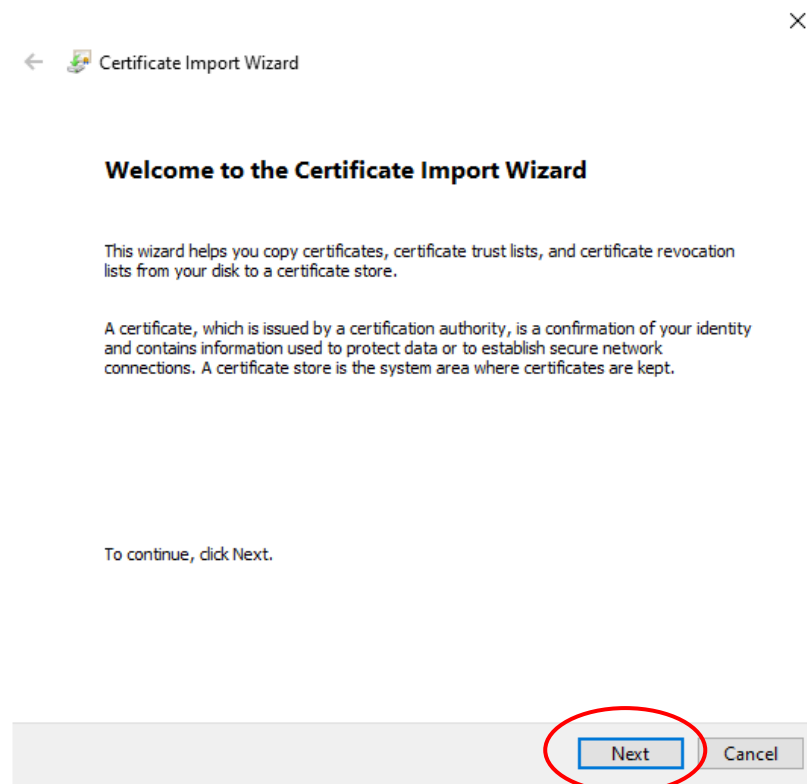
Chrome Settings => Privacy and security => Security => Manage certificate



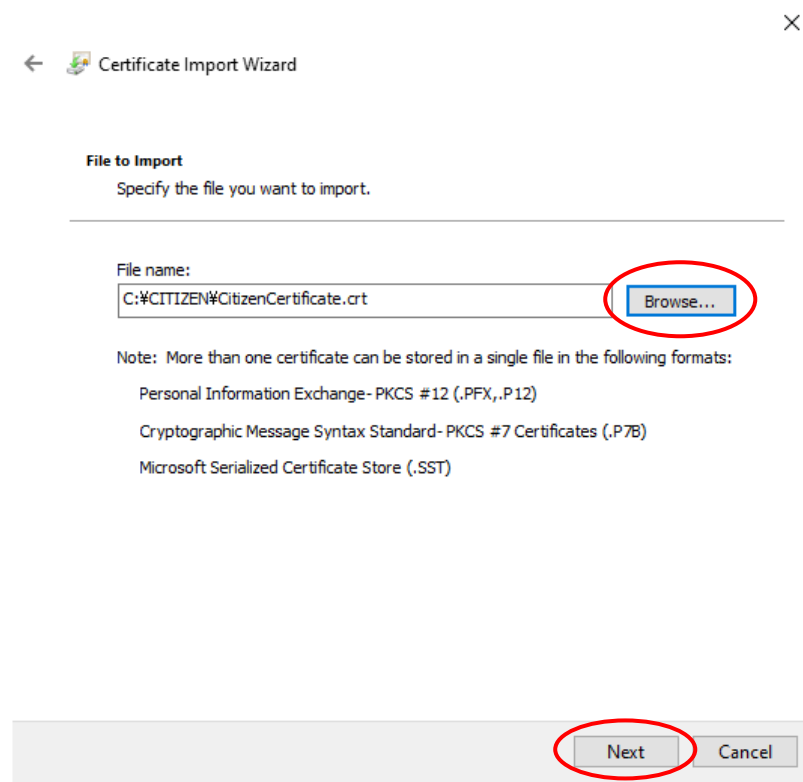
Select the "Trusted Root Certification Authorities" tab and click the "Import" button.



Press "Next".

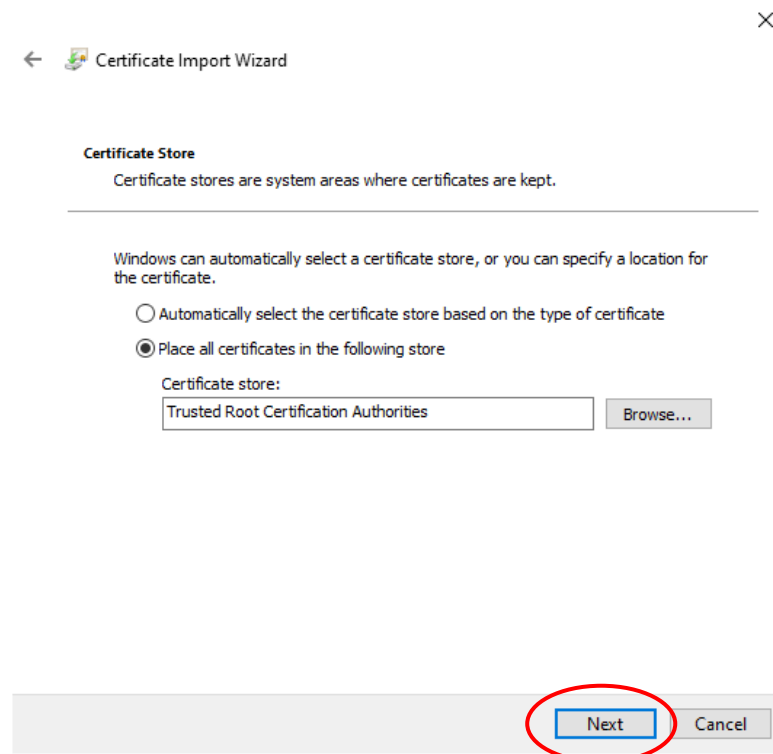


Press "Browse" and choose the self-signed certificate file that you exported in 7-3-1 and press "Next".



#### 4 SSL/TLS function

Press "Next".



← Certificate Import Wizard

**Certificate Store**  
Certificate stores are system areas where certificates are kept.

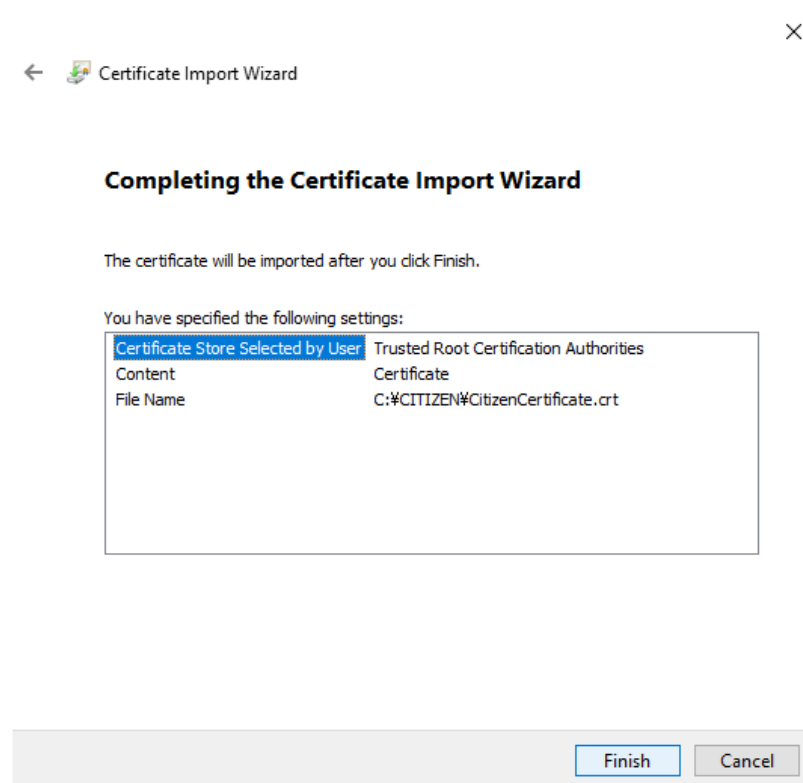
Windows can automatically select a certificate store, or you can specify a location for the certificate.

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

☒ Place all certificates in the following store

Certificate store:

Press "Finish"



← Certificate Import Wizard

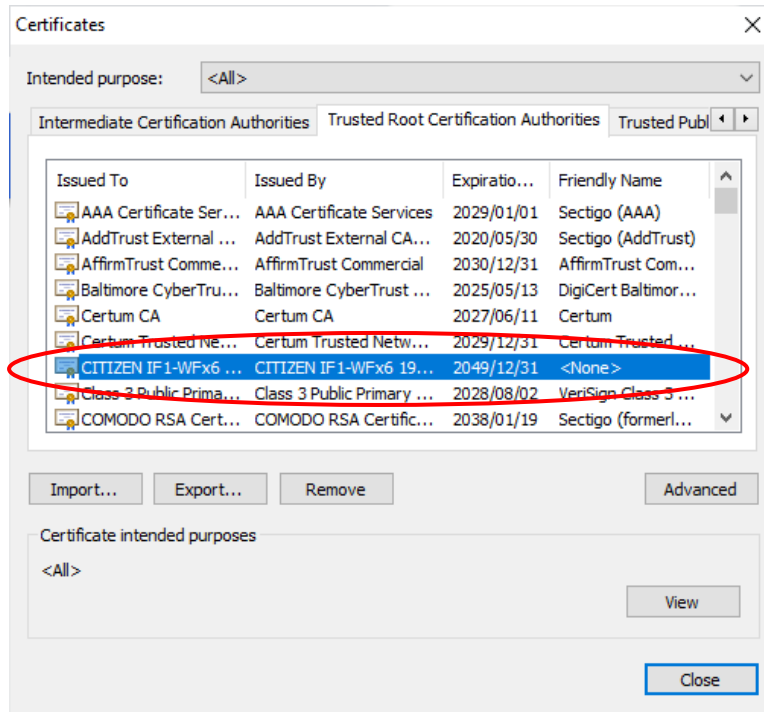
**Completing the Certificate Import Wizard**

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\CITIZEN\CitizenCertificate.crt

When a security warning appears, press Yes to complete the certificate installation, Then the printer's self-signed certificate has been registered with the "Trusted Root Certification Authority".



This will allow SSL/TLS communication between this Chrome and the printer using https without warning. The procedure is basically the same for other browsers.

#### Note

When using a self-signed certificate exported from this board, it is necessary to import the certificate for each browser as shown in this procedure to prevent the warning from appearing. However, if the user has prepared a self-signed certificate separately from this board, the self-signed certificate and private key can be registered as a set to this board, just like a public CA signed certificate, so that no warning will be issued without importing the certificate for each browser.

For more information, please contact us.

## 4 SSL/TLS function

---

### 7-4. SSL/TLS and certificate related specifications

#### 7-4-1. SSL/TLS communication specifications

TCP/IP version	TCP/IP v4
SSL/TLS version	TLS1.2(SSL3.3) , TLS1.3*
Application protocol	HTTPS (Server Authentication)
TCP communication port	443
Supported certificate	Self-signed certificate CA signed certificate
Encryption algorithm	AES 128/256
Hash algorithm	SHA2-256/386*, SHA1
Key Exchange Method	RSA 2048 bit
Signature Algorithm	RSA, ECDSA*

\*Only supported on firmware version V1.14 and later.

#### Supported cipher suite

In the case of using TLS 1.3 (Supported only on firmware version V1.14 and later)

Priority	Cipher suite
1	TLS_AES_256_GCM_SHA384
2	TLS_CHACHA20_POLY1305_SHA256
3	TLS_AES_128_GCM_SHA256
Key Exchange	ECDHE
	DHE
Signature	ECDSA
	RSASSA-PKCS1-v1_5

In the case of using TLS 1.2

Priority	Cipher suite
1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
4	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
5	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
6	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384*
7	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
9	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
10	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
12	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
13	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
14	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
15	TLS_RSA_WITH_AES_128_CBC_SHA
16	TLS_RSA_WITH_AES_128_CBC_SHA256
17	TLS_RSA_WITH_AES_128_GCM_SHA256
18	TLS_RSA_WITH_AES_256_CBC_SHA
19	TLS_RSA_WITH_AES_256_CBC_SHA256
20	TLS_RSA_WITH_AES_256_GCM_SHA384*
21	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
22	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
23	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
25	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
26	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
27	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256*

\* Supported only on firmware version V1.14 and later.

## 4 SSL/TLS function

### 7-4-2. Self-signed certificate related specifications

By entering the necessary items on the Web Manager screen, you can issue, save, and export a self-signed certificate on this board. The initial state is without certificate information.

#### Self-signed certificate entry field

Field	Items	Initial value	Available characters and symbols	Max. Chars
Key Type		RSA	RSA, Either RSA or ECDSA*	-
Issuer Subject	Common Name (CN)	IP address in use	Alphanumeric, Space, "-" (Hyphen), "." (Dot) (Inputs other than IP addresses are allowed.)	64 chars
	Organization Unit (OU)	(Blank)	Alphanumeric, Space, "," (Comma), "+" (Plus),	64 chars
	Organization (O)	CITIZEN SYSTEMS JAPAN	"-" (Hyphen), "." (Dot), "/" (Slash), "_" (Underscore),	64 chars
	Locate (L)	(Blank)	"(" (Bracket L), ")" (Bracket R)	128 chars
	State (S)	(Blank)		128 chars
	Country (C)	JP	Alphanumeric	2 chars
Validity (Not After)		2049/12/31 or 1 year after "Create"	YYYY/MM/DD (2020/01/01 ~ 2049/12/31)	
Validity (Not Before)		2020/01/01 or the time of "Create"	YYYY/MM/DD (2020/01/01 ~ 2049/12/31)	

\* Supported only on firmware version V1.14 and later.

The other items set in the certificate creation are entered as shown in the table below. No changes can be made by the user.

#### Self-signed certificate fixed fields

Field	Items	Fixed value
Certificate Subject Alt Name	DNS Name	Common name (CN)
	IP Address	Common name (CN) if common name is IP address.
Certificate Key Usage		Non-repudiation, Digital Signature, Key Encipherment (a0)
Extended Key Usage		TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Basic Constraint	Subject Type	End Entity
	Path Length	None
	Constraint	

Specification for exporting a certificate file signed by a internal certifying authority.

Signature algorithm	RSA	ECDSA*
Encoding type	Base64	
File extension	.crt	
Version	V3	
Public Key	RSA 2048 bit	ECC 384 bit
Signature algorithm	SHA2-256 with RSA	SHA2-256 with ECDSA

\* Supported only on firmware version V1.14 and later.

#### 7-4-3. CA signed certificate related specifications

The specifications of CA signed certificate that can be imported and used are as follows.

Please make sure that the certificate and private key are paired before importing.

Please also make sure that the Common Name (CN) field in the Subject Name is always filled in.

CA signed certificate	“.pem” format / “.der” format
Private key	“.key” format (Password protection not supported)
Encryption algorithm	AES 128/256
Hash algorithm	SHA2-256/384*, SHA1
Key Exchange Method	RSA 2048 bit
Signature Algorithm	RSA, ECDSA*

\* Displayed only for firmware version V1.14 and later.

#### 7-4-4. Handling of saved certificates when restoring factory settings/updating firmware

When the Factory Default process in the CONFIG>Maintenance tab is executed, each setting value will be set to the default value and the registered certificate will be deleted; when the Firmware Upgrade process is executed, each setting value and the registered certificate will be retained.