

# LP-2648 Website User Manual

English

Ver. 1.0, Apr. 2025



## **WARRANTY**

All products manufactured by ICP DAS are warranted against defective materials for a period of one year from the date of delivery to the original purchaser.

## **WARNING**

ICP DAS assumes no liability for damages consequent to the use of this product. ICP DAS reserves the right to change this manual at any time without notice. The information furnished by ICP DAS is believed to be accurate and reliable. However, no responsibility is assumed by ICP DAS for its use, nor for any infringements of patents or other rights of third parties resulting from its use.

## **COPYRIGHT**

Copyright © 2025 by ICP DAS. All rights are reserved.

## **TRADEMARK**

Names are used for identification only and may be registered trademarks of their respective companies.

## **CONTACT US**

If you have any questions, please feel free to contact us via email at:

**[service@icpdas.com](mailto:service@icpdas.com), [service.icpdas@gmail.com](mailto:service.icpdas@gmail.com)**



# Revision History

Revision	Date	Description	Note
1.0	2025/04	<ul style="list-style-type: none"><li>Initial issue</li></ul>	

# Table of Contents

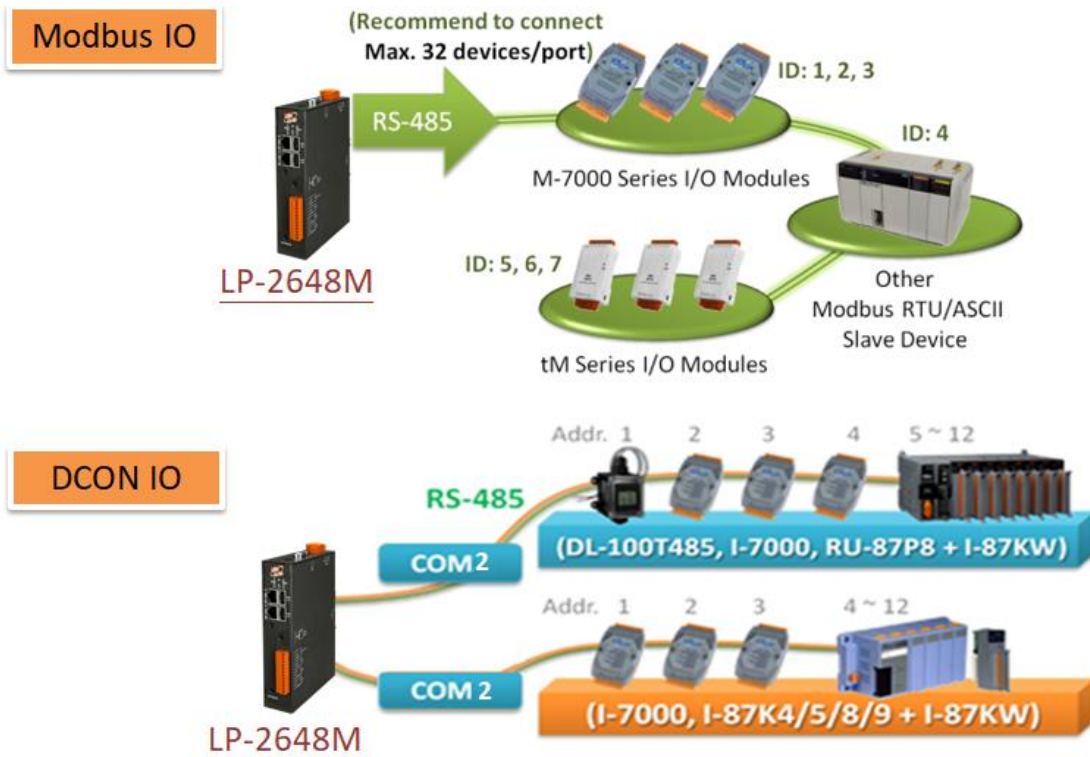
1. Introduction.....	4
2. Getting Started .....	5
2.1. Login into the webpage .....	5
2.2. Web Interface Introduction .....	7
3. System General.....	12
3.1. Date & Time .....	12
3.2. Network .....	13
3.3. Maintenance .....	15
4. System Log.....	17
4.1. Log .....	17
5. PLC.....	20
5.1. Runtime .....	20
5.2. Redundant.....	20
6. OPC UA .....	22
6.1. Server Certificate.....	22
7. Account Settings .....	28
Appendix A. eSearch Tool Software .....	30

# 1. Introduction

LP-2648M is the new generation of Win-GRAF programmable automation controller (PAC) from ICP DAS. It adopts Cortex-A53 quad-core processor (1.4GHz) to run linux kernel operating system to provide high performance and real-time control.

Win-GRAF programmable automation controllers running the Linux operating system offer the advantages of real-time functionality, high-performance precision control, and a PC-like operating environment for the PAC. In addition to supporting Win-GRAF (IEC61131-3 standard) software for developing control programs, the PAC also supports C or C++ for developing data management applications, and can exchange data with Win-GRAF applications to make application design more convenient and practical.

The LP-2648M is integrated with a web server, which allows users to connect to the web server via Ethernet network using a web browser to configure the controller functions such as network, system time, Win-GRAF runtime, OPC UA certificate management, etc. The LP-2648M is used for the following purposes in this manual. Each function is described in detail on each page of this manual.



## 2. Getting Started

### 2.1. Login into the webpage

Please complete the network settings of the PC before entering the webpage. The factory default settings of the hardware LAN network are as follows:

Factory Default		
Network Setting	IP (LAN1)	192.168.255.1
	Netmask	255.255.255.0

1. Change the network settings of the PC to the same network segment as the hardware, for example:

Network Setting	IP (LAN1)	192.168.255.10
	Netmask	255.255.255.0

2. Make sure the hardware and PC are properly connected to the network. Start the browser and type "http://192.168.255.1" in the address bar to enter the login page.
3. Enter the account and password on the login page, and click the "Login" button to log in.
  - Default account: admin
  - Default password: admin



Username

Password

Login

- When using the default account and password to log in for the first time, the system will require the user to change the password. Please log in again after changing the password.



You must change your password before logging on the first time.

Username

Old password

New password

Confirm new password

- After logging into the webpage, change the hardware network settings according to the actual network environment. For detailed network setting, please refer to the section Network.
- Users can also modify the network settings through the eSearch Utility software. For details, please refer to Appendix A. eSearch Tool Software.

## 2.2. Web Interface Introduction

As shown in Figure 2-1, the web interface consists of the following parts:

1. Toolbar
2. Navigation area
3. Workspace

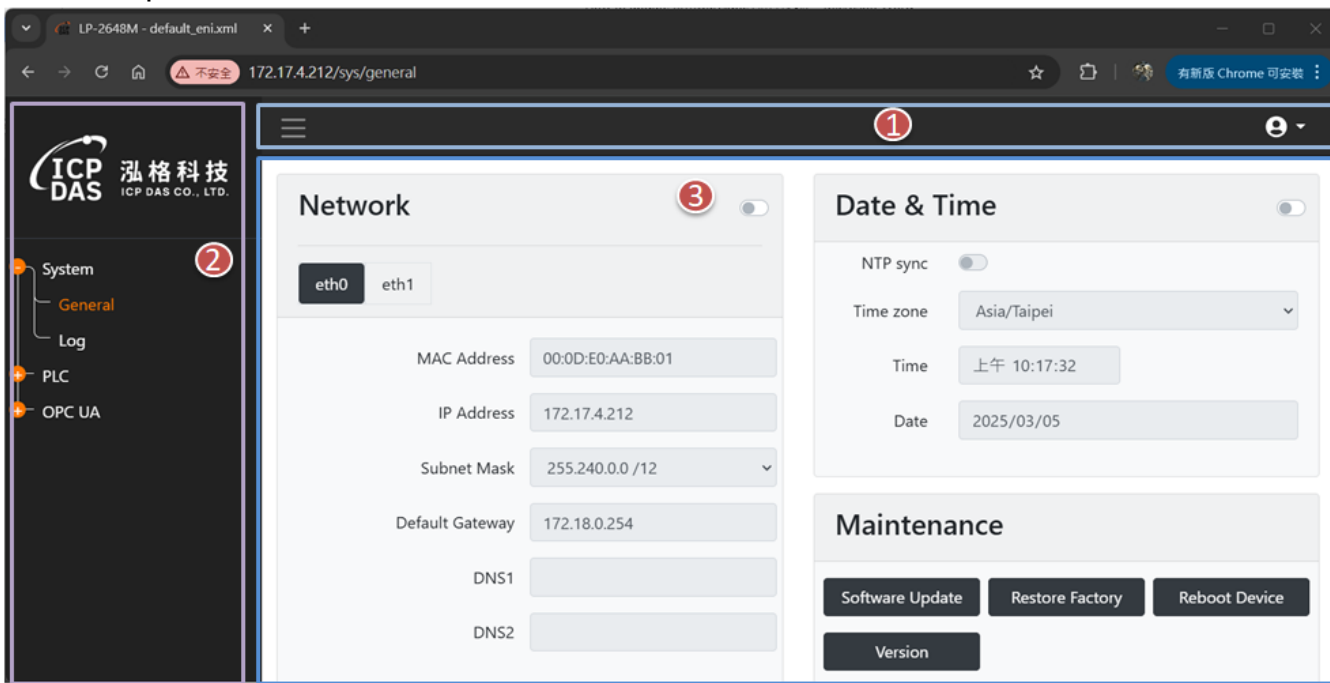


Figure 2-1






## 2.2.1. Toolbar

The toolbar (shown as Figure 2-2) is always displayed at the top of the web interface.



Figure 2-2

The toolbar has the following controls:

-  - Show/Hide "Navigation area" button.
-  - Account drop down menu.
  -  admin - Login account name.
  -  Password - To change the password, please refer to the section: Account Settings for detailed information.
  -  Logout - Log out of account.

## 2.2.2. Navigation Area

The Navigation Area is shown in Figure 2-3, which is located on the left side of the web interface. You can use the toolbar "Show/Hide Navigation Area Button" to display and hide it. The default is the display state. The main purpose of the Navigation Area is to switch the workspace to different work pages.

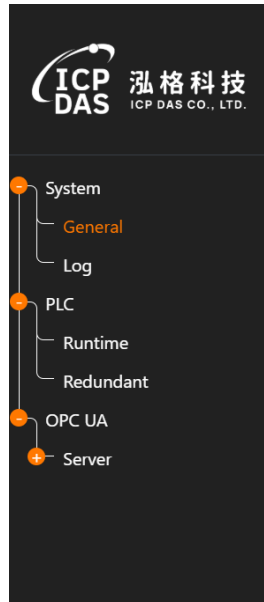


Figure 2-3

The following work pages are accessible:

- System->General  
The user can set system parameters such as: network settings, date & time, software updates, etc. on this page. Please refer to section System General for detailed information.
- System->Log  
It can display various log information. Please refer to section System Log for detailed information.
- PLC->Runtime  
This page can perform operations of runtime (start, stop). Please refer to section PLC Runtime for detailed information.
- PLC->Redundant  
This page shows the LAN1 network settings for PLC Redundant. Please refer to section PLC Redundant for detailed information.

- **OPC UA**  
This page manages the server's certificate files to ensure secure communication.  
See the OPC UA section for more information.

### 2.2.3. Workspace

The workspace is located at the right side of the web interface; it will display the work page the user selected from the Navigation area. The content of the work page is composed of multiple card content container as shown in Figure 2-4, each card represents a function, and these functions can be status, parameter setting or operations of functions.

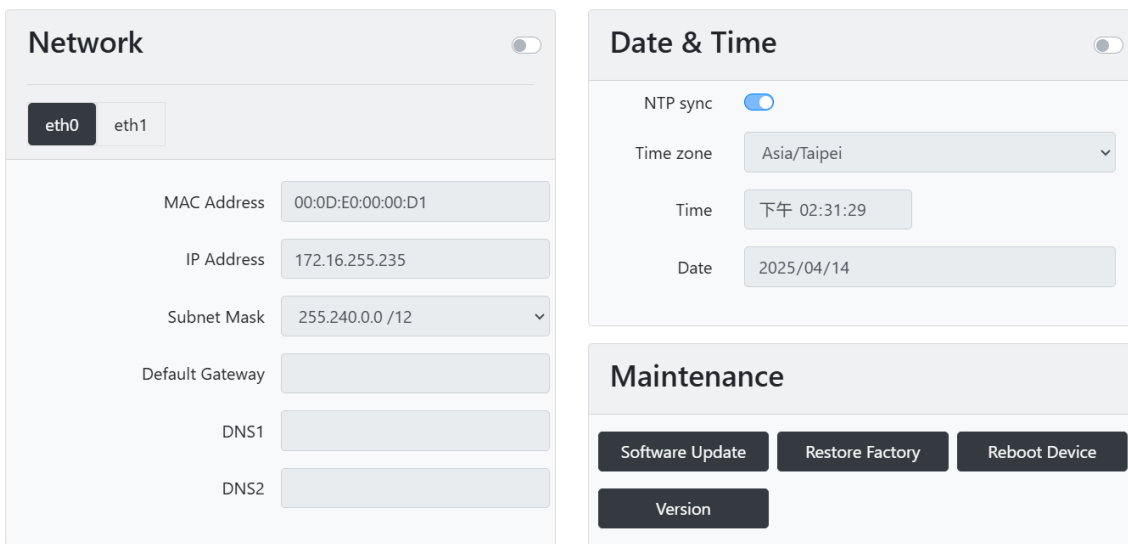


Figure 2-4

### 3. System General




The system general page is for parameter settings such as host name, network setting, date & time, software update, etc. The following are the functions.

#### 3.1. Date & Time

The date and time settings of the controller are shown in Figure 3-1. The parameters and function buttons are as follows:



Figure 3-1

-  The switch on the right side of the title is used to enable or disable the date and time setting function. When it is disabled, it will only display the current date and time. If it is enabled, a  write button will appear.
- NTP sync  
Enable or disable NTP synchronization. The NTP network time protocol will synchronize the system time of the controller to the system time on the network.
- Time zone  
Time zone.
- Time  
Time. Can only be set when NTP sync is disabled.
- Date  
Date. Can only be set when NTP sync is disabled.
-  Write new Settings to the controller, which only appears if the settings function is enabled.

## 3.2. Network

The network settings of the controller are shown in Figure 3-2, and the descriptions of the parameters and function buttons are as follows:

Network

eth1

MAC Address 00:0D:E0:28:48:01

IP Address 192.168.2.81



Subnet Mask 255.255.255.0 /24


Default Gateway 192.168.2.1

DNS1 1.1.1.1

DNS2 8.8.8.8

Figure 3-2

-  The switch is used to enable or disable the network settings. When it is disabled, it will only display the current network interface and network configuration. If it is enabled, a  write button will appear.
- MAC Address  
MAC address.
- IP Address  
IP Address.
- Subnet Mask  
Subnet mask.
- Default Gateway  
Default gateway.
- DNS1  
DNS server 1.

- DNS2  
DNS server 2.
- Connection Type  
Connection Type will only appear when the setting is enabled.  
  
Static IP: Static IP address.  
  
DHCP: Request an IP address by using DHCP.
-  Write new Settings to the controller, which only appears if the settings function is enabled.

### 3.3. Maintenance

The maintenance function of the controller is shown in Figure 3-3, which can be used to update the software, display the software version, etc. The function buttons are as follows:

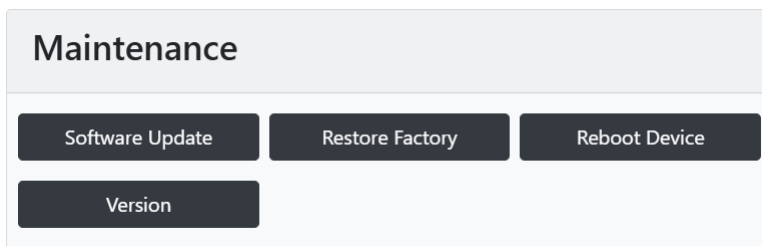
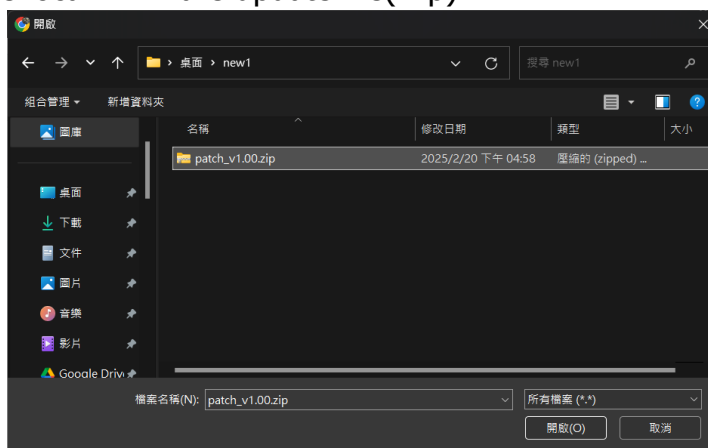


Figure 3-3

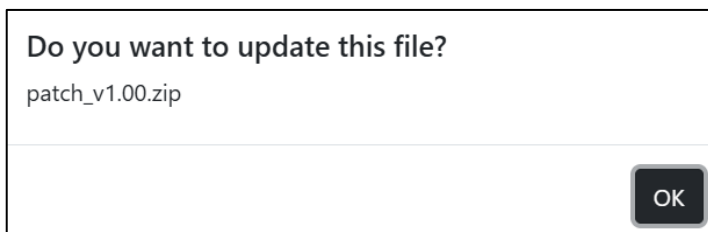
- Software Update

The software update button is used to update the relevant software inside the system. The update steps are as follows:

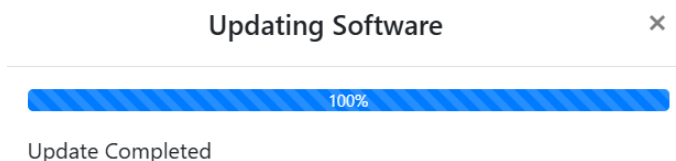
1. After clicking the "Software Update" button, the open file dialog box will appear, select the local firmware update file(.zip).



2. Then a file confirmation dialog box will appear. Click "OK" button to confirm the update.



3. Start the software update process, wait until the progress bar reaches 100% without any error, it means the software update is successful.



- Restore Factory  
When pressed, requires the controller to be rebooted for the settings to take effect.
- Reboot Device  
Reboot controller.
- Version  
Show software version information. The following version information dialog box will appear after clicking this button.

Version			
Name	Version	Architecture	Description
OS Version	OS Version 4.14.78 #30 SMP PREEMPT Mon Apr 14 13:04:22 CST 2025 release		
Application Version	1.00 B1		License: OK
WinGRAF Version	WG14.0 v1.00 B01 20250410		Project: emp_t1, Extra_port: null, Elapsed time : 0. 2:20:35

## 4. System Log

This working page can be used to view the status of the controller service program and view the related logs of the controller. The functions are as follow.

### 4.1. Log

The controller log function is shown in Figure 4-1, which records the errors, warnings and other prompt messages generated by the internal program of the controller. These messages allow developers to understand the operation status of the program and the cause of the error.

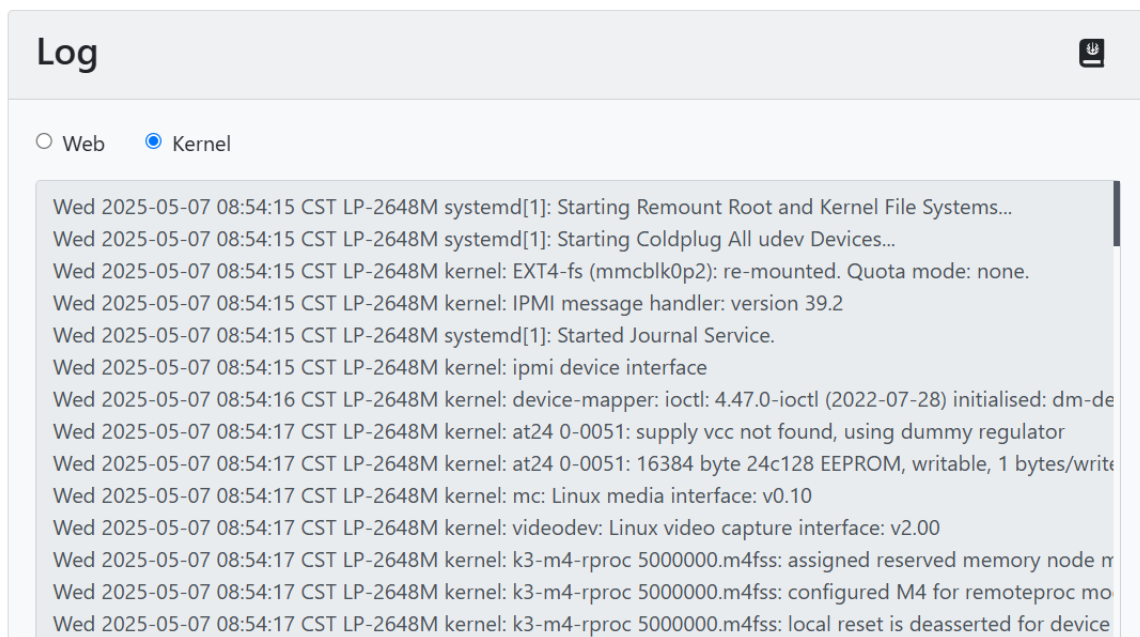


Figure 4-1

The types of logs to be displayed are as follows:

- Web  
Logs of web interface.
- Kernel  
Logs of controller kernel.



The button is used to access the content of the selected log. After clicking the button, the following Log Filter dialog box will appear, and the records within the range of the log time will be filtered according to the filter items.

Filter items are as below:

- Today  
Filter logs within today.
- Yesterday  
Filter logs within yesterday.
- All  
All logs.
- Since - Until  
Filter logs within the specified time range.

The display restriction items are as follows:

- lines  
Limit the number of lines displayed in the log. By default, no matter what filter item is selected, the maximum number of displayed lines is 200 lines. The parameter can be set to limit the number of lines to less than 200 lines.

- **First**  
Based on the filter range, the logs that are order in time will be displayed.
- **Last**  
Based on the filter range, the logs that are later in time will be displayed.

## 5. PLC

This page is mainly used to set up and control the PLC runtime, and each function is described below.

### 5.1. Runtime

As shown in Figure 5-1, this section allows the user to control the Win-GRAF Runtime to start or stop.

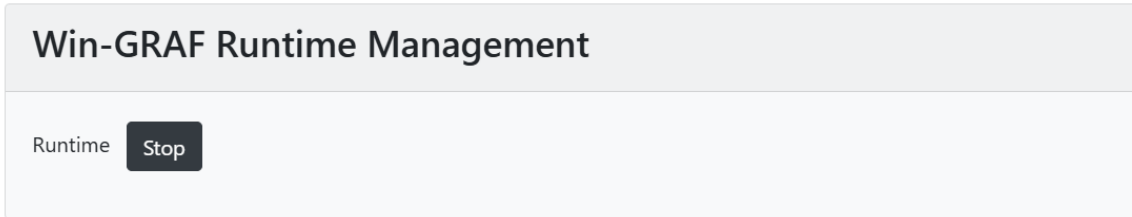


Figure 5-1

- Start: It is currently stopped; you can press this button to enable Win-GRAF Runtime.
- Stop: It is currently enabled; you can press this button to stop the Win-GRAF Runtime.

### 5.2. Redundant

As shown in Figure 5-2, it is mainly used to configure the IP, mask and gateway settings of LAN1 when the controller is in redundant mode.

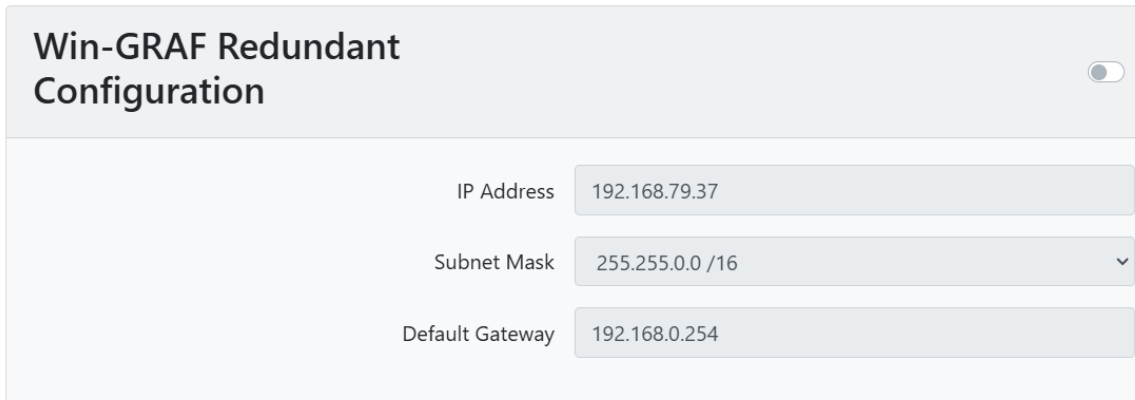




Figure 5-2



The switch is used to enable or disable the network settings. When it is disabled, it will only display the current network interface and network configuration. If it is

enabled, a  write button will appear.

- IP Address  
IP Address.
- Subnet Mask  
Subnet mask.
- Default Gateway  
Default gateway.
-   
Write new Settings to the controller, which only appears if the settings function is enabled.

## 6. OPC UA

OPC UA (Open Platform Communications Unified Architecture) is an open standard communication protocol designed for facilitating data exchange and communication between different devices and systems. Its primary goal is to provide interoperability across platforms, networks, and vendors while ensuring high scalability and security.

### 6.1. Server Certificate

The contents of this page are used to manage the certificate files of the Win-GRAF Runtime OPC UA Server to ensure the security of communications. The following is a detailed description of the contents of each tab:

- Own

This tab displays existing server certificates and allows the creation of new self-signed certificates. Detailed information about server certificates can be accessed through the General/Subject/SAN tabs. The following details are explained:

- General: General information.



General	
Issuer	Thumbprint
UaServer:EMP-OPCUA	7832CFF1D5512CE8815C1A440524F55522F0DA13
Valid From	Valid To
Mon Jan 08 2024 13:06:25 GMT+0800 (台北標準時間)	Tue Jan 07 2025 13:06:25 GMT+0800 (台北標準時間)

- Issuer: Issuer name.
- Thumbprint: This is commonly called a “fingerprint”.
- Valid From: Start date of certificate.
- Valid To: Expiry date of a certificate.

- **Subject:** Subject field.

The screenshot shows a configuration window with three tabs: 'General', 'Subject', and 'SAN'. The 'Subject' tab is selected. The interface contains several input fields for certificate information:

Common Name	Organization
UaServer:EMP-OPCUA	Organization
Organization Unit	Locality
Unit	
State	Country

- **SAN:** Subject Alternative Name.

The screenshot shows a configuration window with three tabs: 'General', 'Subject', and 'SAN'. The 'SAN' tab is selected. The interface contains input fields for Subject Alternative Names:

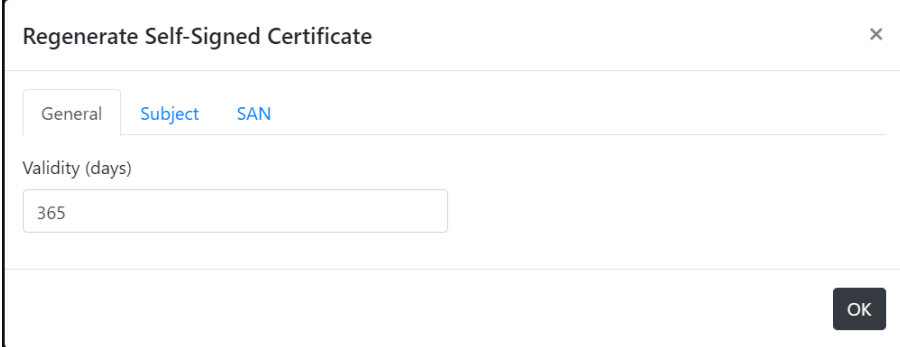
URI	
urn:Company:Product:UA_Serverurn:Company:Product:UA_Server2	
DNS	IP
EMP-OPCUA,EMP-OPCUA2	192.168.2.82,192.168.2.83

- **URI:** Uniform Resource Identifier.
- **DNS:** Domain Name System. Use commas to separate multiple entries.
- **IP:** IP Address. Use commas to separate multiple entries.

Buttons on the right:



Create Self-Signed Certificate. After clicking the button, the following dialog box will appear, and each parameter is described as follows:




- General: General Settings.
  - Validity (days): Certificate validity period, unit days.
- Subject: Please refer to the Subject SubjectSubjectdescription in the Own server certificate information.
- SAN: Please refer to the SAN SubjectSubjectdescription in the Own server certificate information.



Download the server certificate.



Upload the server certificate. After clicking the button, the following dialog box appears, select public key or private key to upload server certificate.



Delete the server certificate.

- Trusted

Used to manage server trust and rejected certificates. You can also trust or reject specific certificates.

Own	Trusted	Issuers
<b>Certificates</b>		
MyCA2 [4310F510486C708D57B01F8323939C5690CFA787].der		
UaExpert@DESKTOP-Q36M1JG [76EF881F3033B2C1DD33600913225EDCDDC8F8D5].der		
<b>Rejected</b>		
UaExpert@DESKTOP-FSVMGHH [785DD568D4A6C30EF14AB5365CAE80B83CD1CA64].der		
<b>Certificate Revocation Lists</b>		
MyCA2 [4310F510486C708D57B01F8323939C5690CFA787].crl		

- **Certificates:** List of trusted certificates.
- **Rejected:** List of rejected certificates.
- **Certificate Revocation Lists:** Certificate Revocation Lists of trusted certificates.

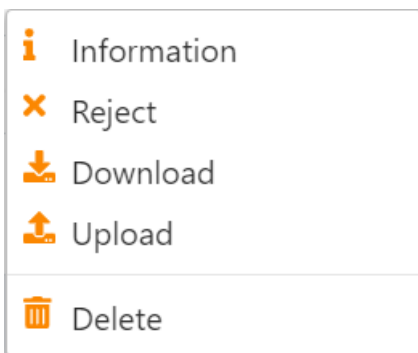
- Issuers

Manage issuer certificates. An issuer certificate is used to verify the legality and authenticity of other certificates. It establishes a trust chain to ensure that it comes from a trusted source.

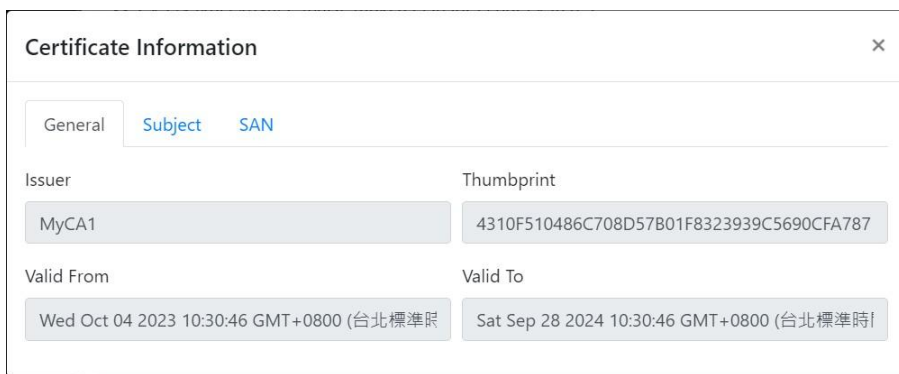
Own	Trusted	Issuers
<b>Certificates</b>		
RootCA [D1FE74C48BABAFAF0DB26B2CB2CBD85C7ACC234D2C].der		
MyCA1 [DE551C4BA4C24FED4288B7754F34A4BCE2361A7A].der		
<b>Certificate Revocation Lists</b>		
MyCA1 [DE551C4BA4C24FED4288B7754F34A4BCE2361A7A].crl		

- **Certificates:** List of issuer certificates.
- **Certificate Revocation Lists:** Certificate Revocation Lists of issuer certificates.

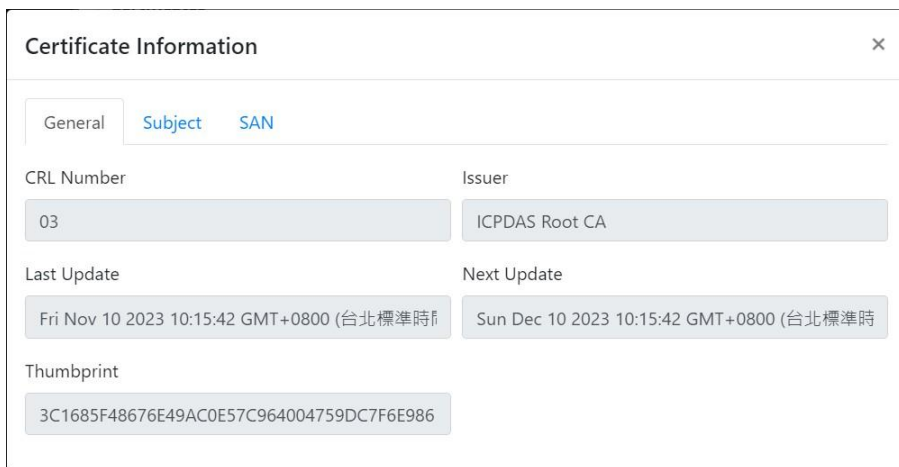
The right-click menu of the Certificates/Rejected/Certificate Revocation Lists file list is as follows:



- Information: Display detailed information for certificates or certificate revocation lists. The instructions are as follows:
  - Certificate Information
    - Please refer to the description of the Own server certificate information.



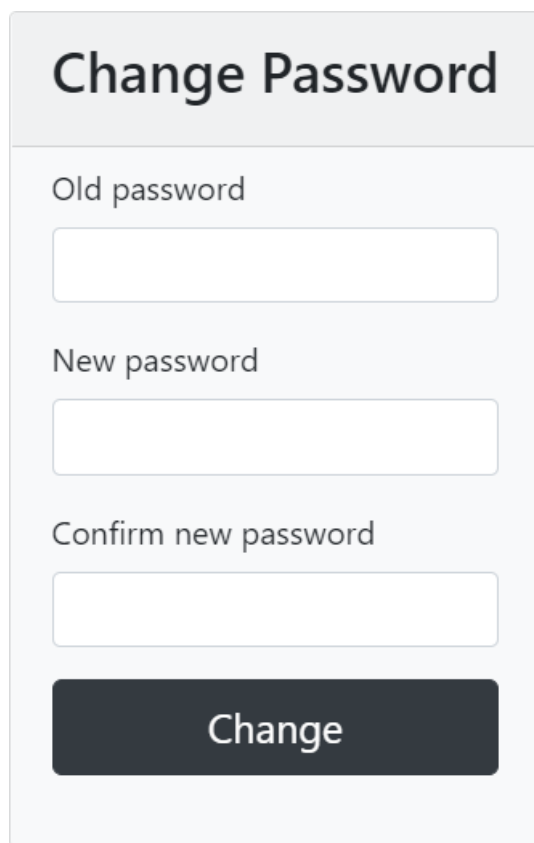
- Certificate Revocation Lists (CRL) Information



- General: General information.
  - Subject: Please refer to the Subject description in the Own server certificate information.
  - SAN: Please refer to the SAN SubjectSubjectdescription in the Own server certificate information.
- 
- Download: Download certificate or certificate revocation lists file.
  - Upload: Upload certificate or certificate revocation lists file.
  - Delete: Delete certificate or certificate revocation lists file.
  - Reject: Move the certificate to the rejected certificate list. (This option is available only in the trusted certificate list.)
  - Trust: Move the certificate to the trusted certificate list. (This option is available only in the rejected certificate list.)

## 7. Account Settings

This page can be used to modify the user account password on the web interface. After the user logs in the web interface for the first time (using the factory default account/password), please change the password as soon as possible. The password change is shown as Figure 10-1.



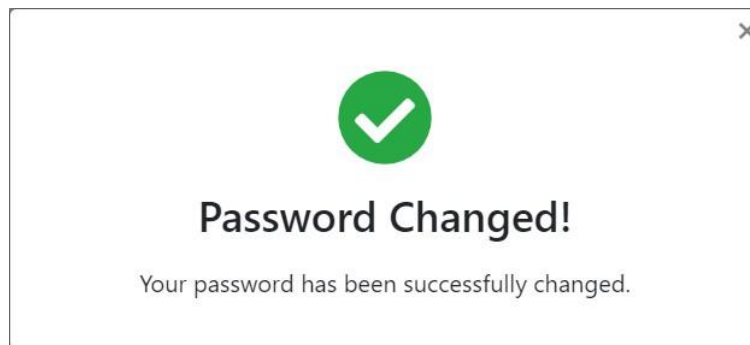
The screenshot shows a web form titled "Change Password". It contains three input fields: "Old password", "New password", and "Confirm new password". Below the input fields is a dark grey button labeled "Change".

Figure 10-1

The modification steps are as follows:

1. Enter the old password in the "Old password" input box.
2. Enter a new password in the "New password" input box.
3. Enter the new password again in the "Confirm new password" input box to confirm the password accuracy.
4. Click the "Change" button. After the password is successfully changed, the following dialog box will appear. When you log in to the web interface next time, please log in with the new password. The new password features the following verification restrictions:

- Which checks the similarity between the password and a set of attributes of the user.
- Which checks whether the password meets a minimum length, the default is 8 characters.
- Which checks whether the password occurs in a list of common passwords. By default, it compares to an included list of 20,000 common passwords.
- Which checks whether the password isn't entirely numeric.



5. If there is an error in changing the password, an error message will be displayed below each input box, as shown in the figure below.

A form titled "Change Password" with a light grey header. It contains three input fields. The first field, labeled "Old password", has a red error message below it: "Your old password was entered incorrectly. Please enter it again." The second field, labeled "New password", is empty. The third field, labeled "Confirm new password", has a red error message below it: "The two password fields didn't match." At the bottom of the form is a dark grey button labeled "Change".

# Appendix A. eSearch Tool Software

## eSearch Utility

( [http://www.icpdas.com/en/product/guide+Software+Utility\\_Driver+eSearch\\_\\_Utility](http://www.icpdas.com/en/product/guide+Software+Utility_Driver+eSearch__Utility) ) is a set of easy-to-use portable software, which can be used to search and configure ICP DAS network communication devices on the Ethernet network. For software usage, please follow the steps below:

### [Steps]

Search for LP-2648M devices on the Ethernet network.

- (1) Click the "Search Server" button to start searching for devices.
- (2) The LP-2648M device will appear in the search list and select LP-2648M.
- (3) Click the "Web" button to automatically open the default browser of the system.

