

CITIZEN

IF1-EFX1 / IF1-EFX2 / IF1-EFX3 IF2-EFX1 / IF2-EFX2 / IF2-EFX3 Ethernet Interface Board User's Manual

Ver.2.20

Target firmware V1.15 or later (IFx-EFX1), V2.30 or later (IFx-EFX2), V2.33 or later (IFx-EFX3)

CITIZEN SYSTEMS JAPAN CO., LTD.

Contents

| | |
|---|-----------|
| Contents | 2 |
| Read before using | 4 |
| 1. Introduction | 7 |
| 1-1. Features | 7 |
| 1-2. Model Classification | 8 |
| 1-3. Specifications | 8 |
| 1-4. Part Names and Functions | 10 |
| 2. Preparation | 11 |
| 2-1. Connecting LAN cable..... | 11 |
| 2-2. Connecting a Peripheral Device | 11 |
| 2-3. Connecting the Interface Board Unit | 12 |
| 3. Network Settings and Operation..... | 14 |
| 3-1. Overview | 14 |
| 3-2. Panel Button..... | 16 |
| 3-3. Printing the Interface Board Configuration..... | 17 |
| 3-4. Returning the Interface Board Configuration to Factory Default Settings..... | 18 |
| 3-5. Display status by LED | 19 |
| 3-6. Simple Setting Procedure Example for Wired LAN | 20 |
| 4. Web Manager | 21 |
| 4-1. Starting the Web Manager | 21 |
| 4-1-1. Initial Setup (Board Firmware v2.57 and later) | 22 |
| 4-2. HOME Window | 23 |
| 4-3. STATUS Window | 24 |
| 4-3-1. STATUS>>System Status Tab | 25 |
| 4-3-2. STATUS>>Network Status Tab | 26 |
| 4-3-3. STATUS>>Printer Status Tab..... | 27 |
| 4-4. CONFIG Window..... | 28 |
| 4-4-1. CONFIG>>General Tab | 29 |
| 4-4-2. CONFIG>>User Account Tab | 30 |
| 4-4-3. CONFIG>>Maintenance Tab | 31 |
| 5. NetToolK..... | 32 |
| 5-1. Installing the NetToolK | 32 |
| 5-2. Information List Window..... | 35 |
| 5-3. Setup Window | 37 |
| 5-3-1. "General" Tab..... | 37 |
| 5-3-2. "Wireless LAN" Tab..... | 37 |
| 5-3-3. "Supported Protocols" Tab | 38 |
| 5-3-4. "User Account" Tab..... | 38 |
| 5-3-5. "Maintenance" Tab | 39 |
| 6. XML Print / Peripheral Device Control Function..... | 41 |
| 6-1. Overview | 41 |

| | | |
|-----------|--|-----------|
| 6-2. | CONFIG>>Service Tab | 42 |
| 6-2-1. | Media Converter..... | 43 |
| 6-2-2. | XML Print..... | 43 |
| 6-2-3. | XML Device Control..... | 43 |
| 6-2-4. | XML Device Control / Line Display | 44 |
| 6-2-5. | XML Device Control / Scanner | 44 |
| 6-2-6. | XML Device Control / Speaker | 44 |
| 6-2-7. | XML Config..... | 44 |
| 6-2-8. | XML Settings (Displayed only for firmware version V2.45 and later) | 45 |
| 6-2-9. | Submit / Reset Button..... | 45 |
| 6-3. | STATUS>>Service Status Tab..... | 46 |
| 7. | SSL/TLS function | 47 |
| 7-1. | Overview | 47 |
| 7-2. | CONFIG>>SSL/TLS Tab | 49 |
| 7-2-1. | SSL/TLS tab | 49 |
| 7-2-2. | Create Self-Signed Certificate..... | 50 |
| 7-2-3. | Update Self-Signed Certificate..... | 51 |
| 7-3. | To enable SSL/TLS communication using a self-signed certificate | 52 |
| 7-3-1. | Generating and exporting self-signed certificates | 52 |
| 7-3-2. | Example of importing a self-signed certificate in a browser (Chrome) | 57 |
| 7-4. | SSL/TLS and certificate related specifications | 61 |
| 7-4-1. | SSL/TLS communication specifications..... | 61 |
| 7-4-2. | Self-signed certificate related specifications | 63 |
| 7-4-3. | CA signed certificate related specifications..... | 64 |
| 7-4-4. | Handling of saved certificates when restoring factory settings/updating firmware | 64 |
| 8. | Request Print function | 65 |
| 8-1. | Overview | 65 |
| 8-2. | CONFIG>>Request Print Tab..... | 66 |
| 8-3. | STATUS>>Request Print Tab | 67 |
| 8-4. | Printing system log | 67 |

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.

Related SDKs and Documentation

Printing with XML data

- * XML Print (For POS printers)
 - POS Print SDK(JavaScript)
 - CITIZEN XML Print Service JavaScript POS Print SDK Programming Manual
- * XML Print (For Label printers)
 - Label Print SDK(JavaScript)
 - CITIZEN XML Print Service JavaScript Label Print SDK Programming Manual

Network board configuration with XML data

- * XML Config (JavaScript)
 - Config SDK(JavaScript)
 - CITIZEN XML Device Control Service JavaScript Device Control SDK Programming Manual

Peripheral device control using XML data

- * XML Device 【JavaScript】
 - Device Control SDK (JavaScript)
 - CITIZEN XML Config Service JavaScript Config SDK Programming Manual

Peripheral device control using dedicated control port

- * Peripheral device control (For POS printer / Windows)
 - POS Print SDK (Windows)
 - Windows POS Print SDK Programming Manual
- * Peripheral device control (For POS printer / Android)
 - POS Print SDK (Android)
 - Android POS Print SDK Programming Manual
- * Peripheral device control (For POS printer /iOS-Swift)
 - POS Print SDK (iOS-Swift)
 - iOS POS Print SDK (Swift) Programing Manual
- * Peripheral device control (For POS printer / iOS Objective C)
 - POS Print SDK (iOS-Objective C)
 - iOS POS Print SDK (Objective-C) Programing Manual

(Peripheral device control from the label printer can also be performed using the SDK for POS printers.)

Request printing

- Programmer's Manual for "Request Print" on XML Print Service (Sample program)

Term Description

Since different documents are intended for different audiences and assume different levels of expertise, different terms may be applied for clarity even when the content being explained is the same. In addition, some terms are easily confused because they are sometimes referred to from the opposite standpoint depending on their function. The following is a glossary and explanation of terms that you should pay attention to when reading this document in conjunction with other related documents.

Printer / Interface board (Wired or Wireless LAN) / Service

Printers that use network and XML related functions have an interface board (wired/wireless LAN) that is a single board computer. On the memory on that interface board, there are several resident programs that perform specific functions, which are called services.

For example, the XML Print service receives XML data for printing, converts it into commands and data for the printer, passes it to the printer, and sends a reply when it is confirmed that the printing is completed. From the point of view of the terminal sending the data, it is easier to recognize network and XML-related services as interface boards or printers, so we may use the terms "board," "interface board," or "printer" instead of "service" in the explanation.

Web server / Web app server

The Web server is the terminal that sends data to the browser for screen display. The Web server receives the information of the operations performed on the browser. When a Web server uses a programming language to process data to be sent and received, the group of programs that process the data is called a Web application (hereinafter referred to as a Web app), and the terminal in charge of the function is called a Web app server.

Since there are many cases where a Web server and a Web app server are both used on the same terminal, the two are not strictly separated and may be referred to as a Web server in the sense of a Web app server.

Server / Client

In addition to Web server and Web app sever, there are various other types of servers depending on their functions, which are sometimes referred to simply as servers in the explanation.

The terminal that sends data to the server is called the client. Server and client are sometimes referred to interchangeably, depending on their function and position.

For example, in the main function of the printer, which is to print the received data, the printer is a print server from the terminal that sends the print data to the printer. The printer also has the function of a Web server, which we call a Web manager, for network settings, etc.

On the other hand, when sending a print data request to the Web app server, the printer is in the position of a client.

1. Introduction

Thank you for purchasing the Citizen IF1-EFX1/EFX2/EFX3, IF2-EFX1/EFX2/EFX3 Ethernet (LAN) interface board.

By using the LAN interface board IF1-EFX1/EFX2/EFX3, IF2-EFX1/EFX2/EFX3 (hereinafter referred to as the interface board, this interface board or this board) with our POS printers and label printers, each printer can be directly connected to the network enabling printing from a PC on the network to the printer. It also enables the PC and printer to communicate with each other, and the printer's operating status and print settings can be checked from the PC. In addition, depending on the printer, it is possible to print from XML format data and control peripheral devices connected to this interface board.

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

For firmware version V2.57 and later, you will be prompted to set an administrator password during the initial setup.

For boards with older firmware versions, please refer to the older manuals.

| Function | Supported Version | | |
|---|-------------------|-----------------|-----------------|
| | IFx-EFX1 | IFx-EFX2 | IFx-EFX3 |
| Raw Port TCP Keep Alive | V1.15 and later | V2.30 and later | V2.33 and later |
| XML Config (version 1.0) | V1.15 and later | V2.30 and later | V2.33 and later |
| SSL/TLS Function (TLS1.2, RSA signature) | - | V2.30 and later | V2.33 and later |
| Request Printing | - | V2.30 and later | V2.33 and later |
| WebSocket Communication | - | V2.45 and later | - |
| SSL/TLS Function (TLS1.3, ECDSA signature) | - | V2.45 and later | |
| XML Config (version 2.0) | - | V2.45 and later | |
| HTTP Keep Alive | - | V2.45 and later | |
| Administrator Password Initial Setup Function | - | V2.57 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 and peripheral device control by XML data depending on the printer
- Secure communication with SSL/TLS function. (IFx-EFX2/EFX3 only)
- "Request Print" allows printing with XML data from a Web server on the Internet (IFx-EFX2 only)
- XML Config function is available for configuration of the board.

4 Introduction

1-2. Model Classification

IF1 type: Applicable to CT-S801(II / III) / 851(II / III) / 601(II / III) / 851(II / III) / CL-S400DT / 6621 / CL-E7xx / CL-S7xxIII

IF2 type: Applicable to CT-D151 / CT-E601 / CT-E601 / CT-E651 / CT-S251 / 751 / 4500 / CL-E3xxEX

| | IF1 type | | | IF2 type | | |
|---------------------------|---------------|---------------|----------------|---------------|---------------|----------------|
| | Normal model | | USB host model | Normal model | | USB host model |
| Name | IF1-EFX1 | IF1-EFX3 | IF1-EFX2 | IF2-EFX1 | IF2-EFX3 | IF2-EFX2 |
| Number of USB ports | 0 | 0 | 2 | 0 | 0 | 2 |
| Peripheral device control | Not supported | Not supported | Supported | Not supported | Not supported | Supported |
| SSL/TLS | Not supported | Supported | Supported | Not supported | Supported | Supported |
| Request print | Not supported | Not supported | Supported | Not supported | Not supported | Supported |

1-3. 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

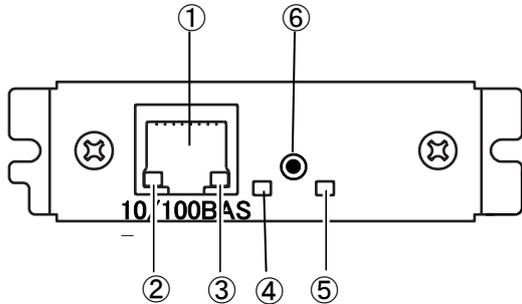
| | | IF1-EFX1 / IF1-EFX2 / IF1-EFX3 | IF2-EFX1 / IF2-EFX2 / IF2-EFX3 |
|----------|------------------|--|---|
| Hardware | Supported Models | CT-S801 / 851 / 601 / 651 (II / III) / CL-S400DT / 6621 / E7xx / S700III | CT-D151 / E601 / E651 / S251 / CT-S751 / 4500 / CL-E3xxEX |
| | Operation panel | LED: 4 (2 on panel, 2 on RJ45 connector), Button: 1 | |
| | USB | USB-A connector 0 or 2 USB Specs: USB2.0 High Speed | |

Software

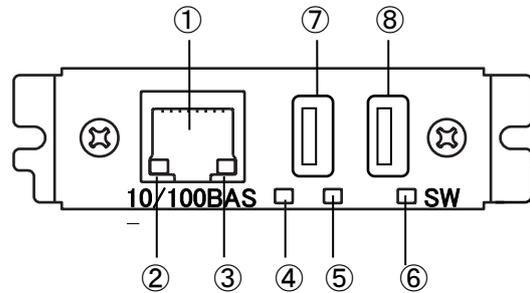
| | | |
|----------|---------------------|---|
| Software | Setting methods | Browser, PC setting tool, Cloud |
| | Firmware upgrade | Browser, PC setting tool, Cloud |
| | Supported Platforms | Windows 7、Windows8, Windows10, Windows11, HTML5 browser |

1-4. Part Names and Functions

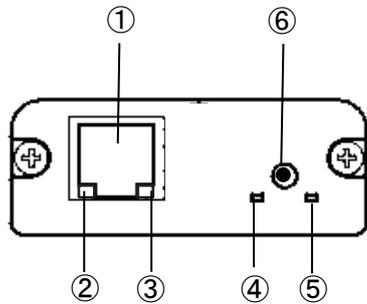
IF1-EFX1 / IF1-EFX3 (No USB Port)



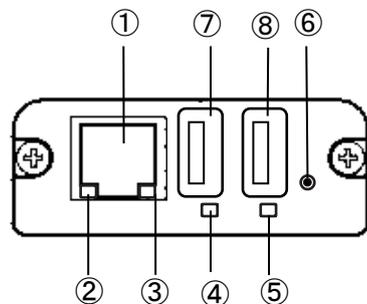
IF1-EFX2 (USB 2 Port)



IF2-EFX1 / IF2-EFX3 (No USB Port)



IF2-EFX2 (USB 2 Port)



- ① RJ45 connector (compatible with 10Base-T/100Base-TX)
Connection for LAN cable
- ② Ethernet transmission speed LED indicator (green)*1
Shows Ethernet transmission speed with steady/blinking light.
- ③ Ethernet status indicator LED (yellow)*1
Shows Ethernet connection status (disconnected, receiving data, etc.).
- ④ Ethernet status LED indicator (green)*1
- ⑤ Ethernet status LED indicator (red)*1
Shows transmission, connection and error statuses with steady/blinking lights combinations.
- ⑥ Panel button*2
Used to operate the Interface board.
- ⑦ USB connector (First)
- ⑧ USB connector (Second)
Connect an approved peripheral device to a USB port.

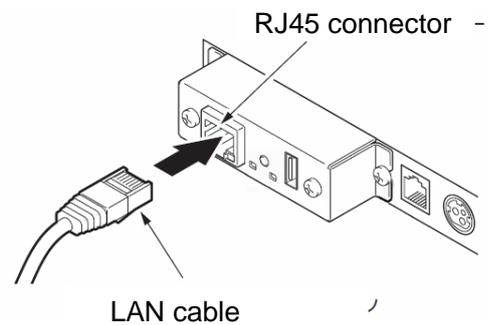
*1 See 3-5, Display status by LED (page 19) for indicator details.

*2 See 3-2, Panel Button (page 16) for panel button operations.

2. Preparation

2-1. Connecting LAN cable

Connect a LAN cable to the RJ45 connector of this interface board. (Diagram on right shows a typical example)



2-2. Connecting a Peripheral Device

The following restrictions apply to peripheral devices. Please use them properly.

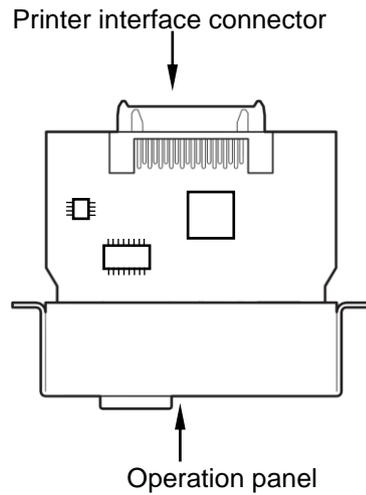
- The connection of unsupported peripherals to the USB port is prohibited. (please inquire about which devices are supported).
- Connecting a tablet or other device to USB ports for supplying power is also prohibited.
- Do not insert or remove peripheral devices from the USB port while the printer power is on.
- Connection through a USB hub is prohibited.
- In the case of the IFx-EFX2 which has two USB ports, connecting to both the left and right ports is possible, but connecting two of the same type of device (two displays, two scanners, etc.) is prohibited.

4 Preparation

2-3. Connecting the Interface Board Unit

1) The interface board can be used by connecting it to the main board of the printer.

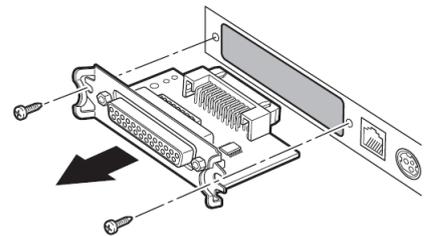
It is connected by plugging the printer interface connector into the connector on the printer's main board. It is possible to replace the other interface with the LAN interface, but extra caution is required. (Diagram below shows a typical example)



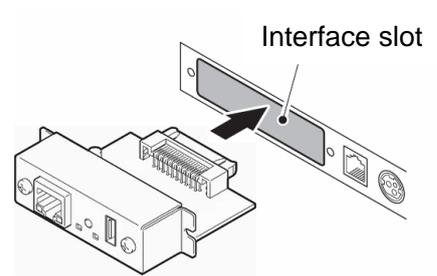
Warning

- Malfunctions may occur if the interface board is removed or re-inserted.
- To install the interface board, please contact your dealer or service person.
- If you replace the interface board by yourself, do so at your own risk, taking care to avoid static electricity, etc.

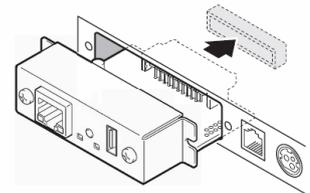
2) If another interface board is installed in the printer, remove it.



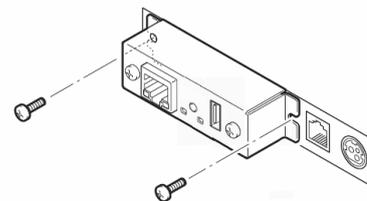
- 3) Insert the interface board into the interface slot of the printer.



- 4) Connect the interface connector of the board to the interface connector inside the printer.



- 5) Fix the interface board in place with screws.



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 V2.57 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.

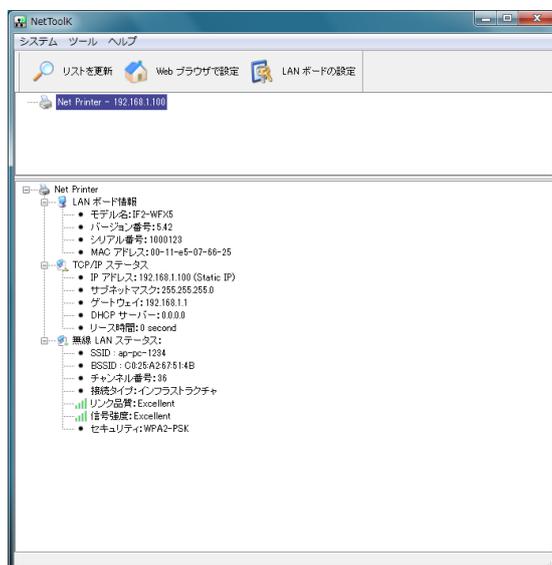
Web Manager

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.



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

See the next captor 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”.

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

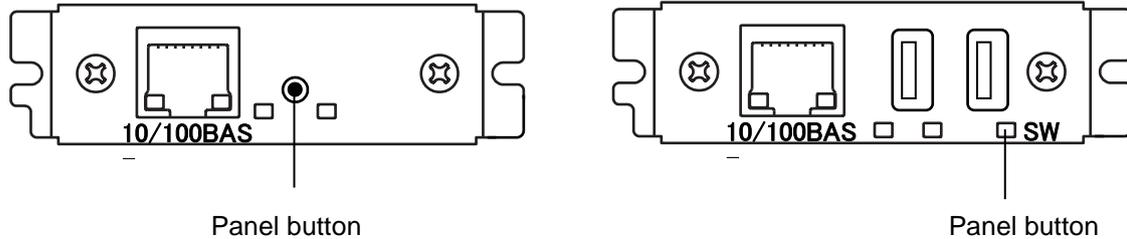
After the firmware upgrade starts, do not disconnect power or transmission to the printer until the upgrade is complete.

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. (Diagram is of IF1-EFX1 / IF1-EFX3 and IF1-EFX2)



■ 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 17) 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 3-4, Returning the Interface Board Configuration to Factory Default Settings (page 18) 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.

■ System log printing

If printing etc. does not work as expected, you may be able to check the situation by checking the system log of this board. The system log can be printed using the panel buttons.

Please refer to Chapter 5 "Useful Functions for Request Print" in the "Programmer's Manual for "Request Print" for a description of system log printing.

3-3. Printing the Interface Board Configuration

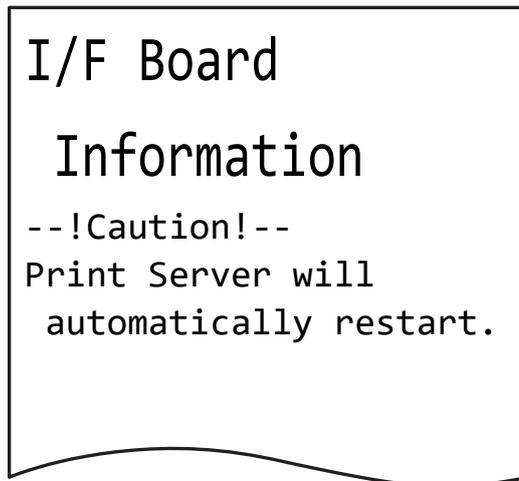
Press the panel button to print out the configuration of the interface board from the printer.

- 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 Information on the connection status of XML-controlled peripheral devices.
- ⑨ SSL/TLS function setting information.
- ⑩ Setting information for the Request Print function.

| | |
|---|---|
| ① | I/F Board Information |
| ② | IFx-EFX1(Rev1.1.2): Ver 1.15 |
| 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 : CT-S801 |
| 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 | XML Device Information Display Status : Offline Scanner Status : Offline Speaker Status : Offline |
| ⑨ | SSL/TLS Certificate : Self-Signed Self-Signed : Not Exist CA-Signed : Not Exist |
| ⑩ | Request Print Service Status : Disable Current URL : http://www.example.net/test.php Proxy Address : 192.168.100.190 Proxy Port : 8080 Interval : 10 sec ID : AA-BB-CC-DD-EE-FF DNS1 : 192.168.10.1 DNS2 : 8.8.8.8 |

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 three 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.
```

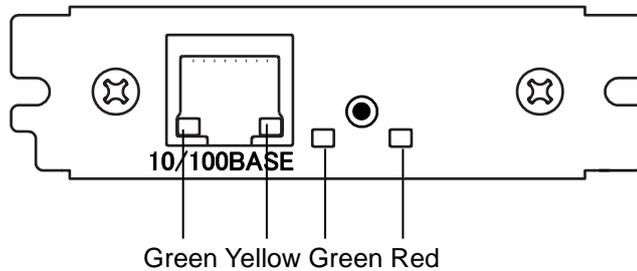
Warning

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

(Diagram shows a typical example. There are interface boards where the positioning of LEDs differs, but the order from left to right is the same.)



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 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 17) 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 21) for details.

Instead of Web Manager, you can also use NetToolK, a network configuration tool for Windows. See "5 NetToolK" (page 32) 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.

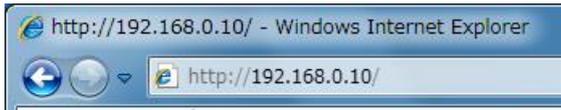
4. Web Manager

The interface board is equipped with a Web manager function, which allows accessing the interface board from a Web browser to check the status of the interface board and change its settings.

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".



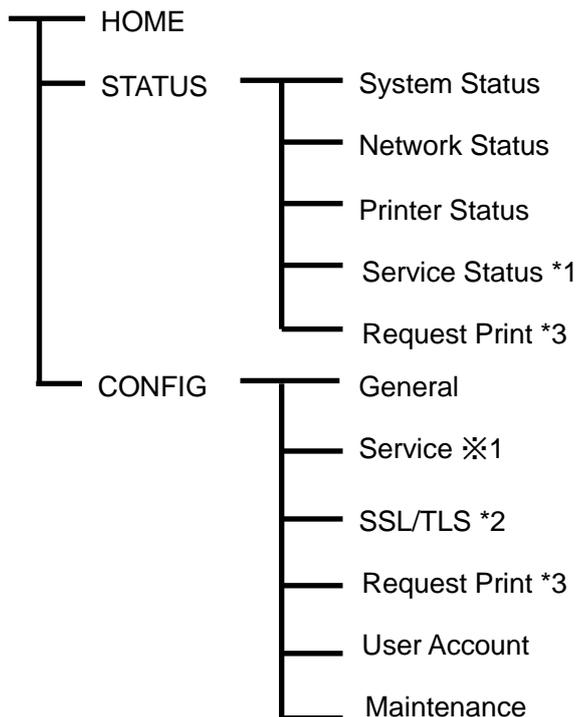
* The image to the left is a sample. Enter the actual allocated value for the IP address.

Warning

- The configuration window of the interface board cannot be displayed if the network settings of your computer and the interface board differ. Ensure that the IP address of the interface board matches the settings of your network.
- The IP address of this interface can be confirmed as described in "Printing the Interface Board Configuration".

Web Manager Window Layout

Web Manager consists of following windows and tabs. It differs depending on supported functions.



*1 If the XML/Peripheral control functions are 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.

*3 If Request Print function is available, Request Print tab will appear on STATUS / CONFIG window.

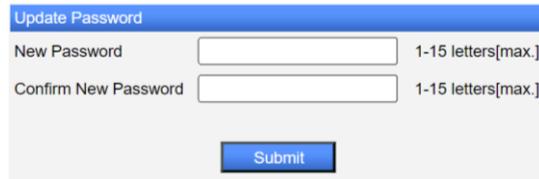
For details, see "6 XML Print / Peripheral Device Control Function," "7 SSL/TLS function," and "8 Request Print function," respectively.

4 Web Manager

4-1-1. Initial Setup (Board Firmware v2.57 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

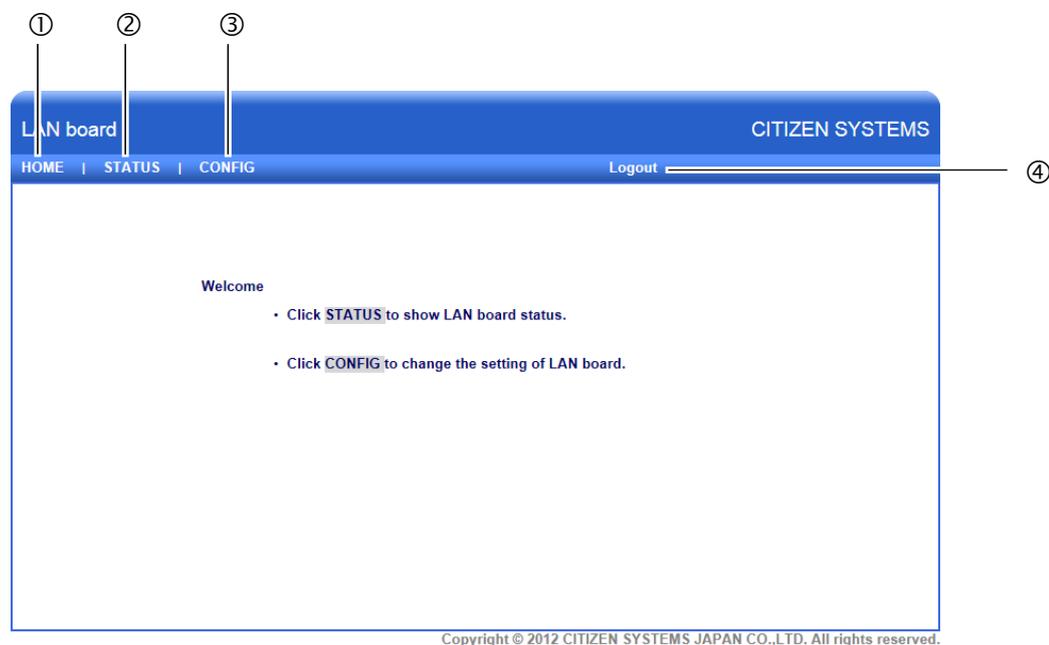
Enter the administrator password and click the "Submit" button. This will display the login screen.

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

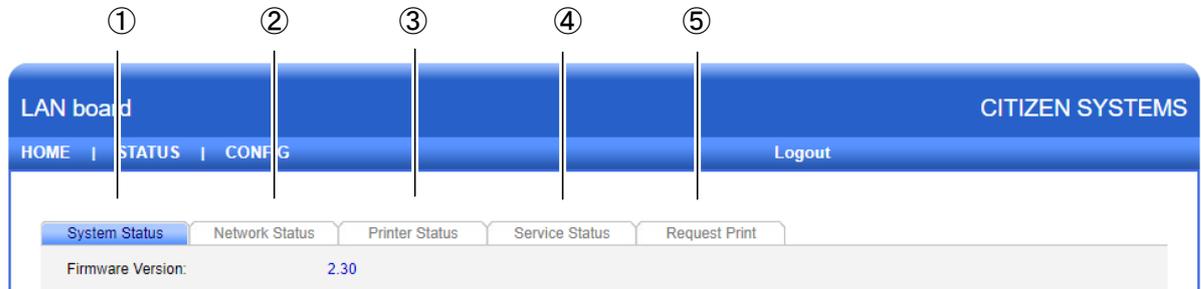
This is the Home window of the Web manager.



- 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. It is not possible to open the CONFIG window at multiple PCs of the same time. You must log out to make settings using another Web manager or NetToolK.

4-3. STATUS Window

Displays the status of the Interface board.



① System Status tab

See 4-3-1, STATUS>>System Status Tab (page 25).

② Network Status tab

See 4-3-2, STATUS>>Network Status Tab (page 26).

③ Printer Status tab

See 4-3-3, STATUS>>Printer Status Tab (page 27).

④ Service Status tab

See 6-3 STATUS>>Service Status Tab (page 46)

⑤ Request Print tab

See 8-3 STATUS>>Request Print Tab (page 67)

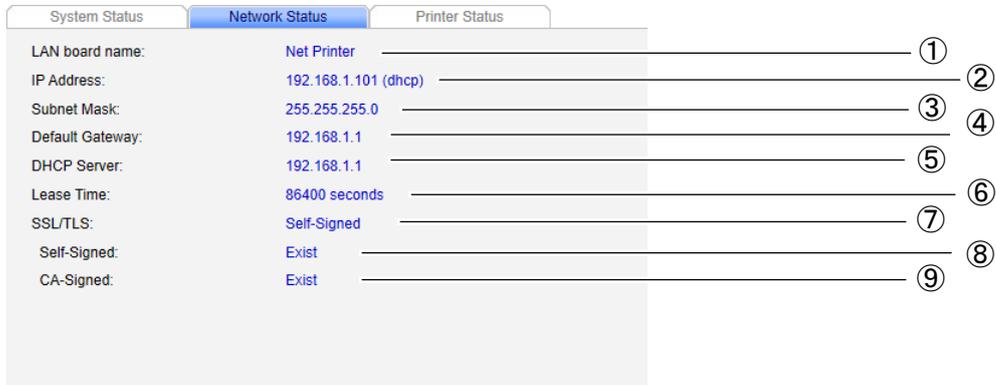
4-3-1. STATUS>>System Status Tab

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

- 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.

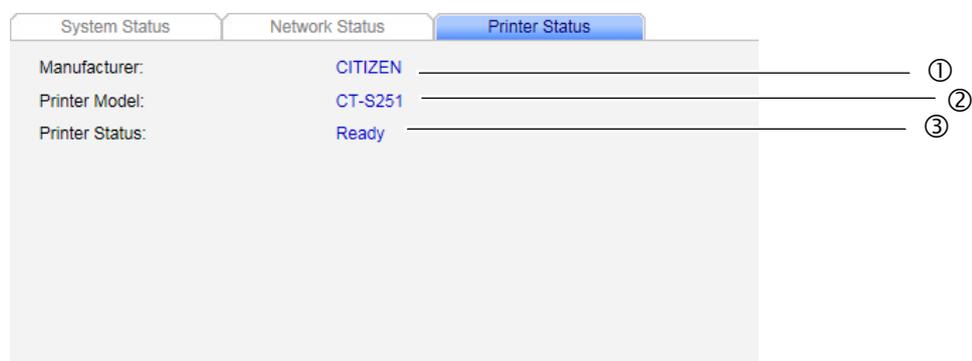
4 Web Manager

4-3-2. STATUS>>Network Status Tab



- 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-Singed: 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



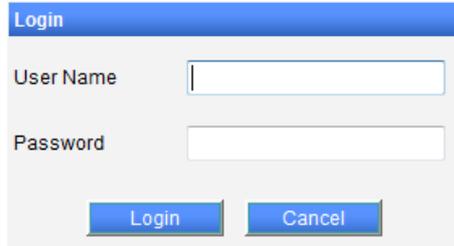
- ① Manufacturer
Displays "CITIZEN".
- ② Printer Model
Displays the model of the printer to which the Interface board is connected.
- ③ Printer Status
Displays the operational status of the printer to which the Interface board is connected.
Ready: Ready to print.
Offline: Not ready to print.
Paper Empty: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

(Note) When the printer is connected to the Interface board and the bi-directional port of the printer driver is enabled, the printer status is not correctly displayed. In such cases, confirm the printer status from the Windows spooler.

4 Web Manager

4-4. CONFIG Window

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



The login form consists of a blue header bar with the word "Login" in white. Below the header, there are two input fields: "User Name" and "Password". At the bottom of the form, there are two buttons: "Login" and "Cancel", both in blue with white text.

User Name / Password

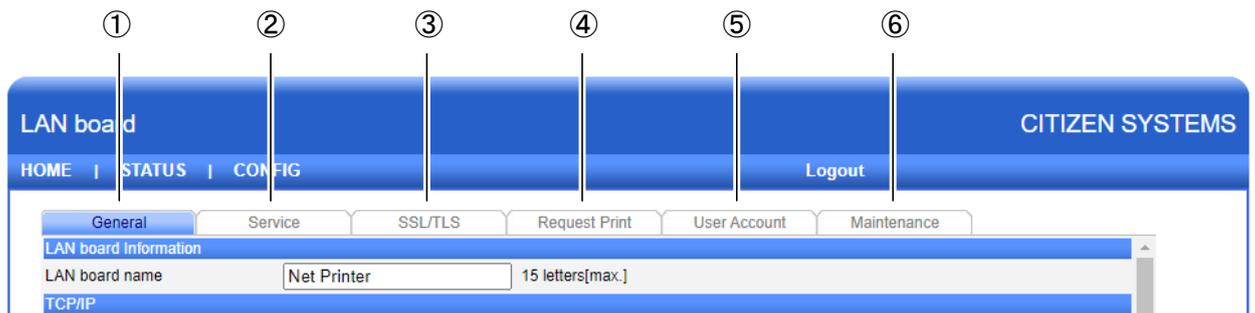
Enter administrator user name and administrator password. (Initial setting: admin / admin. From version 2.57 and later, it is necessary for you to set your own password.)

Login button

Click "Login". The CONFIG window appears.

Cancel button

Cancel login.



- ① General tab
See 4-4-1 CONFIG>>General Tab (page 29).
- ② Service tab
See 6-2 CONFIG>>Service Tab (page 42)
- ③ SSL/TLS tab
See 7-2 CONFIG>>SSL/TLS Tab (page 49)
- ④ Request Print tab
See 8-2 CONFIG>>Request Print Tab (page 66)
- ⑤ User Account tab
See 4-4-2 CONFIG>>User Tab (page 30).
- ⑥ Maintenance tab
See 4-4-3 CONFIG>>Maintenance Tab (page 31).

4-4-1. CONFIG>>General Tab

LAN board Information

- LAN board name (factory default: Net Printer)
Set the ID of the 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
Enter 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.

4 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.

| General | User Account | Maintenance |
|---------------------------------------|------------------------------------|--------------------------------------|
| Set User | | |
| New User name | <input type="text" value="admin"/> | 15 letters[max.] |
| New Password | <input type="text"/> | 15 letters[max.] |
| Confirm New Password | <input type="text"/> | 15 letters[max.] |
| <input type="button" value="Submit"/> | | <input type="button" value="Reset"/> |

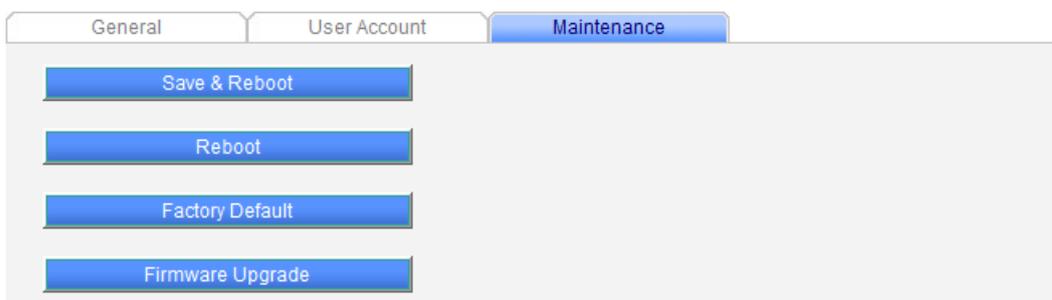
Set User

- 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.

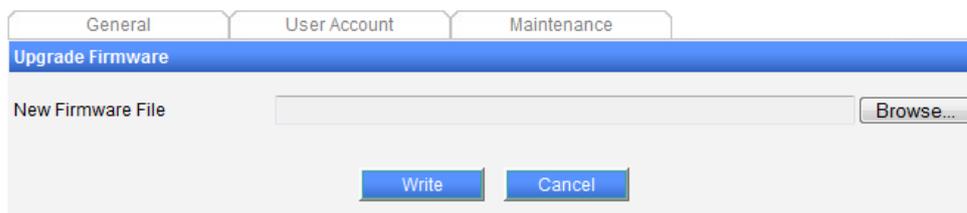
Warning

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>>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.

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

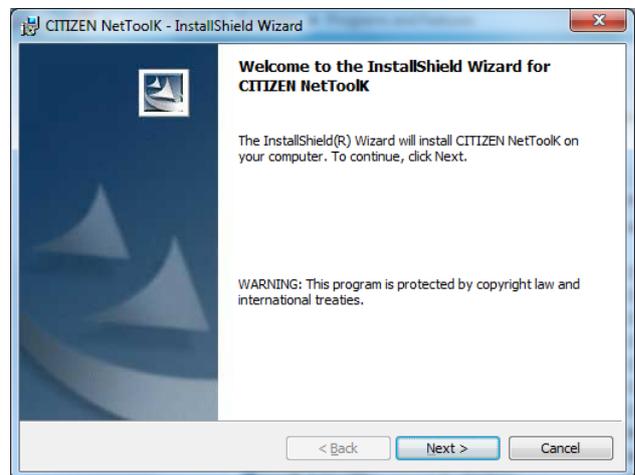
If the firmware is not updated correctly, this interface board may not boot.

5. NetToolK

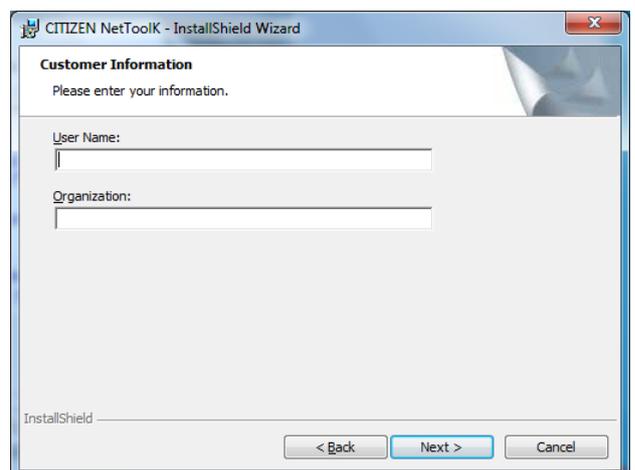
The “NetToolK” utility software runs on the Windows operating system and can be used to change the settings of the Interface board. This tool can be used with both wired and wireless LAN interface boards.

5-1. Installing the NetToolK

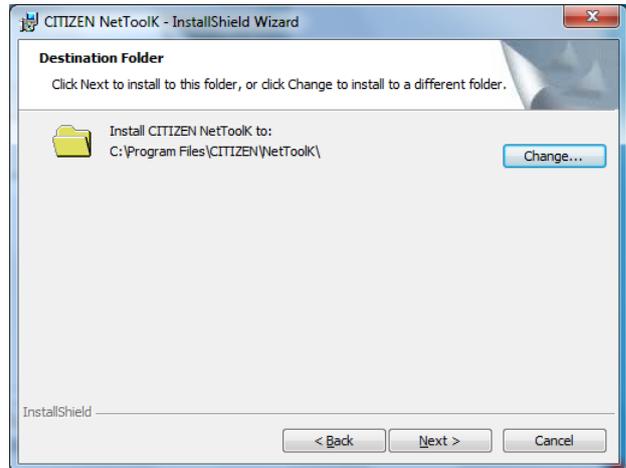
- 1) Acquire the file “NetToolKSetup.exe” from our website. Double click the file.
- 2) If the “User Account Control” screen appears, click “Continue.”
- 3) The screen shown on the right appears.
Click “Next.”



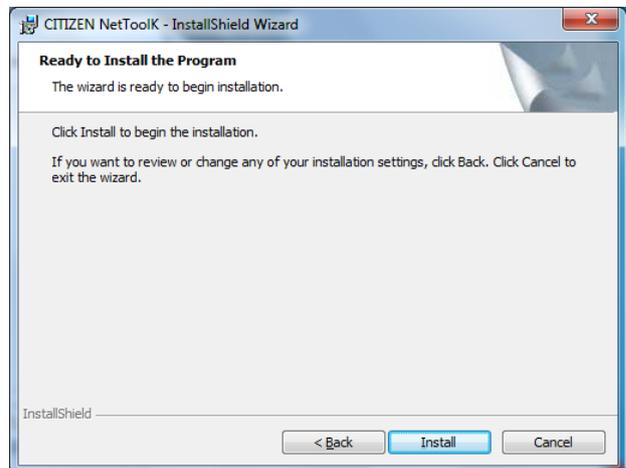
- 4) Enter a username and organization,
and then click “Next”.



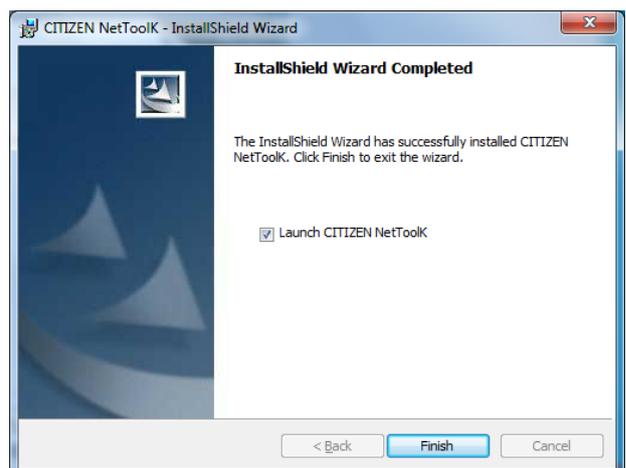
- 5) The screen shown on the right appears.
Click "Next."



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

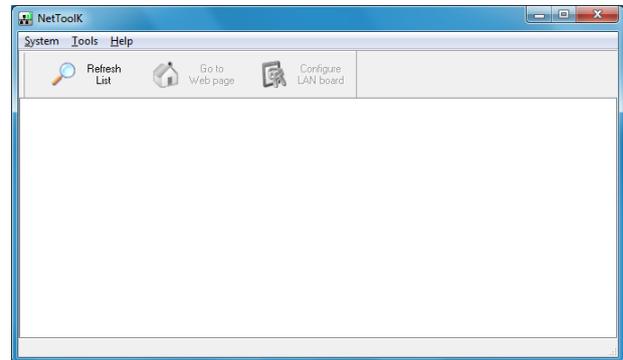


- 7) Click "Finish" to complete installation.



5 NetToolK

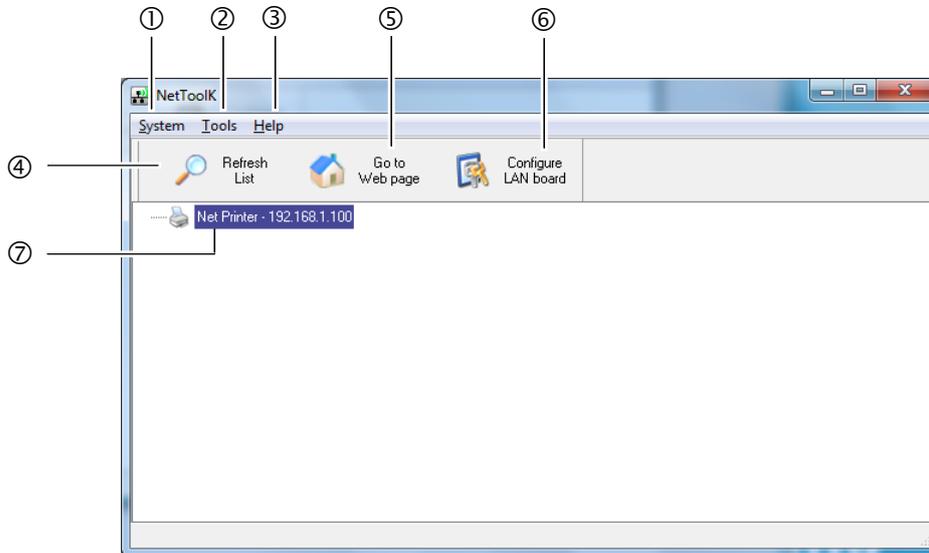
- 8) The PC setting tool starts. From the “System” menu, select “Exit”.



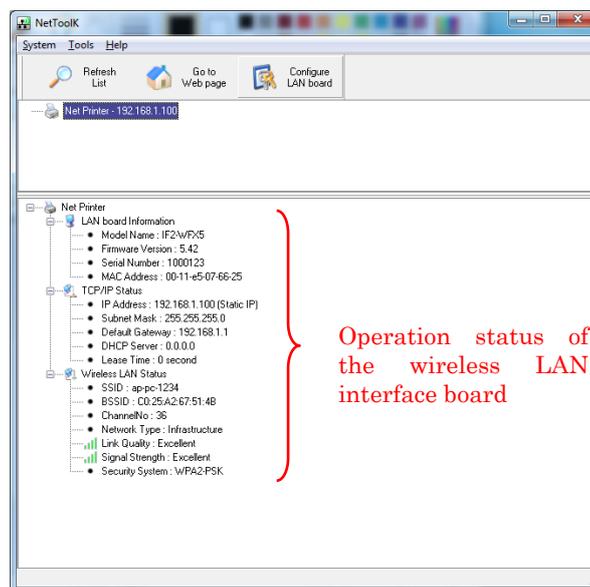
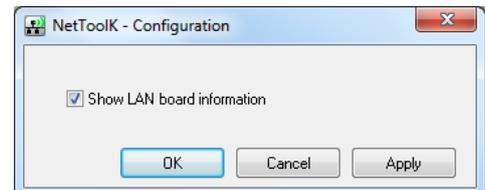
- 9) The icon on the right is placed on the desktop of the computer. You can now start program by double clicking this icon.



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 37).
If the firmware version of this board is V2.57 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”.

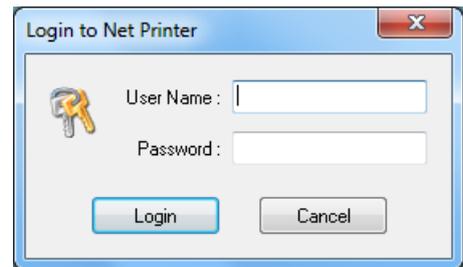
If the firmware version of this board is V2.57 or later, it is necessary to set the user password via Web Manager before performing any configuration.

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

Username: admin (factory default)

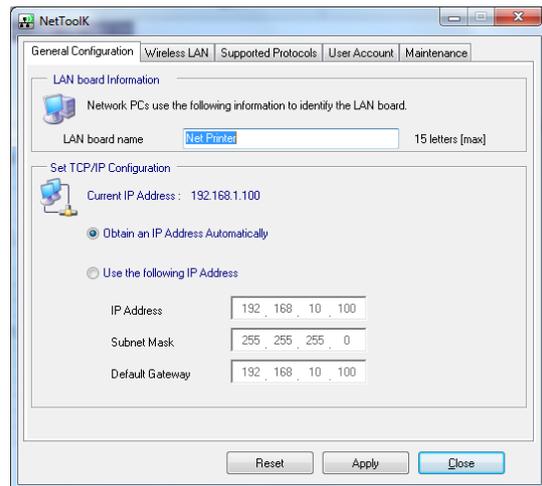
Password: admin: (factory default)

(From version 2.57 and later, it is necessary for you to set your own password.)



5-3-1. “General” Tab

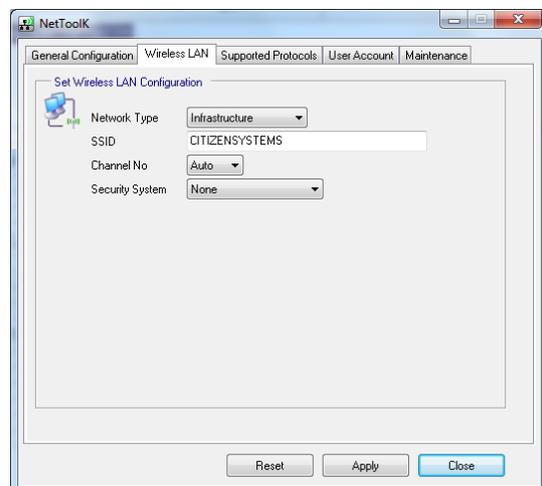
Use the “General” tab to configure the LAN board name and IP address



5-3-2. “Wireless LAN” Tab

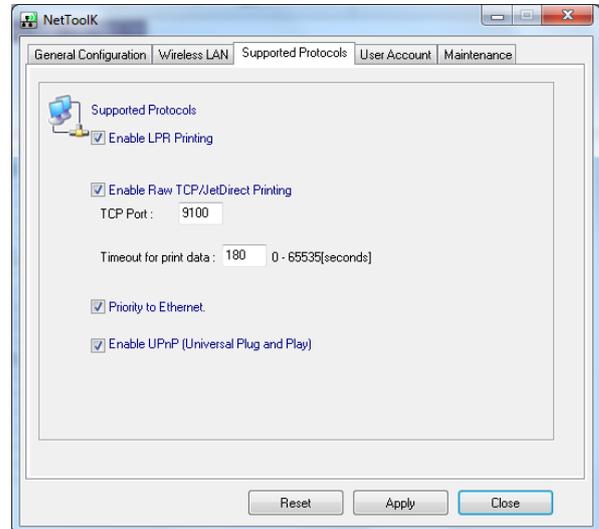
Use the “Wireless LAN” tab to configure the LAN.

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



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.



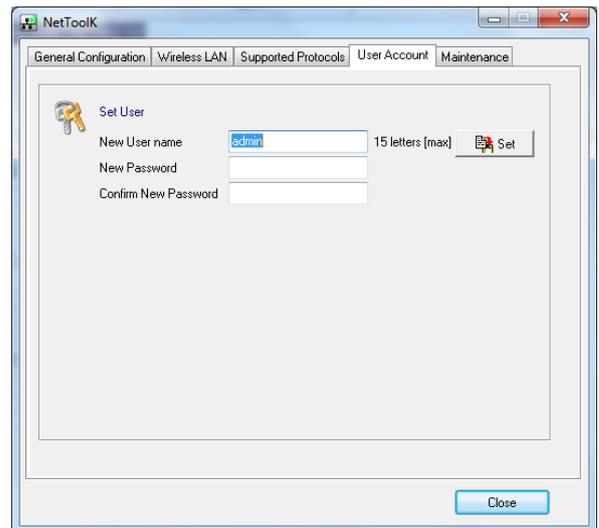
5-3-4. "User Account" Tab

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.)



5-3-5. "Maintenance" Tab

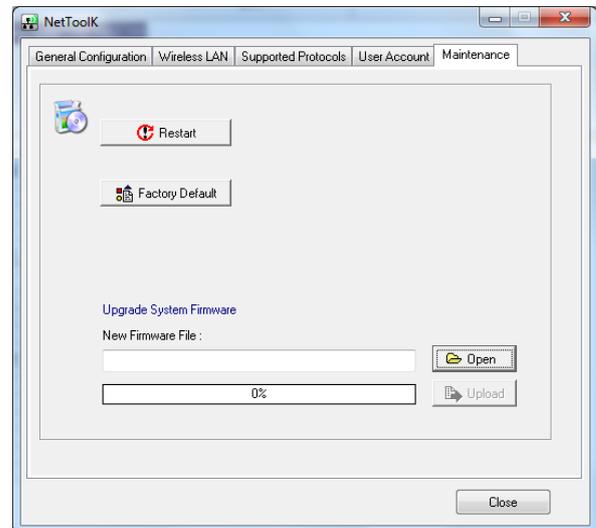
Use the "Maintenance" tab to restart the LAN interface board, return the settings to the factory default settings, and update the firmware.

Warning

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

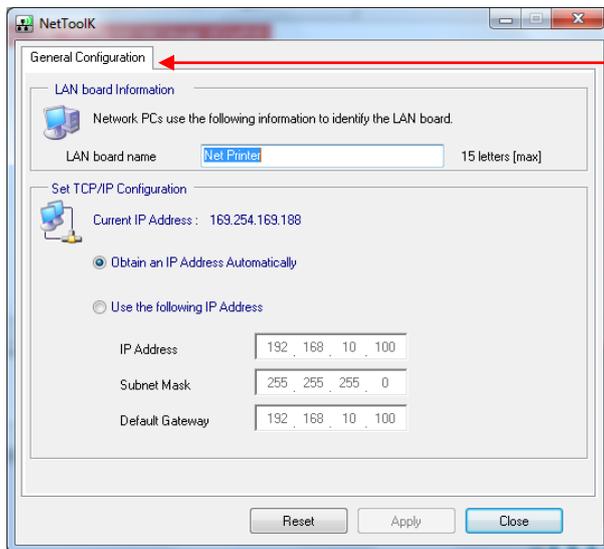
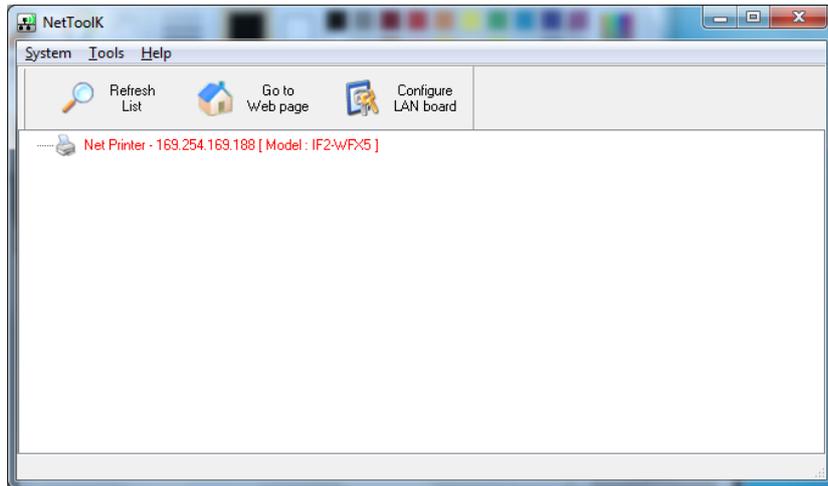
When updating the firmware, it is necessary to obtain the correct firmware data from us.

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



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

6. XML Print / Peripheral Device Control Function

6-1. Overview

The XML Print / Peripheral device control function are functions of this interface board to convert specific data in XML tag format to implement functions such as printing.

The peripheral device control function is a function to control a device connected to USB ports of the interface board by using data in XML tag format. (A method to control a peripheral device without using the XML function is also provided.)

See the separate documents for CITIZEN XML Print Service for details on data in XML tag format, JavaScript library to generate that data, etc.

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 the Service tab & SSL/TLS tab are 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 Device service | http://IP address:8085/ http://IP address/xmldevice/ |
| | XML Config service | http://IP address/xmlconfig/ |
| HTTPS | XML Print service | https://IP address/xmlprint/ |
| | XML Device service | https://IP address/xmldevice/ |
| | XML Config service | https://IP address/xmlconfig/ |

5 XML Print / Peripheral Device Control Function

6-2. CONFIG>>Service Tab

The setting items that are displayed differ depending on the type of interface board that is connected to the printer.

IFx-EFX2: All items

IFx-EFX1 / IFx-EFX3: XML Print, XML Config and XML Settings items only

The Media Converter items may be displayed even when the interface board is used in combination with a printer that does not meet the conditions.

| General | Wireless LAN | Service | SSL/TLS | Request Print | User Account | Maintenance |
|--|------------------------------------|--|---|---------------|--------------|-------------|
| Media Converter | | | | | | |
| VCOM Convert | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | <input type="checkbox"/> Show configuration | | | |
| HID Scanner Convert | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | <input type="checkbox"/> Show configuration | | | |
| XML Print | | | | | | |
| Port Number | <input type="text" value="8080"/> | | | | | |
| Timeout for connect | <input type="text" value="10"/> | 5-60[Seconds] | | | | |
| Timeout for print | <input type="text" value="60"/> | 10-600[Seconds] | | | | |
| XML Device Control | | | | | | |
| Port Number | <input type="text" value="8085"/> | | | | | |
| Timeout for connect | <input type="text" value="10"/> | 5-180[Seconds] | | | | |
| Max connection | <input type="text" value="2"/> | | | | | |
| XML Device Control / Line Display | | | | | | |
| Baud rate | <input type="text" value="9600"/> | | | | | |
| Data | <input type="text" value="8 bit"/> | | | | | |
| Parity | <input type="text" value="None"/> | | | | | |
| Stop | <input type="text" value="1 bit"/> | | | | | |
| Flow Control | <input type="text" value="Off"/> | | | | | |
| <input type="button" value="Test Device"/> | | | | | | |
| XML Device Control / Scanner | | | | | | |
| <input type="button" value="Test Device"/> | | | | | | |
| XML Device Control / Speaker | | | | | | |
| <input type="button" value="Test Device"/> | | | | | | |
| XML Config | | | | | | |
| Timeout for connect | <input type="text" value="10"/> | 5-180[Seconds] | | | | |
| XML Settings | | | | | | |
| HTTP Keep Alive | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable | | | | |
| HTTP Keep Alive Timeout | <input type="text" value="5"/> | 5-30[Seconds] | | | | |
| HTTP Keep Alive Max Requests | <input type="text" value="100"/> | 1-100 | | | | |
| <input type="button" value="Submit"/> <input type="button" value="Reset"/> | | | | | | |

6-2-1. Media Converter

| Item | Initial value | Configurable range | Description |
|---------------------|---------------|------------------------|---|
| VCOM Convert | Disable | Enable Disable | Set Enable when using a display or scanner using OPOS without XML control. |
| HID Scanner Convert | Disable | Enable Disable | Set Enable when using a scanner in HID mode without XML control. |
| Show Configuration | Unselected | Selected Unselected | If you select this, the advanced settings for communication with the device are displayed. The initial value of each item is the value for the corresponding device so there is no need to change it. |

6-2-2. XML Print

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

6-2-3. XML Device Control

Configure the following general settings for XML Device Control Service.

| Item | Initial value | Configurable range | Description |
|---------------------|---------------|--------------------|--|
| Port Number | 8085 | 1025 - 65535 | Connection port number |
| Timeout for connect | 10 | 5 - 180 | Timeout time to wait for control to start (sec.) |
| Max Connections | 2 | 1 - 3 | Maximum number of simultaneous connections (normally use with the initial value) |

6-2-4. XML Device Control / Line Display

Configure the following general settings for a display. The setting initial values are already the appropriate values for the corresponding display so do not change them in the case of normal use.

| Item | Initial value | Configurable range |
|--------------|---------------|---|
| Baud rate | 9600 | 2400, 4800, 9600, 19200, 38400, 57600, 115200 |
| Data | 8 bit | 7 bit, 8 bit |
| Parity | None | None, Odd, Even |
| Stop | 1 bit | 1 bit, 2 bit |
| Flow Control | Off | Hardware, Xon/Xoff, Off |

If you press the "Test Device" button, a text string is displayed on the display according to these settings. If a connection with the display cannot be confirmed, an alert message ("Test failed") is displayed in the browser.

6-2-5. XML Device Control / Scanner

If you press the "Test Device" button, the connection with the scanner (USB HID keyboard method) is checked. If a connection with the scanner cannot be confirmed, an alert message ("Test failed") is displayed in the browser.

6-2-6. XML Device Control / Speaker

If the "Test Device" button is pressed while a USB speaker is connected, the sound (chime) prerecorded in the interface board is played. If a connection with the USB speaker cannot be confirmed, an alert message ("Test failed") is displayed in the browser.

If you wish to use this function, submit an inquiry to us.

6-2-7. 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 for waiting for processing to start |

6-2-8. XML Settings (Displayed only for firmware version V2.45 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. |

6-2-9. 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.

5 XML Print / Peripheral Device Control Function

6-3. STATUS>>Service Status Tab

| System Status | Network Status | Printer Status | Service Status | Request Print |
|---------------------------|----------------|----------------|----------------|---------------|
| Media Converter | | | | |
| Service Version: | | | 1.0 | |
| VCOM #1 | | | | |
| Status: | | | Disabled | |
| Port Number: | | | 9200 | |
| Type: | | | | |
| VCOM #2 | | | | |
| Status: | | | Disabled | |
| Port Number: | | | 9201 | |
| Type: | | | | |
| HID Scanner | | | | |
| Status: | | | Disabled | |
| Port Number: | | | 9210 | |
| XML Print | | | | |
| Service Version: | | | 3.0 | |
| Port Number: | | | 8080 | |
| XML Device Control | | | | |
| Service Version: | | | 1.2 | |
| Port Number: | | | 8085 | |
| LineDisplay Status: | | | Offline | |
| Scanner Status: | | | Offline | |
| Speaker Status: | | | Offline | |
| XML Config | | | | |
| Service Version: | | | 1.0 | |

The settings on the Service tab, the connection state of the peripheral device, etc. are reflected here.

WebSocket URL is displayed only when Media Converter is enabled.

(Displayed only for firmware version V2.45 and later)

| System Status | Network Status | Wireless LAN Status | Printer Status | Service Status | Request Print |
|---------------------------|----------------|---------------------|----------------|----------------|---------------|
| Media Converter | | | | | |
| Service Version: | | | | 2.0 | |
| VCOM #1 | | | | | |
| Status: | | | | Offline | |
| Port Number: | | | | 9200 | |
| Type: | | | | VCOM | |
| WebSocket URL: | | | | Link | |
| VCOM #2 | | | | | |
| Status: | | | | Offline | |
| Port Number: | | | | 9201 | |
| Type: | | | | CDC | |
| WebSocket URL: | | | | Link | |
| HID Scanner | | | | | |
| Status: | | | | Offline | |
| Port Number: | | | | 9210 | |
| WebSocket URL: | | | | Link | |
| XML Print | | | | | |
| Service Version: | | | | 3.0 | |
| Port Number: | | | | 8080 | |
| XML Device Control | | | | | |
| Service Version: | | | | 1.2 | |
| Port Number: | | | | 8085 | |
| LineDisplay Status: | | | | Disabled | |
| Scanner Status: | | | | Disabled | |
| Speaker Status: | | | | Offline | |
| XML Config | | | | | |
| Service Version: | | | | 3.0 | |

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.

5 SSL/TLS function

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 signed by a public certification authority (CA) on the Internet and imported into the board.

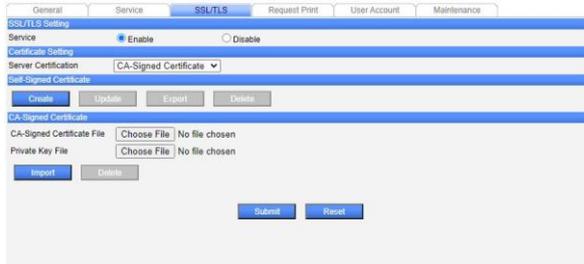
The descriptions in the following chapters correspond to certificate A, B, or C as follows.

| 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 V2.45 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

| Field | Value | Notes |
|----------------------------------|-----------------------|--------------|
| Common Name * | 192.168.1.100 | |
| Organization Unit | | |
| Organization * | CITIZEN SYSTEMS JAPAN | |
| Locate | | |
| State | | |
| Country * | JP | 2 characters |
| Validity (Not Before) * | 2020/04/01 | YYYYMMDD |
| Validity (Not After) * | 2021/04/01 | YYYYMMDD |
| Internal Certification Authority | | |
| Validity (Not Before) * | 2020/04/01 | YYYYMMDD |
| Validity (Not After) * | 2049/12/31 | YYYYMMDD |

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

- Issuer
 - Enter the information about the organization that operates the server (administrator).
- 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.

7-2-3. Update Self-Signed Certificate

Update Self-Signed Certificate

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

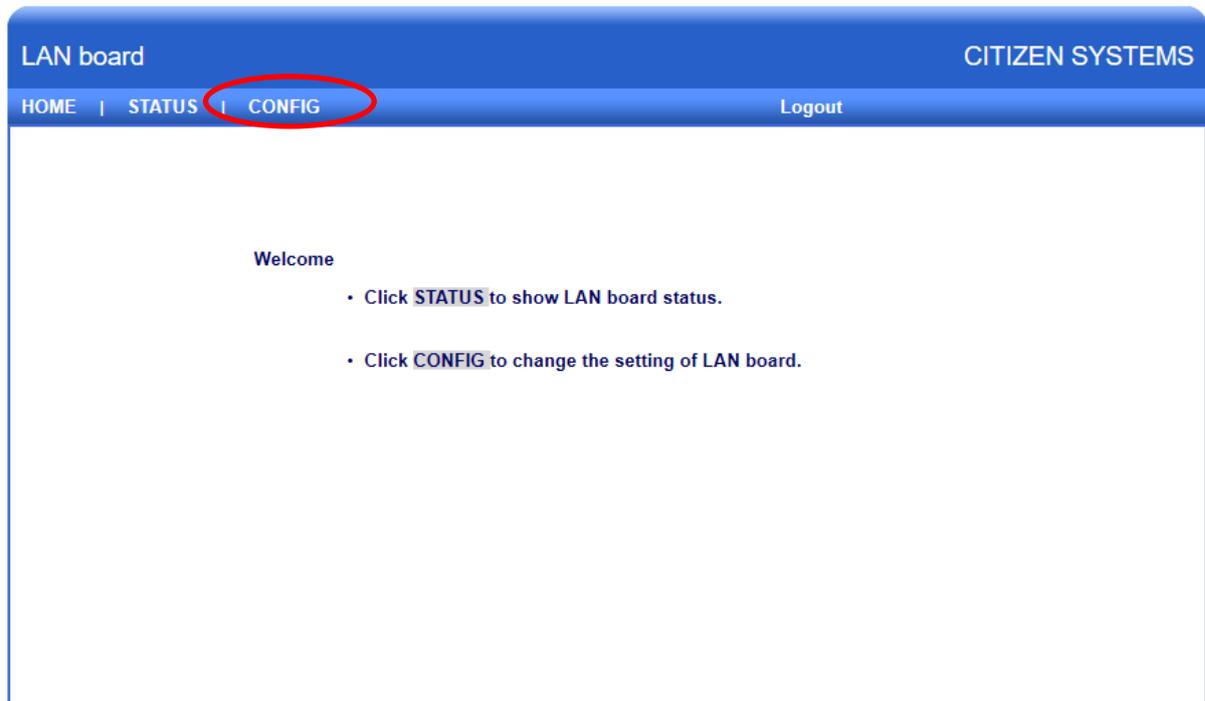
- Issuer
Enter the information about the organization that operates the server (administrator).
- Common Name
Enter the IP address or FQDN of the print server.
- Organization Unit
Enter the name of the department of the operating organization.
- Organization
Enter the name of the operating organization.
- 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.

5 SSL/TLS function

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

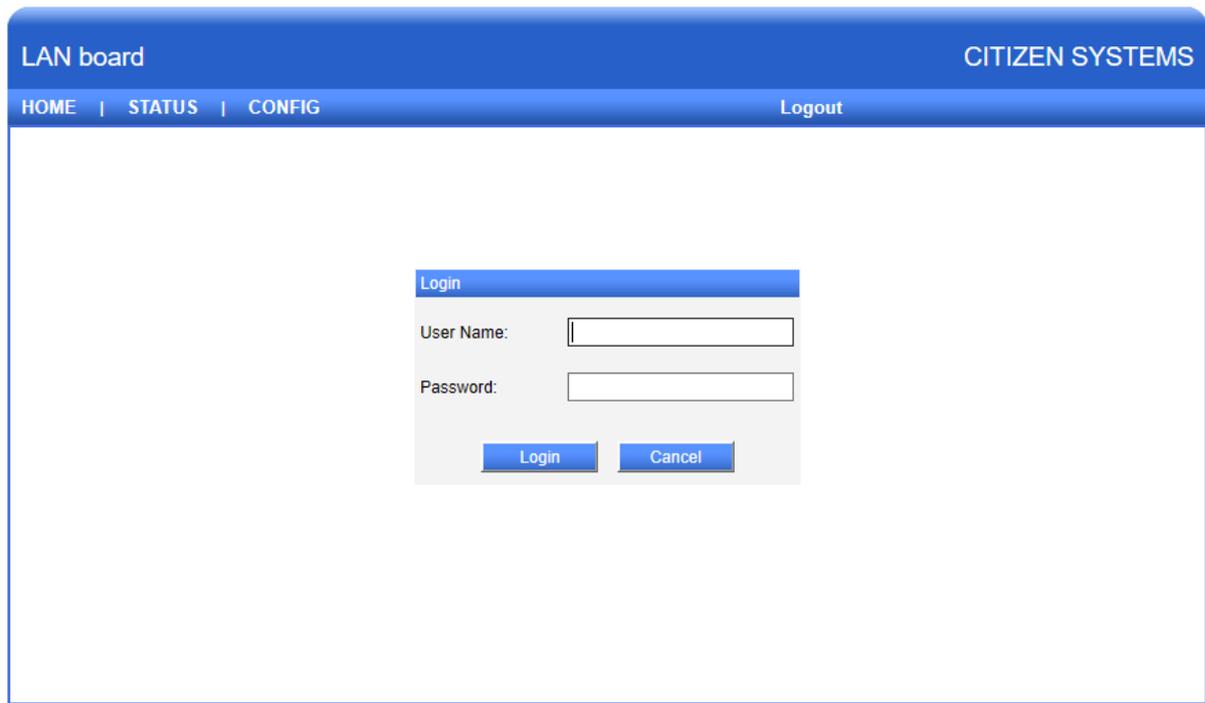
7-3-1. Generating and exporting self-signed certificates

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



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

(Default: admin / admin. From version 2.57 and later, it is necessary for you to set your own password.)



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

LAN board CITIZEN SYSTEMS

HOME | STATUS | CONFIG Logout

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

LAN board Information

LAN board name 15 letters[max.]

TCP/IP

Obtain an IP Address Automatically

Use the following IP Address

IP Address 15 letters[max.]

Subnet Mask 15 letters[max.]

Default Gateway 15 letters[max.]

UPnP Setting

UPnP Enable Disable

Print Settings

Raw Port Number

Timeout for print data 0-65535[Seconds]

Action at Timeout Close all connections Move to next connection

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.

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

CA-Signed Certificate

CA-Signed Certificate File 選択されていません

Private Key File 選択されていません

Note: Only unencrypted files are supported.

5 SSL/TLS function

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.

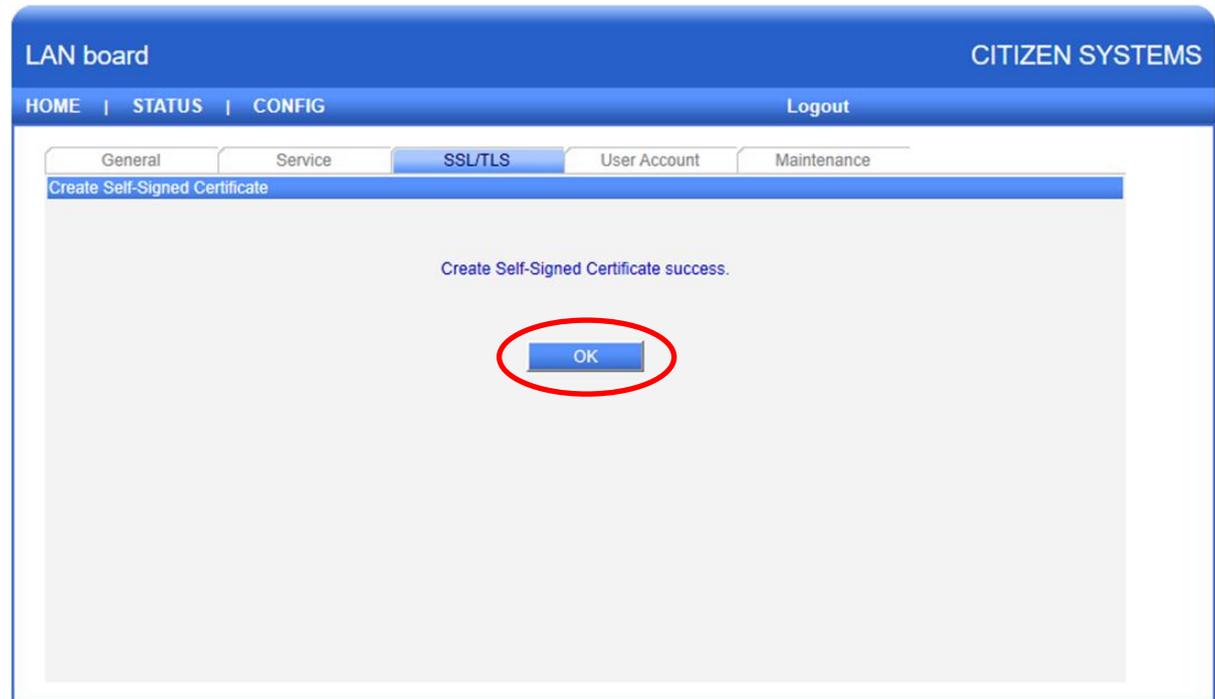
The screenshot shows the 'Create Self-Signed Certificate' form in the LAN board configuration interface. The form is titled 'Create Self-Signed Certificate' and is part of the 'SSL/TLS' configuration section. The form fields are as follows:

| Field | Value | Format/Requirement |
|----------------------------------|-----------------------|--------------------|
| 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

Buttons: Create, Cancel

9) Press the "OK" button.

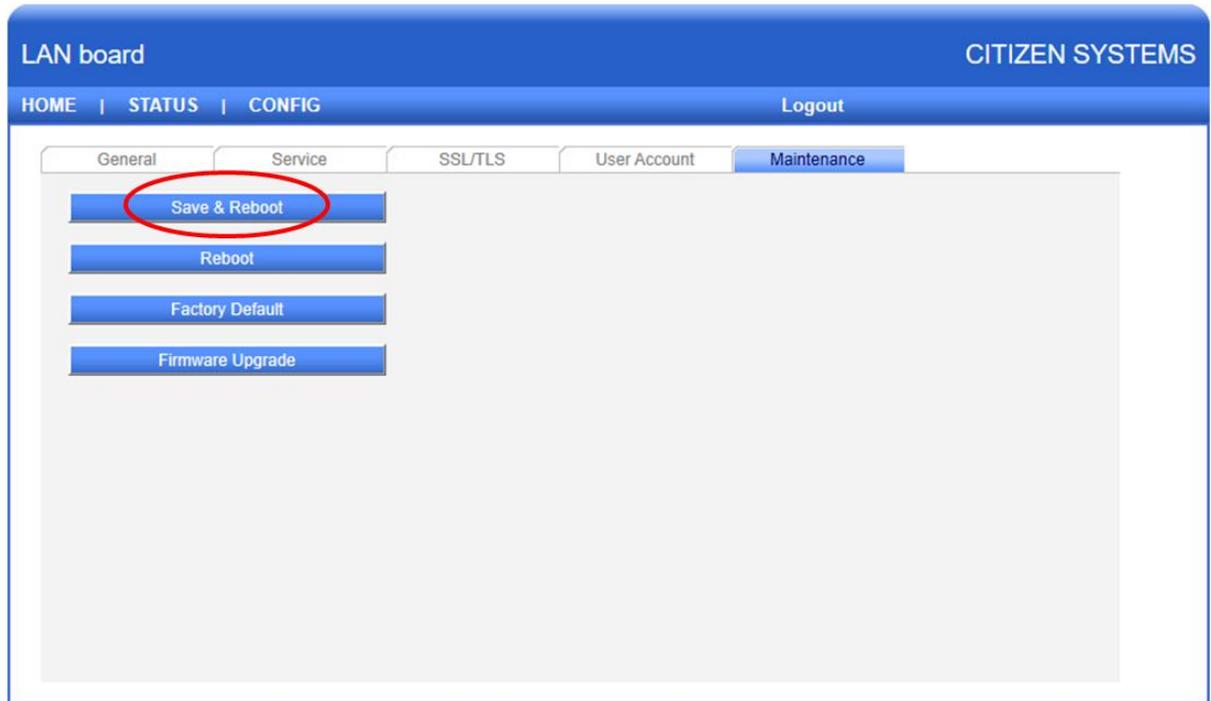


- 10) Select "Enable" for Service and CA-Signed Certificate for Server Certification in SSL/TLS Setting.
11) Click the "Export" button to save the self-certificate file. The file will be used for importing into your browser.
12) Press the "Submit" button.

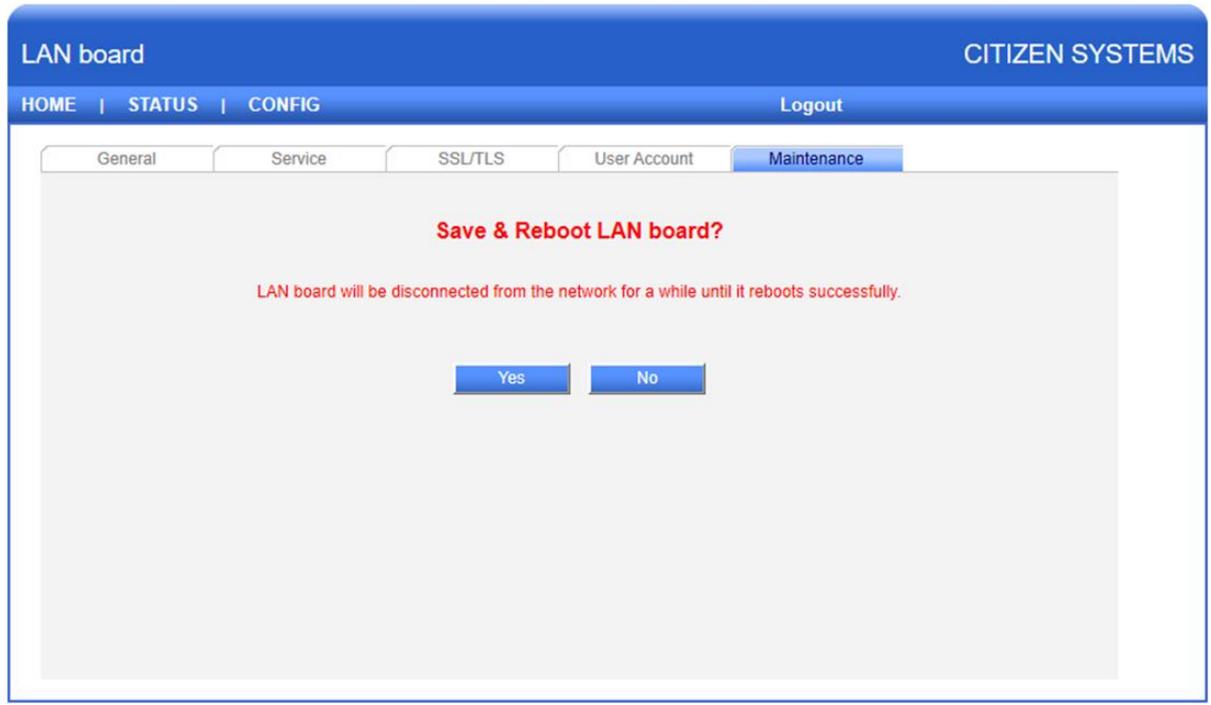


5 SSL/TLS function

13) Press "Save & Reboot".



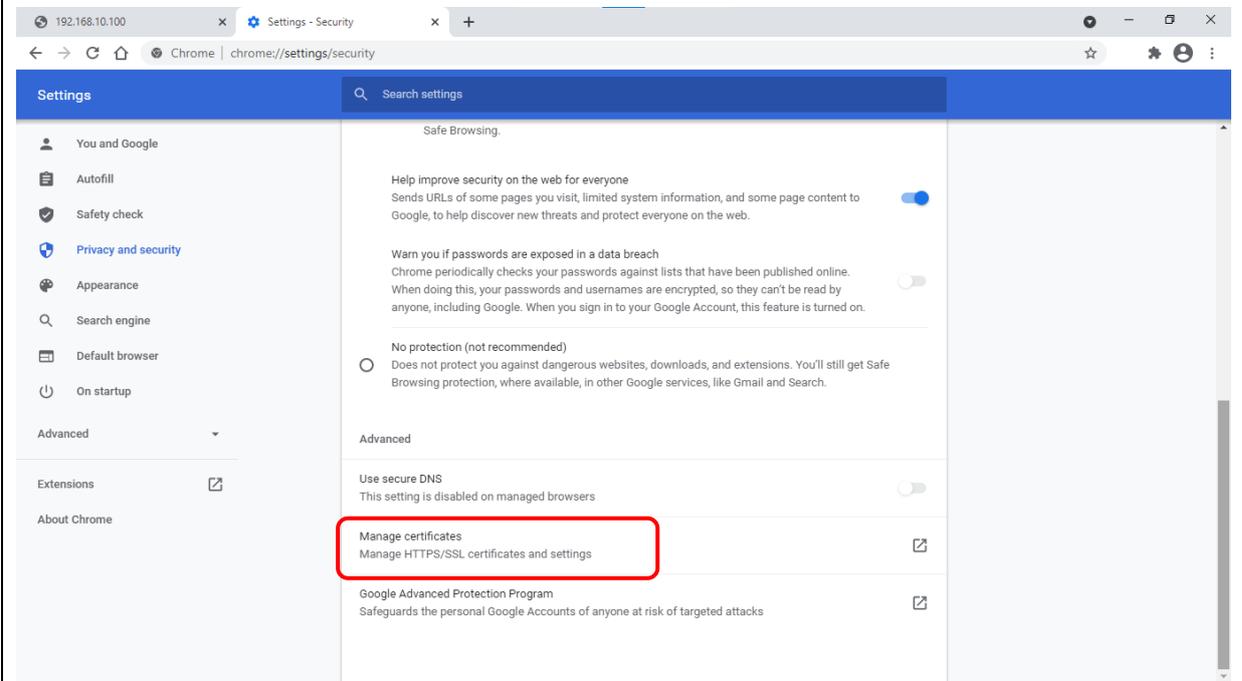
14) Click the "Yes" button to save & reboot.



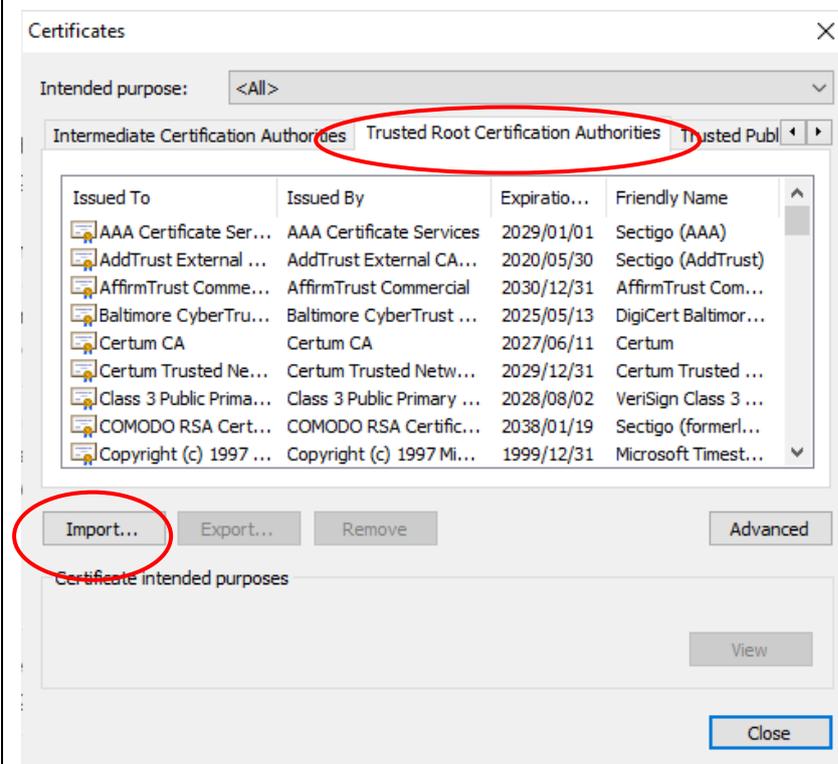
Please wait until the board reboots. The configuration changes will be reflected after the reboot.

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

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

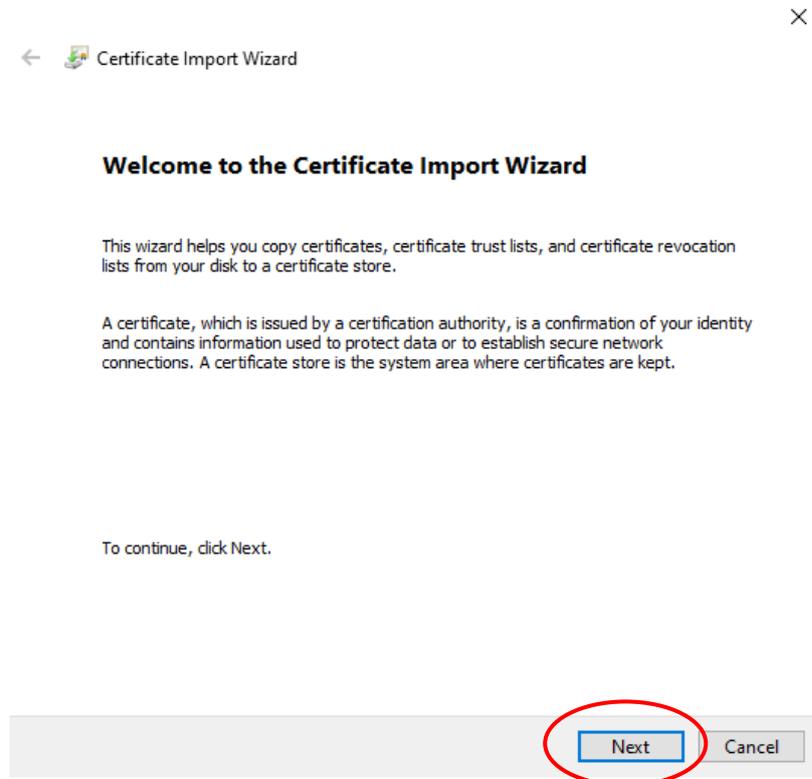


Select the "Trusted Root Certification Authorities" tab and click the "Import" button.

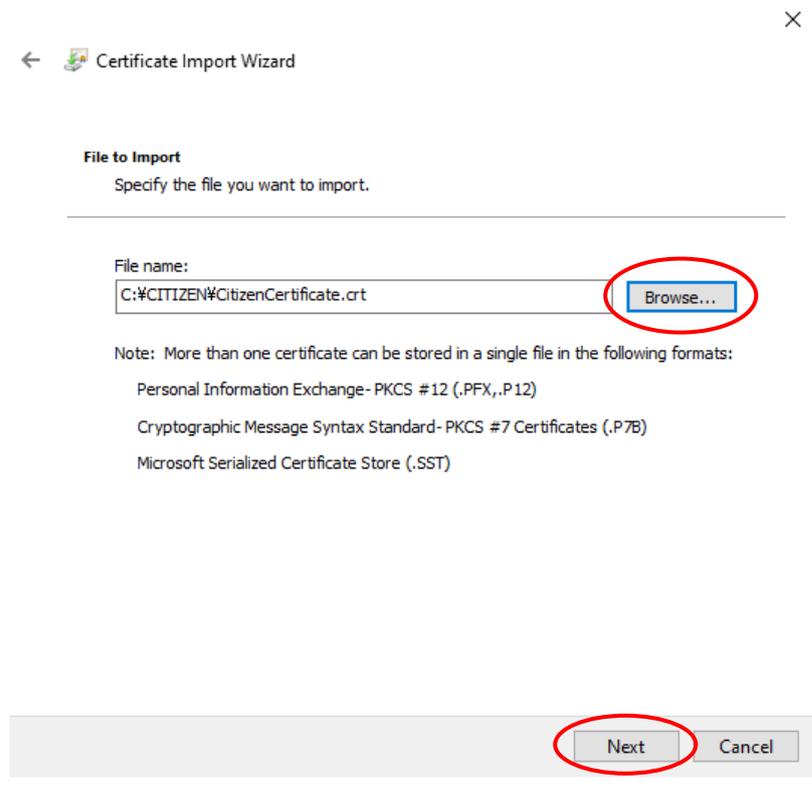


5 SSL/TLS function

Press "Next".



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



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

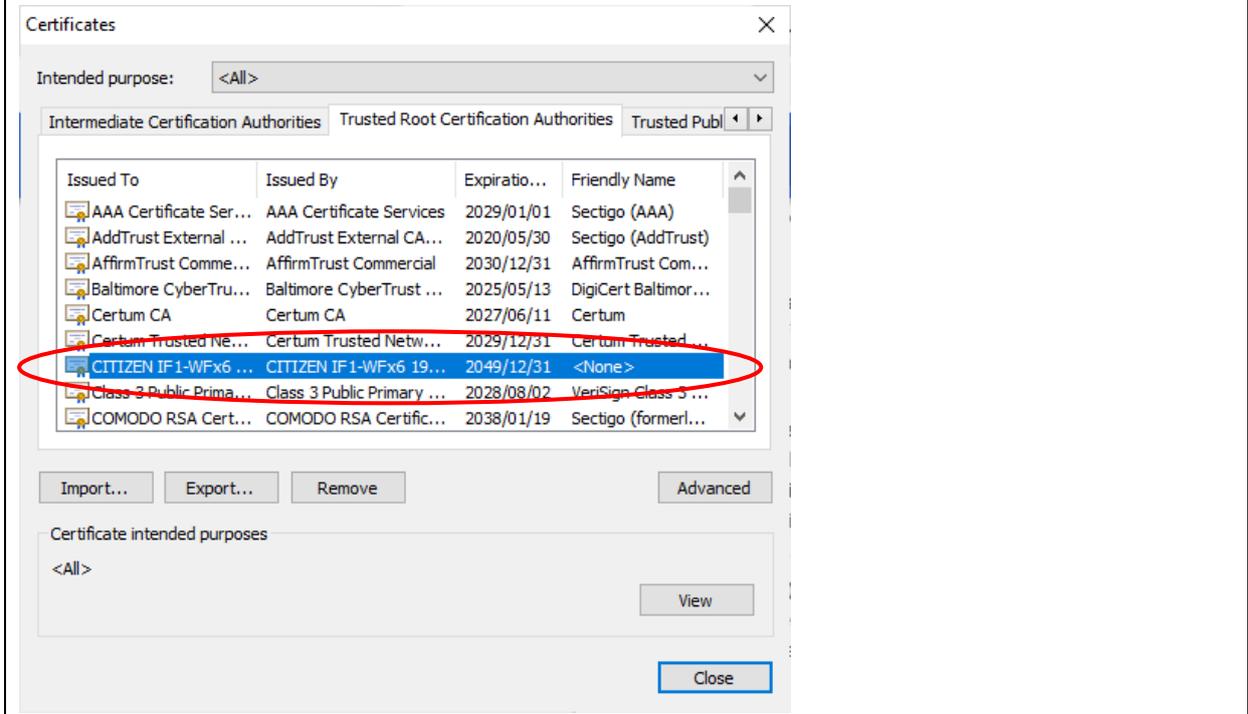
The certificate will be imported after you click Finish.

You have specified the following settings:

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

5 SSL/TLS function

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.

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 V2.45 and later.

Supported cipher suite

In the case of using TLS 1.3 (Supported only on firmware version V2.45 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 |

5 SSL/TLS function

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 V2.45 and later.

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 V2.45 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 | |

5 SSL/TLS function

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 V2.45 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 |

* Displayed only for firmware version V2.45 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.

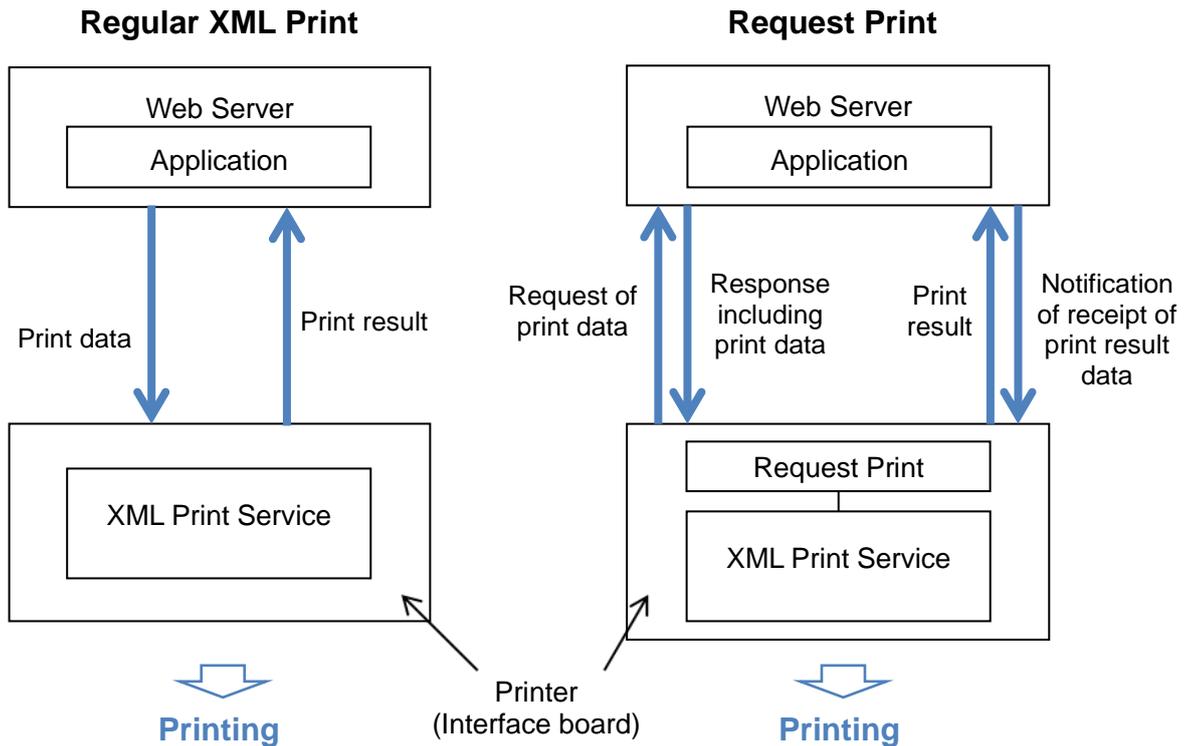
8. Request Print function

8-1. Overview

The request printing function is required to realize printing from the Web server to the printer.

The general procedure is as follows.

This board periodically sends to the Web server a print data request. On the other hand, the server needs to respond to the print data request when the request comes in, and if the print data exists on the server, server needs includes the print data in the response



This chapter describes the settings for request printing on this board side.

The request, response, and print data are in XML format. For details on the messages structure etc., please refer to the Request Print Programmer Manual prepared separately.

A sample kit that can be installed on a Web server for demonstration is also available, and the manual explains how to install it.

This function is available when the following conditions are met

- The printer must be a model that supports the XML function.

- IFx-EFX2 with firmware version 2.30 or higher is connected to the printer.

- The printer's firmware must support the connection to the IFx-EFX2.

When these conditions are met, the Request Print tab will appear on the STATUS window and the Request Print tab will appear on the CONFIG window in the Web Manager.

5 Request Print function

8-2. CONFIG>>Request Print Tab

| General | Service | SSL/TLS | Request Print | User Account | Maintenance |
|--|---|--|---------------|--------------|-------------|
| Request Print Settings | | | | | |
| Request Print | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | | | | |
| URL | <input type="text" value="http://example.com/test.php"/> | 2048 letters[max.] | | | |
| Via Proxy Server | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | | | | |
| Proxy Address | <input type="text" value="192.168.100.190"/> | 15 letters[max.] | | | |
| Proxy Port | <input type="text" value="8080"/> | 1025-65535 | | | |
| Interval | <input type="text" value="10"/> | 1-600[Seconds] | | | |
| ID | <input type="text" value="00-11-E5-07-4A-6A"/> | 64 letters[max.] | | | |
| DNS | | | | | |
| DNS1 | <input type="text" value="8.8.8.8"/> | 15 letters[max.] | | | |
| DNS2 | <input type="text" value="8.8.4.4"/> | 15 letters[max.] | | | |
| Basic Authorization Settings | | | | | |
| Basic Authorization | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | | | | |
| User | <input type="text" value="admin"/> | | | | |
| Password | <input type="password" value="****"/> | | | | |
| Warning print for failed Requests | | | | | |
| Number of allowed failure before warning | <input type="text" value="0"/> | 0-100(Set 0 to disable this function.) | | | |
| Beep for warning | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | | | | |
| <input type="button" value="Submit"/> <input type="button" value="Reset"/> | | | | | |

Request Print Settings

- Request Print (Default: Disable)
Set whether to enable the request printing function.
- URL
Enter the server URL of the request.
- Via Proxy Server (Default: Disable)
Enables or disables the proxy setting.
- Proxy Address
Enter the IP address of the proxy server.
- Proxy Port
Enter the port of the proxy server.
- Interval
Enter the interval at which you want to make requests to the server.
- ID (Default: Mac address of this interface board)
Enter the individual identification code to be sent upon request.
- DNS
Enter IP addresses of "preferred DNS" and "alternate DNS" to be used when making requests.

Basic Authorization Settings

If the server to which printer is communicating requires Basic authentication, it can pass the authentication and communicate with the server by this function.

- Basic Authorization (Default: Disable)
Sets whether to send Basic authentication credentials to the request destination server.
- User
Enter the user name to be used for basic authentication.

- Password
Enter the password to be used for Basic Authentication.

Warning print for failed Requests

If communication with the server for the request print fails, this board can notify you of it by printing or beeping.

- Number of allowed failure before warning (Default: 0)
Enter the number of consecutive failures before an alarm printout is executed.
If 0 is entered, the alarm printing function is disabled.
- Beep for warning (Default: Disable)
Sets whether to enable the buzzer function for alarm printing.

8-3. STATUS>>Request Print Tab

| System Status | Network Status | Printer Status | Service Status | Request Print |
|---|-----------------------------|----------------|----------------|---------------|
| Request Print Settings | | | | |
| Service Version: | 1.0 | | | |
| Status: | Disable | | | |
| URL: | http://example.com/test.php | | | |
| Proxy | | | | |
| Proxy Address: | | | | |
| Proxy Port: | | | | |
| Interval: | 10 sec | | | |
| ID: | 00-11-E5-07-4A-6A | | | |
| DNS | | | | |
| DNS1: | 8.8.8.8 | | | |
| DNS2: | 8.8.4.4 | | | |
| Basic Authorization Settings | | | | |
| Status: | Disable | | | |
| User: | admin | | | |
| Warning print for failed Requests | | | | |
| Number of allowed failure before warning: | 0 | | | |
| Beep for warning: | Disable | | | |

The settings on the Request Print tab and the connection status of peripheral devices are shown here.

8-4. Printing system log

If Request Print did not work as expected, you may be able to check the situation by checking the system log of this board.

Please refer to Chapter 5 "Useful Functions for Request Print" in the "Programmer's Manual for "Request Print" for a description of system log printing.