Software Operation

701ServerSQL Software Manual

V250117

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1. Introduction to 701ServerSQL and 701ClientSQL Functions and Installation Timing

The main function of 701ServerSQL is hardware connection, controller monitoring, parameter editing, and bridging across heterogeneous platforms with database system host functionalities. Each system requires and can only have a single 701ServerSQL computer. The main function of 701ClientSQL is to provide a user interface for operations, including personnel access permissions, entry and exit records, attendance reports, message broadcasting, and graphical central monitoring. Users can install one or multiple sets of 701ClientSQL software based on their needs, for example, choosing one Client computer specifically for managing personnel access permissions and another one or more Client computers dedicated to graphical control management and monitoring entry and exit records.

1.1 Overview of 701Server Version Names

- 701Server 6.X: Supports Windows 2000 system, no database functionality
- 701Server 8.X: Supports Windows XP system, no database functionality
- 701Server 9.X: Supports Windows 7–10 and above systems, no database functionality
- 701ServerSQL 10.X: Supports Windows 7–10 and above systems, supports MariaDB / JSON data format.
- 701ServerSQL 11.X: Supports Windows 7–10 and above systems, supports MariaDB / MSSQL / JSON data format.
- 701ServerSQL 2025: Supports Windows 7–10 and above systems, supports WEB API / MariaDB / MSSQL / JSON data format.

1.2 Features of 701ServerSQL

- **Database system or traditional file system mode**

  Users can choose between MariaDB database system, MSSQL database system, or traditional file system based on their needs.

- **Support for Remote Sharing Mode for Multiple Client PCs**

  Support for Multiple Client PCs Remote Sharing Server PC Data (This feature is only supported when installing the database system mode)

- **Synchronous Multitasking in 16 Areas,Supporting up to 4064 Controllers**

  Support for Multi-Area Mode, Able to Simultaneously Control up to 16 Areas * 254 Stations = 4064 Access Control and I/O Devices

- **Unicode Architecture Supports Global Languages / Time Download Across Time Zones**

  Easily Translate Software Resource Documents into Multiple Languages; Support for 16 Independent Time Zone Settings in Each Area

- **Support for Card Reader/IO Module Devices(TCP/RS485/Modbus)**

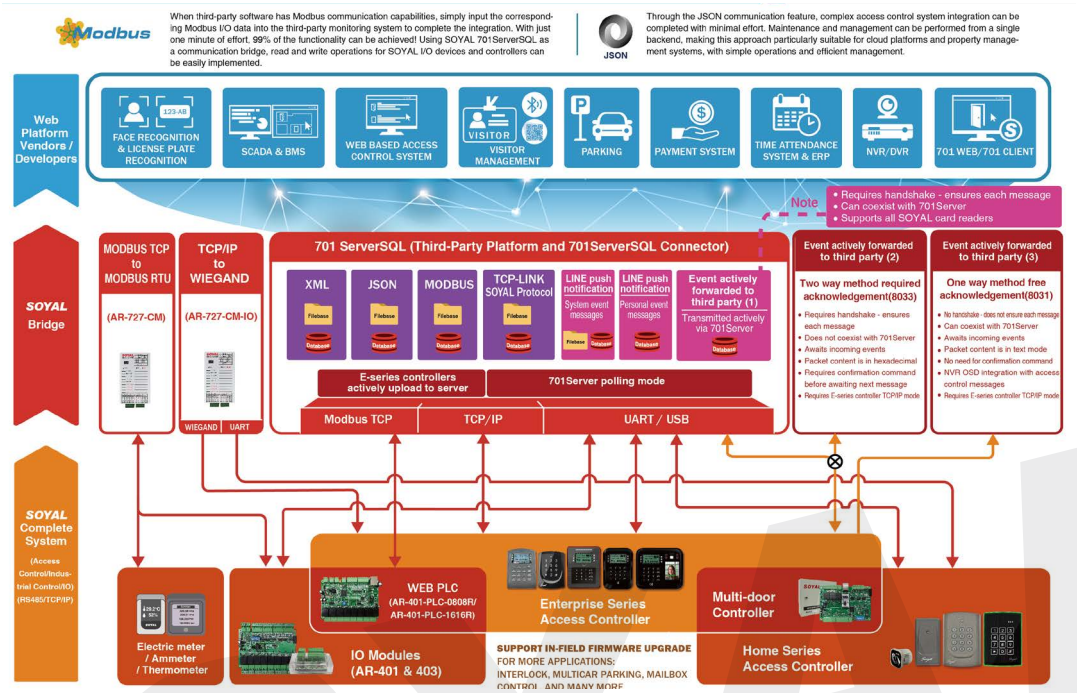
  TCP IO, LAN model options: TCP_IO; RS485 IO, LAN model options: RS485_IO; Modbus I/O, LAN model options: MODBUS_TCP

- **Support for Remote Active Message Upload (Enterprise Edition E Series Controllers)**

  Eliminates Waiting Time in Passive Polling Mode Queues, Immediately Reports New Events or Status Changes, Fast Speed, No Waiting, Reduces Server Polling Workload

- **SOYAL-LINK provides a rich and user-friendly interface for integrating with third-party heterogeneous platforms**

701ServerSQL 10V5 can act as a communication bridge, facilitating integration applications with SOYAL access control, I/O devices and various third-party platform software. It can use JSON commands to integrate with visitor system, attendance system, monitoring system; Use Modbus commands to integrate with central monitoring BMS, SCADA system.



- More Details :
  SOYAL-LINK provides a rich and user-friendly interface for integrating with third-party heterogeneous platforms

1.3 Functions of 701Server

Once all hardware is set up, user settings need to be configured. In a standalone system, each unit must be configured individually, while in a networked system, settings can be unified and user data can be downloaded to the controllers either separately or synchronously, allowing for the quickest completion of access control settings. Additionally, all entry and exit records, attendance reports, etc., can be viewed on the computer, making the networked approach the best option for access control systems.

701ServerSQL is a resident software responsible for hardware configuration, computer communication settings, and system hardware planning. This includes communication port settings, data collection, controller parameter configuration, network architecture, connection status checks, etc., all operated by system engineers.

Access Control / WEB PLC Network Architecture Settings

Controller Active Messaging Mode / Controller Passive Polling Mode

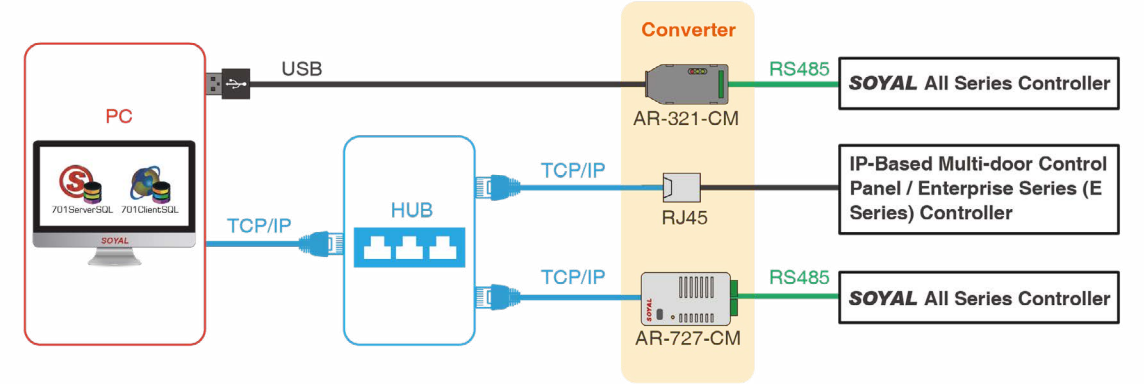
Controller Connection Status Display

Controller Parameter Settings

Fingerprint and Facial Data Upload/Download

1.4 Three Ways to Connect 701ServerSQL to Controllers

701ServerSQL supports TCP/IP and RS485 communication interfaces, making it compatible with the entire range of SOYAL controllers. For devices that only have an RS485 interface, network connectivity can be achieved through the AR-727-CM serial network server.



1. RS485 to TCP/IP → Connect via the AR-727-CM network communication converter
2. Direct TCP/IP → Connect through the built-in RJ45 of the Enterprise Edition (E Series) controller
3. RS485 to USB → Connect via the USB/RS-485 converter AR-321-CM

2.Differences Between Legacy Data File System and Database System & Single Computer/Multi-Computer Modes

2.1 Comparison Table of Differences Between Traditional File System and Database System & Single Computer/Multi-Computer Modes

System Requirements			Manage hardware and human-machine interface on the same computer	One computer manages hardware while multiple computers manage human-machine interfaces	
Computer management			Manage hardware and human-machine interface	Only manage hardware	Only manage human-machine interface
Software installation required	701ServerSQL		Installation required	Installation required	X
	701ClientSQL		Installation required	X	Installation required
Data Access Modes NOTE	A. File System		X	X	X
	B.MariaDB	MariaDB	Installation required	Installation required	X
		ODBC Connector (32-bit version installation file)	Installation required	Installation required	Installation required
		ODBC 32 DSN (701Server)	Installation required	Installation required	Installation required
	C. MSSQL	MSSQL	Installation required	Installation required	X
		ODBC Connector (X86version installation file)	Installation required	Installation required	Installation required
		ODBC 32 DSN (701ServerSQL)	Installation required	Installation required	Installation required

NOTE • Data Access Mode - Choose One of Three

701ServerSQL
(Only one computer installation per system)

Essential Software:

Database Software

1. Using MariaDB as example:
   Select **64-bit** version installation

2. MSSQL : Database installation file
   (Microsoft official website)

ODBC Connector

1. MariaDB:
Select **32-bit** version installation
(ODBC Connector Official Website)

2. MSSQL :
Select the X86 version of the
installation file (Microsoft official website)

701ServerSQL

Input IP Address and Port in [Local TCP-LINK Address] of COM Setting

701ClientSQL
(Multiple computer installations allowed)

Essential Software:

ODBC Connector

1. MariaDB:
Select **32-bit** version installation
(ODBC Connector Official Website)

2. MSSQL
Select the X86 version of the
installation file (Microsoft official website)

701ClientSQL

It is required to input the same setting of PC IP Address and Port of 701ServerSQL software in "Connect to 701Server" .

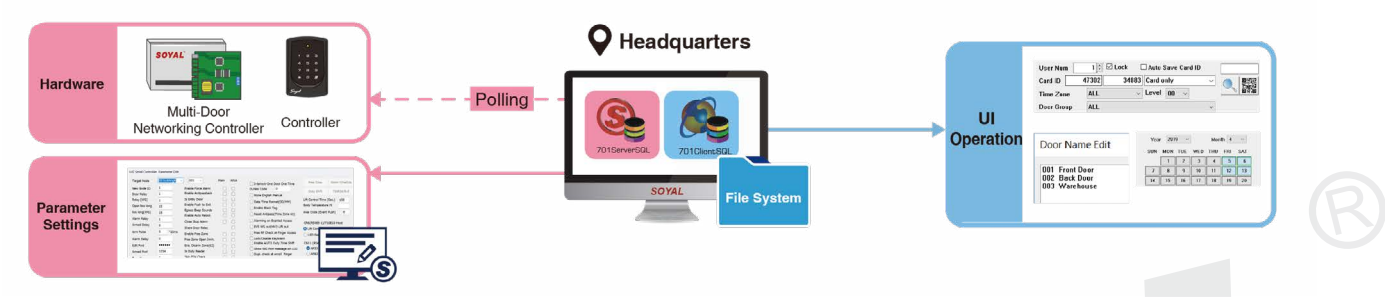
※ This document is for educational purposes only; please obtain software licenses from the original manufacturer.

2.2 Single PC Operation Mode: 701ServerSQL & 701ClientSQL Installation under same PC

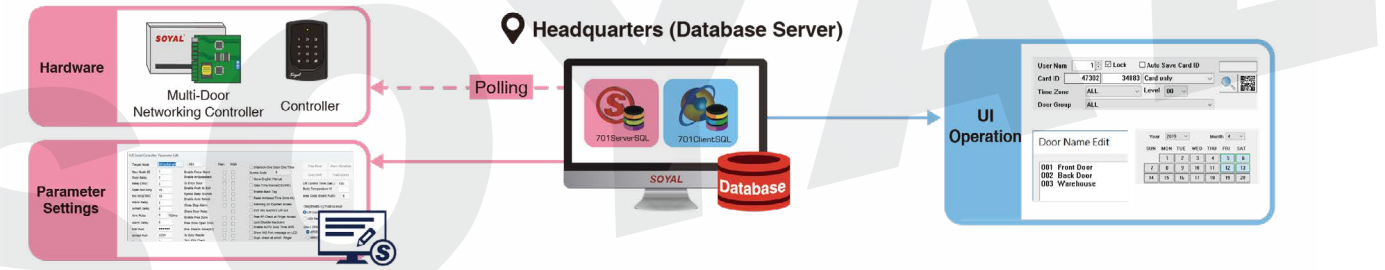
User can choose Database mode or File System mode according to needs and requirement. Built-in the same operation user interface for both modes provides seamless upgrade from File System to Database easy and can be done without relearning.

- File System: Easy to set up and maintain, suitable for small to medium scale system
- Database System: Suitable for complex exchange data and transaction, centralized system, and medium to large scale system that required higher security.

The two systems supported on a single computer have the same functionality; the main difference lies in the operating system modes.



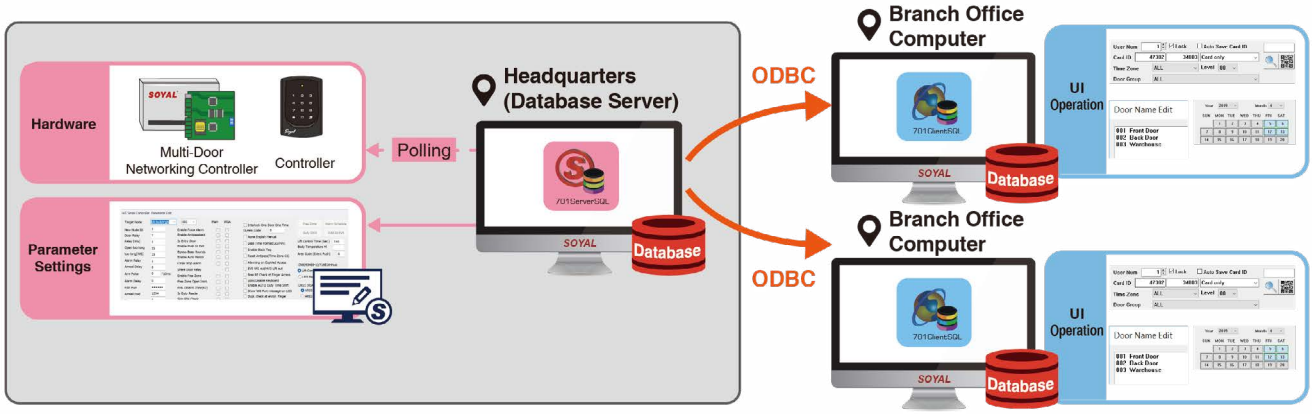
Legacy Data File system



Database system

2.3 Multi PC Operation Mode (Install one 701ServerSQL computer and multiple 701ClientSQL computers)

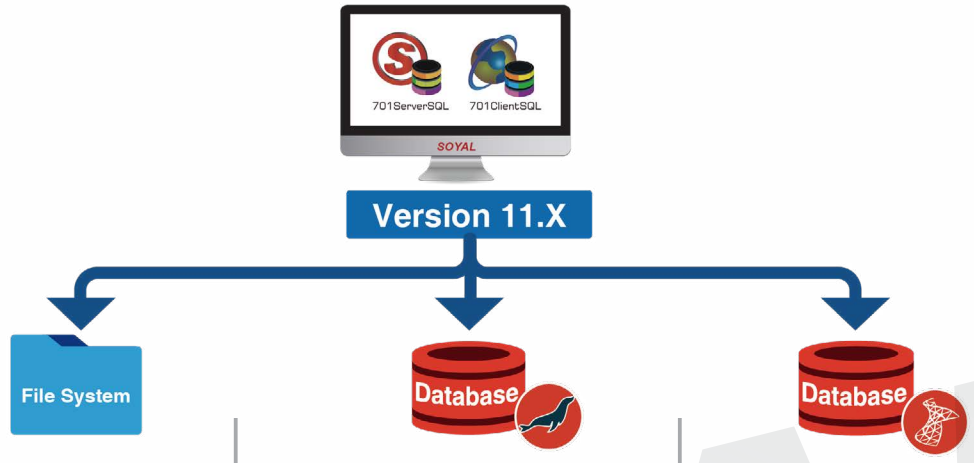
701ServerSQL is installed on the main computer, while 701ClientSQL is installed on the computers of operators in different locations.



2.4 Three Ways to Manage the Database

Microsoft SQL Server, abbreviated as MSSQL. The term MSSQL will be used to refer to the Microsoft SQL Server database throughout the explanation.

※ The system offers three modes. Please choose carefully before installation, as once selected, they cannot be changed.



Legacy Data File system

- Single computer operation without managing the database
- No multi-701ClientSQL management mode

MariaDB Database system

- Suitable for single computer mode or one system 701ServerSQL with multiple 701ClientSQL computers
- Does not support the future web version 701ServerSQL 2025

MSSQL Database system

- Suitable for single computer mode or one system 701ServerSQL with multiple 701ClientSQL computers
- Seamless upgrade to the future web version 701ServerSQL 2025 is supported

3. Downloading and Installing 701ServerSQL

3.1 Software Installation Precautions

You can choose to use either the database system or file system mode as needed. The same user interface is used, so no re-learning is required, ensuring an easy and seamless upgrade.

If you plan to use a database, ensure the following are prepared in advance:

A. Install the appropriate database engine
B. Add ODBC 32 DSN
C. Create a database named "701Server"
D. Create users for 701ServerSQL and 701ClientSQL

NOTE

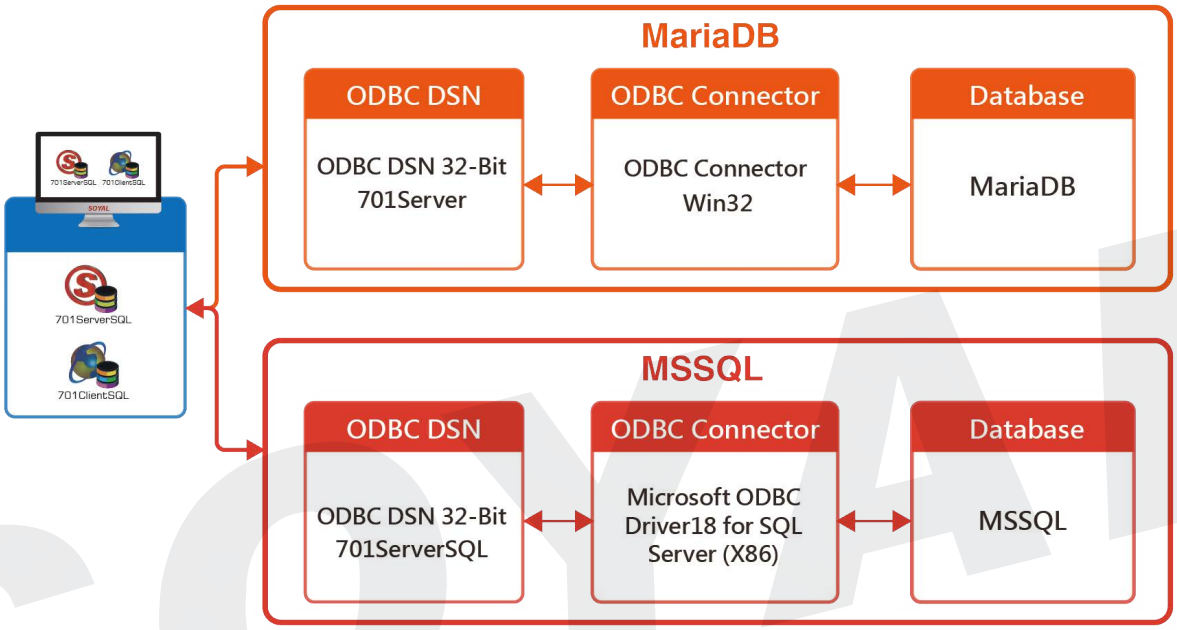
• The maximum disk sector/cluster size supported by SQL Server is 4096 bytes. Some high-end drives may have their sector/cluster sizes set above 4096, which can cause SQL Server to fail to start after installation. Therefore, please check the disk sector/cluster size before installation. For detailed information, refer to the official Microsoft documentation: Troubleshoot errors related to system disk sector size greater than 4 KB

3.2 Installation Process

NOTE

Before the initial installation of the software or updating to version 11.X, a backup must be performed. For detailed backup steps, please refer to section 11.5-Back Up DATA

3.2.1 Database System Installation Instructions



• How to Transfer Setting Parameters & Relevant Data Back to File System Mode from Database Mode?

The message recorded in Database Mode is non reversible, we cannot read the message from 701ClientSQL with File System Mode. The recommendation is using Export to Text File Function to record the relevant data as txt or excel file via 701ClientSQL.

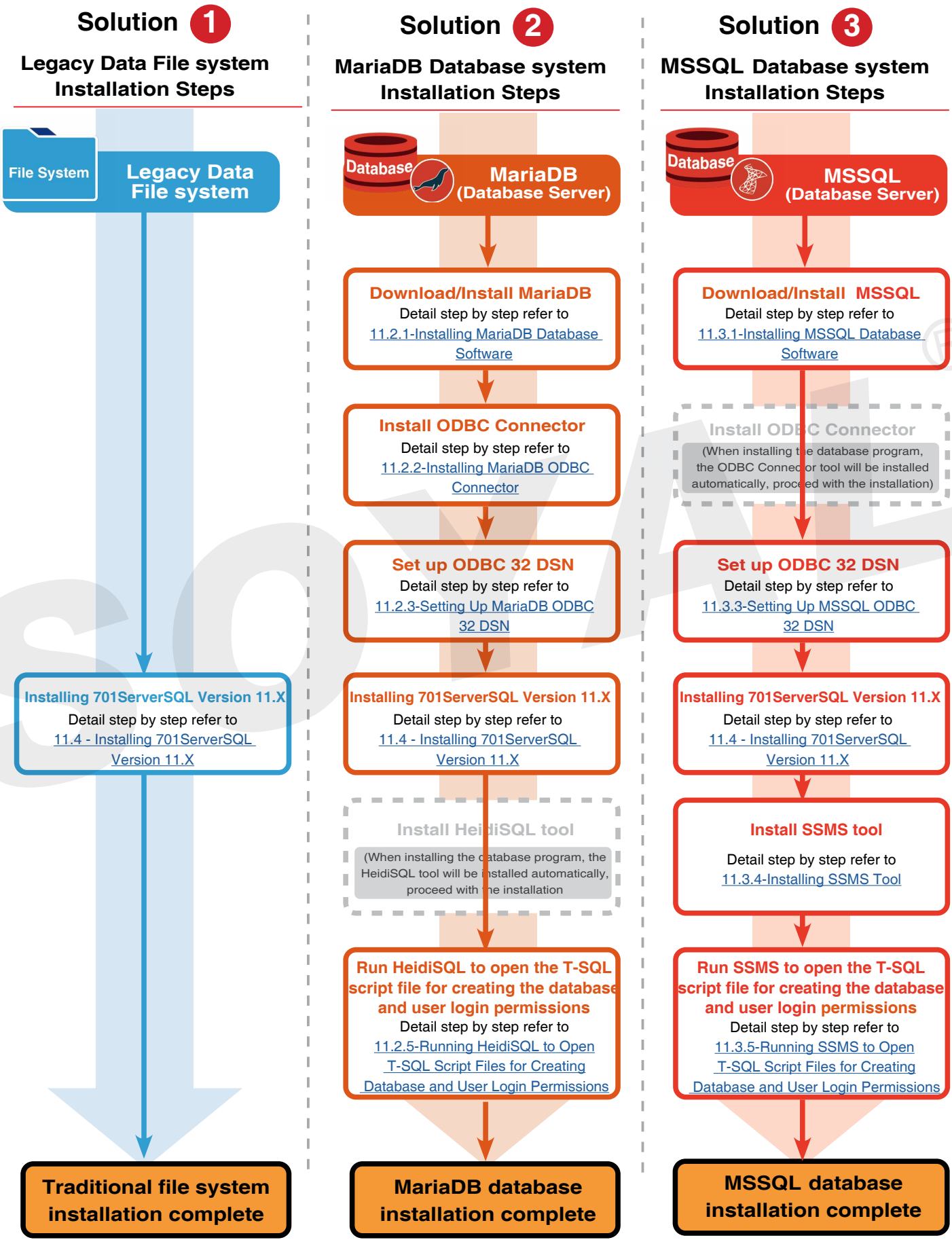
The introduction about Export to Text File Function please refer to 701ClientSQL Manual 7.1 Export to Text File

User data, Parameter Setting and etc. can use Import/Export Function to get back from Database Mode.

The introduction about Import/Export Function please refer to 701ClientSQL Manual 3. Backup

- User interface of database and its operation is the same like file base system, but all the data is saved on the database.
- When upgrading to Database Mode, the old data that is recorded on file system mode will still save under file system format. Once you upgrade into the database, all of old data will automatically transferred to database and cannot be converted back to file system data. For event log (msg files), you required to do ‘Message Import’ manually from 701ServerSQL to convert the data from file system into database format.
- If you want to preserve the old data under file system format, make a copy and stored in a safe place (refer to 11.5-Back Up DATA)
- Data that is remain on file system base even after upgrade to database mode:
  1.time attendance report such as DUTY file
  2.lift and floor data
  3.fingerprint and face data
- Upgrade from Windows XP to Windows 10, all of the data must be copy and directly paste to C:\Program Files (x86)

3.2.2 Installation Process for Traditional File Mode & Database Mode



3.3 Windows Service Auto Start Setup

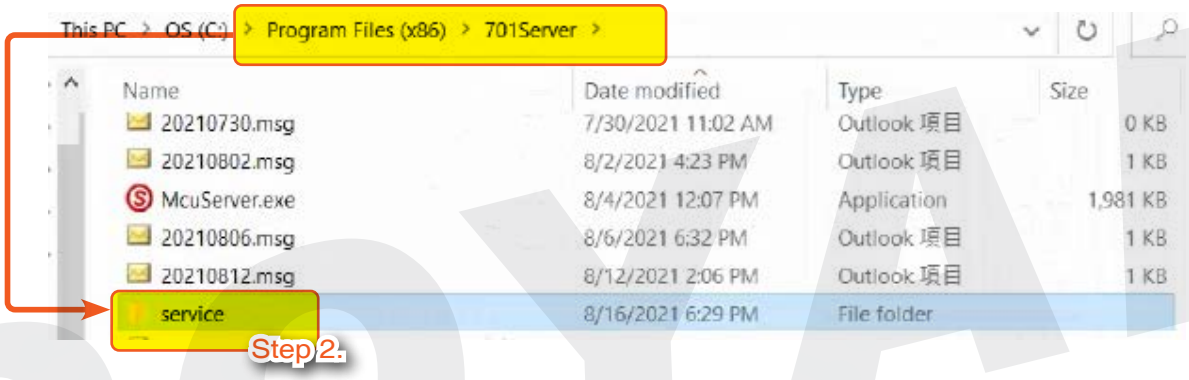
Reason:

- Windows automatic updates
- Windows restarts, causing some programs to malfunction

701ServerSQL is a resident software that usually starts up during boot. However, when multiple users share a computer, at least one user must be logged in to start the software set to start up with the computer. This is especially problematic when Windows is set to automatically update and restart the system after installation. In this case, 701ServerSQL may not start up, causing 701ClientSQL to fail to return record data. To solve the problem of 701ServerSQL failing to start up during Windows system boot, the Windows Service feature must be enabled to start up 701ServerSQL and 701ClientSQL without any user login.

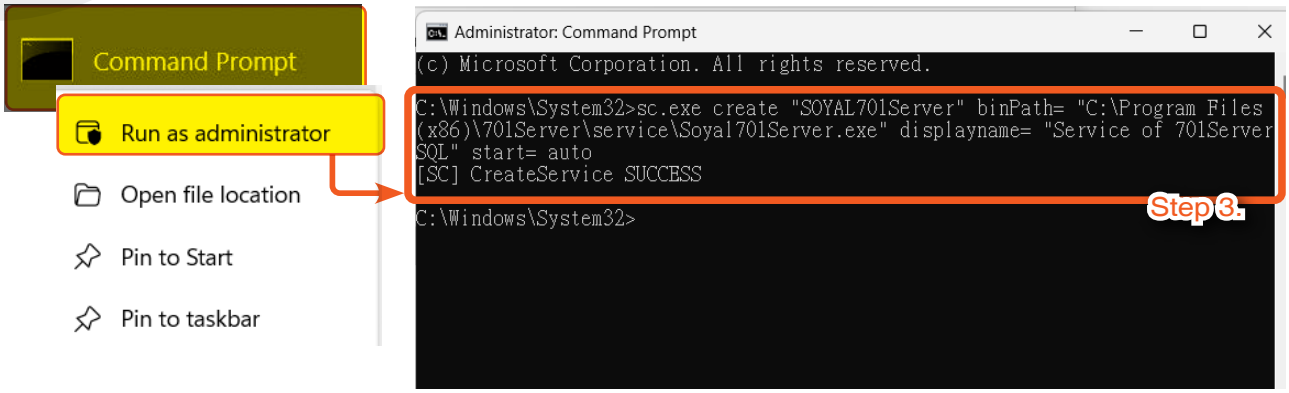
※The installation file of 701ServerSQL after version 10V5 includes the activation file for Windows Service, which is stored in the "..\701Server\service" path.

※Note: Below step is applied for PC with operating system Win 10/11



Step 1. If there is no "service" folder in the path "..\701Server\service", please download and install the necessary files first. (Download the necessary installation files)

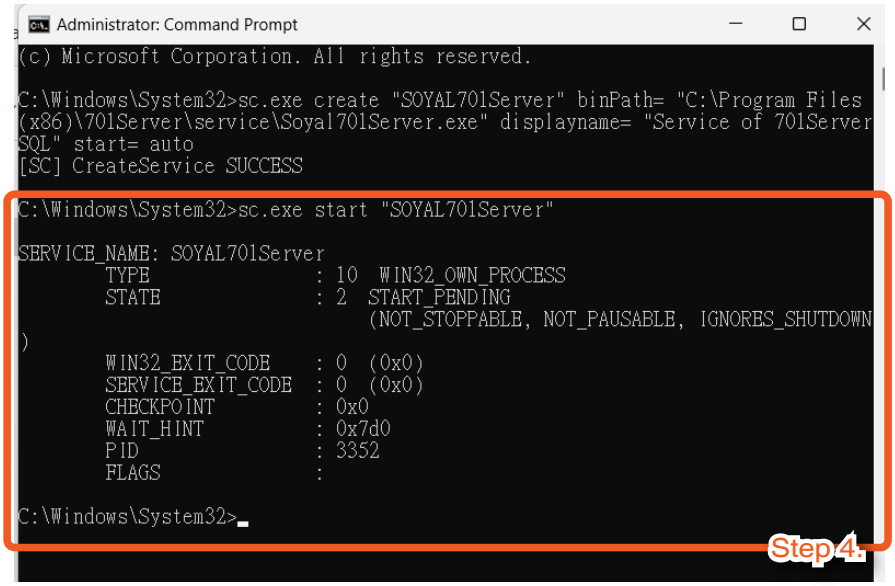
Step 2. Place the files in the path of 701ServerSQL (C:\Program Files (x86)\701Server) inside the "service" folder.



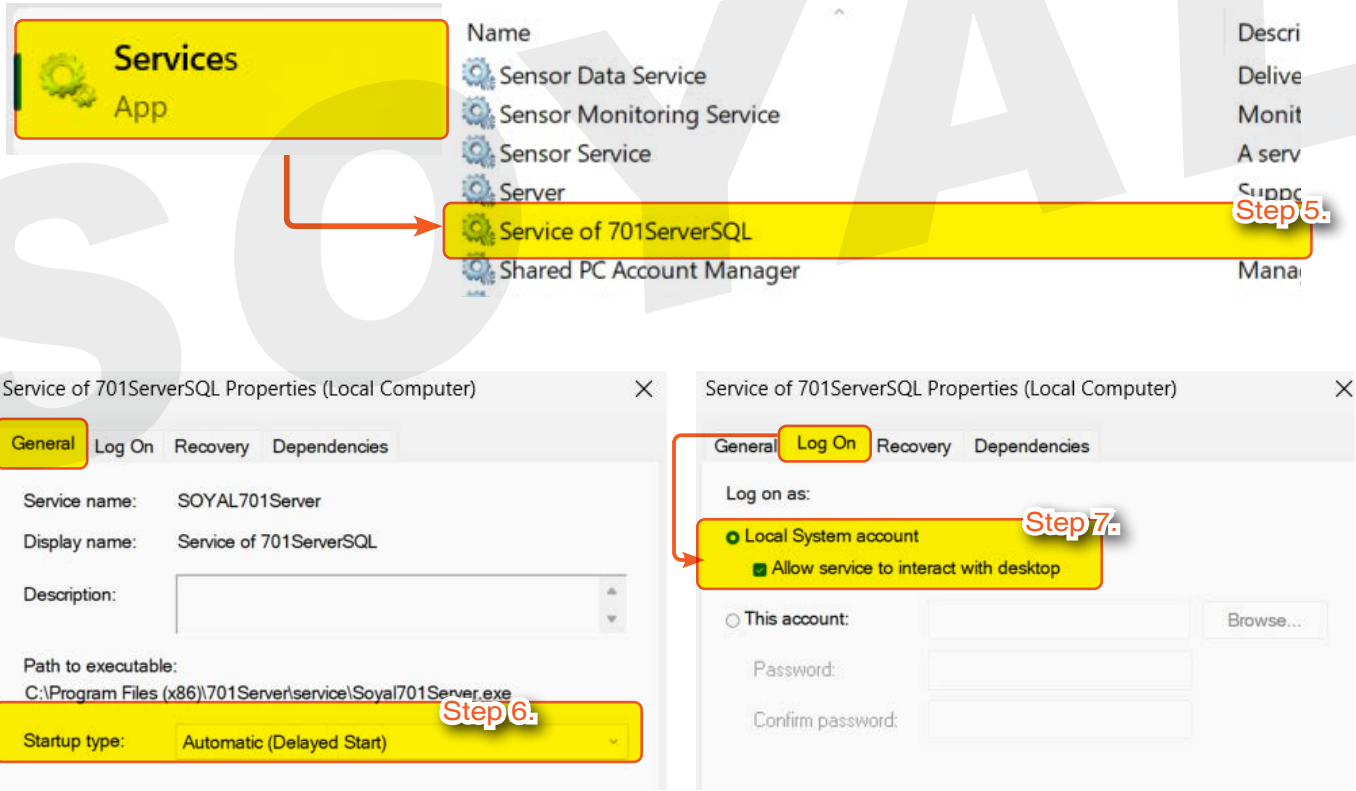
Step 3. Enter cmd or PowerShell and execute it (administrator privilege required).

Enter the code:

sc.exe create "SOYAL701Server" binPath= "C:\Program Files (x86)\701Server\service\Soyal701Server.exe" displayname= "Service of 701ServerSQL" start= auto



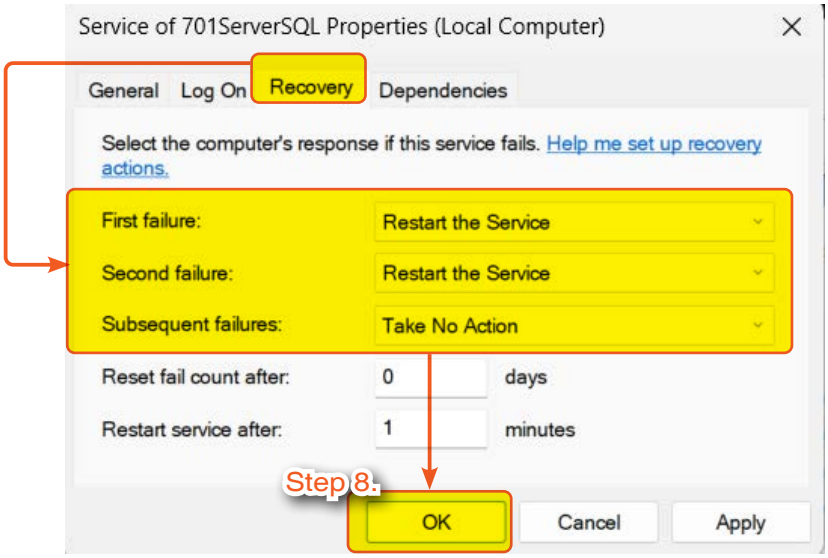
Step 4. Then enter the code: sc.exe start "SOYAL701Server"

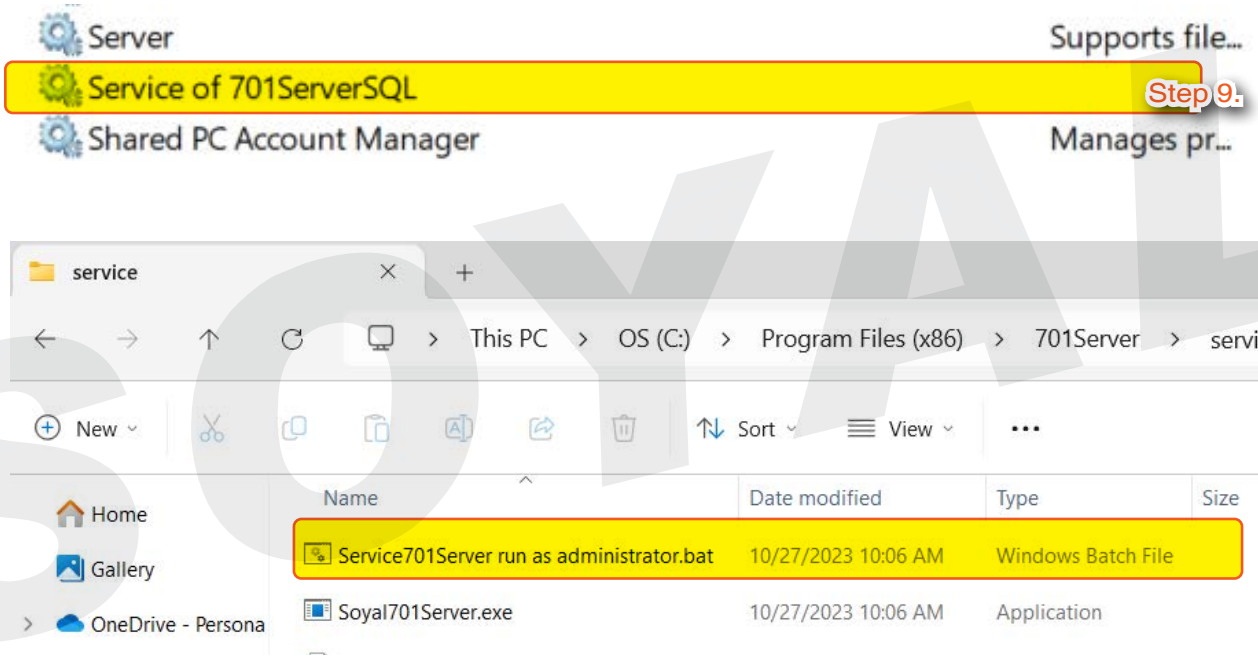


Step 5. Go to the "Services" menu, find the item "Service of 701ServerSQL," and double-click to open.

Step 6. In the menu bar, select "General," and choose [Automatic (Delayed Start)] as the startup type.

Step 7. In the menu bar, select "Log On," and check [Allow service to interact with desktop].





Step 8. In the menu bar, select "Recovery," and after selecting the items, press OK:

- First failure: Restart the Service.
- Second failure: Restart the Service.
- Subsequent failures: Take No Action.

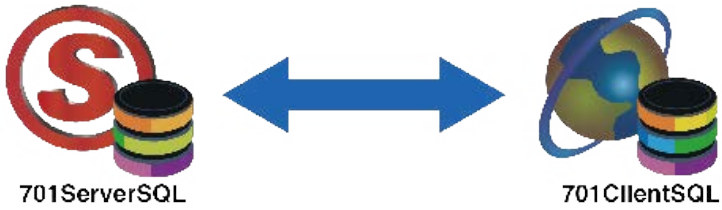
Step 9. The Service of 701ServerSQL will display "Automatic (Delayed Start)."

Step 10. Click on "Service701Server run as administrator.bat" to start.

After startup, 701ServerSQL will launch approximately 1 minute after booting without logging in.

4. Download and Install 701Software Troubleshooting

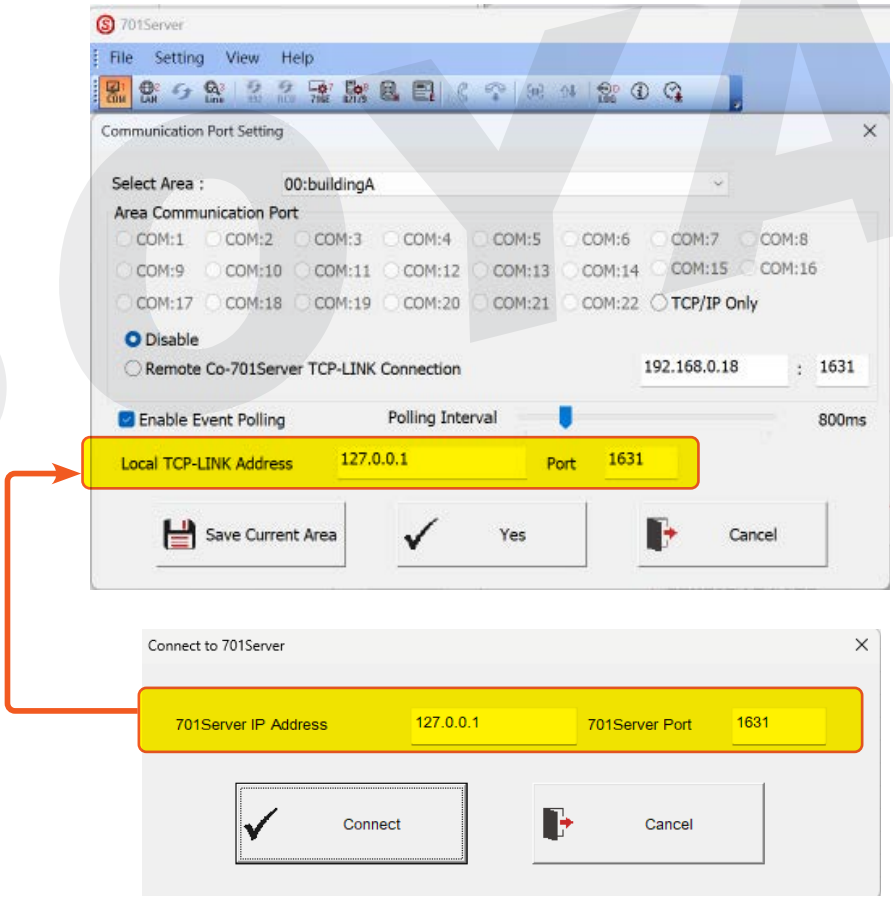
Key Points for Connecting 701ServerSQL and 701ClientSQL



Essential Checkpoints for Connecting 701ServerSQL and 701ClientSQL

1- IP / PORT

701ServerSQL needs to configure the IP/Port in COM settings for communication with the 701ClientSQL software. Therefore, when running 701ClientSQL for the first time with administrator privileges, an IP/Port configuration window will pop up. At this point, you should enter the IP/Port of 701ServerSQL in the COM section marked in red.



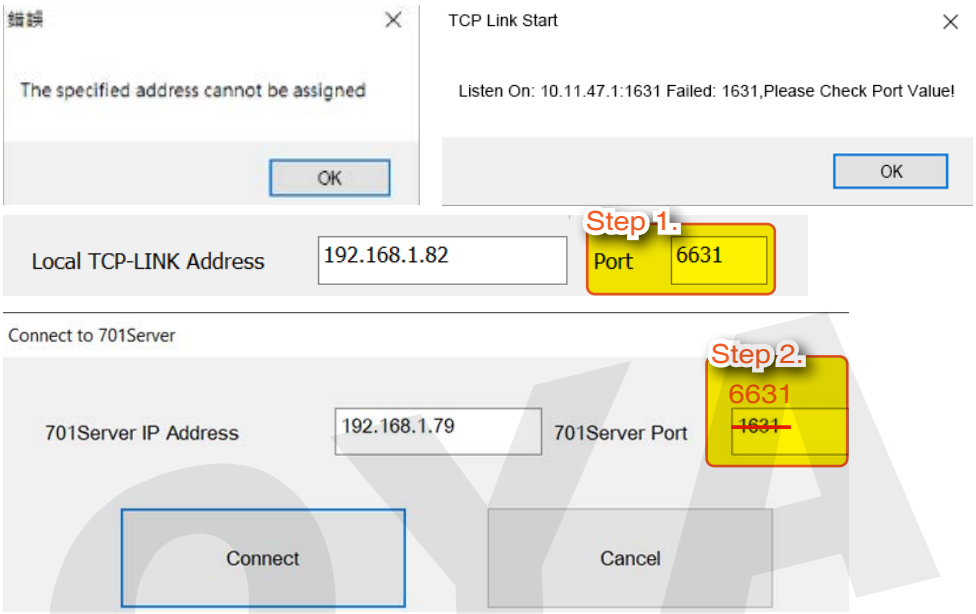
NOTE

Many people mistakenly fill in the IP/Port of the 727CM converter or the E-series card reader in these two fields, resulting in errors. For those who encounter this error, please consider how you would fill in the IP/Port if your architecture includes multiple 727CM converters or E-series card readers.

2-Firewall

To avoid communication abnormalities or blocking of messages returned by card readers, ensure that 701ServerSQL and 701ClientSQL are excluded from the firewall settings. For detailed instructions, please refer to --> Q2: Device connection to 701Software become offline and unable to connect

Q1. "The specified address cannot be assigned" error message or "Listen on: XXXX Failed: 1631, Please Check Port Value"



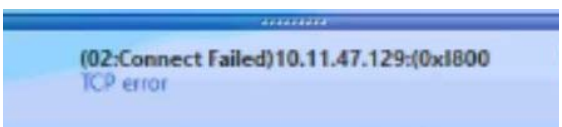
A3. Both of the error is as a result that your antivirus software is blocking connection to 701 Software. To solve this issue, please change the Listen Port connection between TCP-LINK Server and TCP-LINK Client into other Port that is not 163, for example 6631.

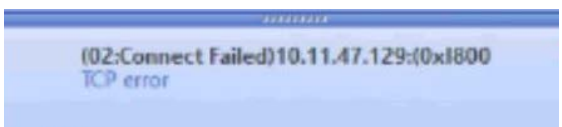
Step 1. On 701ServerSQL's COM section change the Port from 1631 into 6631

Step 2. After changing the Port on 701ServerSQL, all of the 701ClientSQL Port (connection to 701ServerSQL) must also be changed from 1631 into 6631

Q2. Device connection to 701Software become offline and unable to connect

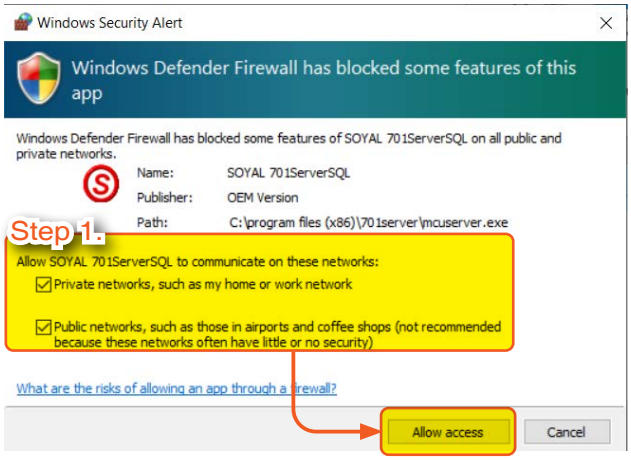
A4. Because Software 10.2 Version is enabling multiple port and connection that leaning on internet connection, sometimes Windows defender Firewall and/or antivirus software might block the connection to 701Software. If doing Troubleshooting Q3 problem still persists, please follow the steps listed below:





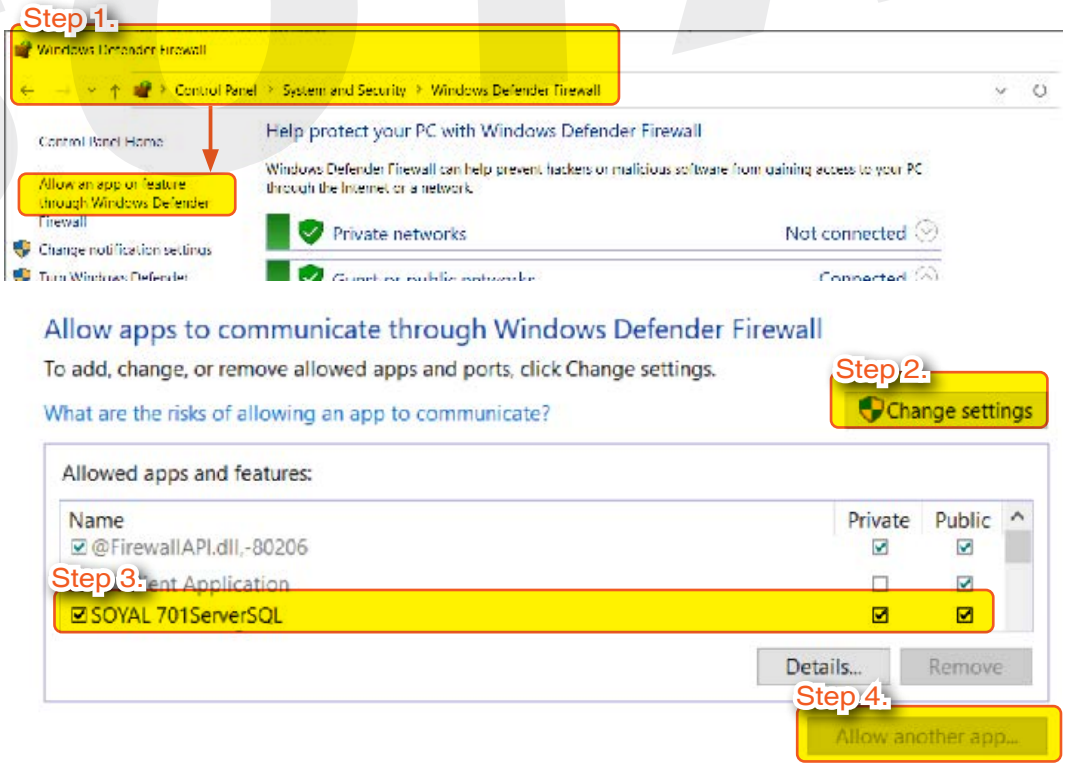
1- Allowing both 701ServerSQL and 701ClientSQL on Windows Defender Firewall

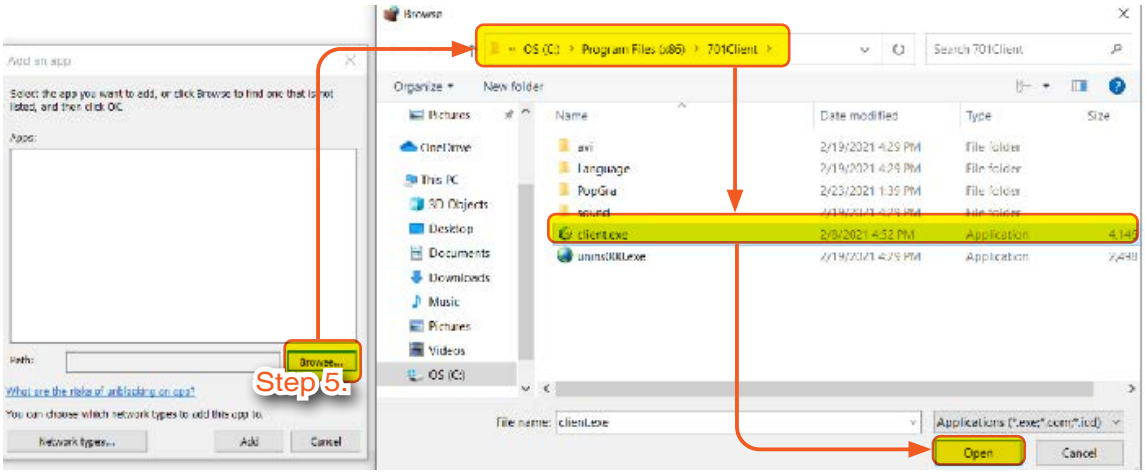
1: Windows Security Alert message

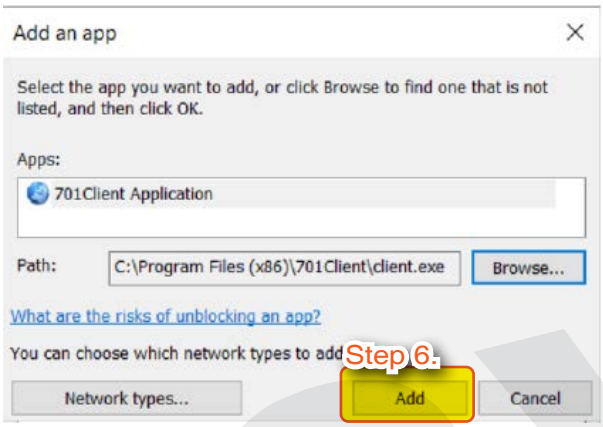


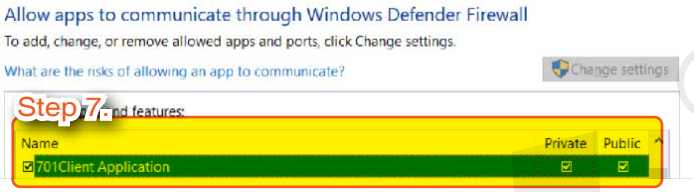
Step 1. If you are installing 10.2 directly in the first place you will find Windows Security Alert message. Tick both private networks and public networks.
This procedure must also be done with both 701ServerSQL and 701ClientSQL.

2 : Check the Windows Defender Firewall inside the Control Panel









Step 1. If you happened to skip the procedure, go to Control Panel > System and Security > Windows Defender Firewall and manually added 701ServerSQL and 701ClientSQL to allow connection on both public and private networks. Select [Allow an app or feature through Windows Defender Firewall]

Step 2. Select [Change Settings]

Step 3. Tick Private and Public on [SOYAL 701ServerSQL]

Step 4. Select [Allow another app] to setup 701ClientSQL for the next step

Step 5. Select Browse and enter [C:\Program Files (x86)\701ClientSQL] > then select client.exe > click [Open]

Step 6. Select [Add]

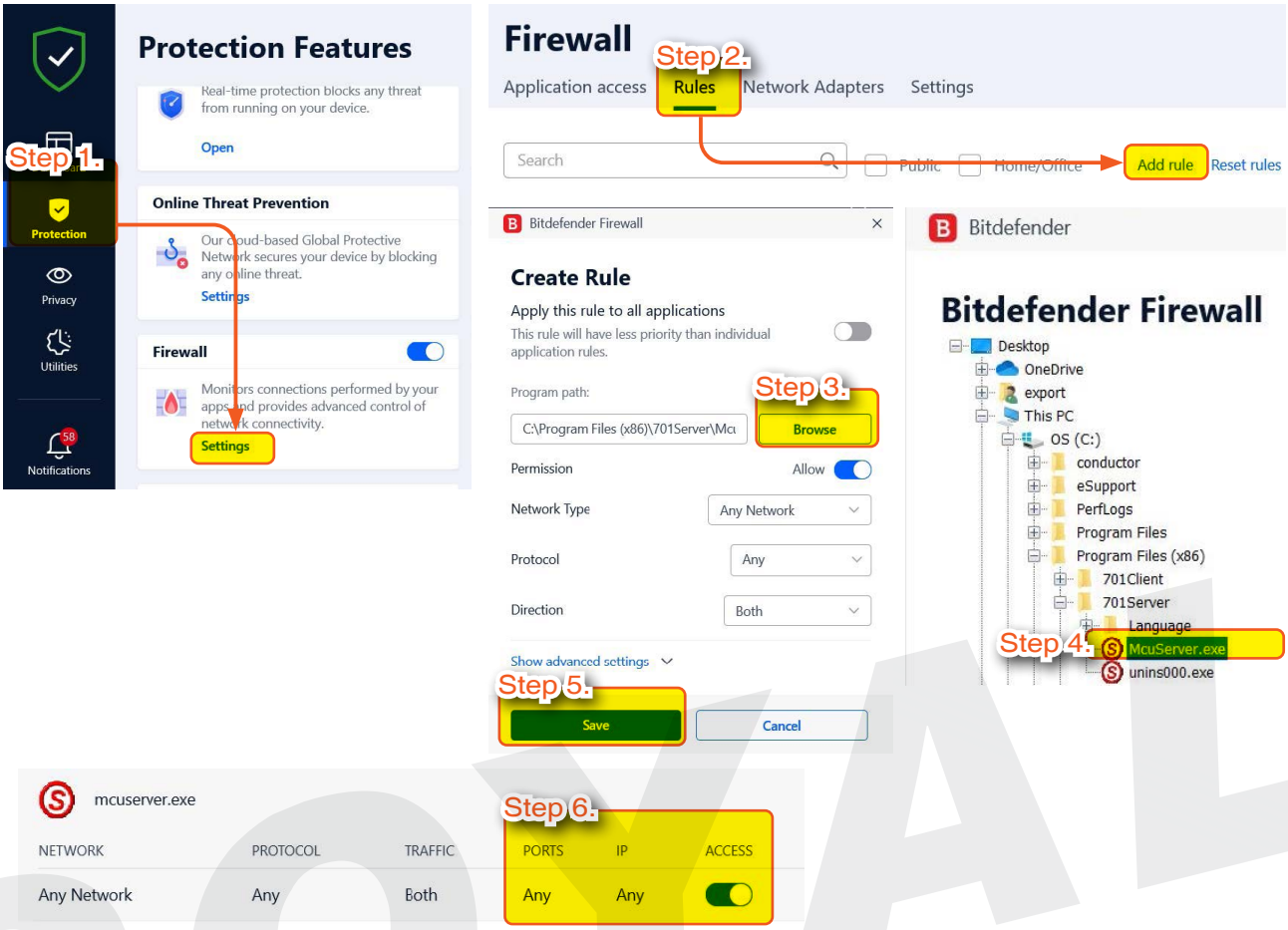
Step 7. Tick both Private and Public for [701ClientSQL Application]

2- Allowing both 701ServerSQL and 701ClientSQL on Antivirus Software

Example 1: Norton Antivirus

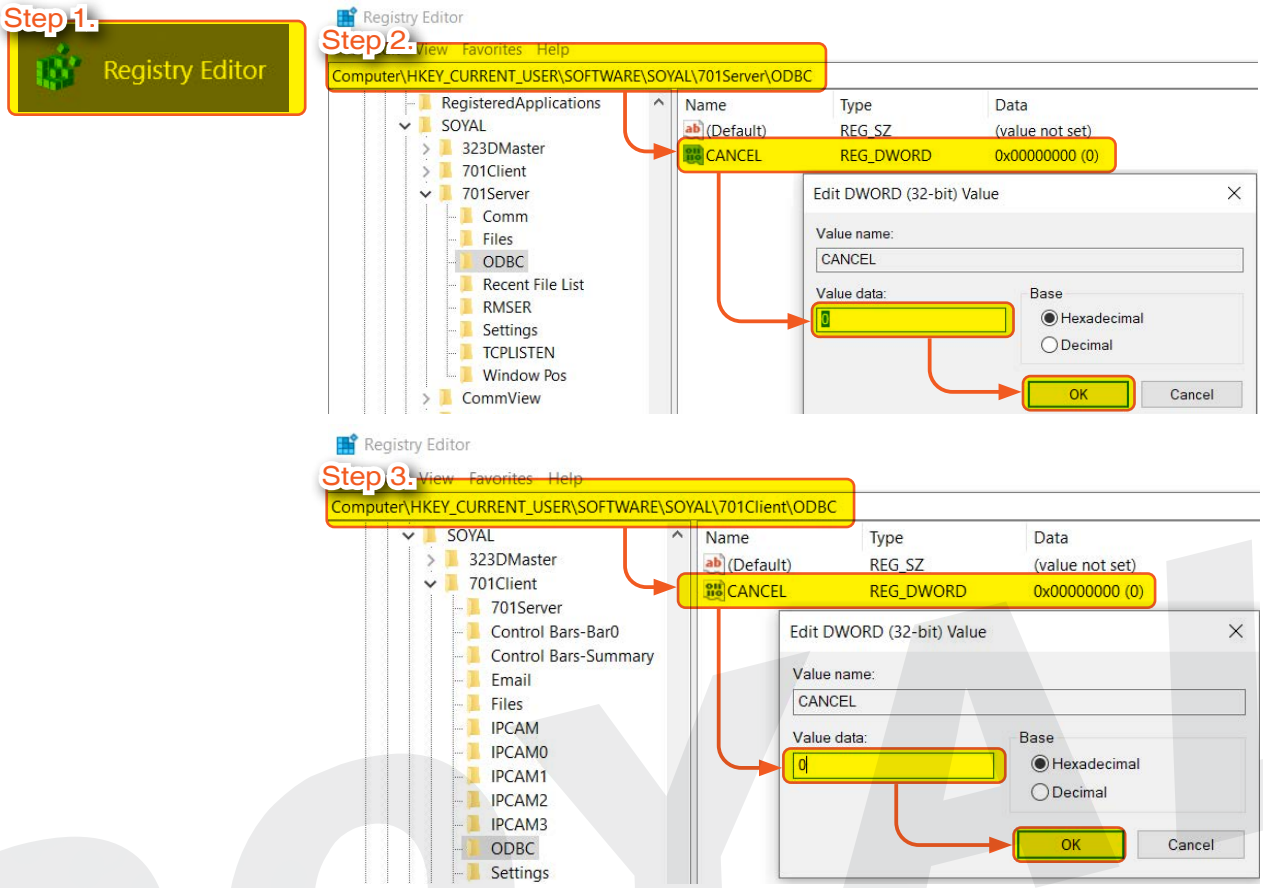
Step 1. On Firewall Alert setting options, select Allow Always on McuServer.exe

Example 2: Bitdefender



Step 1. Run Bitdefender software and select Protection > Firewall Setting
Step 2. Select Rules > Add rule
Step 3. Click Browse
Step 4. Enter C:\Program Files (x86)\701ServerSQL > and select ‘McuServer.exe’
Step 5. Select Save
Step 6. McuServer.exe has been added to Firewall Setting and Access is allowed. This also allowing access to Any Ports and IP Address without restriction

Q3. Already following the installation step by step and install DBMS with its ODBC Connector but software still shows 'File System Mode'



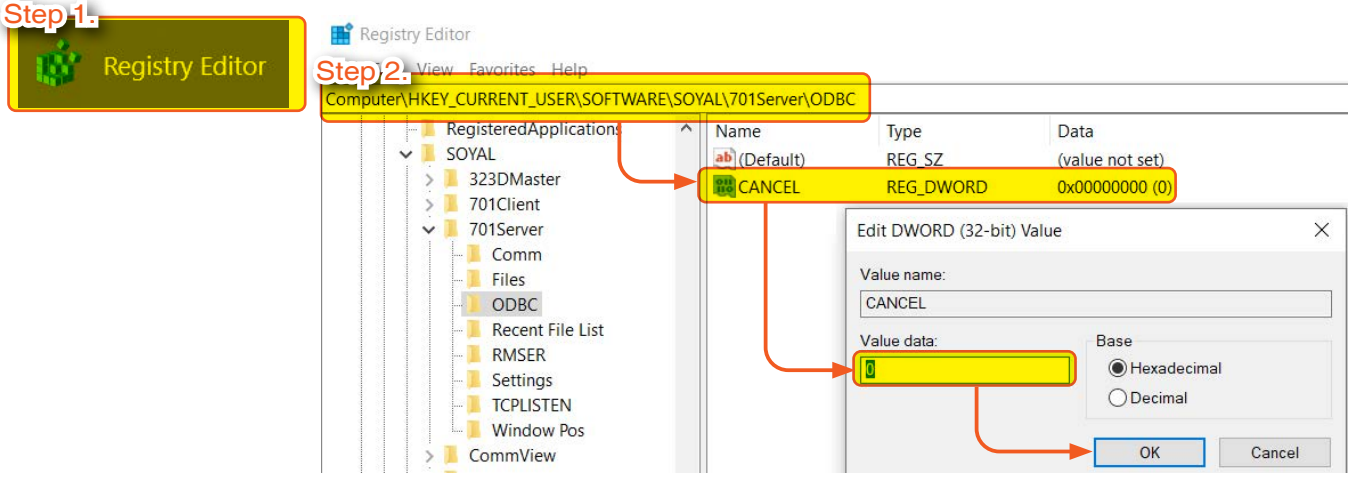
A1. 701ServerSQL and 701ClientSQL connection to Database is not successful so software will remain as File System Mode.

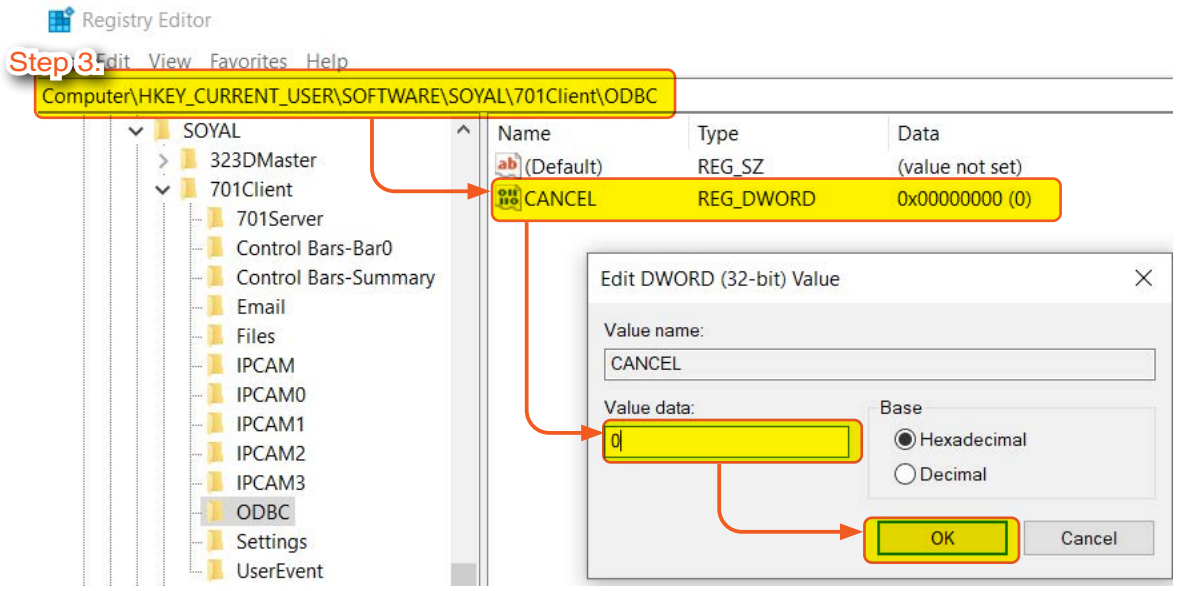
Step 1. Go to Registry Editor

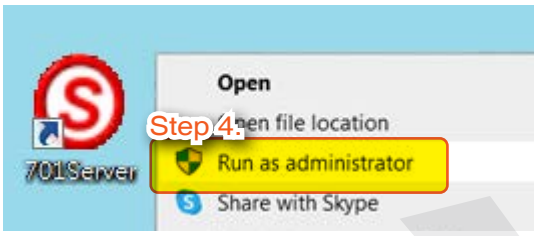
Step 2. Select Computer\HKEY_CURRENT_USER\SOFTWARE\SOYAL\701ServerSQL\ODBC → double click [CANCEL] value and change from 1 into 0 → select [OK]

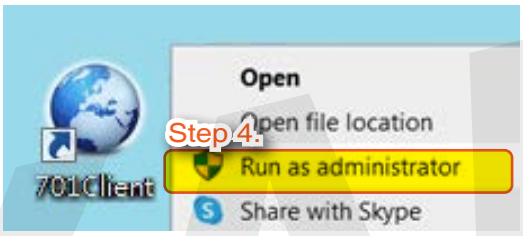
Step 3. Select Computer\HKEY_CURRENT_USER\SOFTWARE\SOYAL\701ClientSQL\ODBC→ double click [CANCEL] value and change from 1 into 0 → select [OK]

Q4. Does not select "Run as Administrator", when running software it does not convert to SQL Database Mode





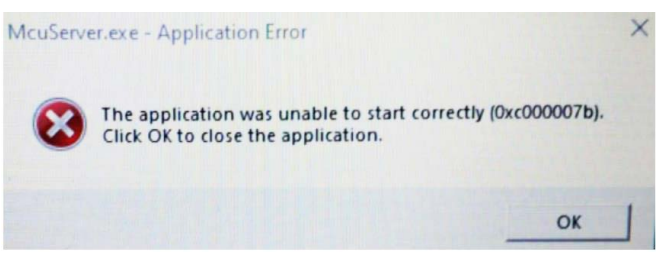


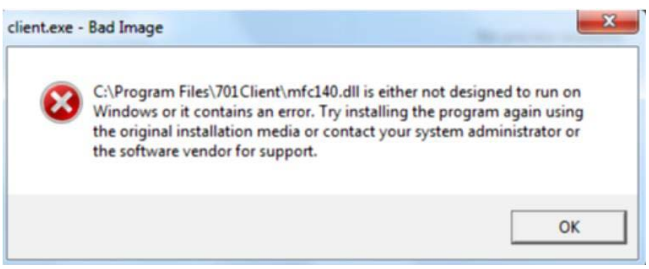


Step 1. Go to Registry Editor
Step 2. Select Computer\HKEY_CURRENT_USER\SOFTWARE\SOYAL\701ServerSQL\ODBC → double click 'CANCEL' value and change from 1 into 0 → select 'OK'
Step 3. Select Computer\HKEY_CURRENT_USER\SOFTWARE\SOYAL\701ClientSQL\ODBC → double click 'CANCEL' value and change from 1 into 0 → select 'OK'
Step 4. Right click on 701ServerSQL and choose "Run as administrator". Repeat the same method with 701ClientSQL software.

Q5. 0xc000007b, mfc140u.dll and api-ms-win-crt-runtime-l1-1-0.dll problems when installing 701ServerSQL and 701ClientSQL

After installing 701ServerSQL and 701ClientSQL, when running the application it shows an error 0xc000007b, mfc140u.dll and api-ms-win-crt-runtime-l1-1-0.dll



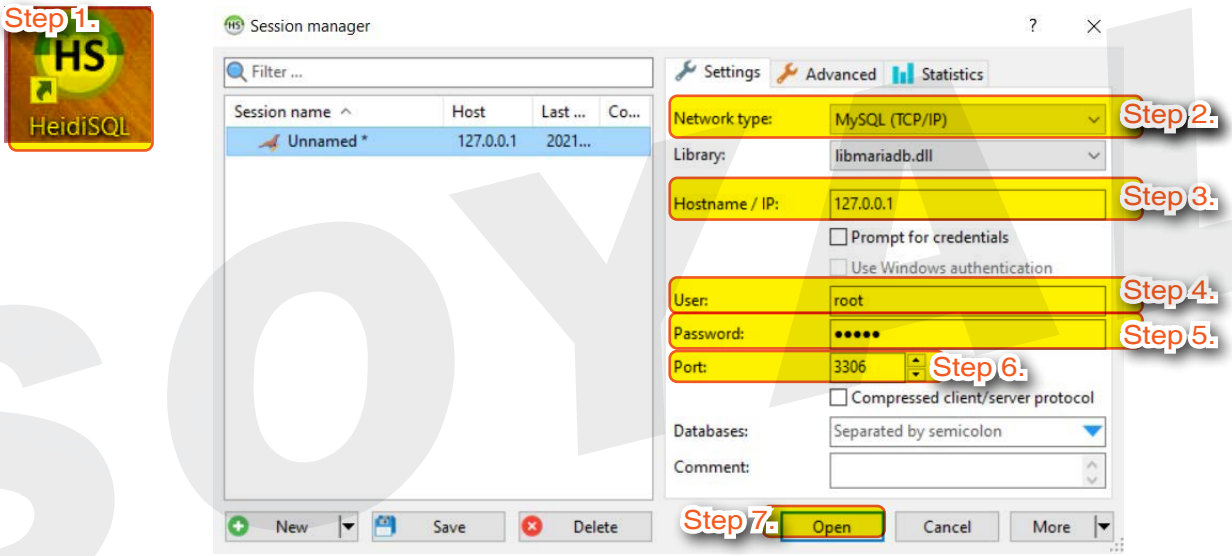


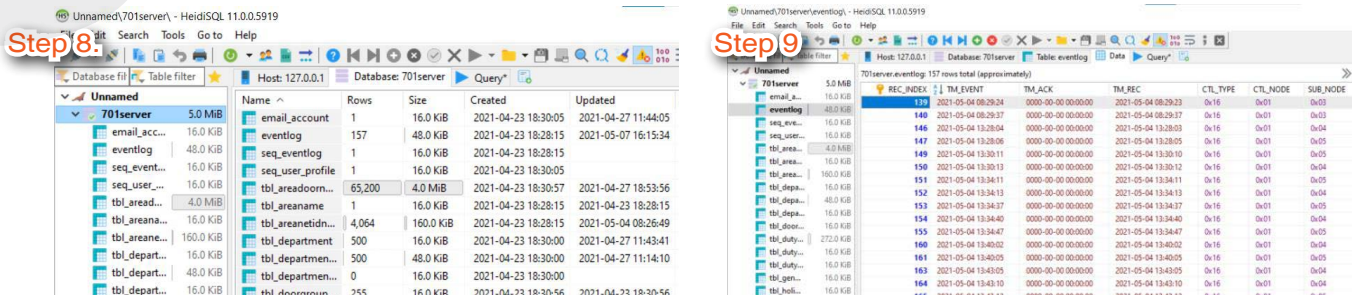
Both problems can be solved after installing below file.
For OS Win32, please download vc_redist.x86.exe
For OS Win64, please download vc_redist.x64.exe
Reference: https://support.microsoft.com/zh-tw/help/2977003/the-latest-supported-visual-c-downloads

Redistributable version for Windows operating system:
Win 7： redistributable version 2010
Win 10 : distributable version 2015-2019

Q6. Could not load previous date data when loading msg files, how to track the data stored on the database?

A6. Taking MariaDB for example, after download and install MariaDB, HeidiSQL shortcut will be automatically created
Logged in into HeidiSQL and you will get to see database and table item.

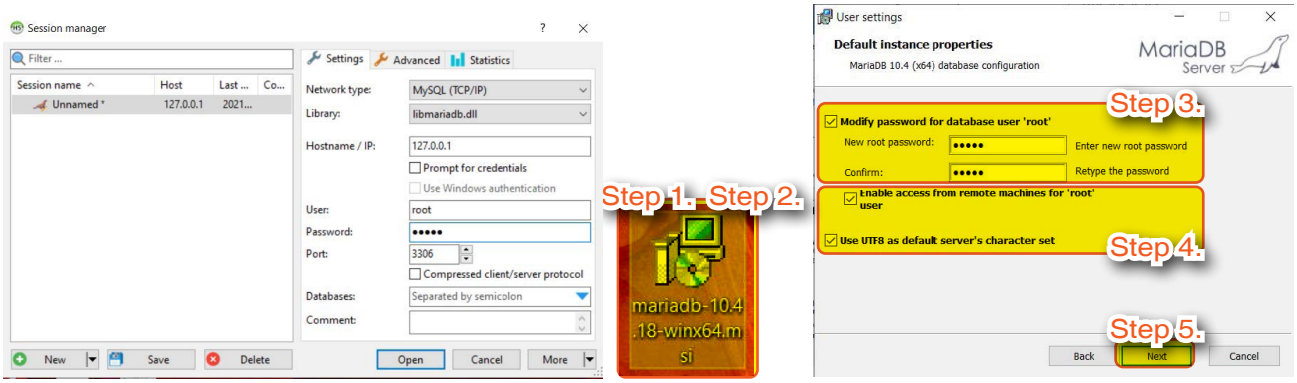


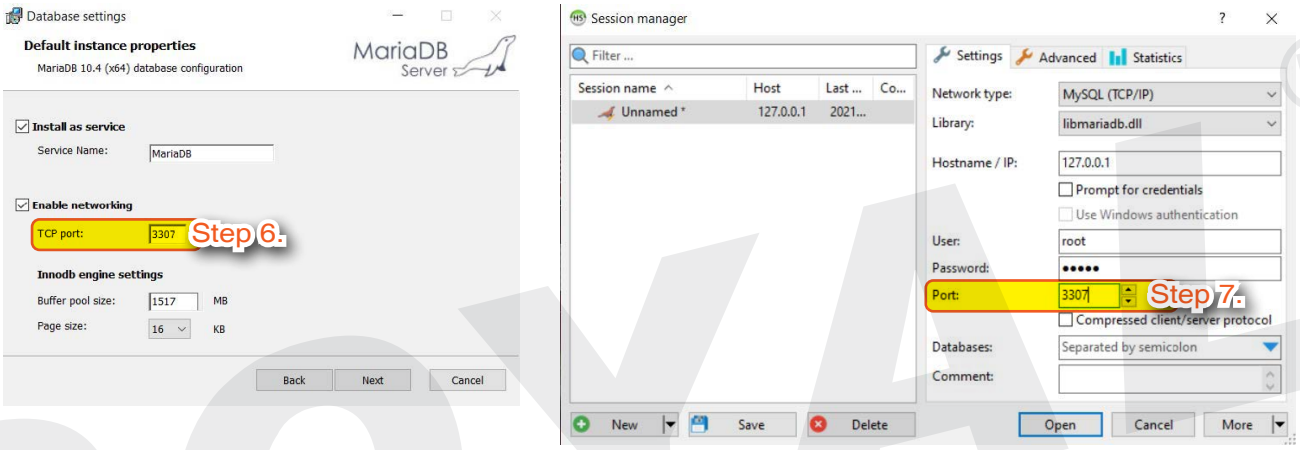


Step 1. Double click to open HeidiSQL
Step 2. Select Network type, if you are newest version of HeidiSQL, select [MySQL (TCP/IP)]
Step 3. Hostname / IP: select 127.0.0.1 for host computer, if enabling TCP-LINK enter server PC's IP address
Step 4. User enter [root]
Step 5. Password enter [admin]
Step 6. Port enter [3306]
Step 7. Select [Open]
Step 8. You will see the table of 701Software UI and data here
Step 9. Select table that you want to look the data of, and then select [Data].

Q7. Could not logged in to HeidiSQL

A7. Make sure the Network type, Hostname/IP, User, and Password has already correct

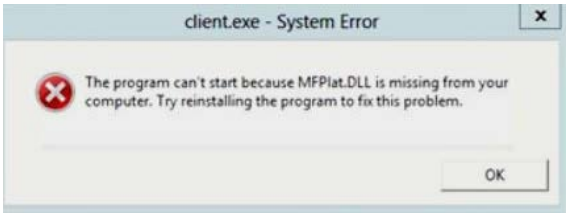




Then there is a possibility that you have download and install W701S software before which using the same port 3306. Then for 701ServerSQL connection to database instead of Port 3306, change it into Port 3307.

Step 1. On the MariaDB program files, right click > select [Uninstall]
Step 2. After finished uninstall MariaDB, right click > Select [Install] again
Step 3. During the installation, Enter [New root password] and [Confirm] as admin. This password is used for connection to database, please **do not forget** this password.
Step 4. Then tick [Enable access from remote machine for 'root' user] and [User UTF8 as default server's character set]
Step 5. Select [Next]
Step 6. Enter TCP Port [3307]
Step 7. Logged in to HeidiSQL and change the Port into [3307].

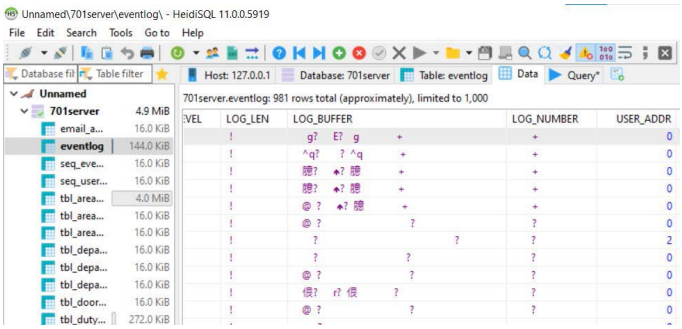
Q8. Installation on Windows Server 2012 show MFPlat.DLL Error when running 701ClientSQL



A9. Required to enable some Media Feature Role in administrator console and download Windows Server Essentials Media Pack in order for 701ClientSQL to running normally.

Q9. Why it shows error input on HeidiSQL?

Example of error:

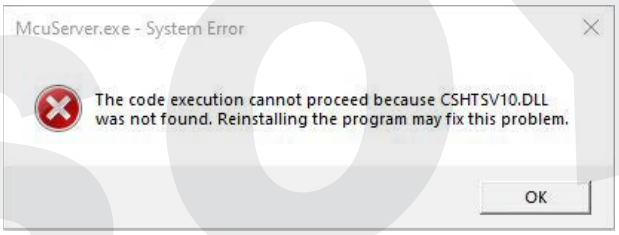


A8. It is because the data shows is under HEX format, please click  to show binary data on text format instead of HEX format.

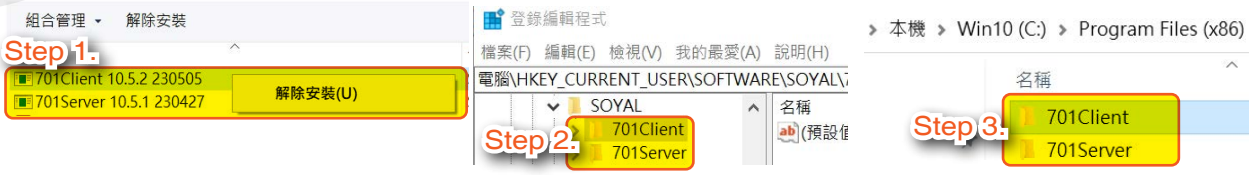
Q10. Installation on Windows 7 in Database Mode show “This application is only supported on Windows 10, Windows Server 2016, or higher.”

A10. Please install MariaDB version 10.4.12 and before, ODBC version 3.1.0, and Redistributable 2010

Q11. When running the software, an error message "CSHTSV10.DLL not found" is displayed.



Please make sure to install Microsoft Visual C++ Redistributable before backing up the data.
※*Backup procedure > Backup and Restore 701ServerSQL and 701ClientSQL



Step 1. Please uninstall the 701Server & 701Client software from the "Programs and Features" section in the Control Panel.

Step 2. Search for "regedit" (Registry Editor) on your computer. Find the SOYAL software path at "Computer\HKEY_CURRENT_USER\SOFTWARE\SOYAL" and delete the 701Server & 701Client folders.

Step 3. Delete the 701Server & 701Client folders from the installation directory. If you have any backup requirements, please make sure to copy them before deleting.

Step 4. Run the installation file for 701ServerSQL/701ClientSQL again to proceed with the software installation.

More Details :

- FAQ : After install and execute 701Server/701Clinet, the screen will appear "Reinstall program" message...

5. Frequently Asked Questions

Q1. Current software version 8.06, could it perform to upgrade directly to Ver. 10.2?

A1: We recommend to do the upgrade step by step, 8.06 > 9.02 > 10.2
First, please do the backup data of 8.06 software and directly update with 9.02 version.
After that follow the instruction on Chapter 1. Please note that Version 8.06 can only be used on Windows XP meanwhile, 701 Software version 10.2 can only be used on Windows 7 or 10.

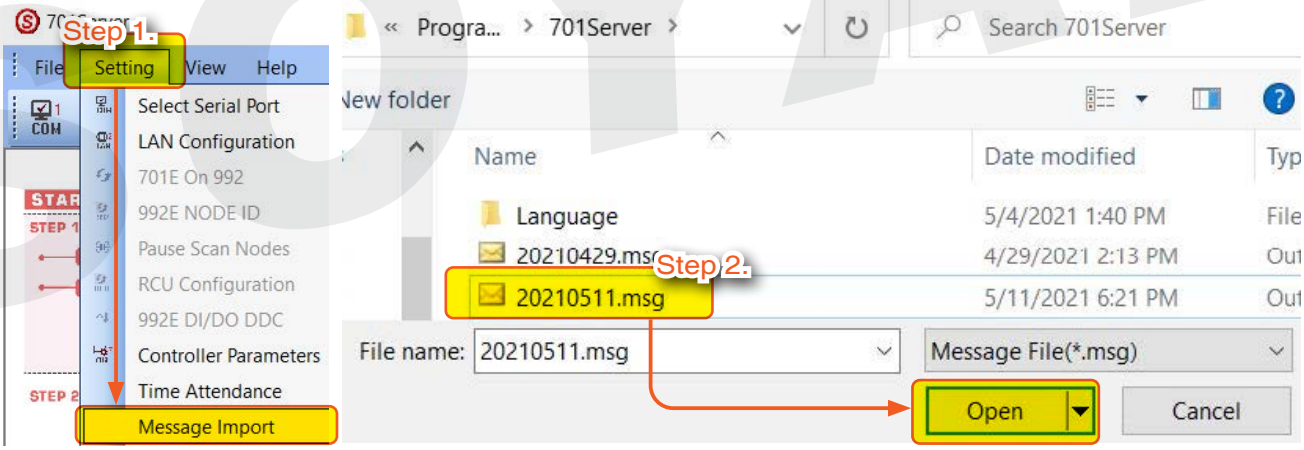
Q2. After updating software to Ver. 10.2 and, is preserving old data under file system is possible?

Yes you can. Please refer to 2.3.3 Back Up DATA

Q3. How to convert old data from file base to database?

File Mode to Database Mode Conversion Original Data Migration:

- Configuration Data: Configuration data from the old file mode will be automatically converted to the database format.
- Access Records (*.msg files): Manual selection of "Message File Import" is required in 701ServerSQL to switch file system data. The operation steps are as follows:



Step 1. Open 701ServerSQL > Select [Setting] > Select [Message Import]
Step 2. Select msg files to import > Select [Open]

Database Mode to File Mode Conversion Data Requires Rebuilding (Avoid if Possible):

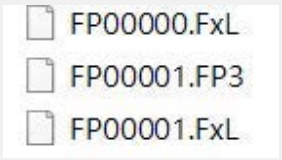
- Configuration Data: Database data does not support file conversion and requires import and rebuilding. Before system conversion, export the old configuration data to text file format. After the system is converted to file format, import the text files one by one to restore the old data.
- Access Records (*.msg files): Old data can only be accessed in the old system.

Files Not Related to Operating System Format:

1.Attendance reports (*.DUT) / 2.Face (*.FxL) / 3. Fingerprint Feature Files (*.FP3/*.FP5)

- Example of Attendance Report DUTY Files

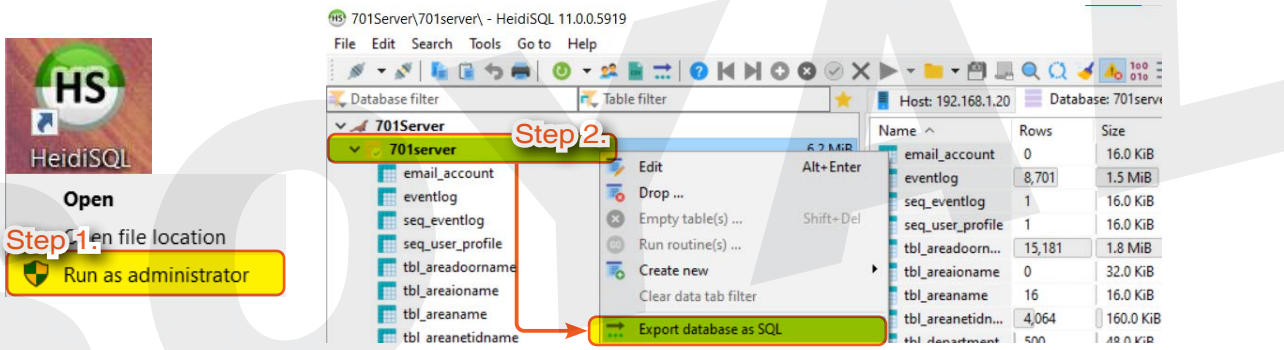
- Face and Fingerprint Feature Files

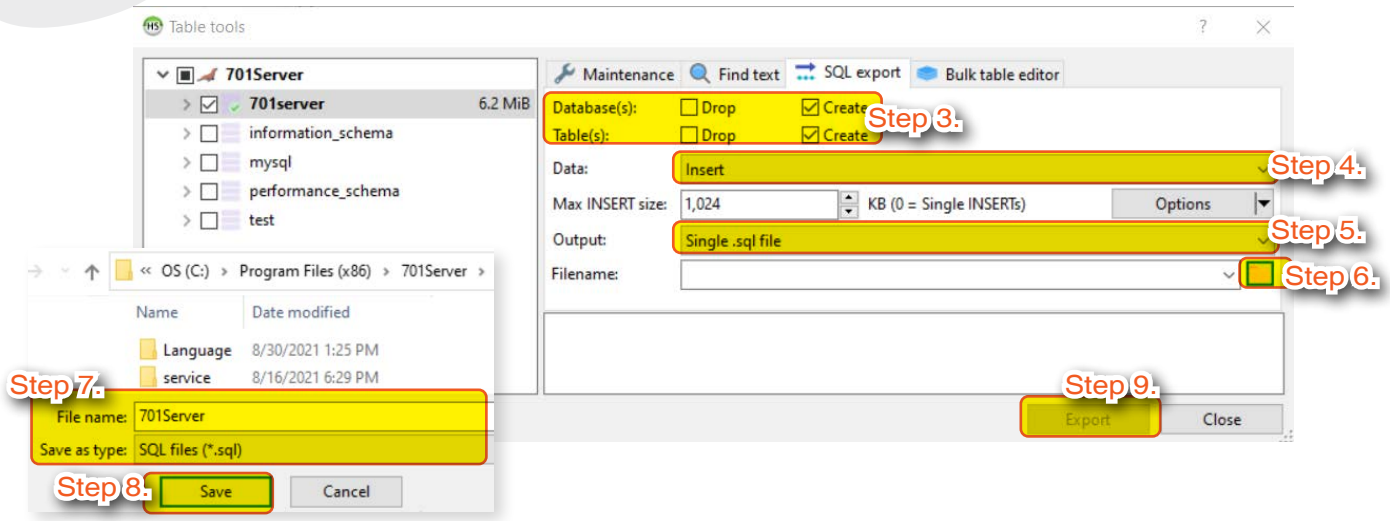


Q4. How to backup data in Database Mode?

Example tools as an example: HeidiSQL

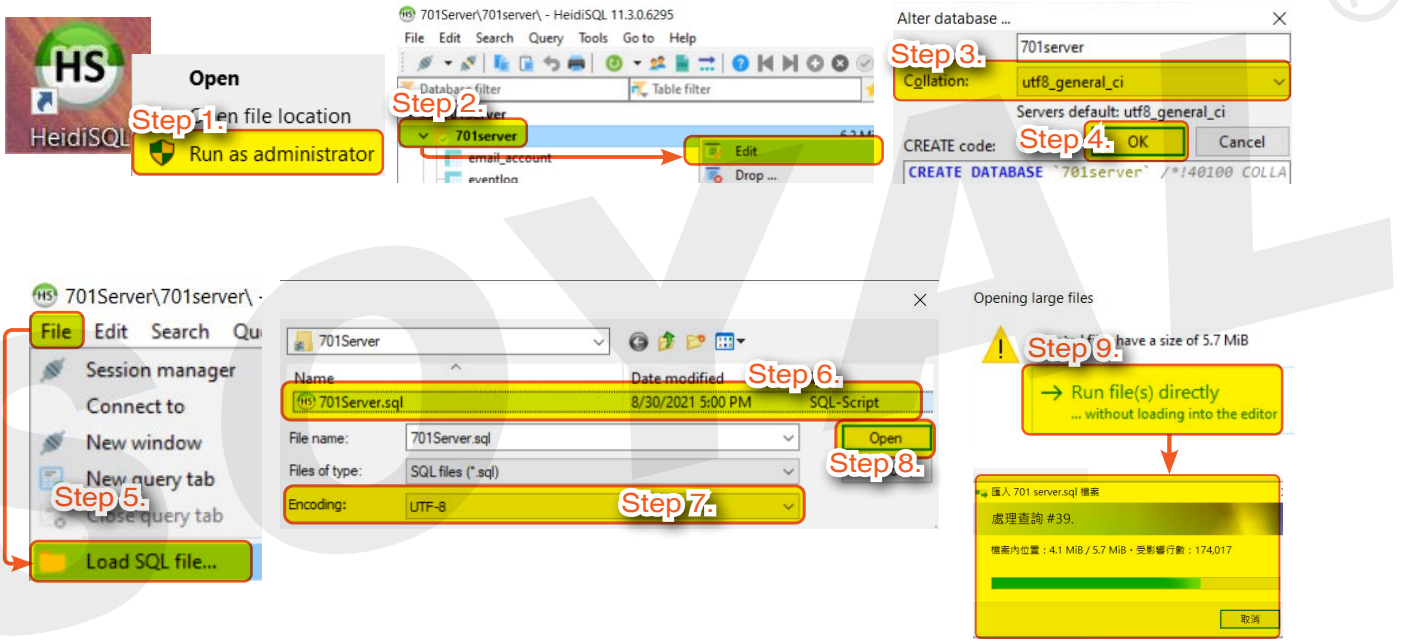
1- Backup Data Step by Step:





Step 1. Run HeidiSQL and open the database by selecting [Run as administrator]
Step 2. Select the database you want to back up, click right and select [Export database as SQL]
Step 3. On Database and Table option, choose [Create] by ticking the box
Step 4. On Data option select [Insert]
Step 5. Output option select [Single .sql file]
Step 6. Select folder path to save file
Step 7. Name the backup file, for example: 701Server; and save under extension file .sql
Step 8. Click [Save]
Step 9. Select [Export] to start exporting data for backup
The backup file has been created on the designated path under format SQL-Script

2- Restore Data Step by Step:



Step 1. Run HeidiSQL and open the database by selecting [Run as administrator]
Step 2. Select the database you want to restore, click right and select [Edit]
Step 3. Select Collation and change into [utf8_general_ci]
Step 4. Select [OK]
Step 5. Select [File] > select [Load SQL File]
Step 6. Select backup file to restore
Step 7. Select Encoding type [UTF-8]
Step 8. Select [Open]
Step 9. Select [Run file(s) directly] and data will be restore back to database

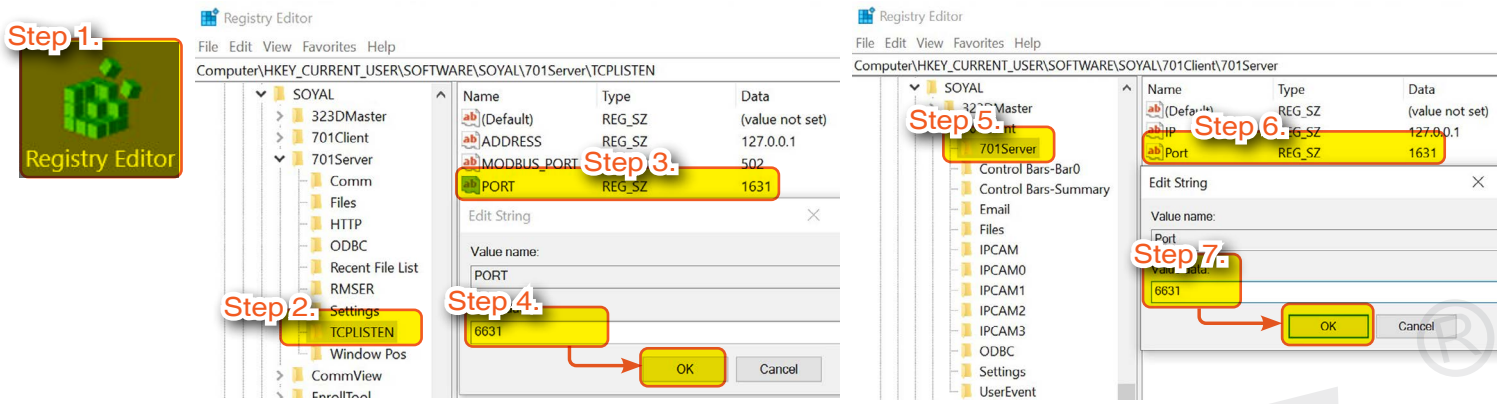
Q5. How to configure or change TCP Port and Modbus Port?

After 701ServerSQL startup, two TCP ports will be opened:

- Soyal Link for 701Client : 1631
- Modbus TCP: 502

To configure or change them, please refer to the following instructions:

1- TCP Port :



Step 1. Run the [Registry Editor]

Step 2. Navigate to the path:Computer\HKEY_CURRENT_USER\Software\SOYAL\701Server\TCPLISTEN

Step 3. Right-click on the PORT and select Modify.

Step 4. Set the string value to [6631] or any other allowed value, and click OK.

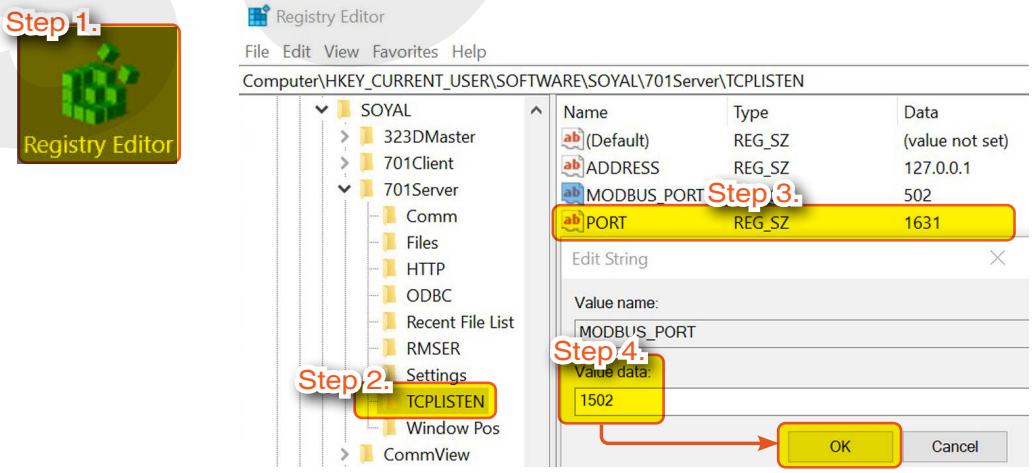
Step 5. Navigate to the path: Computer\HKEY_CURRENT_USER\SOFTWARE\SOYAL\701Client\701Server

Step 6. Right-click on the PORT and select Modify.

Step 7. Set the string value to [6631] or any other allowed value (must be the same as the setting in Step 4), and click OK.

※ Note: The Port settings in Step 4 and Step 7 must be consistent.

2- Modbus Port :



※ Please update the instructions to version 10V5 230531 onwards.

Step 1. Run the [Registry Editor].

Step 2. Navigate to the path: Computer\HKEY_CURRENT_USER\Software\SOYAL\701Server\TCPLISTEN

Step 3. Right-click on MODBUS_PORT and select Modify.

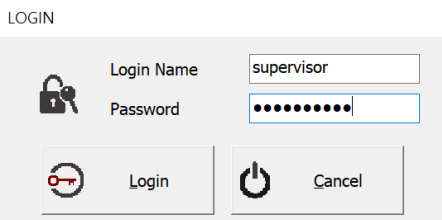
Step 4. Set the string value to [1502] or any other allowed value, and click OK.

NOTE

- If the MODBUS_PORT entry is missing in the Registry Editor even after updating 701ServerSQL to version 10V5 230531 onwards, please restart 701ServerSQL and press F5 to refresh the Registry Editor screen.

6. 701ServerSQL Basic Concept

6.1 Log in 701ServerSQL

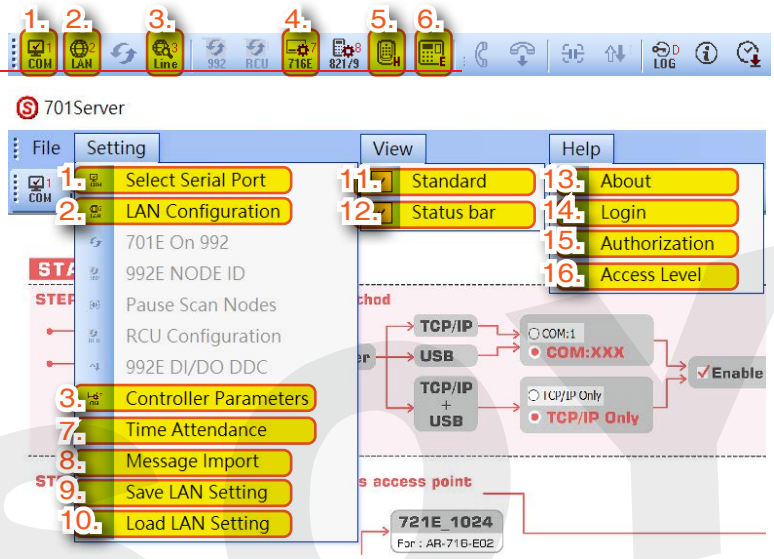


To enhance the security, please change the password and user permission immediately after first time logging in.
When log in 701Server for the first time, please enter the default Log in Name and password

Login Name: supervisor
Password: supervisor

More Details : ● FAQ : If I forgot password for 701Server and 701Clietnt , may I get the password back?

6.2 Main Menu & Toolbar



Setting:

1. Select Serial Port:
   - Select a serial port (COM port or TCP/IP) that can link the PC and controllers.
   - Setting of Local TCP-LINK IP Address and Port]
   - Start or stop polling

2. LAN Configuraton:
   Set the Area, Node ID, model no. type, IP Address and Port (for IP-Based controller), and Net-Point Name (editable) of the controller to help achieve the correct connection and data transmission.

3. Controller On/Off Line:
   Controller connection status, including access controller direct wiring (Node) and/or bypass wiring control panel (Node) and controller beneath (SubNode)

4. Controller Parameters:
   Set the Node ID and related parameters of AR-716-E18

5. Parameter Setting for Home Series (H Series) Controller

6. Parameter Setting for Enterprise Series (E Series) Controller and Control Panel AR-716-E16

7. Time Attendance:
   Set Time Attendance setting and user capacity of the system

8. Message Import:
   Import other message files (.msg file)

9. Save LAN Setting:
   Save and back-up LAN Configuration setting

10. Load LAN Setting:
    Load saved LAN Configuration setting

View:

11. Standard:
    Show or hide tool bar
    (tick means show toolbar)

12. Status bar:
    Show or hide status bar (tick means show status bar)

Help:

13. About:
    Check 701ServerSQL version and mode (file system file or database system)

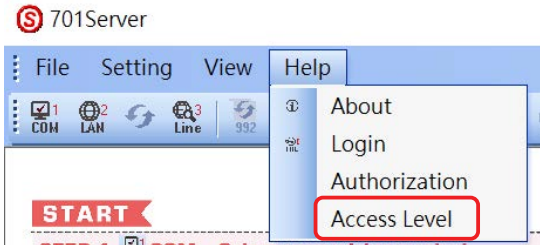
14. Login: re-log in or change log in user

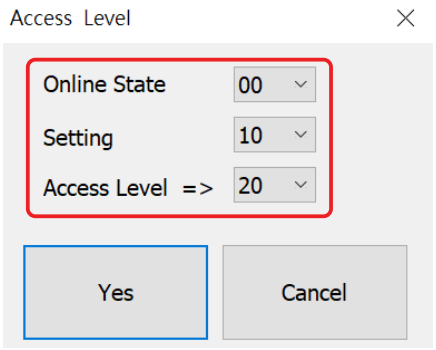
15. Authorization:
    Operator authorization edit, to change log in user Login Name and Password, for authorized user to modify user's access level

16. Access Level:
    Setting of access level for user that assigned below or above specified access level function such as view or modify setting of:
    1. controller online status (LINE)
    2. COM and LAN setting, controller parameter setting
    3. Access Level setting

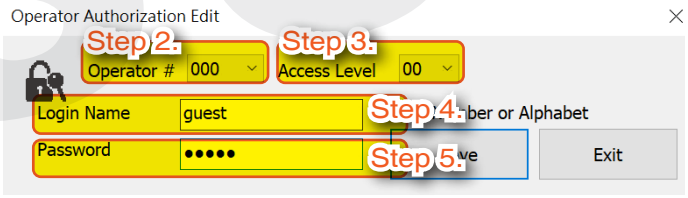
More Details : ● FAQ :How to revise the 701Software Toolbars?

6.3 Authorization & Access Level

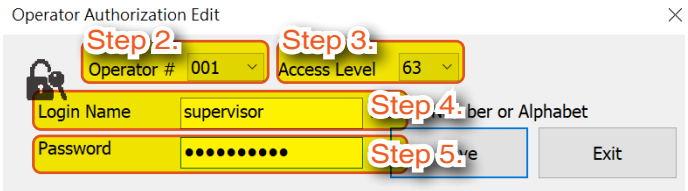




Only highest Access Level Level 63 has permission to create new and edit user Access Level. User with Access Level below 63(0-62) can only managed to change their own username and password.



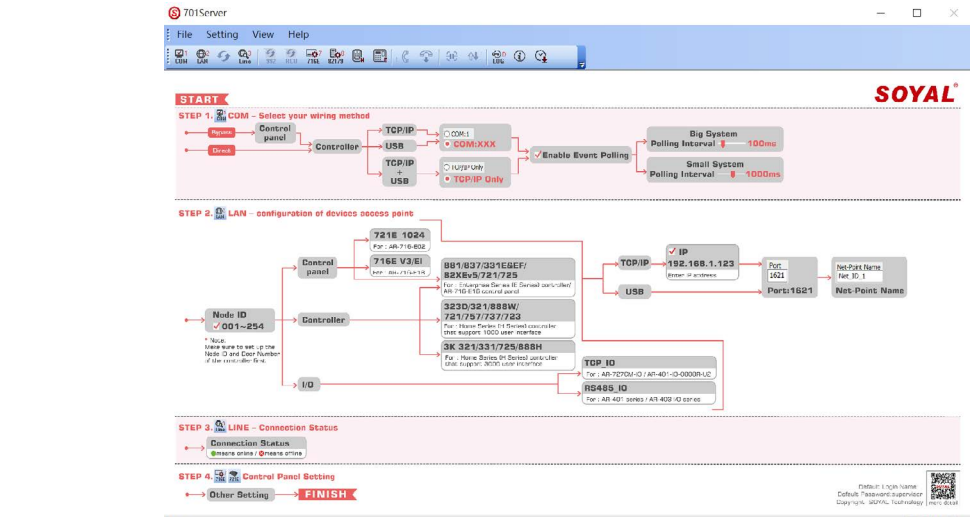
Guest Access Level
Can only view the Controller On/Off Line, Time Attendance, Message Import, Save LAN Setting, and Load LAN Setting

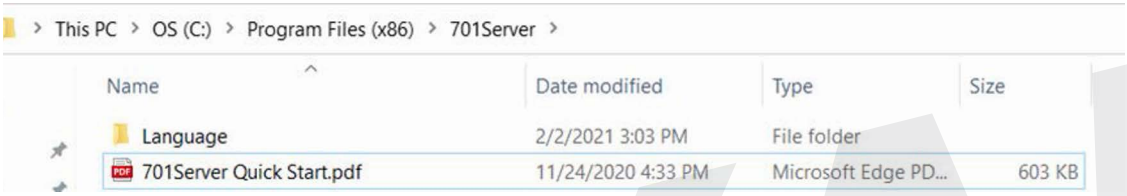


Supervisor (default) Access Level:
All function

Step 1. Select 'Authorization'
Step 2. Operator #: 0-119 operators for editing their access level, login name and password.
Step 3. Access Level: 0-63 access level for editing. 63 is the highest authority.
Step 4. Login Name: login name can have up to a total of 18 English letters or 9 Chinese characters.
Step 5. Password: password can have up to a total of 18 English letters or 9 Chinese characters.

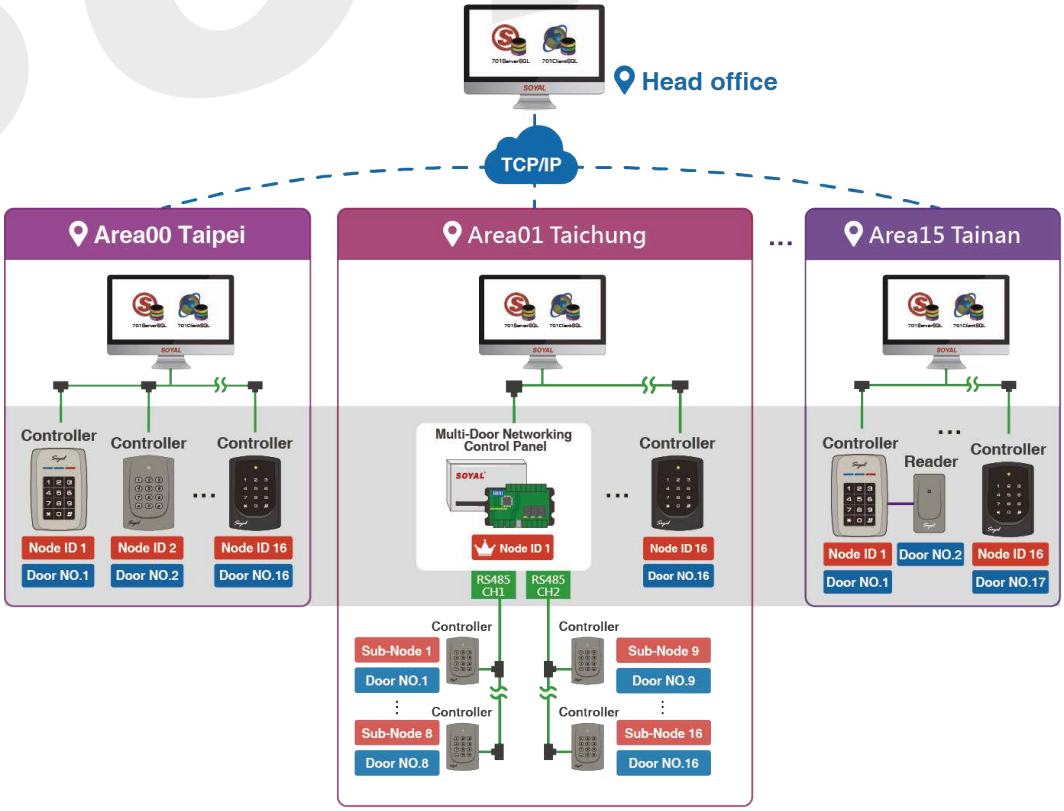
6.4 701ServerSQL Base Map





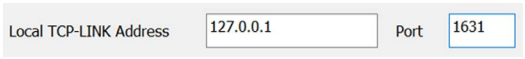
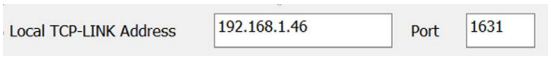
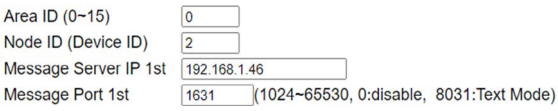
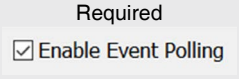
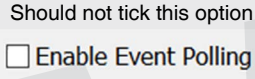
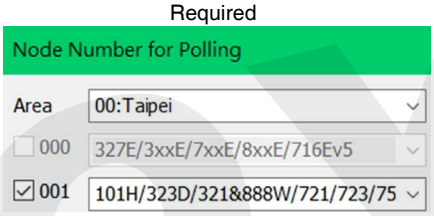
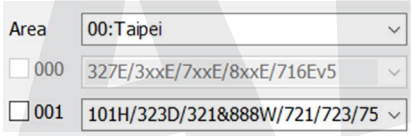
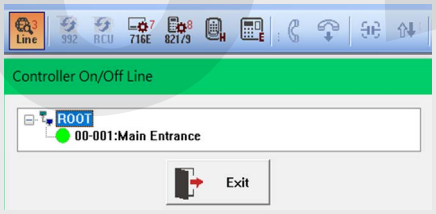
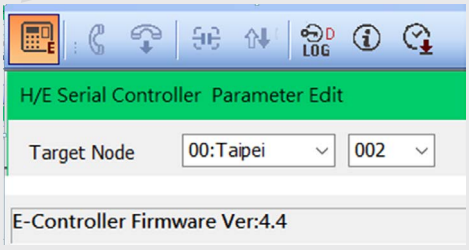
When first logged in into 701ServerSQL, the base map will show 701ServerSQL quick guide. For more detail please refer to the PDF file in the installation path C:\Program Files (x86)\701ServerSQL

6.5 Area > Node ID > Door Number

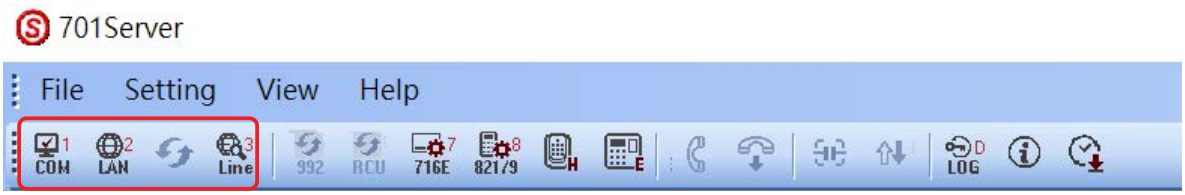


7. 701ServerSQL Networking Architecture

There are slight differences in between setting under Passive Polling Mode and Active Communication Mode (Non-Polling), other than that all of the setting is the same.

Difference	Passive Polling Mode	Active Communication Mode (Non-Polling)
Must set TCP-Link Setting	Does not required, only required when software system under database system and enabling Multi-Client mode 	Required, the setting is to paired 701ServerSQL TCP-Link IP Address and Port setting equivalent to Hardware Message Server setting - 701ServerSQL Setting  - Hardware Message Server point to 701ServerSQL as main server 
Enable Event Polling	Required 	Should not tick this option 
Tick connected Node ID	Required 	Should not tick Node ID of the connected software 
Checking Connection Status	Via 3 LINE menubar 	Via E Series Controller Parameter Setting 

7.1 Polling Mode Setting



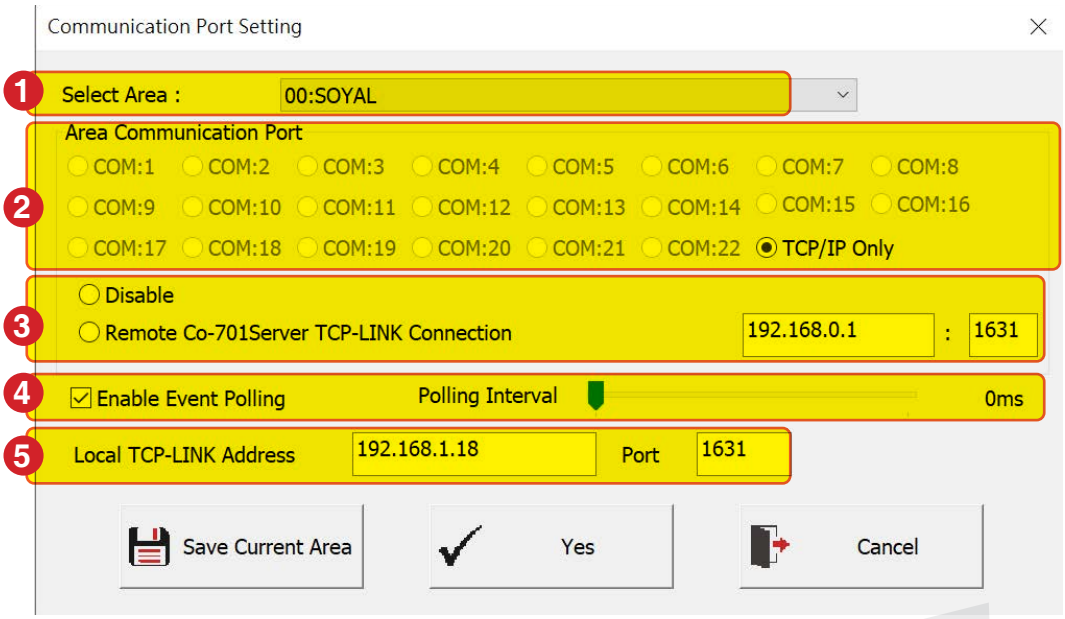
3 steps to setting up the hardware to the software:

1. COM: Serial Port Communication

2. LAN: Hardware Setting

3. LINE: Connection Status

7.1.1 COM: Serial Port Communication

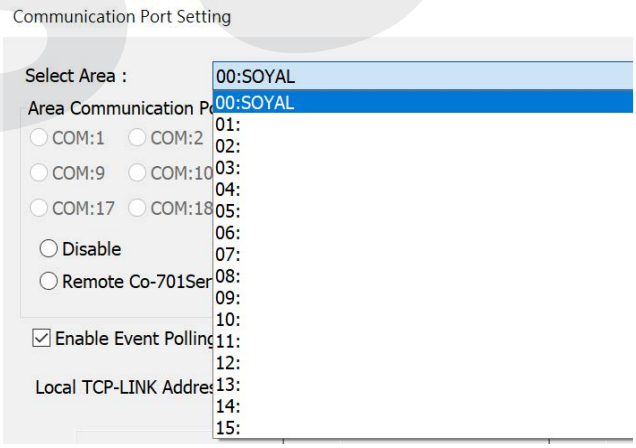


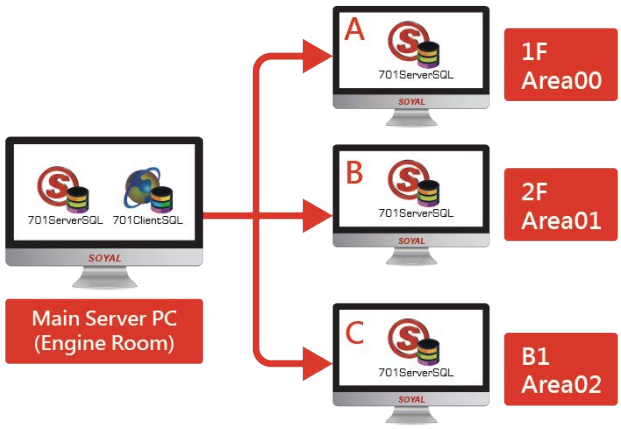
1. Select Area
2. Select communication setting
3. Remote Co-701Server Setting
4. Polling Setting
5. 701ServerSQL TCP-LINK Setting

More Details :

- FAQ : Why could not see Event Log while 701Server Setting is correct?

1 Select Area





Area selection range: 00-15, total 16 Areas (upgrade to 10.2 version all of the controller will automatically classified to Area00)

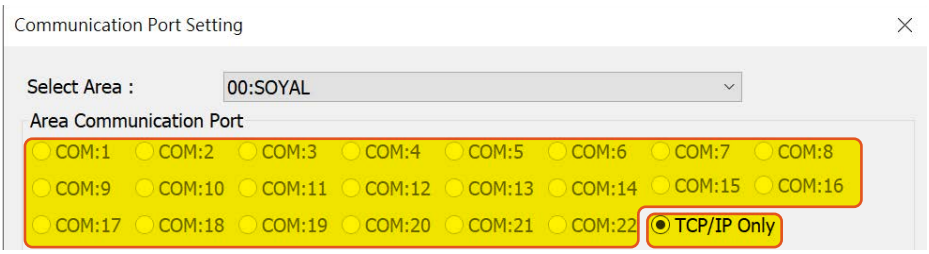
※ Area Name can be changed in LAN Setting, details referring to page 4-1-39 Select and rename Area

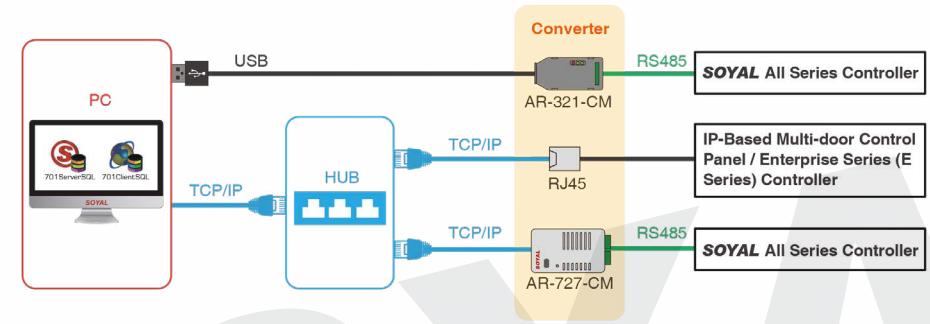
2 Select communication setting

When selecting communication setting, it is divided into two method: Local Area (Single-Server) and Remote Area (setting required software under Database Mode and suitable for Multi-Server system).

- Local Area

Communication port come from COM Port and/or TCP/IP





1. COM:1 - COM:22 : for hardware wiring via USB (Via AR-321-CM*; RS485 to USB Conveter) OR for system with two way wiring both USB and TCP/IP (according to the USB COM Port)
2. TCP/IP Only: Via Ethernet cable or AR-727-CM, RS485 to Ethernet Converter

NOTE

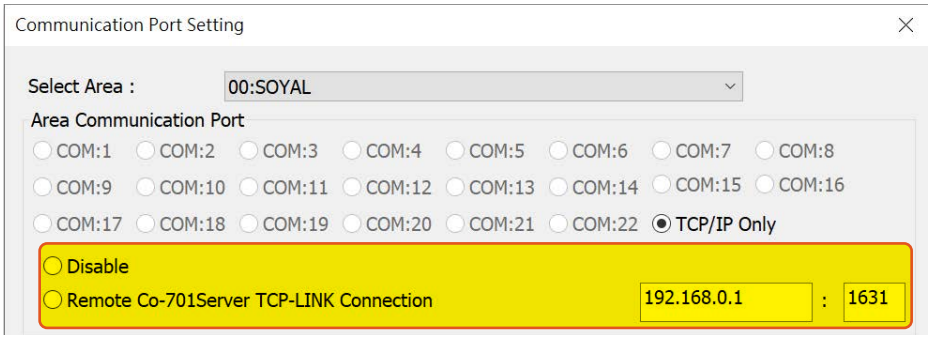
*AR-321-CM required USB driver installation. To check what is your AR-321CM COM port, right click on Windows ICON >> Device Manager

>> Ports (COM & LPT) >> Prolific USB-to-Serial Comm Port (COMXX) is your COM Port for AR-321CM.

More Details :

- FAQ : How many controllers can be connected to a converter, or Is necessary to use one converter for each controller?
- FAQ : Is it possible to use TCP/IP and RS485 for connection and with 701Server at same time?

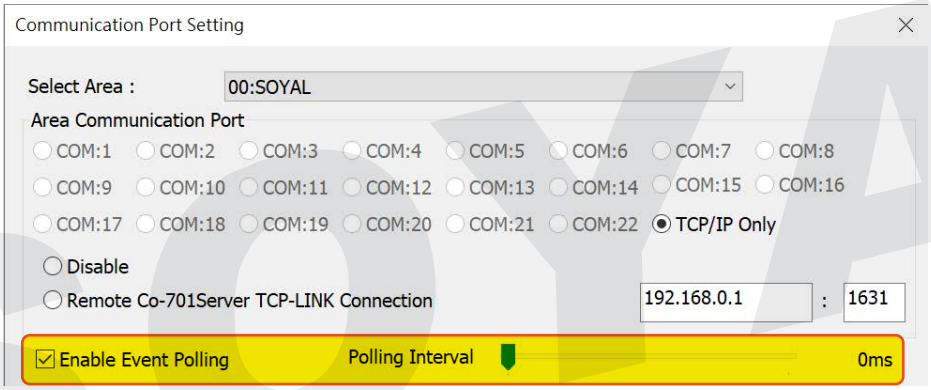
3 Remote Co-701Server Setting



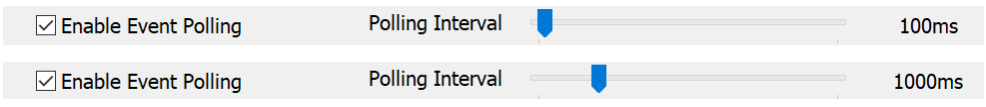
1. Disable (default): if there is no remote Area, the setting is disable
2. If the system is enabling Multi-Server, fill in the remote Area's Server IP Address and Port

4 Polling Setting

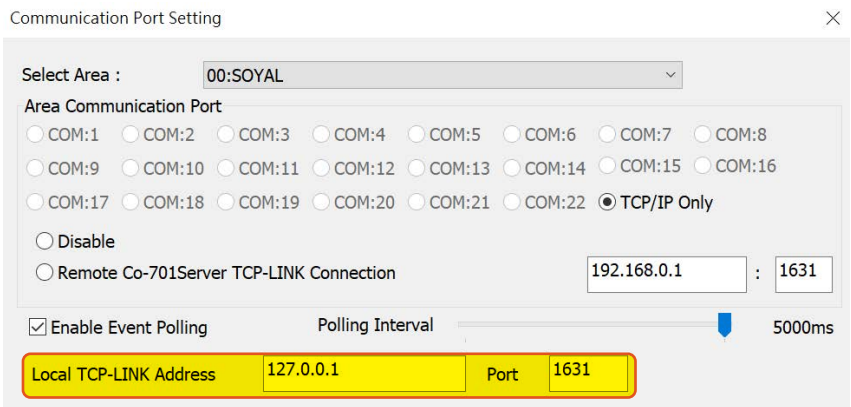
When selecting communication setting, it is divided into two method: Local Area (Single-Server) and Remote Area (setting required software under Database Mode and suitable for Multi-Server system).



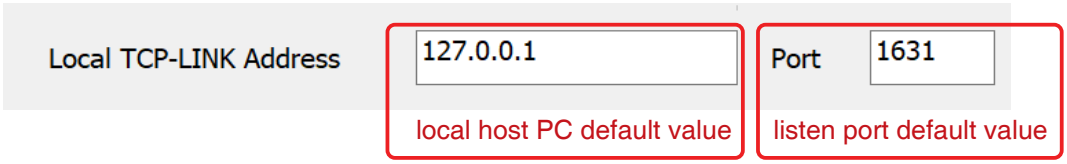
- Enable Event Polling:
  by ticking Enable Event Polling will polling all real time transaction log on 701 Client and untick it will stop the polling
- Polling Interval:
  Polling Interval is defining interval of event polling is received by the software. For small system we recommend to set it to 1000ms (polling per min.) for bigger system, recommend to set it to 100ms.



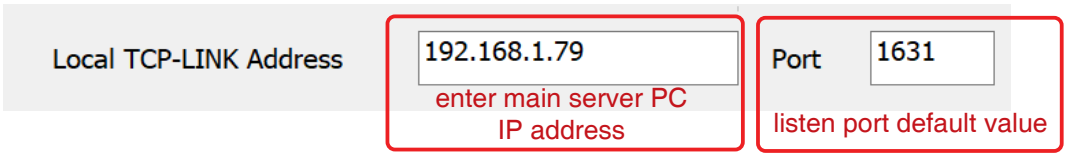
5 701ServerSQL TCP-LINK Setting



• Default Setting:



• Under Database Mode and enable TCP-LINK connection to Multi-Server and Multi-Client required setting.

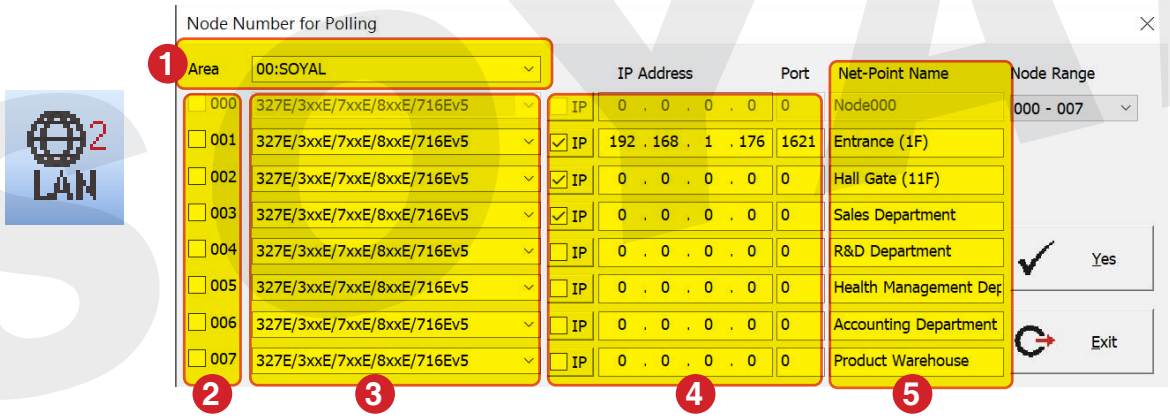


Refer to Installation Guide Chapter 3. Download and Install 701Software Part 6-Setting TCP-LINK Server and TCP-Link Client

More Details :

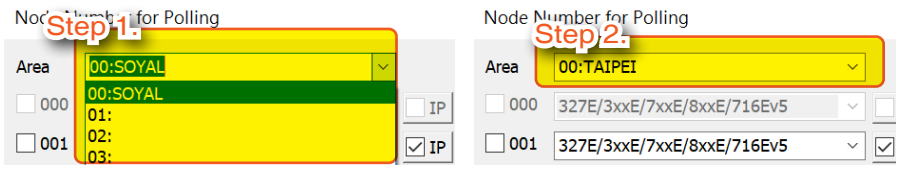
- FAQ : Sometimes the selected Com Port Number always change , how to fix it?

7.1.2 LAN: Specify Device Connection Settings



1. Select and rename Area
2. Hardware Node ID
3. Hardware type
4. TCP/IP configuration
5. Net-Point Name

1 Select and rename Area

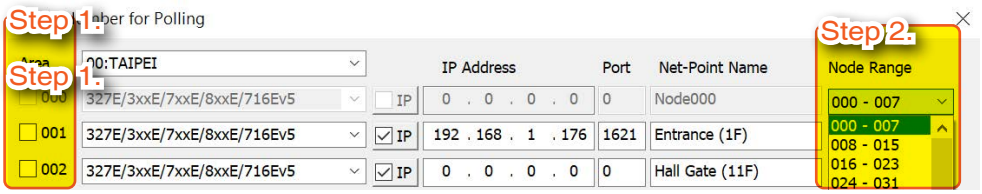


Step 1. Select Area to be set

Step 2. Rename the Area if required

(Software will input the area number automatically, ex. 00:XXX /01:XXX… and etc.)

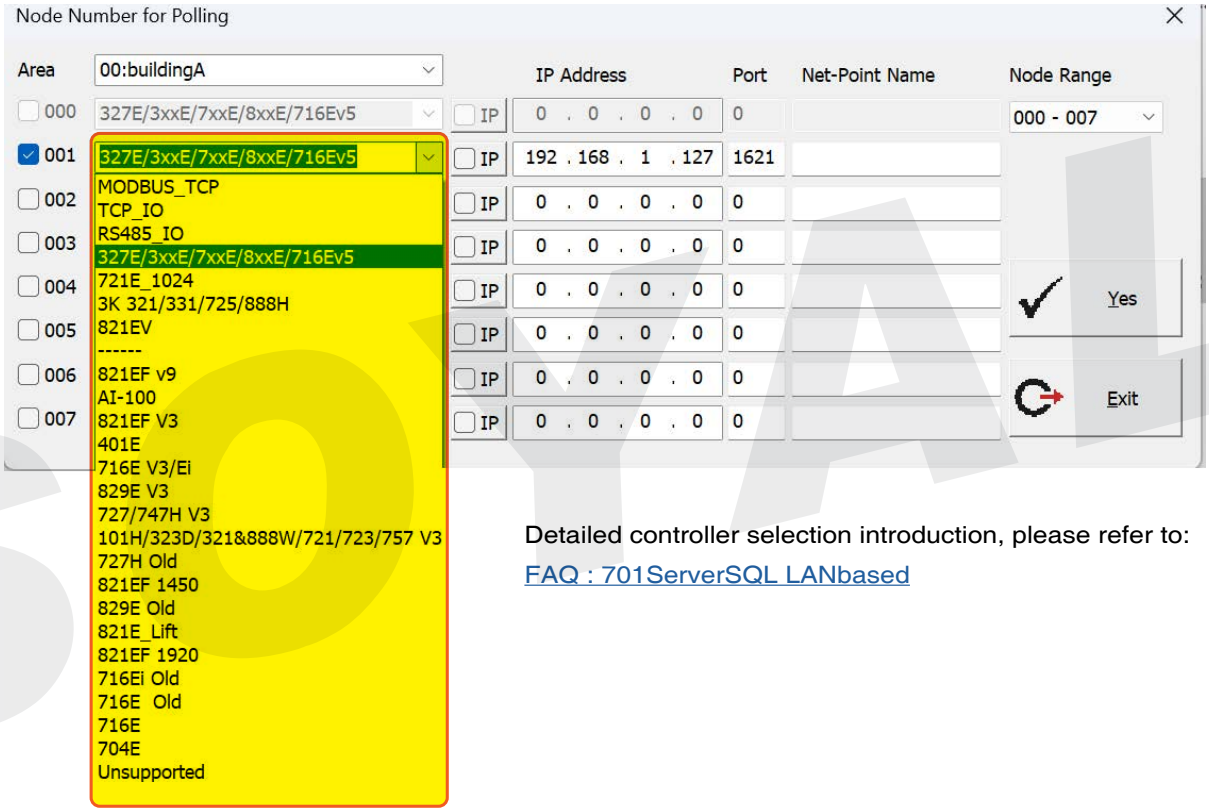
2 Hardware Node ID



Step 1. Select Node ID of the Hardware

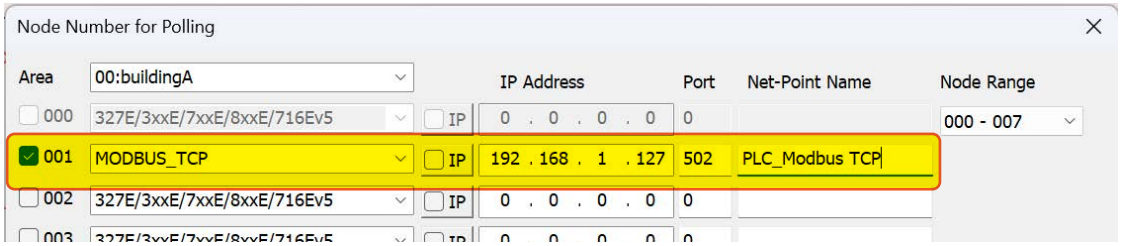
Step 2. Node Range: Each page contains 7 Node ID, to go to the other Node ID range, select Node Range

3 Hardware type

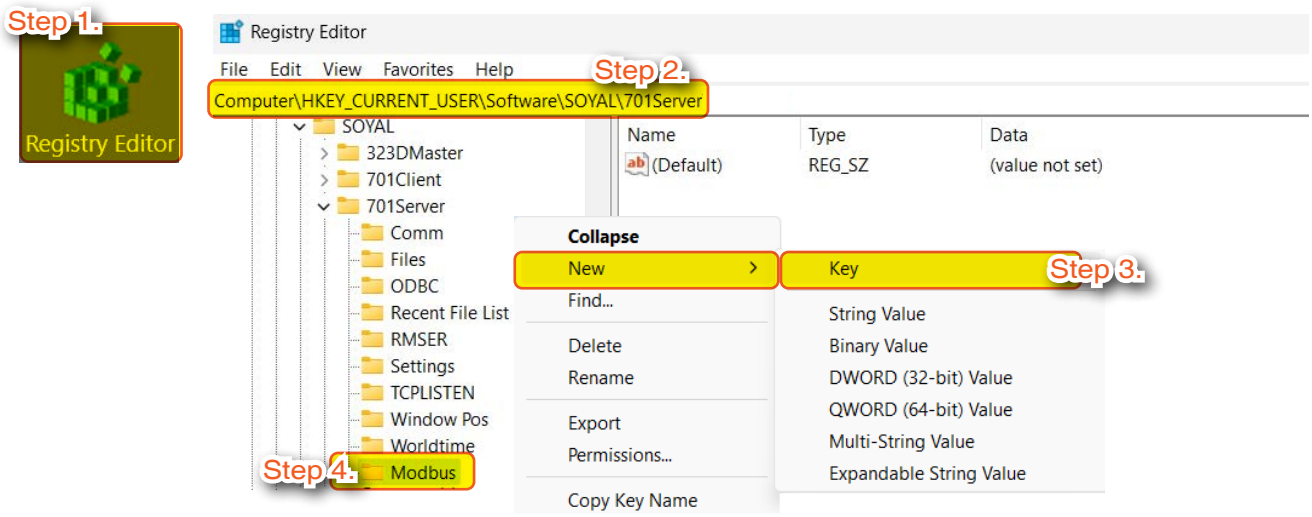


Detailed controller selection introduction, please refer to:
FAQ : 701ServerSQL LANbased

【 Modbus_ TCP 】 : Used for Modbus devices, enter Port 502, and you need to set it in Regedit. The settings are as follows:



Example: Device Area: 00, Station Number: 001, Digital Input/Output: 16 DI/8 DO

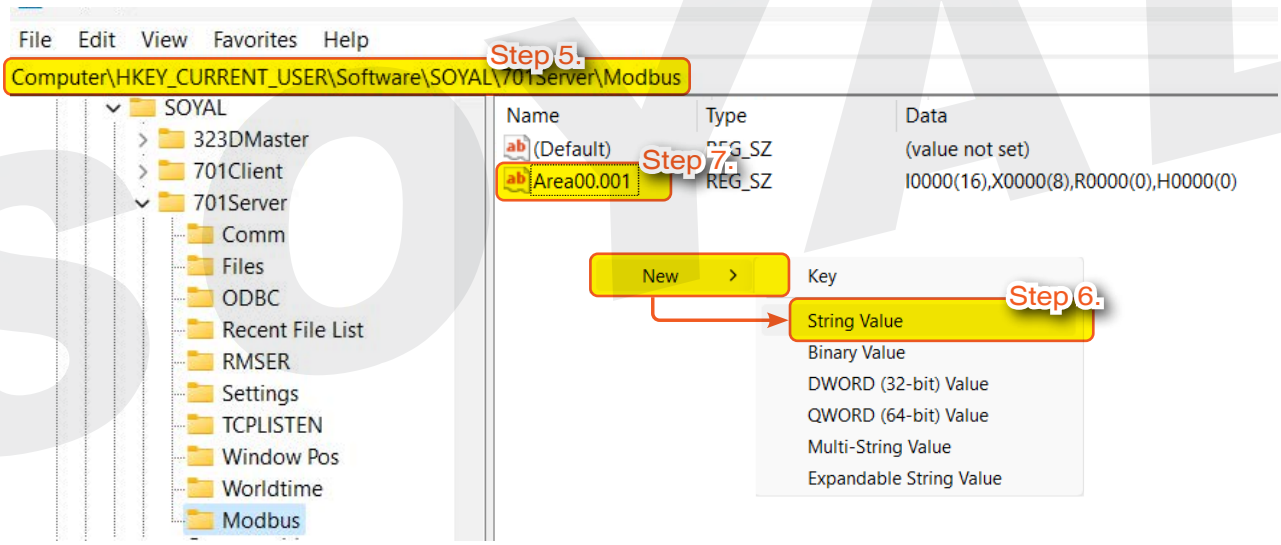


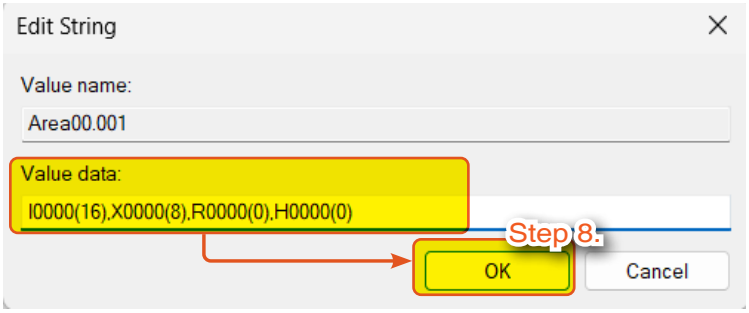
Step 1. Go to Registry Editor

Step 2. Navigate to the path: Computer\HKEY_CURRENT_USER\Software\SOYAL\701Server

Step 3. Right-click and select New -> Key.

Step 4. Enter "Modbus" to create the Modbus folder.





Step 5. Navigate to the path: Computer\HKEY_CURRENT_USER\Software\SOYAL\701Server\Modbus

Step 6. Right-click and select New -> String Value

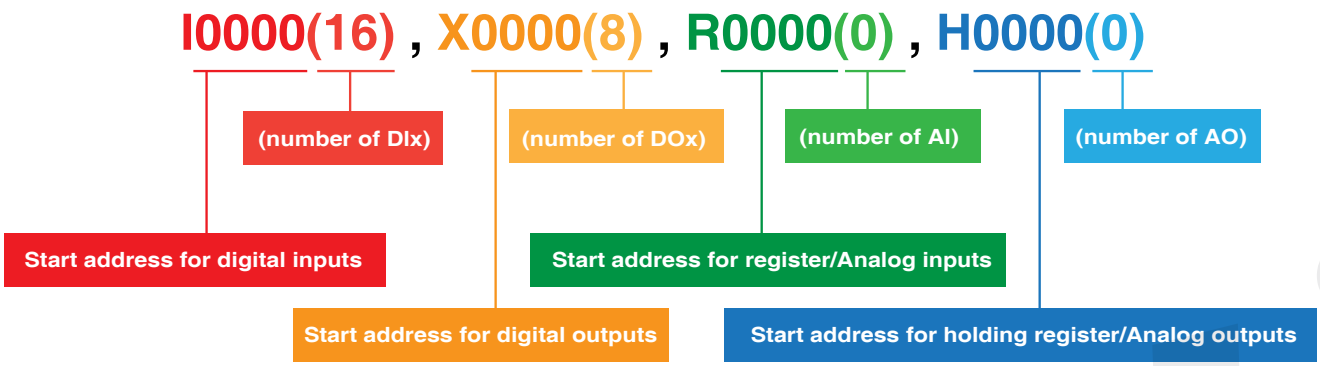
Step 7. Enter the name "Area00.001" (it is recommended to use the area and station number as the name).

Step 8. Enter the numerical data (refer to the data format definition in the following figure), and click OK to complete the setup.

The data format for numerical values is defined as follows:

- I: Start address for digital inputs (number of DIx)
- X: Start address for digital outputs (number of DOx)
- R: Start address for register/Analog inputs (number of AI)
- H: Start address for holding register/Analog outputs (number of AO)

※Note: Address calculation is in decimal.



701ServerSQL LANbased summary of options

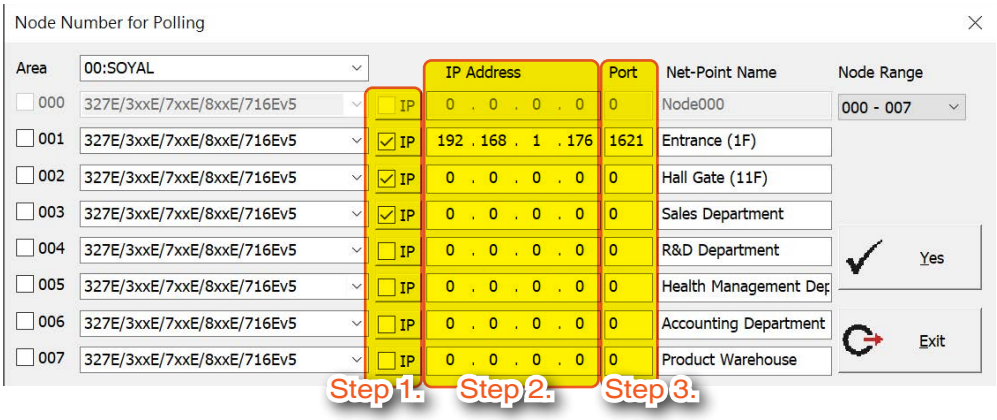
No.	LAN Model No. 10.2 version and before	LAN Model No. 10.2 version and after	Correspondent Hardware Model No.	Communication Interface	Port	Active Communication Mode (Non-Polling)
1.	Modbus_TCP	Modbus_TCP	PLC Modbus TCP	Modbus	502	X
2.	TCP_IO	TCP_IO	IP Based I/O Module - AR-727-CM-IO- 0804M - AR-401-PLC-0808R - AR-401-PLC-1616R NOTE	TCP/IP	1601	YES (required additional setting of Message Server IP point to 701ServerSQL's Local TCP Link Address & TCP Port)
3.	RS485_IO	RS485_IO	RS485 I/O Module - AR-401-IO-0016R - AR-401-IO-1709R - AR-403-IO Series	RS485 (via AR-321-CM converter)	1601	X
4.	881/837 /331E&EF /82xEv5/721 /725Ev2/727 /327Hv5	327E/3xxE/ 7xxE/8xxE/ 716Ev5	All Enterprise Series Controller (E Series) : AR-725-E / AR-331E&EF / AR-837-E&EF / AR-727-E / AR-327-E	TCP/IP (if onboard TCP/IP module)	1621	YES (required additional setting of Message Server IP point to 701ServerSQL's Local TCP Link Address & TCP Port)
			Control Panel -AR-716-E16 NOTE	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
			Enterprise Series Controller(Old Version): AR-881-EF / AR-829-EV5	RS485 (via AR-321-CM converter)		X
5.	721E_1024	721E_1024	Dual WG control panel - AR-716-E02	RS485 (via AR-321-CM converter)		X

No.	LAN Model No. 10.2 version and before	LAN Model No. 10.2 version and after	Correspondent Hardware Model No.	Communication Interface	Port	Active Communication Mode (Non-Polling)
6.	3K 321/331/ 725/888H	3K 321/331/ 725/888H	Home Series (H Series) controller that support 3000 user interface AR-321H / AR-331-H /AR-725-H / AR-888-H	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
				RS485 (via AR-321-CM converter)		X
7.	821EV	821EV	Controller: AR-821-EV	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
				RS485 (via AR-321-CM converter)		X
8.	821EF V9	821EF V9	Controller: AR-821-EF	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
				RS485 (via AR-321-CM converter)		X
9.	716E V3/Ei	716E V3/Ei	Control Panel: AR-716-E18	TCP/IP	1621	
				RS485		X
10.	829E V3	829E V3	Controller: AR-829-H	RS485 (via AR-321-CM converter)		X
11.	727/747 H V3	727/747 H V3	Controller AR-327-H / AR-727-H / AR-747-H	RS485 (via AR-321-CM converter)		X
12.	323D/321&888W /721/757/737 /723/101H V3	101H/323D /321&888W /721/723/757	Home Series (H Series) controller that support 1000 user interface: AR-101-H / AR-323D / AR-888-W / AR-721-H / AR-723-H / AR-757-H	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
			Controller (Old version): AR-757-H / AR-321W	RS485 (via AR-321-CM converter)		X
13.	829E Old	829E Old	Controller (Old version): AR-829-E	RS485 (via AR-321-CM converter)		X

NOTE

To display fire alarm door release messages from AR-727-CM-IO or AR-716-E16 in 701ClientSQL, you need to set the IP and Port of AR-727-CM-IO or AR-716-E16 in the LAN settings. For detailed configuration instructions, please refer to
→AR-727-CM HTTP Server Manual

4 TCP/IP configuration (Skip this step connection via COM)



This step is necessary for controller wired with Ethernet. Skip this step and left it untick and blank if your controller is wired via USB instead.

Step 1. Tick the IP

Step 2. Input the IP address of the controller (default IP address is 192.168.1.127)

Step 3. Each controller default value is 1621, thus you need to type 1621 in the PORT field.
Other case that your controller PORT is not 1621:
If you are wiring through AR-727CM via CH2, the PORT is 1623.
If your hardware is I/O module to control I/O enter 1601.

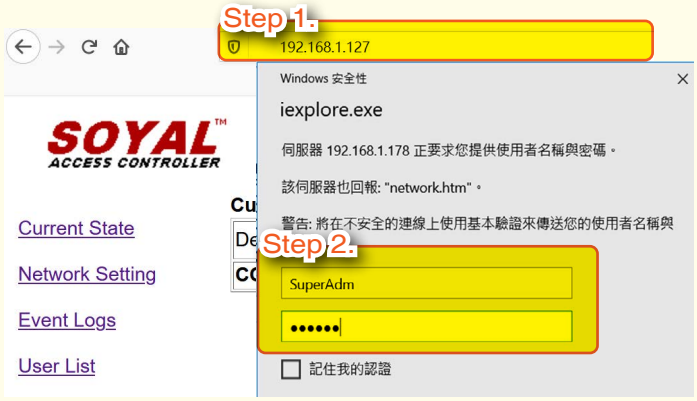
More Details :

- FAQ : How to copy 701Server LAN Setting from Computer A to Computer B?
- FAQ : How to add new model option for selecting under 701Server LAN Base setting?

NOTE

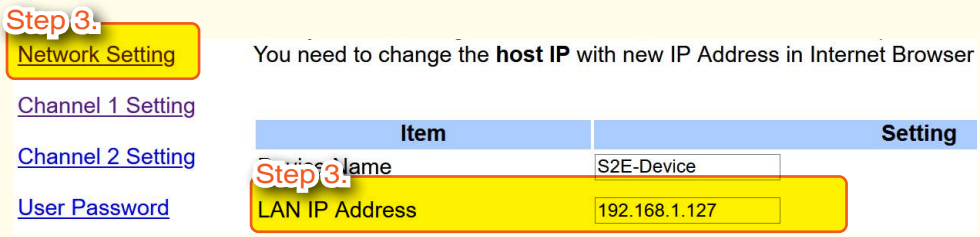
How to change default IP Address to designated IP Address?

• Enterprise (E Series) Controller :
Default IP Address: 192.168.1.127



Step 1. Confirm the hardware is TCP/IP Module flash TX/RX (green/orange LED), indicated the TCP/IP module works then enter default IP Address 192.168.1.127
*If the PC network segment is different with hardware, please set the PC network segment to have the same value with hardware.

Step 2. Select [Network Setting] and enter log in account.
Default value: Account: SuperAdm / Password: 721568



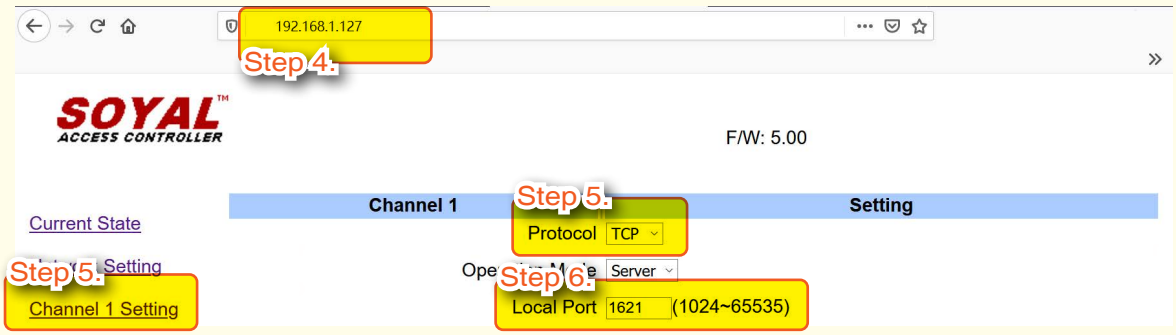
Step 3. After Modifying the IP address, click [Update].
Important: please complete the modification within 15 seconds

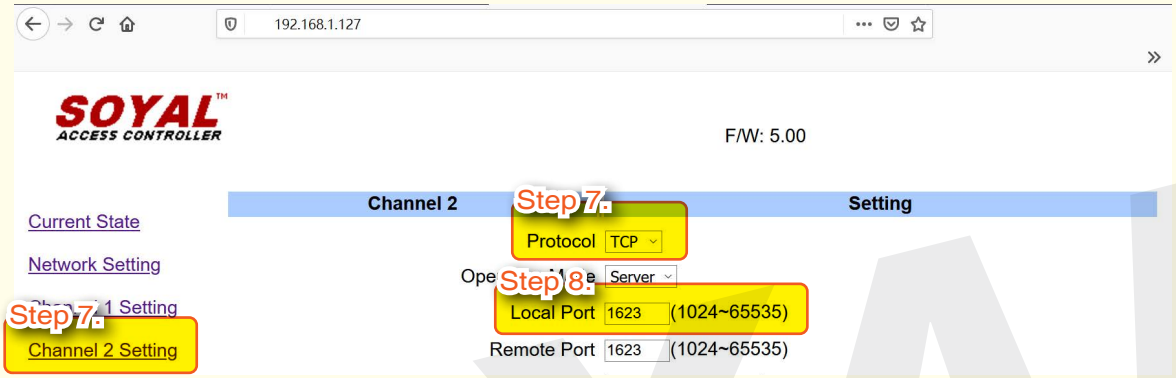
• AR-727-CM :
Default IP Address: 192.168.1.127

Step 1. Confirm the hardware is TCP/IP Module flash TX/RX (green/orange LED), indicated the TCP/IP module works then enter default IP Address 192.168.1.127
*If the PC network segment is different with hardware, please set the PC network segment to have the same value with hardware.

Step 2. Select [Network Setting] and enter log in account.
Default value: Account: SuperAdm / Password: 721568

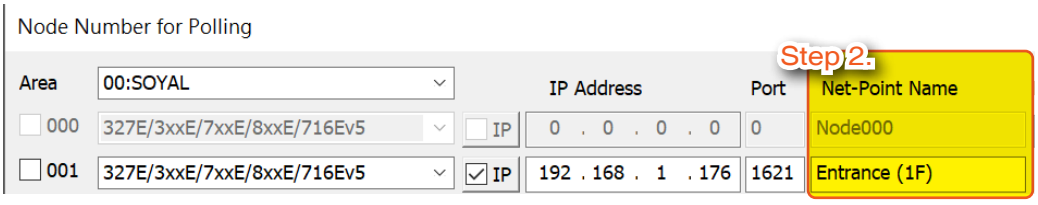
Step 3. After Modifying the IP address, click [Update].
Important: please complete the modification within 15 seconds





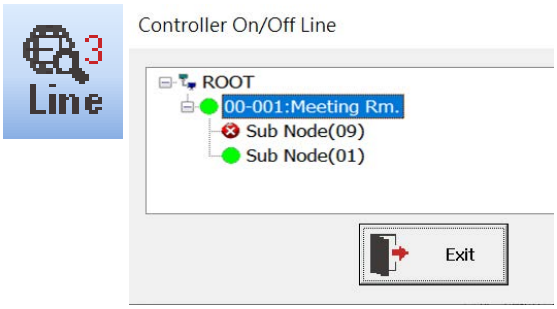
Step 4. Enter the new IP Address on the browser
Step 5. Select [Channel 1 Setting] > on the Protocol field select as [TCP]
Step 6. [Local Port] default setting is 1621, after completed the setting click [Update]
Step 7. Select [Channel 2 Setting] > on the Protocol field select as [TCP]
Step 8. [Local Port] default setting is 1623, after completed the setting click [Update]

5 Net-Point Name



Step 1. Change the Net-Point Name to desire name to easily distinguish each hardware and position.

7.1.3 LINE: Connection Status



Hardware Indicator:

00 : Area

01 : Node ID

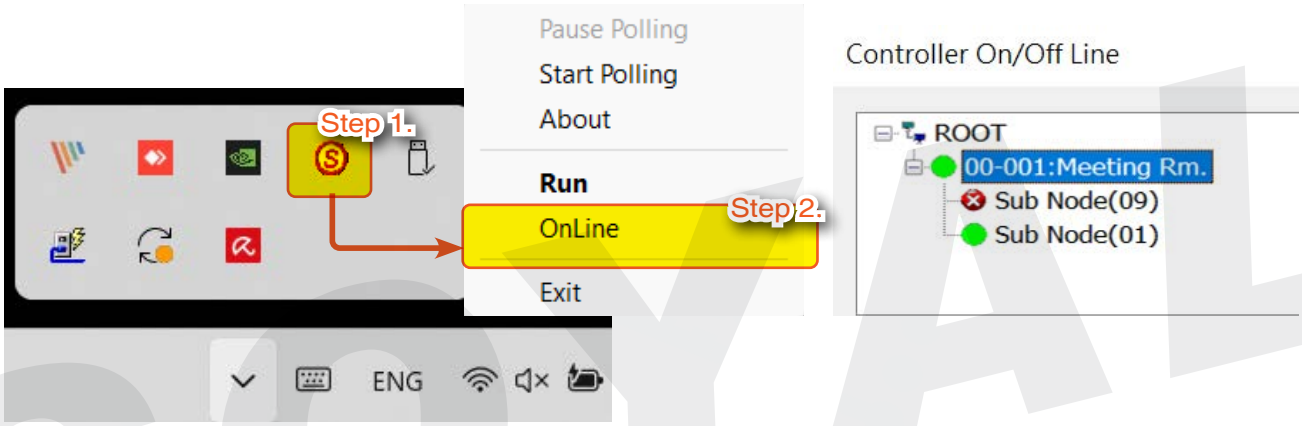
Sub Node : Control Panel and Access Controller Connection Status

Status Indicator:

X : Offline

Green : Online

You can check the connection status without logging into the software:



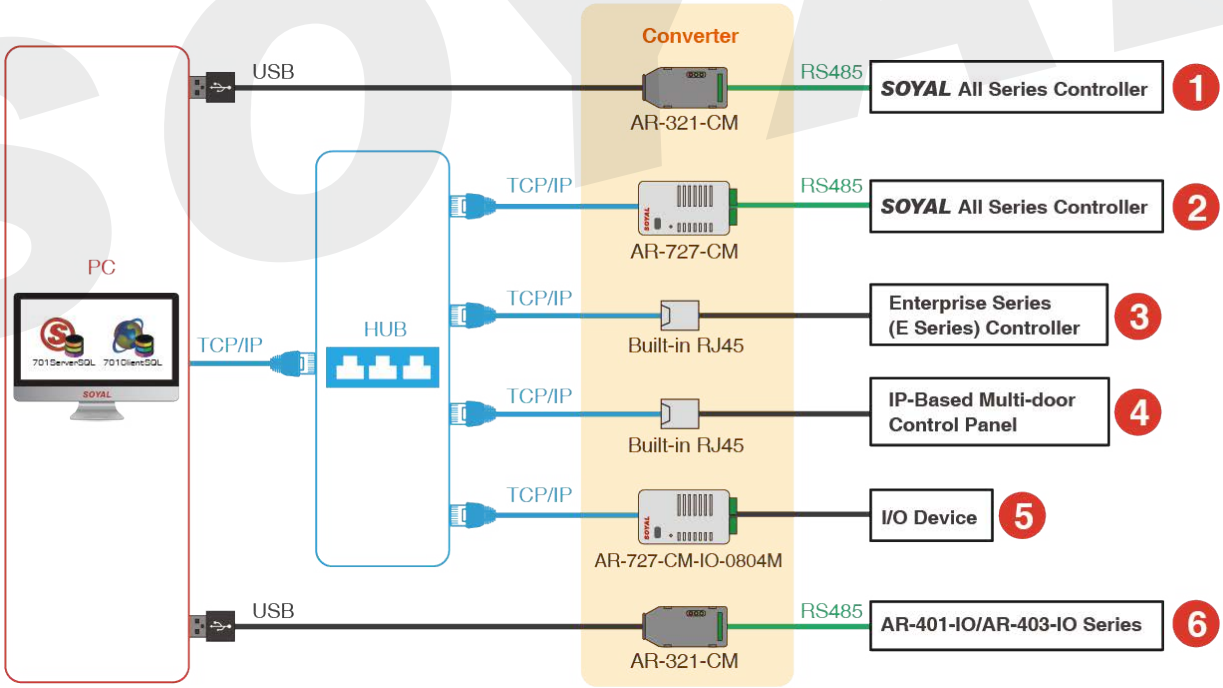
Step 1. Right-click on the 701ServerSQL icon in the bottom right corner of the computer.

Step 2. Select [OnLine] to check the connection status.

7.2 The Demonstration of Controller Connect with 701ServerSQL

SOYAL Controllers and IO Module can connect with 701ServerSQL via different methods, the methods are as below:

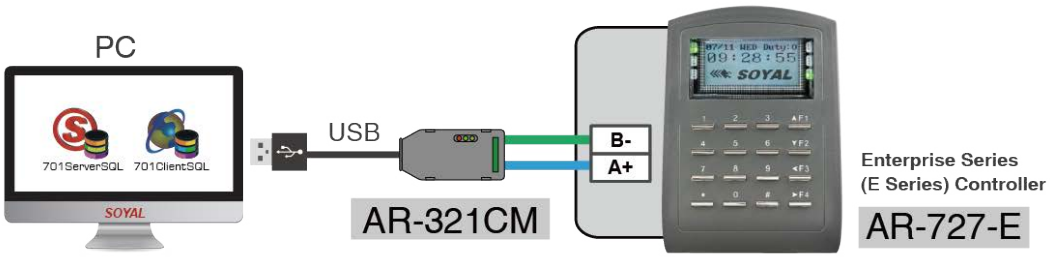
1. RS485 convert USB →
   Connection of SOYAL ALL Series Controller via USB / RS-485 Converter AR-321-CM
2. RS485 convert TCP/IP →
   Connection of SOYAL ALL Series Controller via TCP/IP / RS485 Converter AR-727-CM
3. TCP/IP directly →
   Connection via RJ45 built-in the Enterprise Series (E Series) Controller
4. TCP/IP directly →
   Connection via Multi-door Networking Control Series (ex.AR-716-E16)
5. TCP/IP directly →
   Remotely control electricity equipment via TCP/IP with Industry Series I/O Module (ex.AR-727-CM-IO-0804M)
6. RS485 convert USB →
   Connection of AR-401/AR-403 IO Module Using AR-321CM to Connect PC via RS-485



7.2.1 RS485 convert USB →Connection of SOYAL ALL Series Controller via USB / RS-485 Converter AR-321-CM

Applicable Model: SOYAL All Series Controller

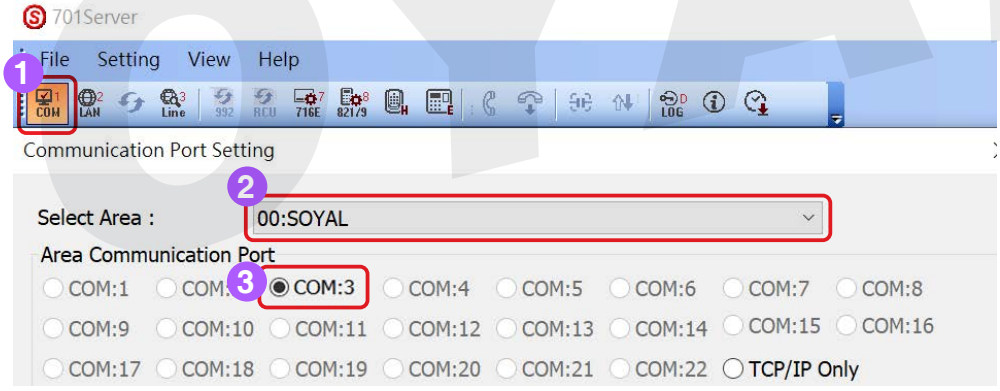
Step 1. Connect the controller with PC via AR-321CM (using E Series Controller AR-727-E as example)

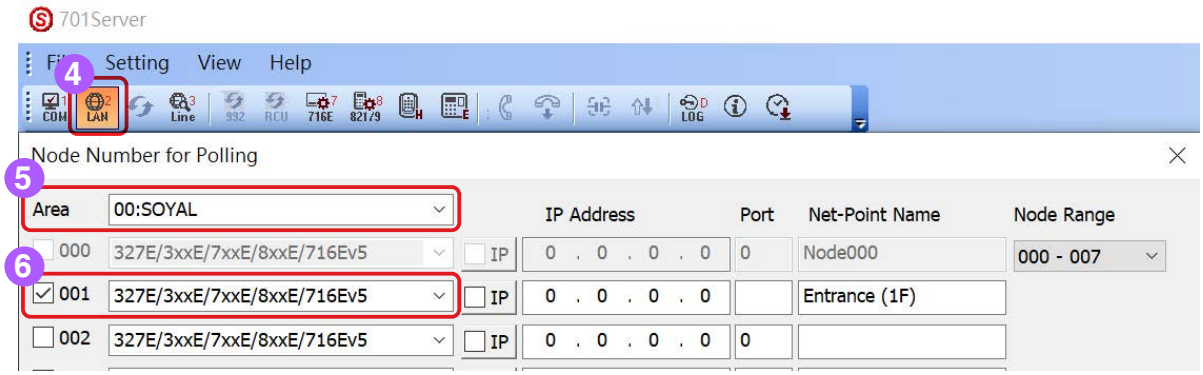


Step 2. Modify the Controller Node ID

The default Node ID is 001, please change it if you already have the same Node ID.
The function is as below (using AR-727-E as example):
(1)Enter the program mode by keypad: ＊123456#
(2)Select the options through LCD screen:
3.Parameters 1 -> 1.Node ID -> Input New Node ID: Range 001~254 -> Press # until the setting complete.

Step 3. Connect the Controller via 701ServerSQL



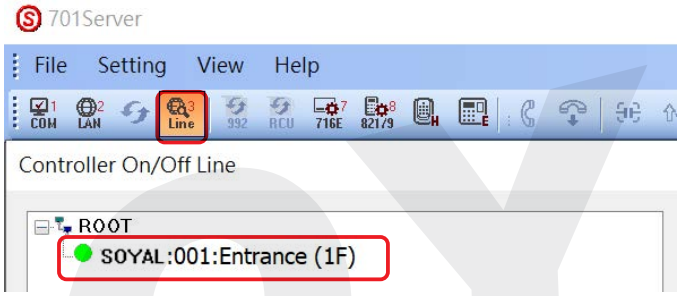


(1) Start 701ServerSQL, select [1.COM]
(2) Select Area
(3) Select Area Communication Port and Save

(4) Select [2.LAN]
(5) Select Area
(6) Tick the Controller Node ID and model (ex. AR-727-E with Node ID 001)
Details please refer to the introduction: FAQ : 701ServerSQL LANbased

Step 4. Check the Line Status

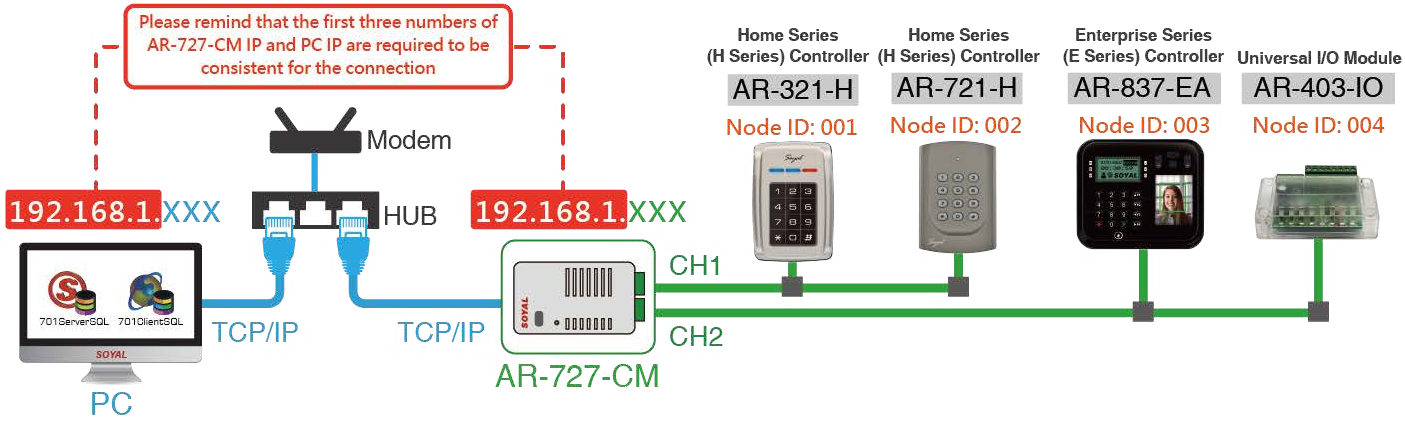
Select [3.Line] to check the Controller on/off line



7.2.2 RS485 convert TCP/IP → Connection of SOYAL ALL Series Controller via TCP/IP / RS485 Converter AR-727-CM

Applicable Model: SOYAL All Series Controller

Architecture Diagram:



Step 0. Determine whether the IP Addresses' are consistent
(AR-727-CM default IP is 192.168.1.127)

- Example 1: PC IP is 192.168.1.XXX, and then the IP Address are consistent.
  → Please start from Step 2

- Example 2: PC IP is 192.168.0.XXX, and then the IP Address are inconsistent.
  → Please start from Step 1

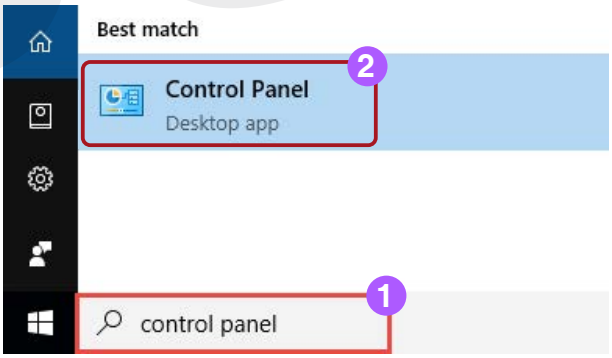
NOTE

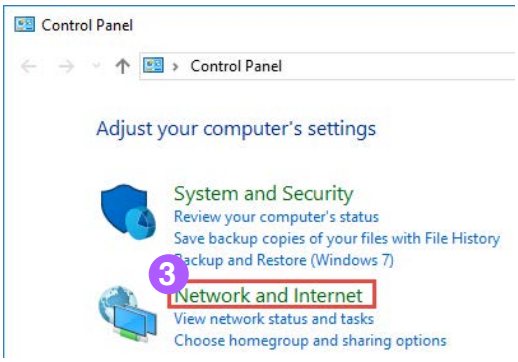
- This features required connection to the internet. Step below is how to know your PC's IP Address:

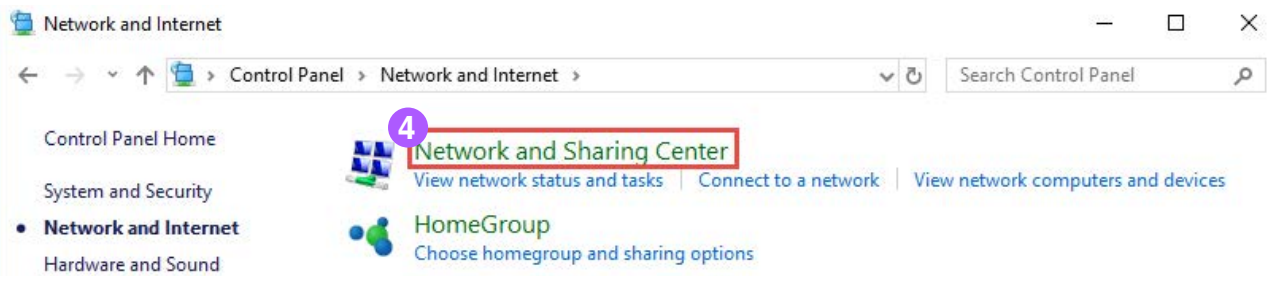
Step 1. Search for [Command Prompt]
Step 2. Enter [ipconfig] and press [Enter]
Step 3. IPv4 Address is your PC's IP address. In this example, 192.168.1.82 is the IP Address.

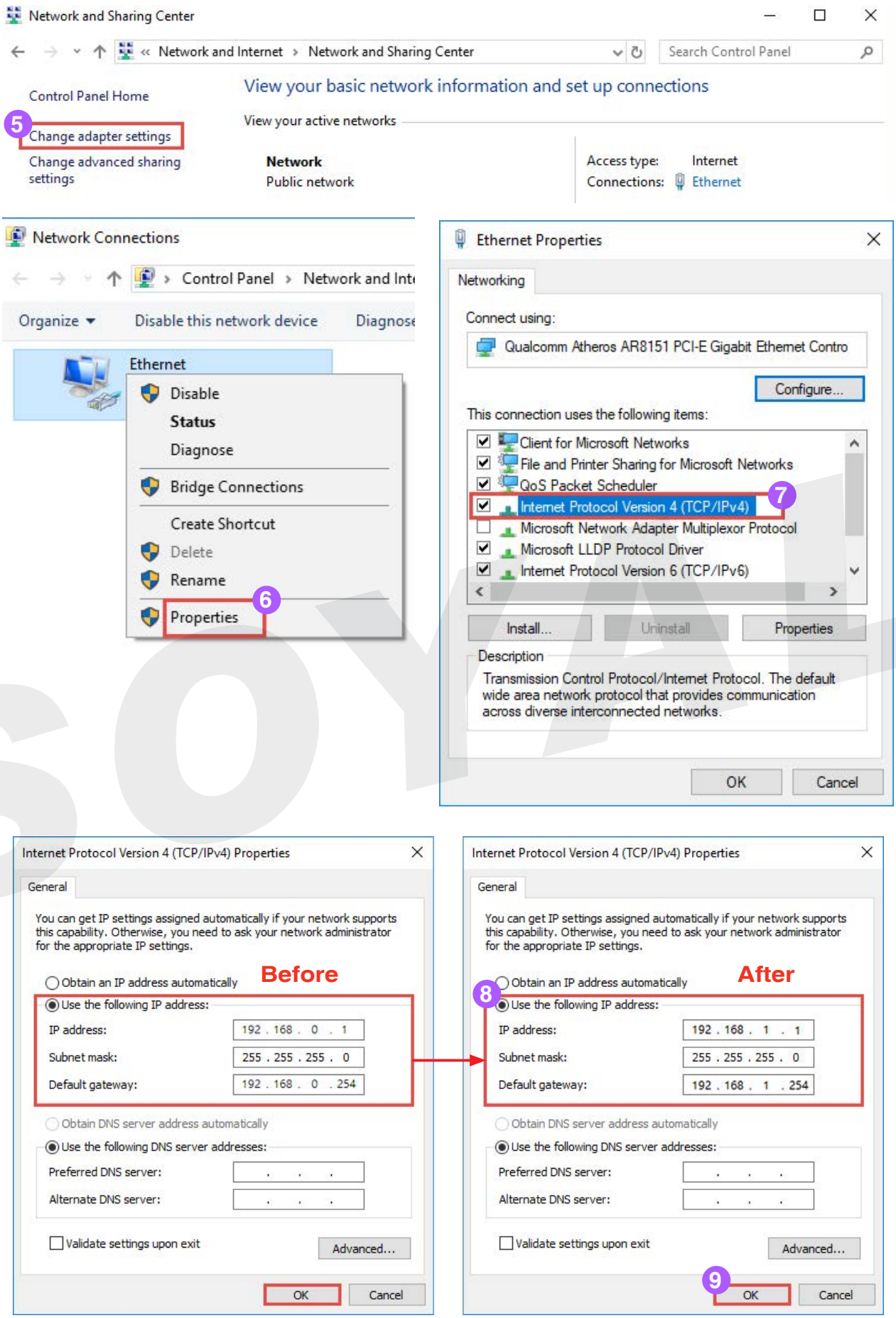
Step 1. Modify the PC IP Address to match the AR-727-CM IP Address

The PC IP Address range is 192.168.0.1~86 in example2, so that we need to change the AR-727-CM IP from 192.168.1.127 to 192.168.0.87 to match the internet.
Firstly, we need to modify the PC IP from 192.168.0.XXX to 192.168.1.XXX to control AR-727-CM, the institution is as below:
(Additional Information: Subnet Mask 255.255.255.0 means the fourth number of IP range is changeable from 1~255)

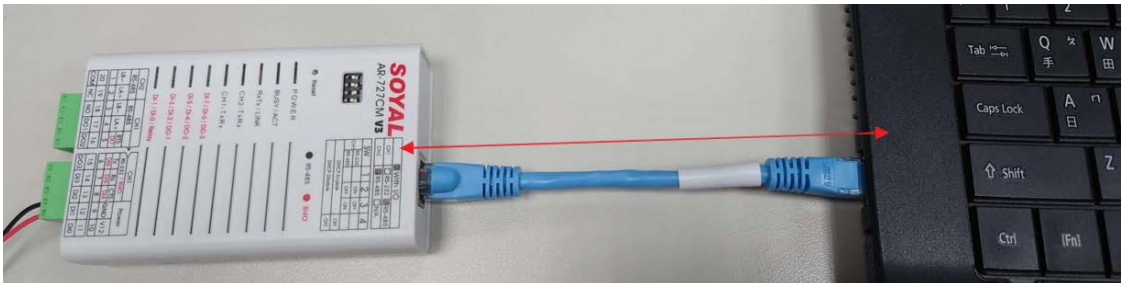


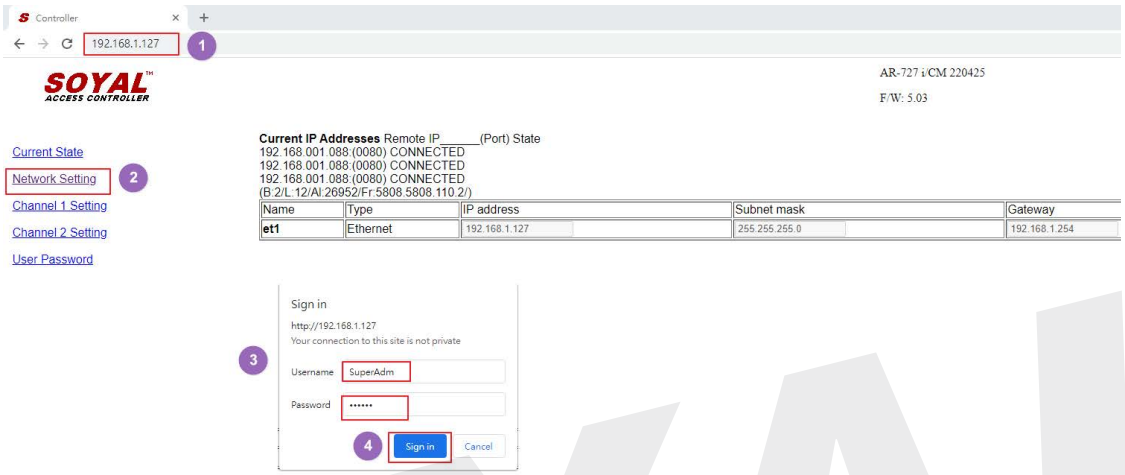





Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
5
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Network
Public network
Access type: Internet
Connections: Ethernet
Network Connections
Control Panel › Network and Int
Organize
Disable this network device
Diagnose
Ethernet
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
6
Properties
Ethernet Properties
Networking
Connect using:
Qualcomm Atheros AR8151 PCI-E Gigabit Ethernet Contro
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
7
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Before
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
After
8
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
9
OK
Cancel

Step 2. Modify the AR-727-CM IP Address



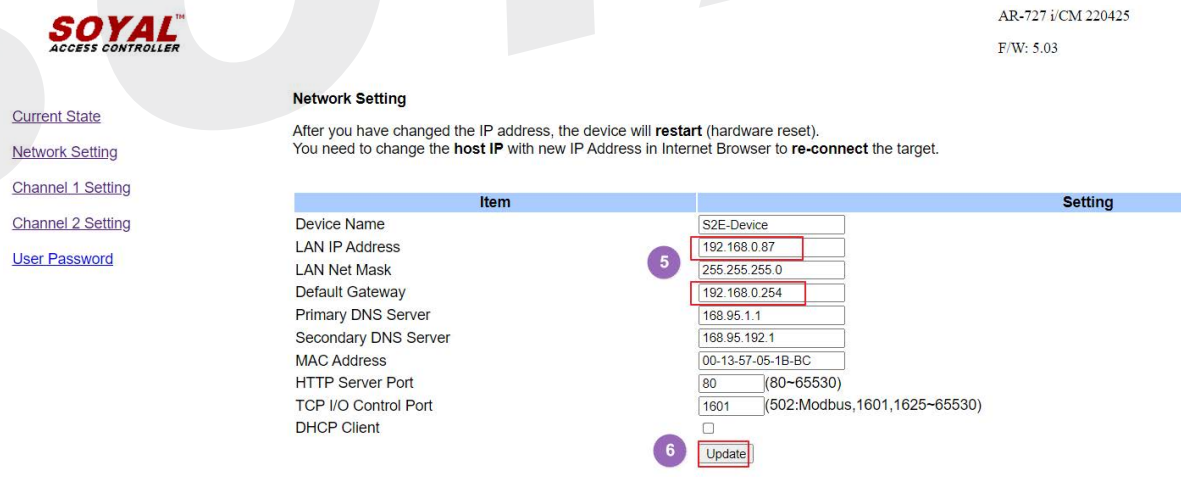


(1) Input the AR-727-CM IP Address 192.168.1.127 in browser

(2) Press ”Network Setting”

(3) Default Username: SuperAdm: Password: 721568

(4) Press “Sign in”



(5) Change the AR-727-CM IP Address(default value 192.168.1.127)

• Example1 : PC IP and AR-727-CM IP are consistent

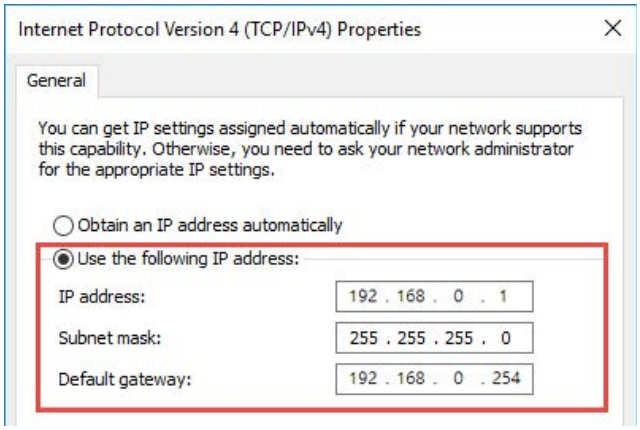
→ change the IP to 192.168.1.87

• Example1 : PC IP and AR-727-CM IP are inconsistent

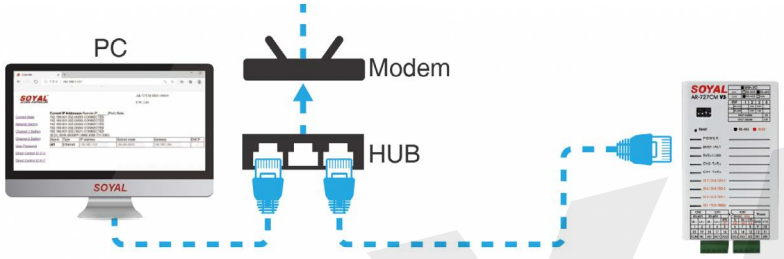
→ change the IP to 192.168.0.87

(6) Press “Update”

Step 3. Modify the PC IP back to the default value, ignoring this step if you did not change the PC IP (Step 1.)



Step 4. Connect the PC and AR-727-CM to the same HUB



Step 5. Setting Controller Node ID

5-1. Using AR-721-H as example

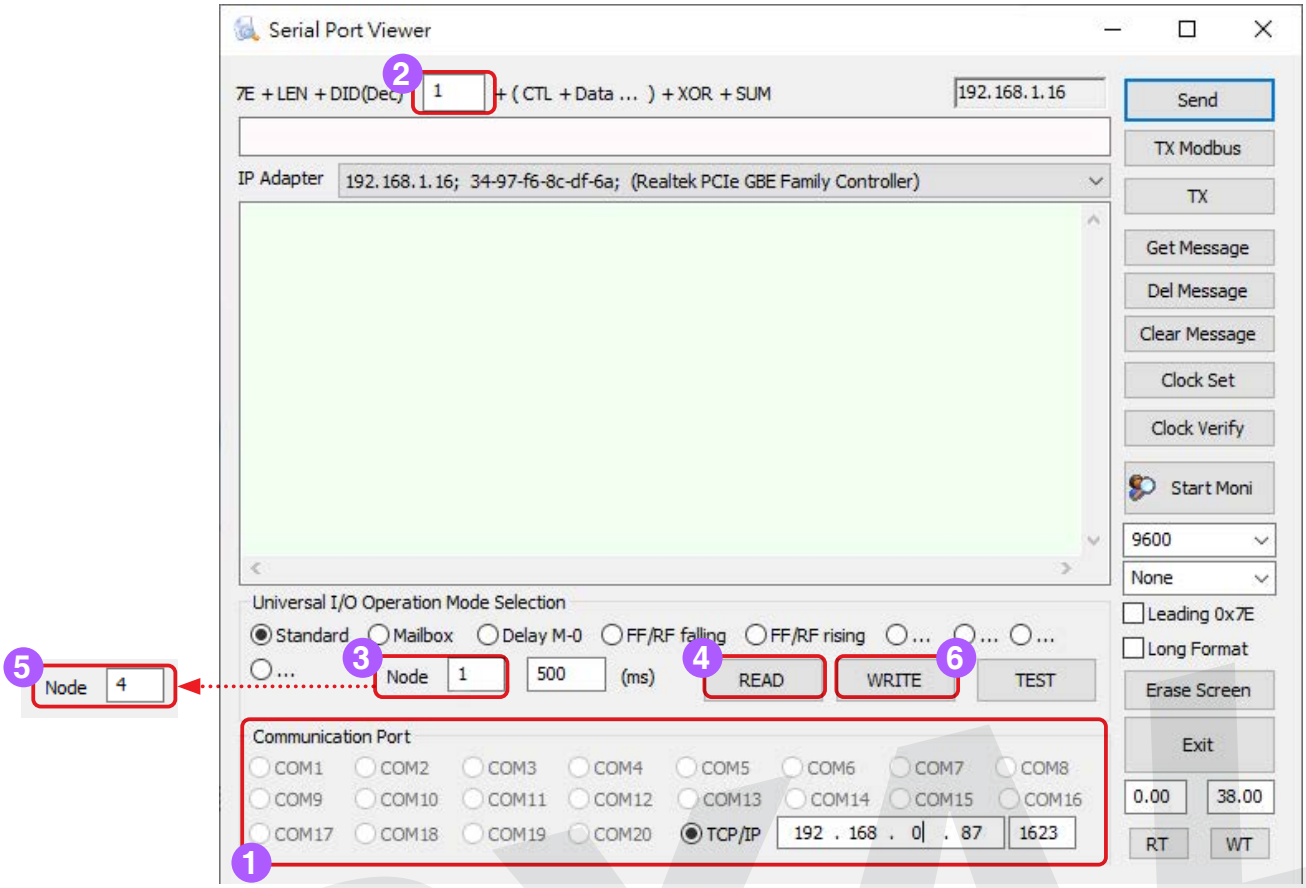
Please use command to set up Controller Node ID by keypad (do not be duplicate)

(1) Enter the program mode: ＊123456#
(2) Set the Node ID to 002: 00＊002#
(3) Exit the Program Mode: ＊#

5.2 Using AR-403-IO Universal IO Module as example

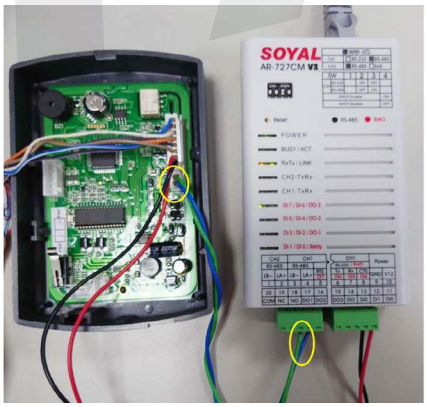
Please note that AR-403-IO Universal IO Module can only modify Node ID via CommView software

(1) Select COM Port
(2) Input the current Node ID(default Node ID is 1)
(3) Input the current Node ID, or you can input 255 for auto research if you forgot it, but please note that the IO Module must connect with PC 1 on 1
(4) Press "READ" to read data
(5) Input the new Node ID(ex.4) in field below, please be aware that the field above is still the current Node ID
(6) Press "WRITE" to complete the modification

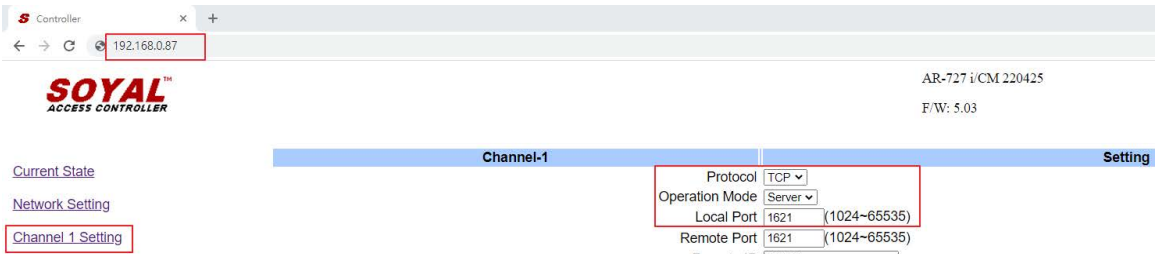


Step 6. Connect the Controller and the AR-727-CM (using AR-721-H as example)

Wiring AR-721-H to Channel 1 of AR-727-CM(refer to the picture below)

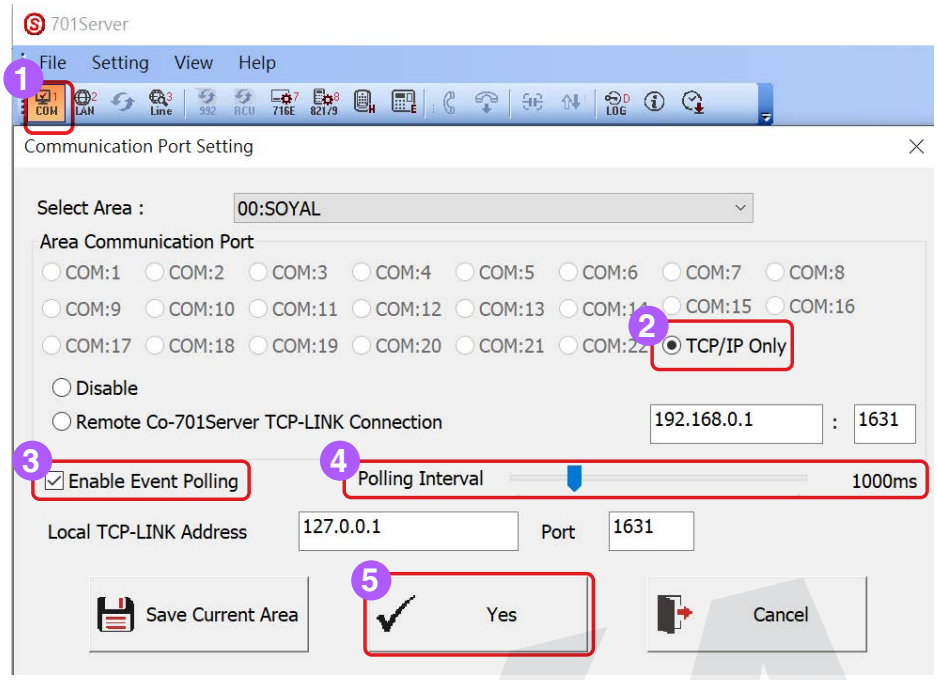


The default Port of Channel 1 of AR-727-CM is 1621, we can also input the IP Address on browser to get the Port number

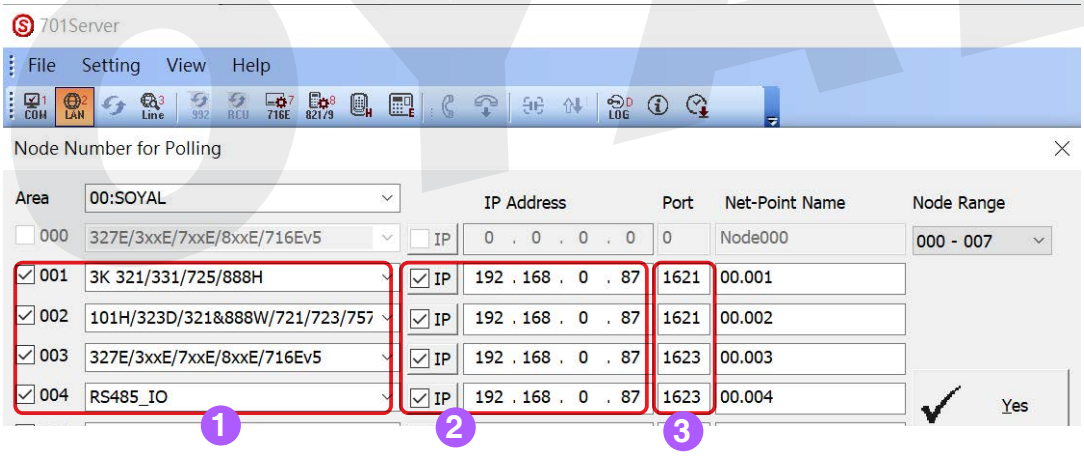


Step 7. Connect the Controller via 701ServerSQL

(1) Start 701ServerSQL, select [1. COM], tick “Enable Event Polling” and set the Polling Interval as 500ms, press “Save Current Area”.



(2) Select [2. LAN], and set up the parameters as below:



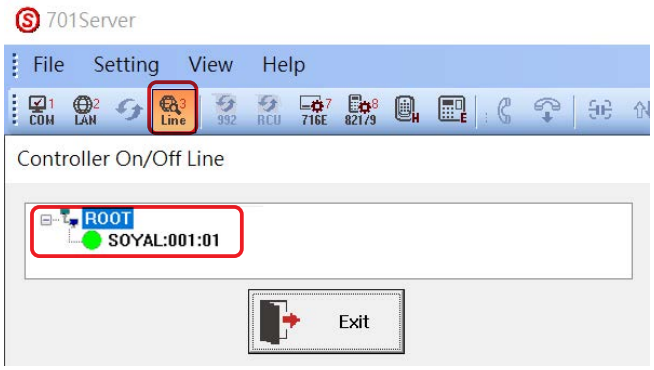
(2-1) Tick the Controller Node ID and select the model
Details please refer to the introduction: FAQ : 701ServerSQL LANbased

(2-2) Tick IP, input AR-727-CM IP Address

(2-3) Input Port number, 1621 for controller connect to Channel 1, 1623 for controller connect to Channel 2

Step 8. Check the Line status

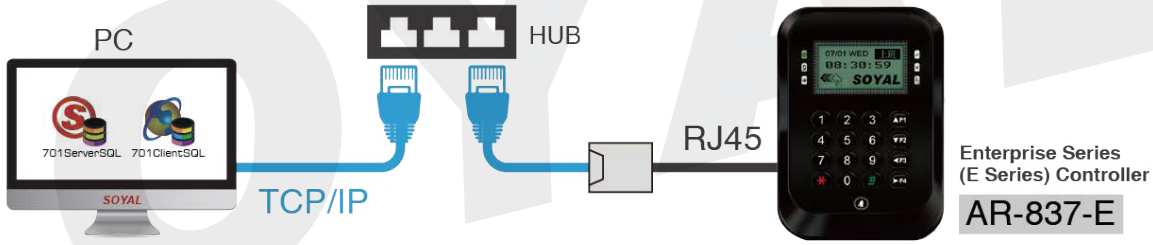
Select [3.Line] to confirm the controller is on/off line, or you can check the LED on AR-727-CM also. CH1-TxRx's red and green LED flashing turns means the communication is online.



7.2.3 TCP/IP directly → Connection via RJ45 built-in the Enterprise Series (E Series) Controller

Applicable Model: SOYAL All Series Controller

Step 1. Connect the Controller and PC to the same HUB (using AR-837-E as example)

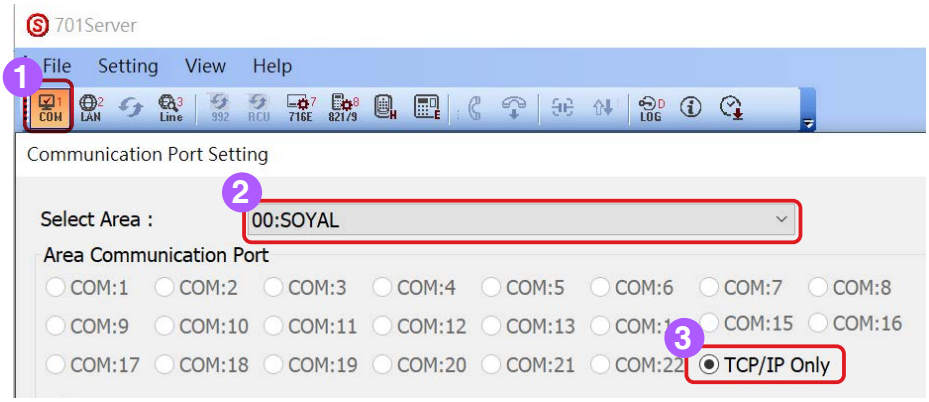


Step 2. Modify the Controller IP Address and Node ID

Controller default IP is 192.168.1.127, default Node ID is 001, modification requirement via browser to login E Series Controller's built-in HTTP Server website.

Details please refer to: Enterprise Series HTTP Server Manual

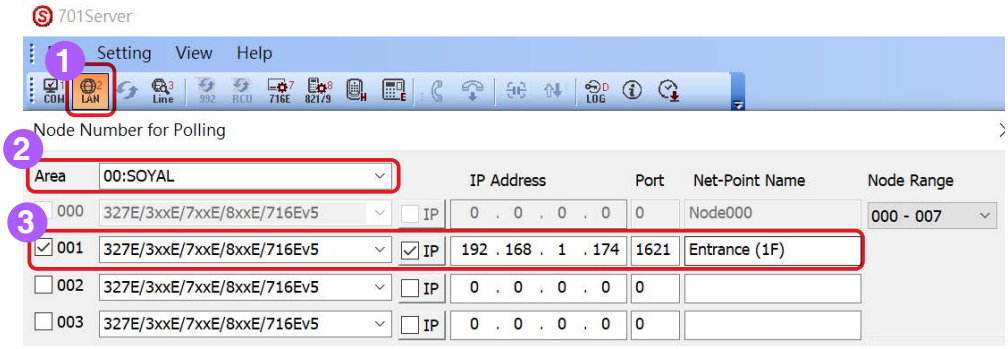
Step 3. Connect the Controller via 701ServerSQL



(1) Start 701ServerSQL, select [1. COM]

(2) Select Area

(3) Select Port as "TCP/IP Only", press "Save Current Area"



(4) Select [2.LAN]

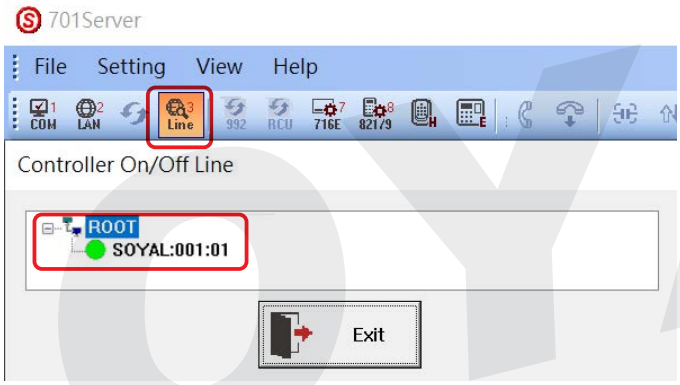
(5) Tick the Area

(6) Tick the Controller Node ID and select the model (using AR-837-E with Node ID 001 as example)

Details please refer to the introduction: FAQ : 701ServerSQL LANbased

Step 4. Check the Line status

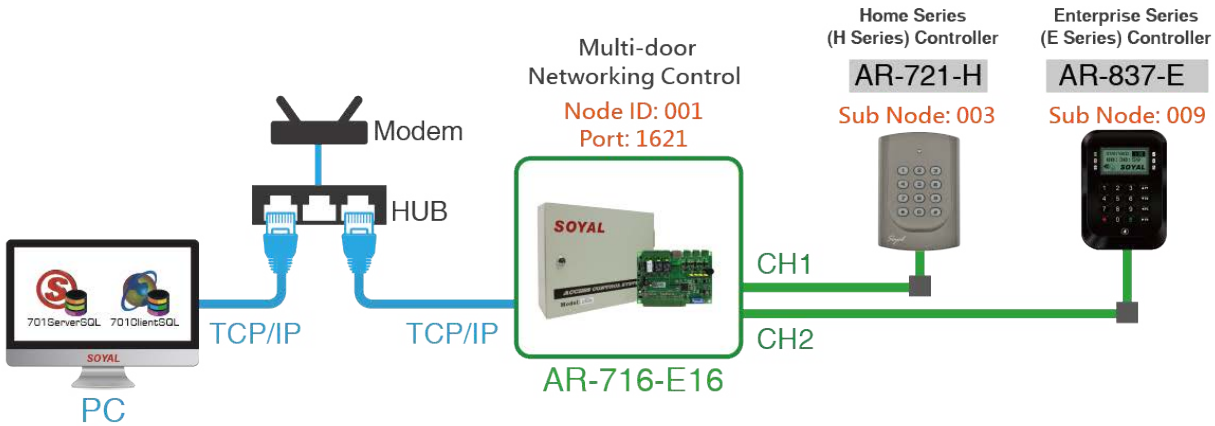
Select [3.Line] to confirm the controller is on/off line, green light means online.



7.2.4 TCP/IP directly → Connection via Multi-door Networking Control Series(ex.AR-716-E16)

Applicable Model: SOYAL Multi-door Networking Control and All Series Controller

Architecture Diagram:



Step 0. Precautions:

(1) Before wiring to Control Panel, each of Access Controller should be assigned to a specific Sub-Node ID range 1~16, or we can only change it by the keypad after we connect Access Controller to the AR-716-E16.

(2) Multi-door Networking Control Series' Port is set up default value 1621, and it has the subordinate relationship with the Access Controllers under control. LAN Setting is for Control Panel or Access Controller Node ID, but Access Controller wire under Control Panel is assigned as Sub-Node ID so it is not required for Access Controller to set up in LAN setting. Only Control Panel needs to set up on LAN setting

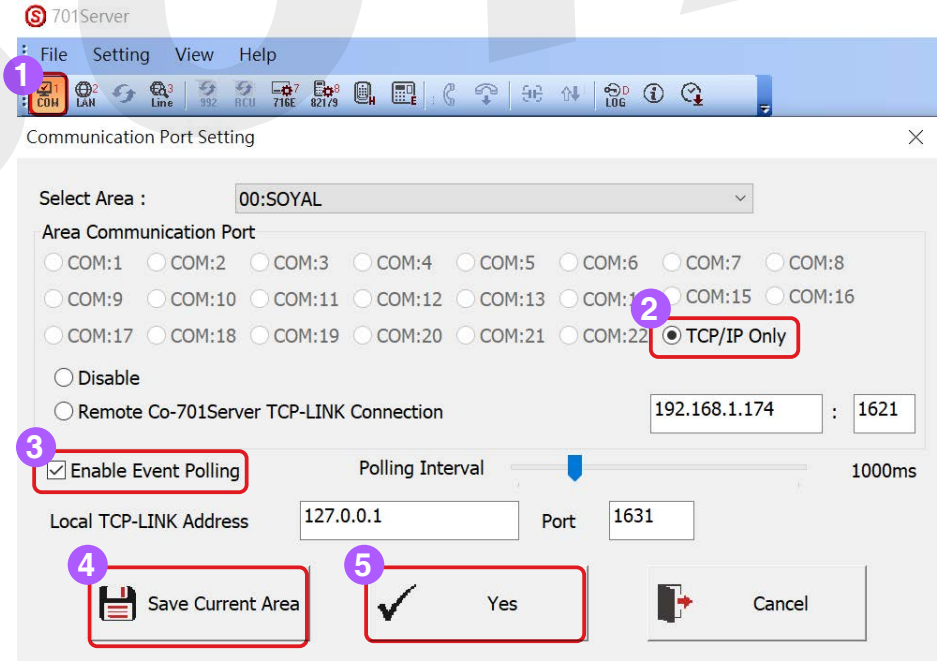
Step 1. Setting the Controller Node ID (AR-721-H、AR-837-E)

(1) Please set up the Controller Node ID following the connection CH of AR-716-E16:
WG0: Node ID is fixed to 17 while connected and fixed to trigger the K1 Relay
WG1: Node ID is fixed to 18 while connected and fixed to trigger the K2 Relay
CH1: RS-485 Reader Node ID must be set up from 03~08
CH2: RS-485 Reader Node ID must be set up from 09~16

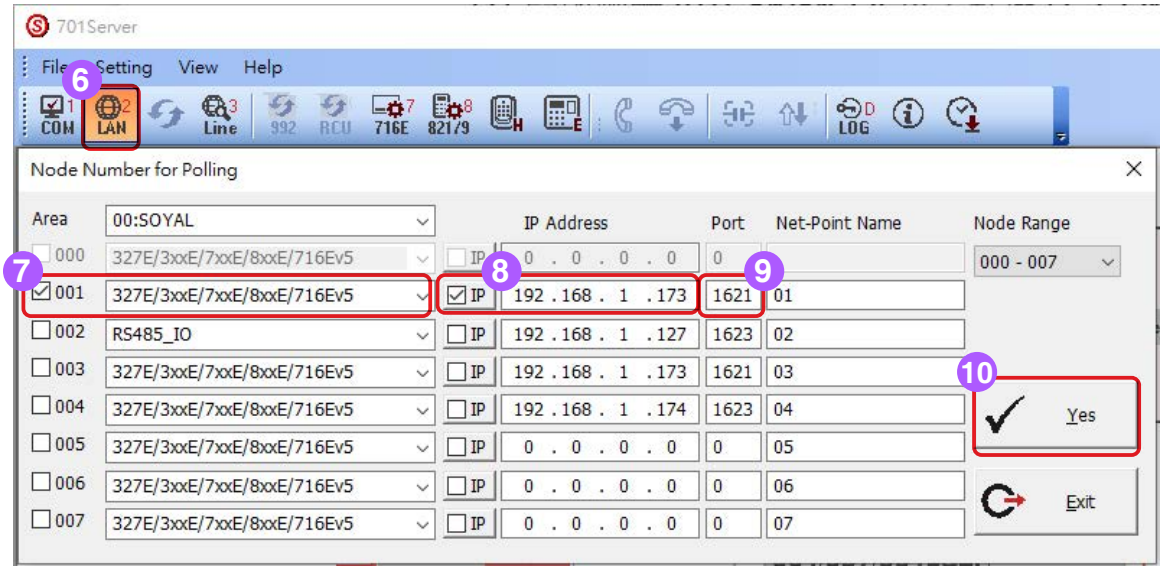
(2) Setting the Controller Node ID (ex. AR-721H)
Please set up the Node ID as the rule above, we can change it with the command below,
1. Enter the Program Mode: ＊123456#
2. Set the Node ID to 003: 00*003#
3. Exit the Program Mode: ＊#

Step 2. Wiring the Controllers with AR-716-E16, and connect AR-716-E16 with PC by the same HUB.

Step 3. Using 701Server to communicate Multi-door Networking Control Panel



(1) COM Setting
(2) Select TCP/IP Only
(3) Select Enable Event Polling
(4) Save
(5) Yes



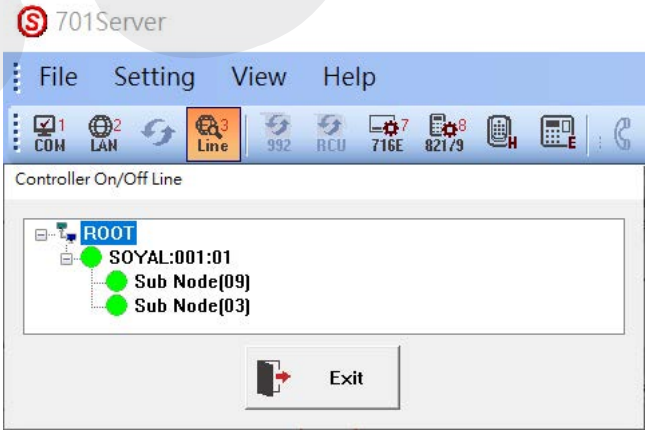
(6) LAN Setting
(7) Select the Node ID& Model Type (remind it is the type as above)
(8) Select IP and input the correct IP Address
(9) Input AR-716-E16 Port 1621
(10) Yes

Step 4. Connect the Controllers and setting door numbers

Please refer to AR-716-E16 Manual page 4~6 IP Setting

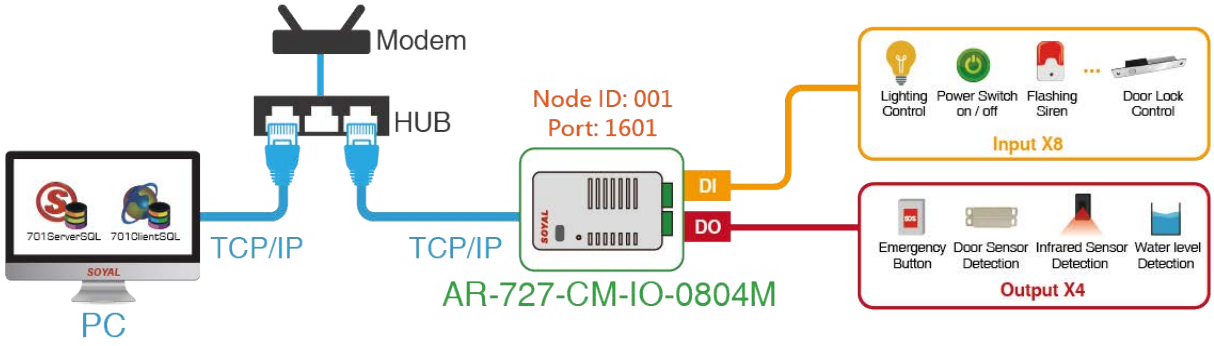
Step 5. Check the Connection

Open Line to confirm the connection status, green light means online.



7.2.5 TCP/IP directly → Remotely control electricity equipment via TCP/IP with Industry Series I/O Module (ex.AR-727-CM-IO-0804M)

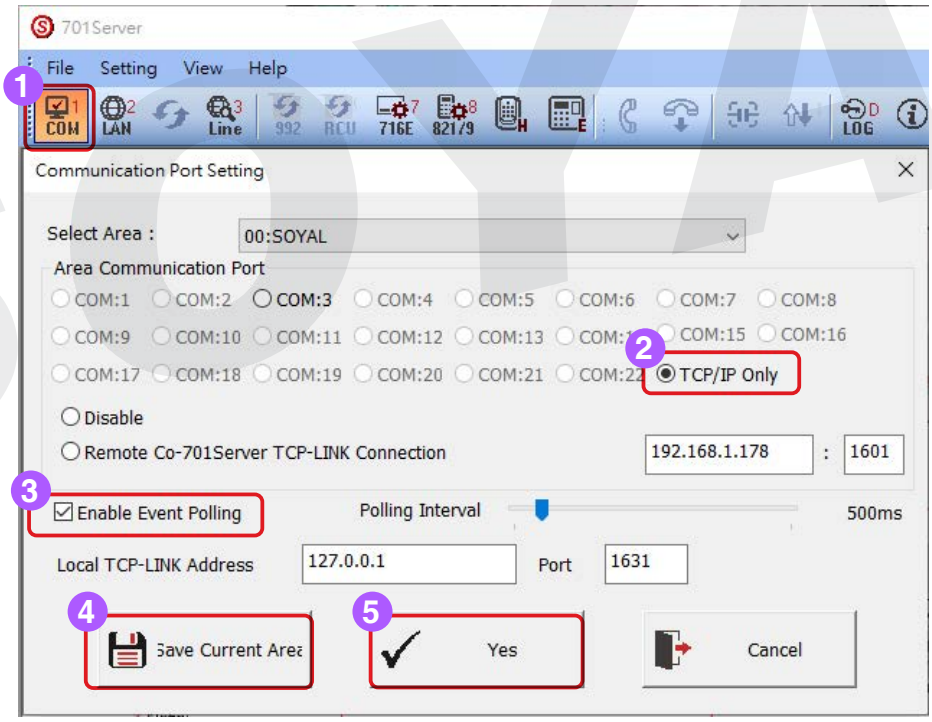
Architecture Diagram:



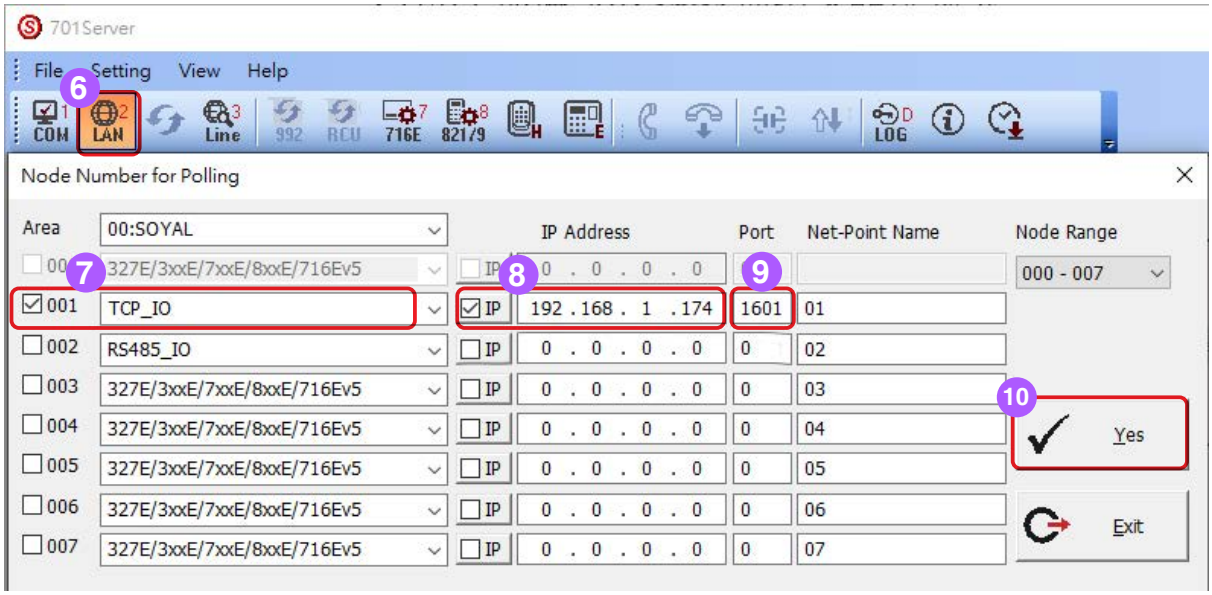
Step 1. Connect AR-727-CM-IO-0804M with PC by the same HUB

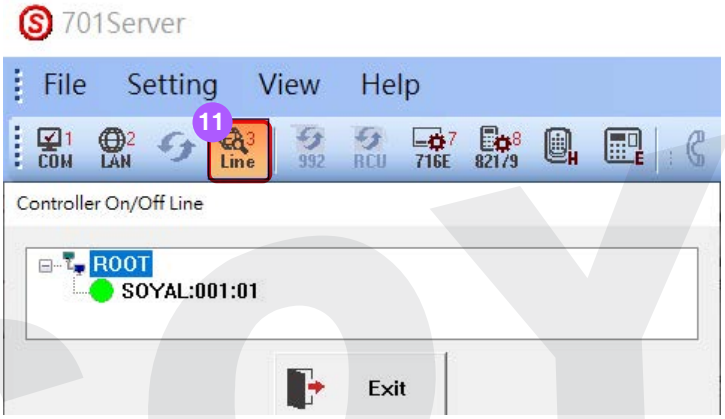
Step 2. Change the IP and Node ID of AR-727-CM-IO-0804M
AR-727-CM-IO-0804M has the virtual value IP 192.168.1.127 & virtual Node ID 001, refer to AR-727-CM HTTP Server Manual if you want to change them.

Step 3. Using 701Server to communicate TCP I/O Module



(1) COM Setting
(2) Select TCP/IP Only
(3) Select Enable Event Polling
(4) Save
(5) Yes

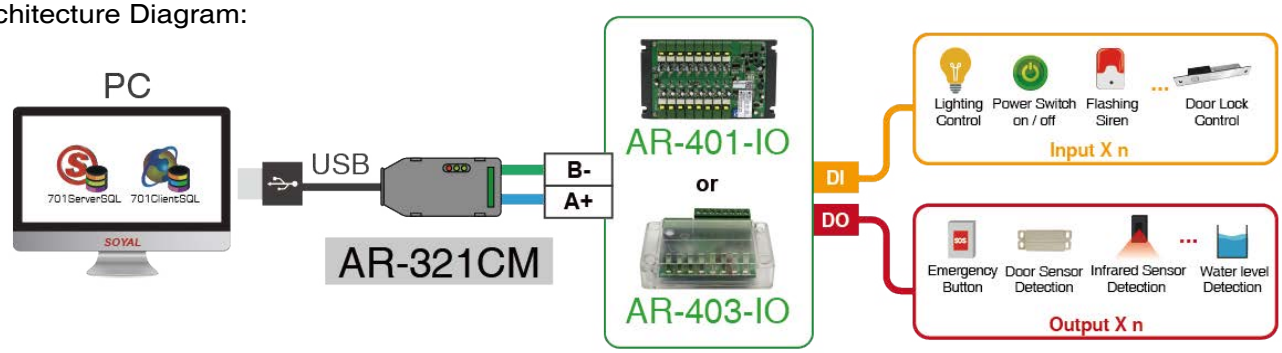




(6) LAN Setting
(7) Select the Node ID& Model Type (TCP_IO)
(8) Select IP and input the correct IP Address
(9) Input Port 1601
(10) Yes
(11) Check the Connection
Open “Line” to confirm the connection status, green light means online.

7.2.6 RS485 convert USB → Connection of AR-401/AR-403 IO Module Using AR-321CM to Connect PC via RS-485

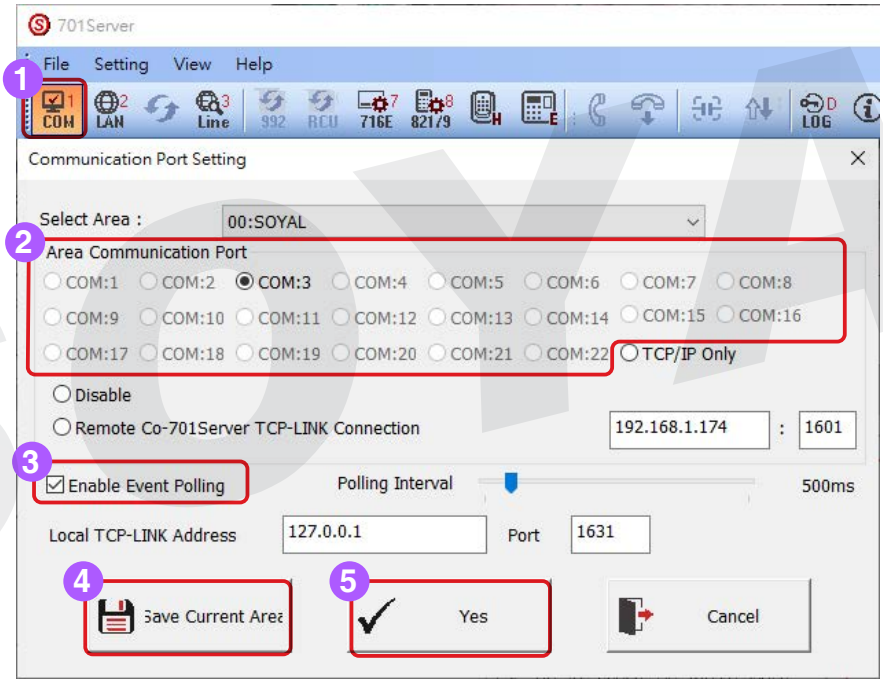
Architecture Diagram:



Step 1. Connect AR-401/AR-403 I/O Module with PC

Step 2. Set up the Node ID of AR-403-IO-0404M, refer to the AR-403 IO Series Manual

Step 2. Using 701Server to communicate AR-401/AR-403 I/O Module



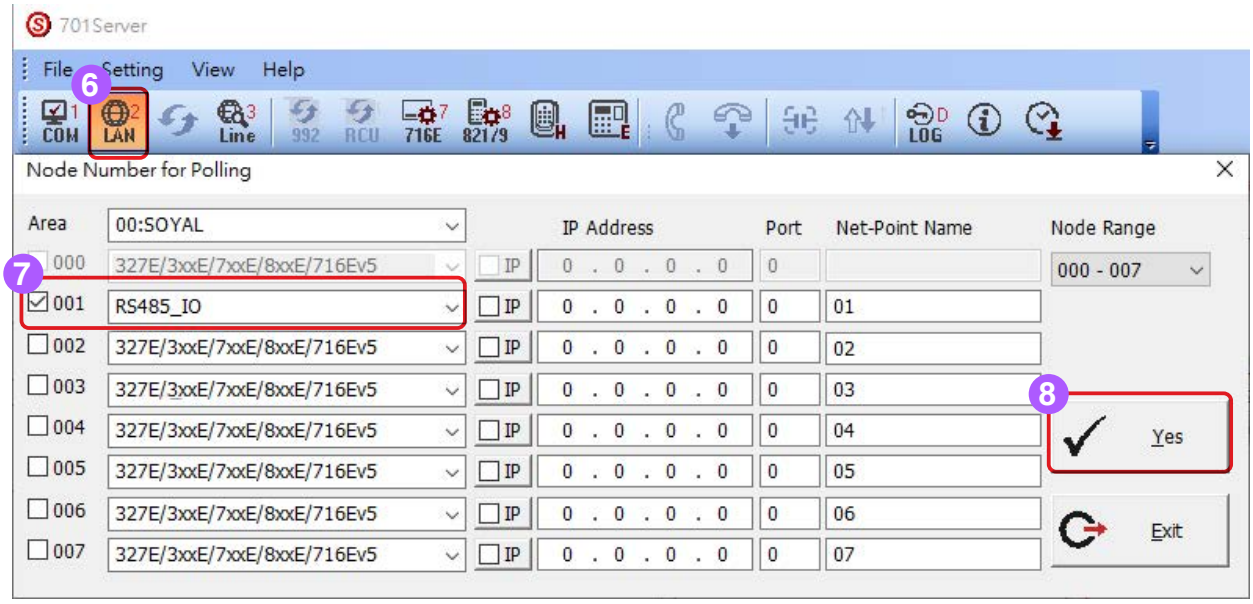
(1) COM Setting

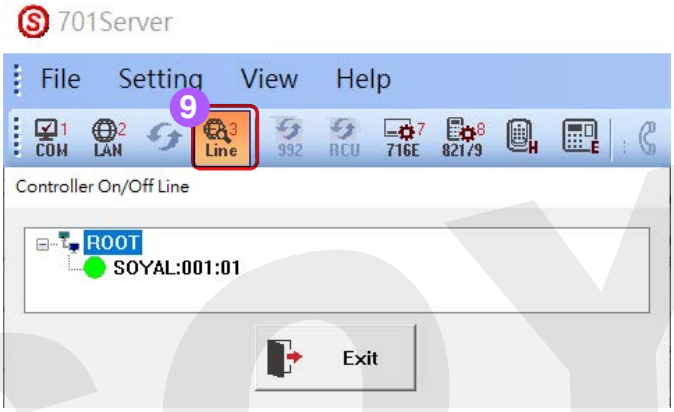
(2) Select COM Port (To check what is your AR-321CM COM port, right click on Windows ICON >> Device Manager)

(3) Select Enable Event Polling

(4) Save

(5) Yes





(6) LAN Setting
(7) Select the Node ID& Model Type (RS485_IO)
(8) Yes
(9) Check the Connection
Open “Line” to confirm the connection status, green light means online.

7.3 Enable card machine event message proactive delivery server.

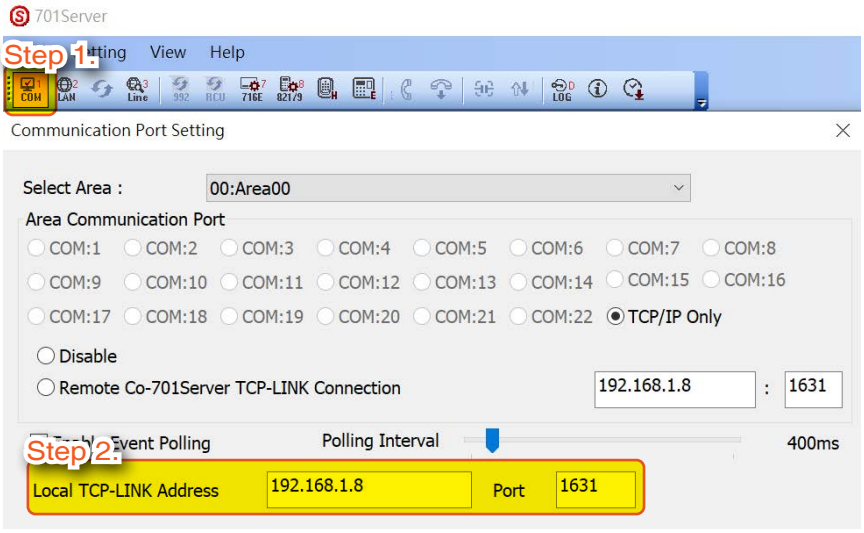
More related information :

- FAQ : How to improve the response speed of card machine messages and how to connect to a dynamic IP device.

Setting Procedure:

1. Set up 701 Server TCP Link IP/Port on 701Server
2. Set up controller parameter on HTTP Browser
   - Change the controller door number/Area number/Node ID
   -Enable the setting of MSG Server IP Addr. (701 Server TCP Link IP/Port)
3. Set up Controller Parameters on 701Server
4. Test the message reception on 701Client

7.3.1 Set up 701ServerSQL TCP-Link IP Address & Port

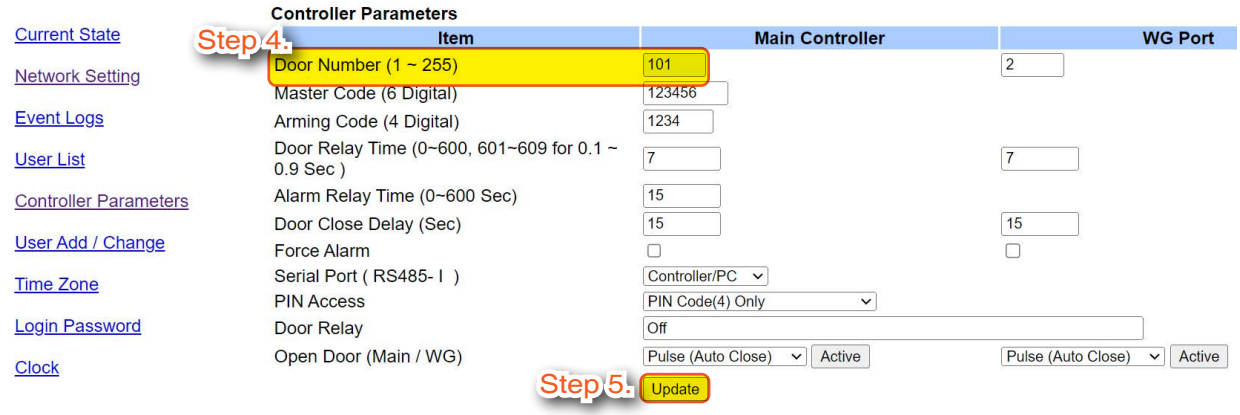


Step 1. Select COM

Step 2. Fill in 701Server IP number /Port Number

Note: Fill in the IP address of the computer's network card, Port default value is 1631; if the default port number is blocked by anti-virus or firewall, please change

7.3.2 Controller HTTP Browser Setting



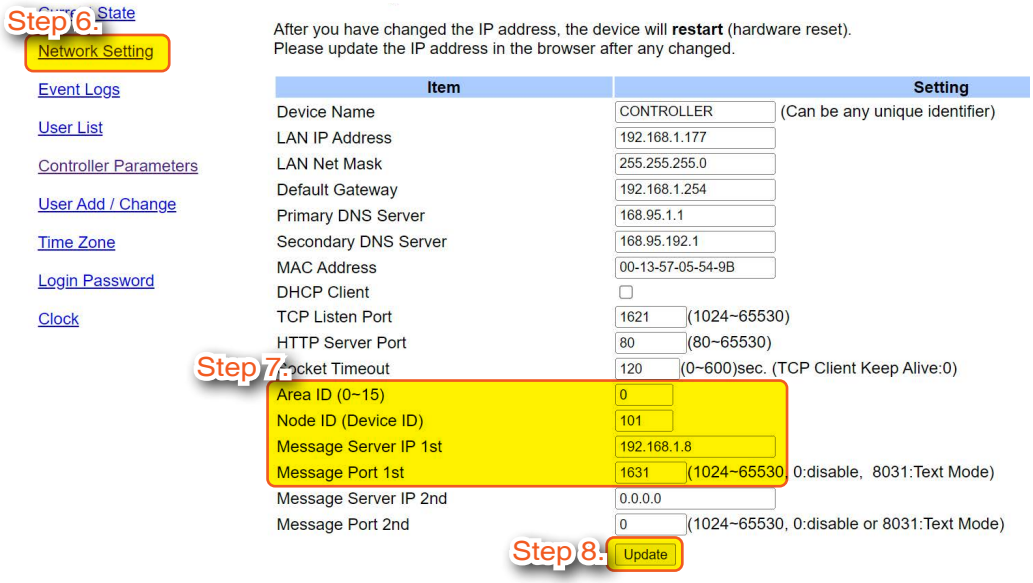
Step 1. Enter IP address {Default 192.168.1.127}

Step 2. Click [Controller Parameters]

Step 3. Enter Login Username{Default SuperAdm}{Password 721568}

Step 4. Go to [Controller Parameter] > Enter Door number [101] WG[101] (for example)

Step 5. Click [Update] to save changed

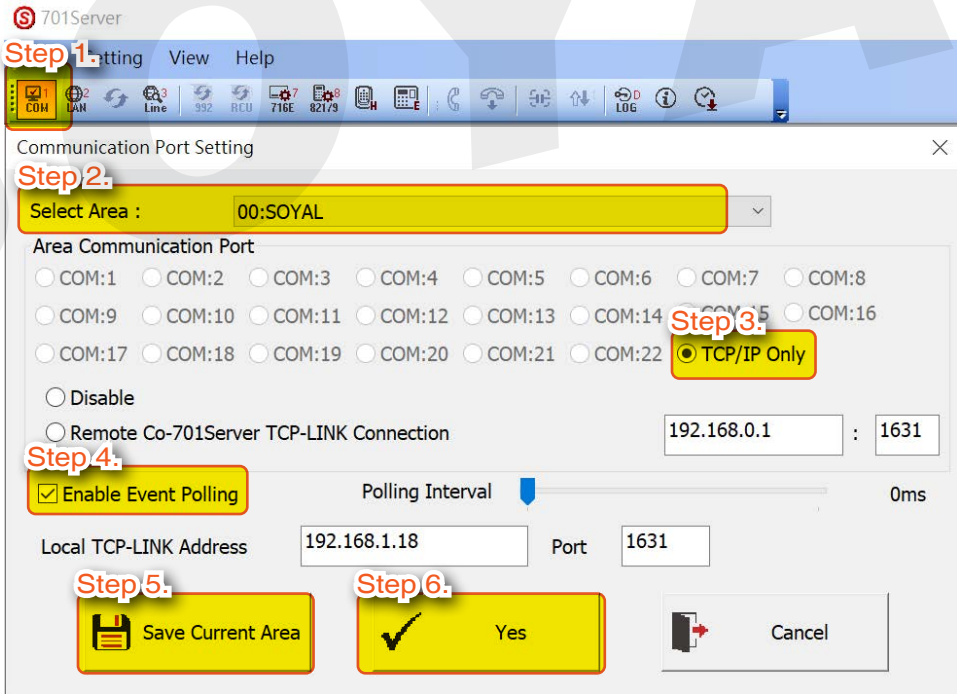


Step 6. Go to [Network Setting]

Step 7. - Set up Area ID [0]
- Enter Node ID for example [101] (controller Node ID must be changed accordingly)
- Message [IP 192.168.1.18], equivalent to 701ServerSQL 'Local TCP-Link Address' setting
- Message Port [1631], equivalent to 701ServerSQL 'Local TCP-Link Port' setting

Step 8. Click [Update], the controller will automatically restart

7.3.3 COM: Serial Port Communication



Set up Controller Parameters on 701Server

Step 1. Click [1 COM]

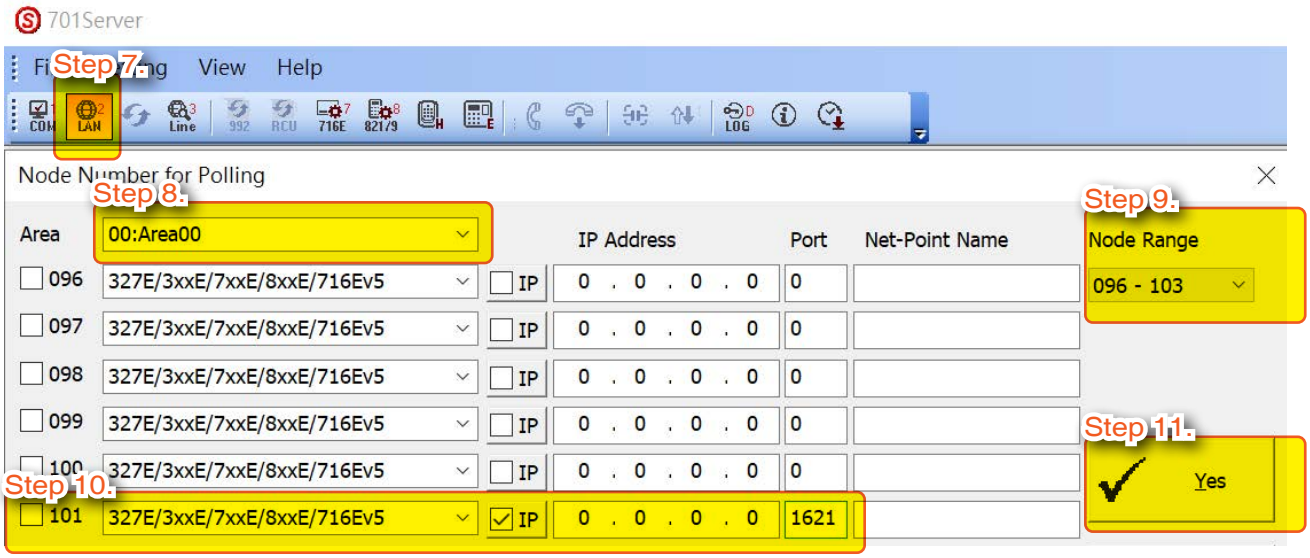
Step 2. Select Area [0]

Step 3. Tick [TCP/IP Only]

Step 4. Please don't tick [Enable Event Polling]

Step 5. Click [Save Current Area]

Step 6. Click [Yes] to finish setting



Step 7. Click [2 LAN]

Step 8. Select Area [0]

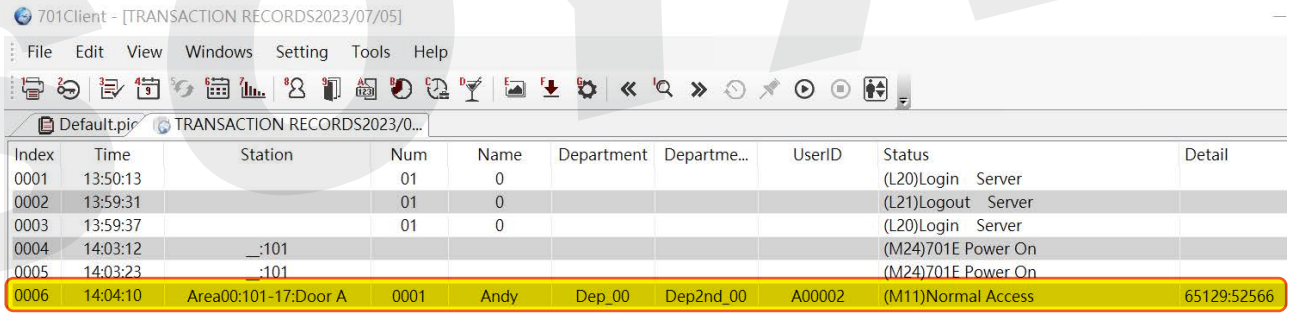
Step 9. Select Node Range [[096-103]

Step 10. Enter [101] Controller IP Address and Port 1621

Note: Don't tick Node ID number

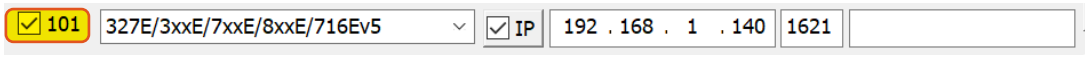
Step 11. Click [Yes] to finish setting

Card presentation on the controller will immediately transmit the event log to 701ClientSQL through the operation above, not required to wait for the polling procedure of 701ServerSQL, improving the message receiving efficiency significantly.

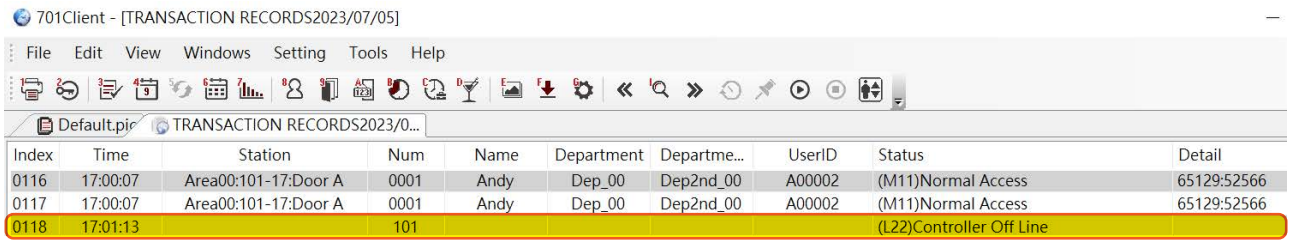


If not all devices are connected remotely, when the "Enable Event Polling" option is selected and the remote card reader is set to actively return messages, once the connection is established, messages can be polled.

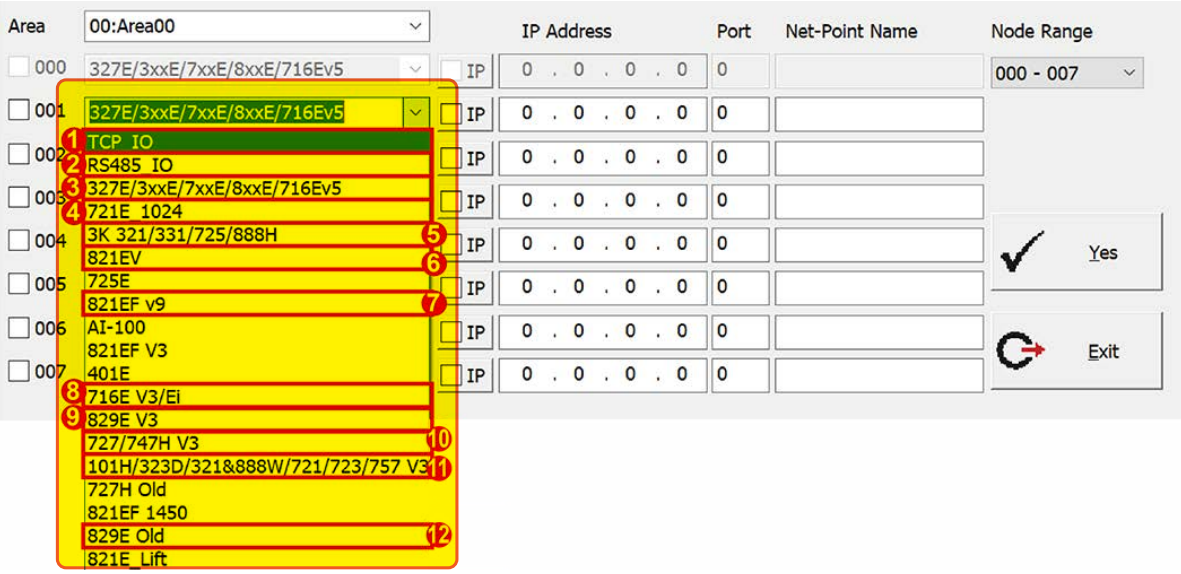
After the controller is connected, the Node ID should be selected.



In the event of a controller disconnection, the server will send a notification message, allowing monitoring of the controller's connection status at any time.



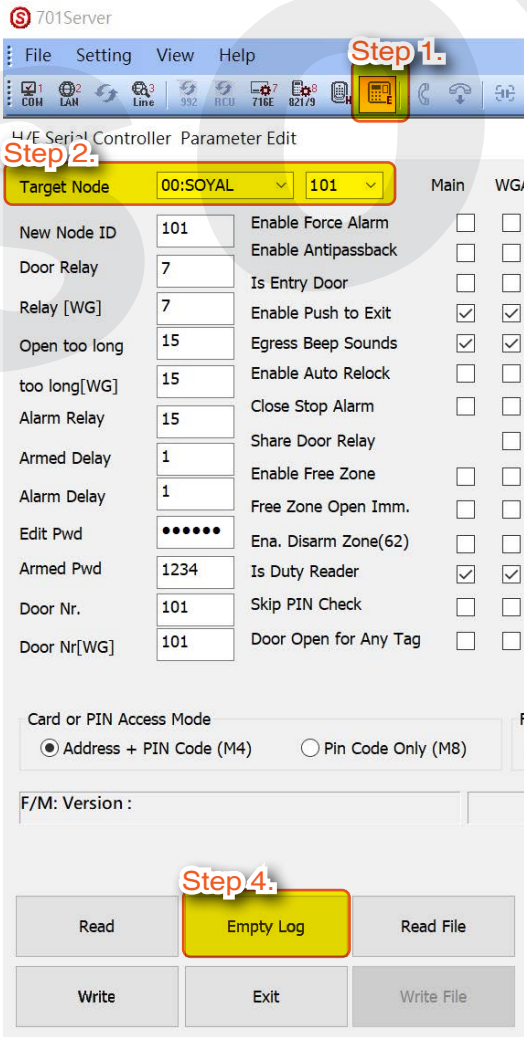
7.3.4 LAN: Hardware Setting



No.	LAN Model No. 10.2 version and before	LAN Model No. 10.2 version and after	Correspondent Hardware Model No.	Communication Interface	Port	Active Communication Mode (Non-Polling)
1.	TCP_IO	TCP_IO	IP Based I/O Module - AR-727-CM-IO- 0804M - AR-401-PLC-0808R - AR-401-PLC-1616R	TCP/IP	1601	YES (required additional setting of Message Server IP point to 701ServerSQL's Local TCP Link Address & TCP Port)
2.	RS485_IO	RS485_IO	RS485 I/O Module - AR-401-IO-0016R - AR-401-IO-1709R - AR-403-IO Series	RS485 (via AR-321-CM converter)	1601	X
3.	881/837 /331E&EF /82xEv5/721 /725Ev2/727 /327Hv5	327E/3xxE/ 7xxE/8xxE/ 716Ev5	All Enterprise Series Controller (E Series) : AR-725-E / AR-331E&EF / AR-837-E&EF / AR-727-E / AR-327-E	TCP/IP (if onboard TCP/IP module)	1621	YES (required additional setting of Message Server IP point to 701ServerSQL's Local TCP Link Address & TCP Port)
			Control Panel -AR-716-E16	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
			Enterprise Series Controller(Old Version): AR-881-EF / AR-829-EV5	RS485 (via AR-321-CM converter)		X
4.	721E_1024	721E_1024	Dual WG control panel - AR-716-E02	RS485 (via AR-321-CM converter)		X
5.	3K 321/331/ 725/888H	3K 321/331/ 725/888H	Home Series (H Series) controller that support 3000 user interface AR-321H / AR-331-H /AR-725-H / AR-888-H	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
				RS485 (via AR-321-CM converter)		X
6.	821EV	821EV	Controller: AR-821-EV	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
				RS485 (via AR-321-CM converter)		X
7.	821EF V9	821EF V9	Controller: AR-821-EF	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
				RS485 (via AR-321-CM converter)		X

No.	LAN Model No. 10.2 version and before	LAN Model No. 10.2 version and after	Correspondent Hardware Model No.	Communication Interface	Port	Active Communication Mode (Non-Polling)
8.	716E V3/Ei	716E V3/Ei	Control Panel: AR-716-E18	TCP/IP	1621	
				RS485		X
9.	829E V3	829E V3	Controller: AR-829-H	RS485 (via AR-321-CM converter)		X
10.	727/747 H V3	727/747 H V3	Controller AR-327-H / AR-727-H / AR-747-H	RS485 (via AR-321-CM converter)		X
11.	323D/321&888W /721/757/737 /723/101H V3	101H/323D /321&888W /721/723/757	Home Series (H Series) controller that support 1000 user interface: AR-101-H / AR-323D / AR-888-W / AR-721-H / AR-723-H / AR-757-H	TCP/IP (via AR-727-CM converter)	CH1 1621 CH2 1623	X
			Controller (Old version): AR-757-H / AR-321W	RS485 (via AR-321-CM converter)		X
12.	829E Old	829E Old	Controller (Old version): AR-829-E	RS485 (via AR-321-CM converter)		X

7.3.5 Controller Parameter: Connection Status



To check the hardware is successfully connected

Step 1. Click [E Controller Parameter Setting]

Step 2. Select [Area 00][Node ID [101]

Step 3. Click[Read] to read controller parameter

Step 4. The firmware will show

[E-controller Firmware Ver: 4.4] means hardware is successfully connected and parameter setting can be read from the software

The mean the controller is connected to setup paramet

NOTE

How to change default IP Address to designated IP Address?

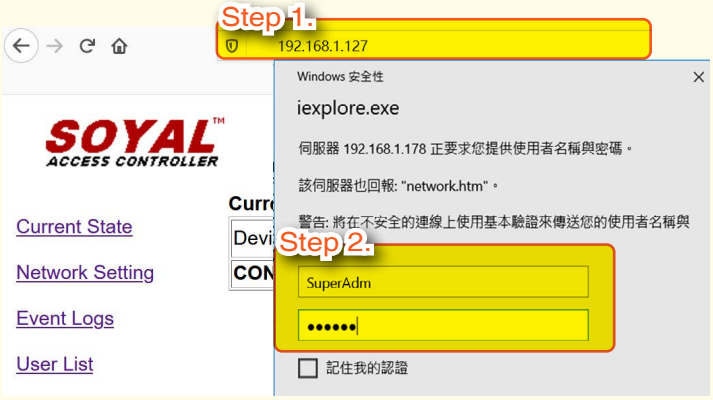
• Enterprise (E Series) Controller :
Default IP Address: 192.168.1.127

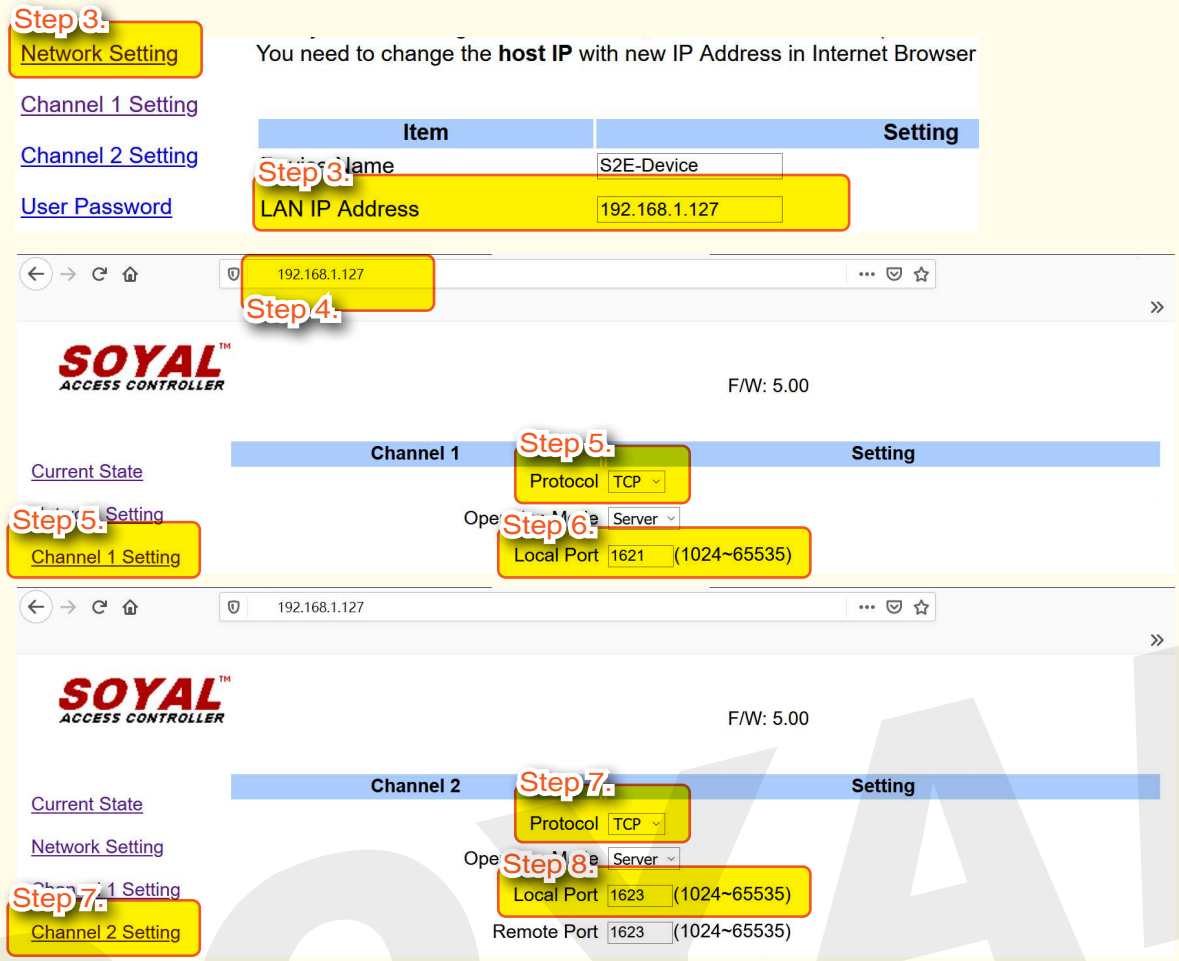
Step 1. Confirm the hardware is TCP/IP Module flash TX/RX (green/orange LED), indicated the TCP/IP module works then enter default IP Address 192.168.1.127
*If the PC network segment is different with hardware, please set the PC network segment to have the same value with hardware.

Step 2. Select [Network Setting] and enter log in account.
Default value: Account: SuperAdm / Password: 721568

Step 3. After Modifying the IP address, click [Update].
Important: please complete the modification within 15 seconds

• AR-727-CM :
Default IP Address: 192.168.1.127





Step 1. Confirm the hardware is TCP/IP Module flash TX/RX (green/orange LED), indicated the TCP/IP module works then enter default IP Address 192.168.1.127
*If the PC network segment is different with hardware, please set the PC network segment to have the same value with hardware.

Step 2. Select [Network Setting] and enter log in account.
Default value: Account: SuperAdm / Password: 721568

Step 3. After Modifying the IP address, click [Update].
Important: please complete the modification within 15 seconds

Step 4. Enter the new IP Address on the browser

Step 5. Select [Channel 1 Setting] > on the Protocol field select as [TCP]

Step 6. [Local Port] default setting is 1621, after completed the setting click [Update]

Step 7. Select [Channel 2 Setting] > on the Protocol field select as [TCP]

Step 8. [Local Port] default setting is 1623, after completed the setting click [Update]

8. Controller Parameter Setting

Controller parameter setting divided into three categories:

Control Panel AR-716-E18

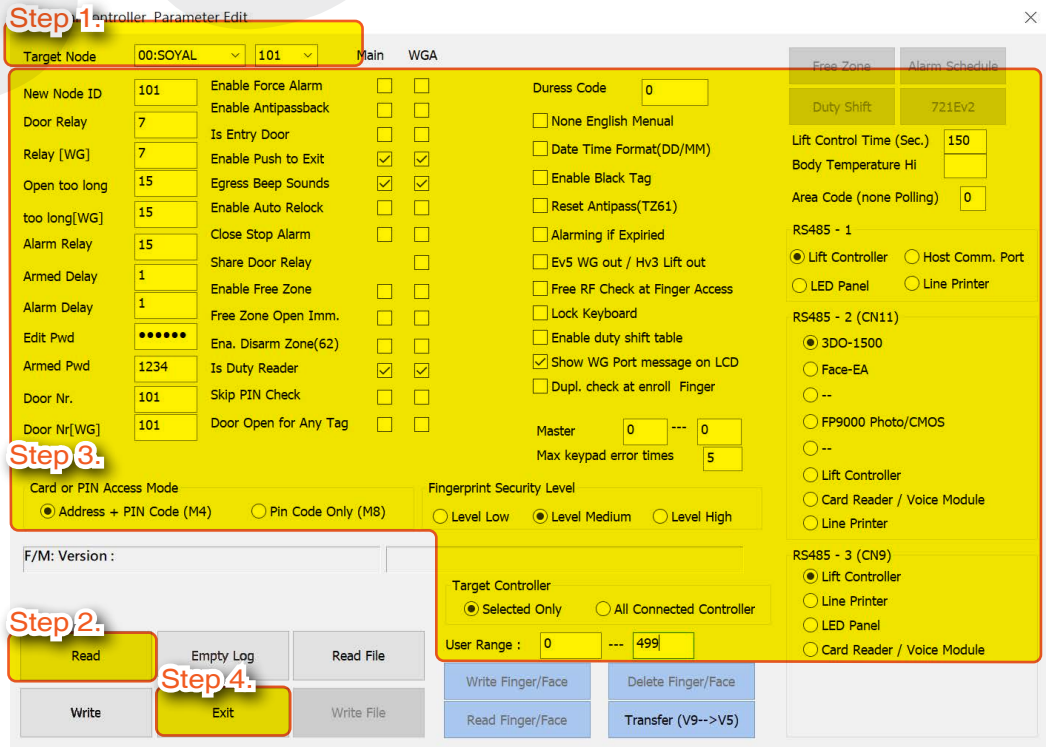
Home Series (H Series) Access Controller

Enterprise Series (E Series) Access Controller and Control Panel AR-716-E16

I. Main Steps to Change Parameter Setting

There are basic four steps required to do every time changing the parameter setting until successfully save the new setting changes.

Note: The default value of each controller is Node ID 1. Before establishing wiring and installation of the whole system, the first thing to do is to assign each controller with different node ID to distinguish between one another. This also mean, one-to-one wiring is required for initial setup.



Step 1. Target Node: Select Area and Node ID of the specified controller
Step 2. Read: Read the current setting of the specified controller
Step 3. Change Parameter Setting
Explained in detail according to controller model no., please refer to:
9.1 Control Panel AR-716-E18
9.2 Home Series (H Series) Access Controller
9.3 Enterprise Series (E Series) Access Controller
9.4 Control Panel AR-716-E16
Step 4. Write: After modifying the parameter setting of the controller, must click Write in order to save changes the new parameter setting and effective.

II. Backup and Restore Parameter Setting

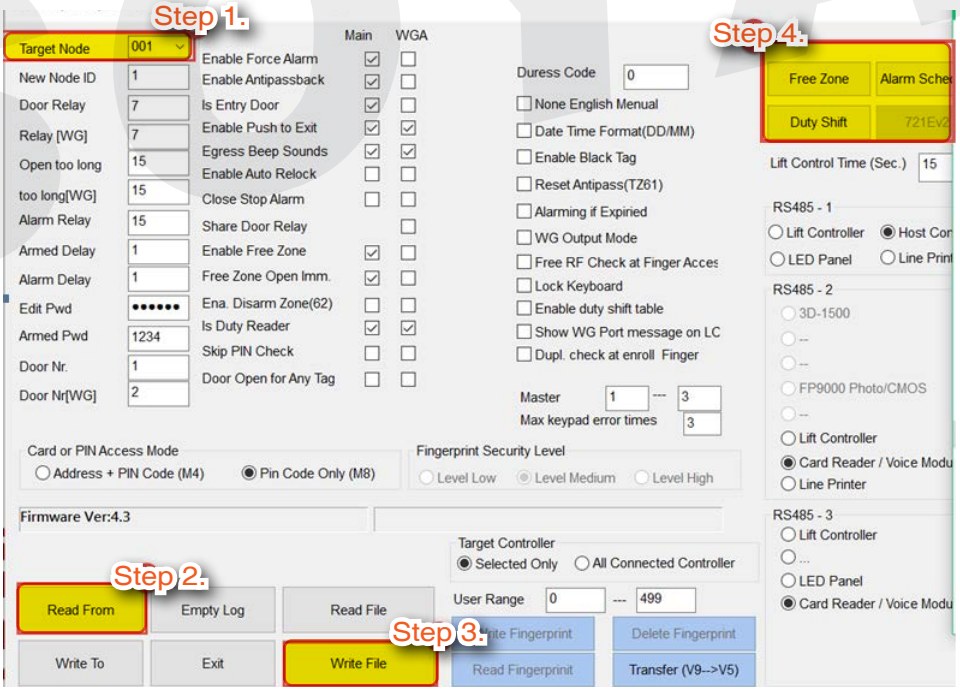
NOTE

Notes: Backup and restore parameter setting feature is only available for:
- Home Series (H Series) Controller
- Enterprise Series (E Series) Controller
- Control Panel AR-716-E16

- **Function:**

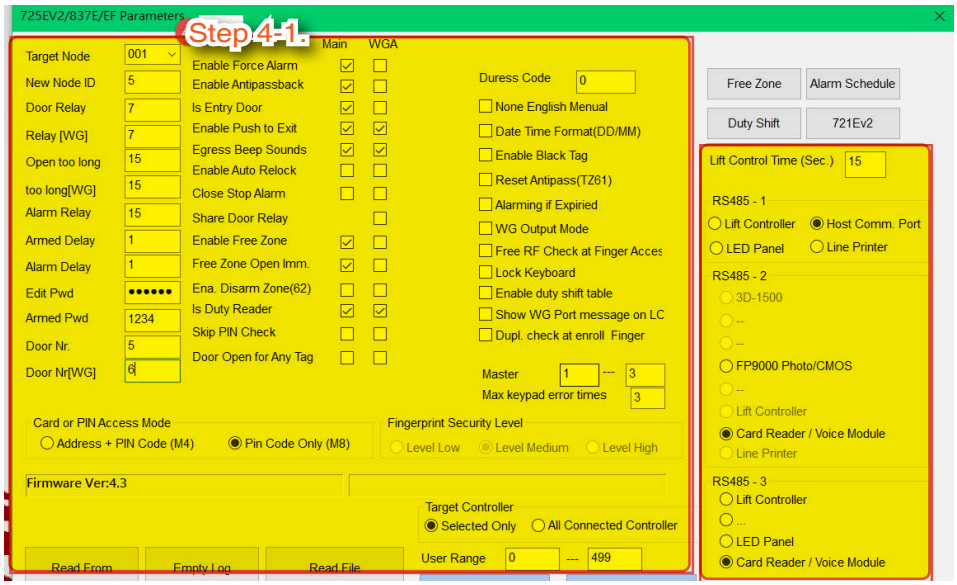
1. Back-up controller's parameter setting

By read parameter setting saved on controller's to be backed up to PC. This features will be handy for back-up purpose if you accidentally factory reset the controller and lost all of the parameter setting, you can still revive it without redo the setting.

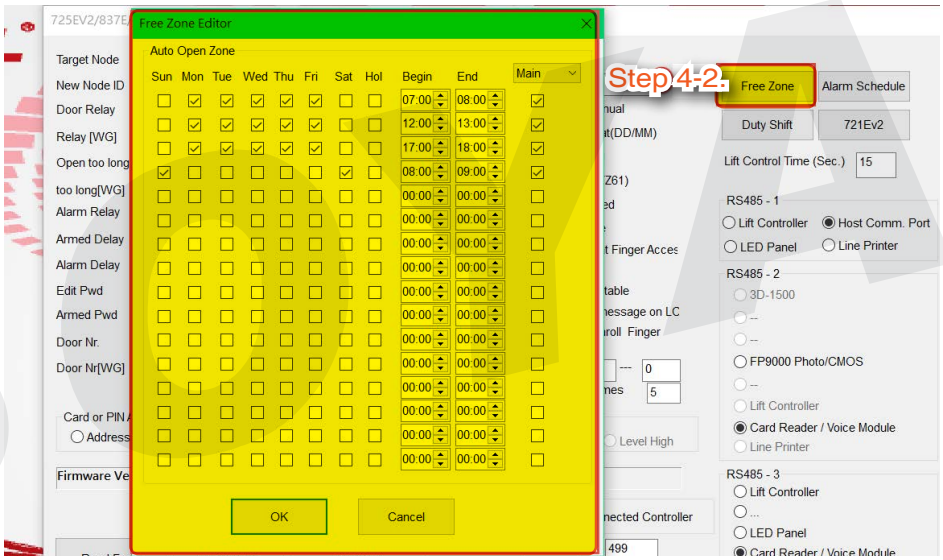


Step 1. Select node ID of your controller that you want to do the parameter setting back-up
Step 2. Select [Read From] to read the saved parameter setting on controller
Step 3. This step only required for Enterprise Series (E Series) Controller & Control Panel AR-716-E16
You need to click 'Free Zone', 'Alarm Schedule', 'Duty Shift' and '721Ev2'(available for multi-door controller AR-716-E16 only) button first in order to activate and enable [Write File] function
-You can also edit parameter setting that you want on 701Server before save and back-up the parameter setting (refer to step 3-1 until 3-5)

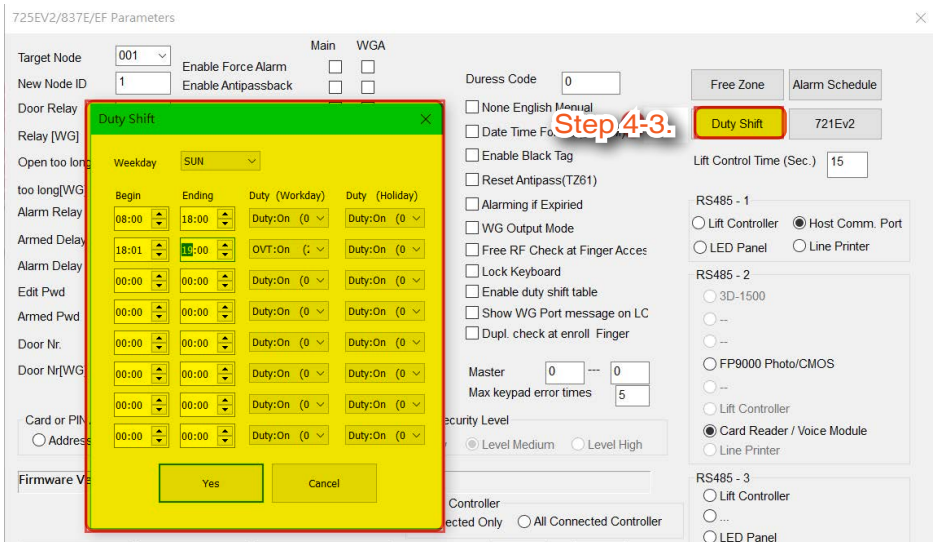
Step 3-1 Basic Parameter Setting (Parameter setting on the main menu)



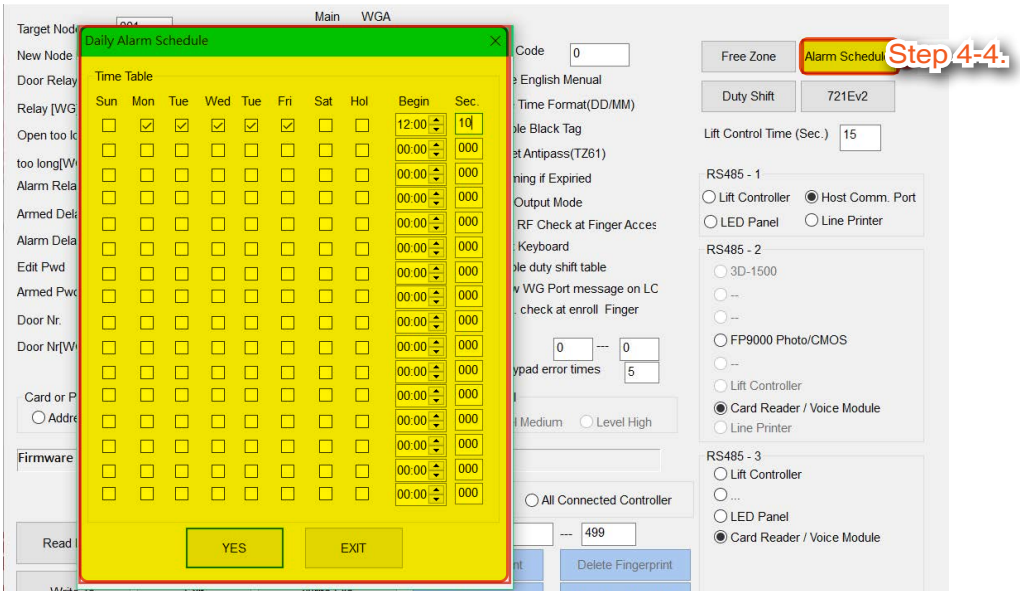
Step 3-2 [Free Zone] Parameter Setting



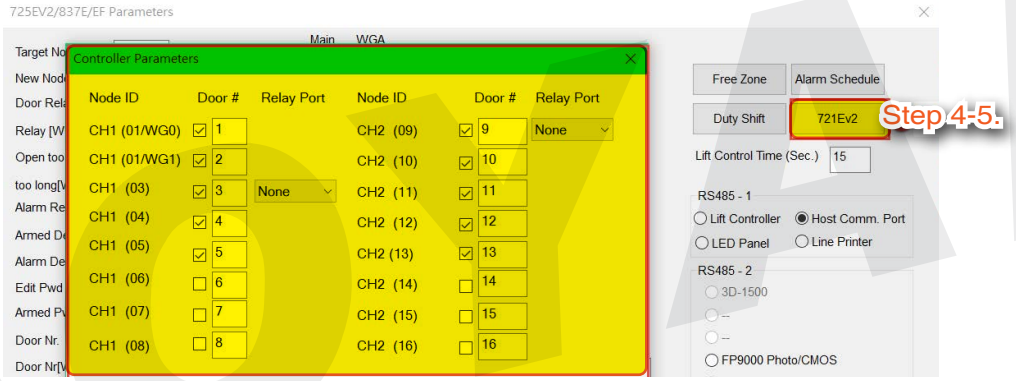
Step 3-3 [Duty Shift] Parameter Setting

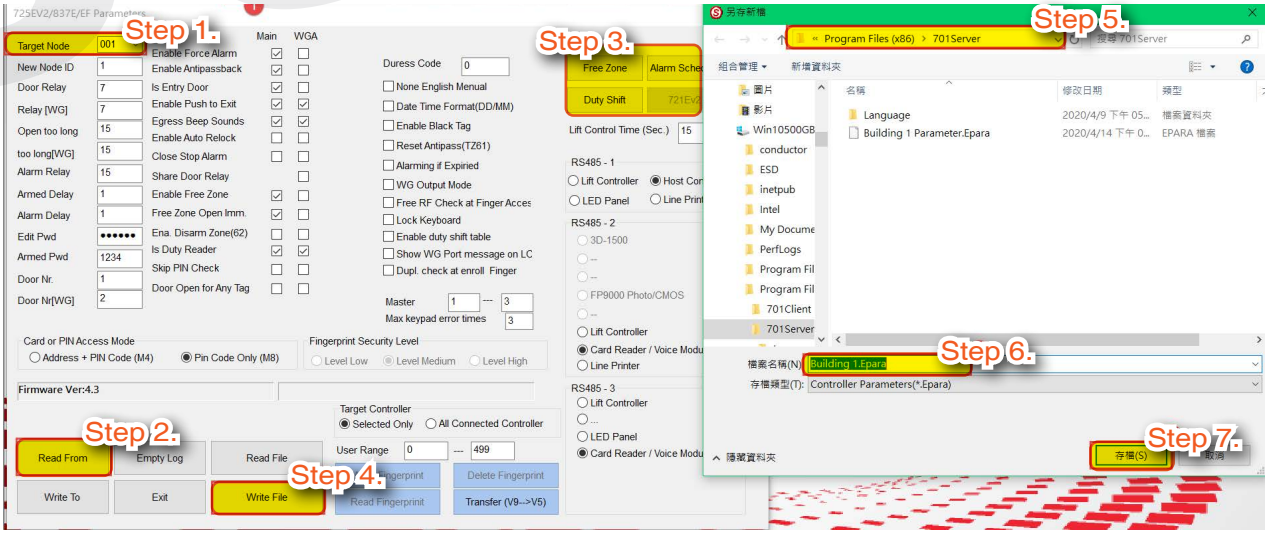


Step 3-4 [Alarm Schedule] Parameter Setting



Step 3-5 [721E-V2] parameter setting for connected controller and WG (only for AR-716-E16)





Step 4. Select [Write File] to save the parameter to PC

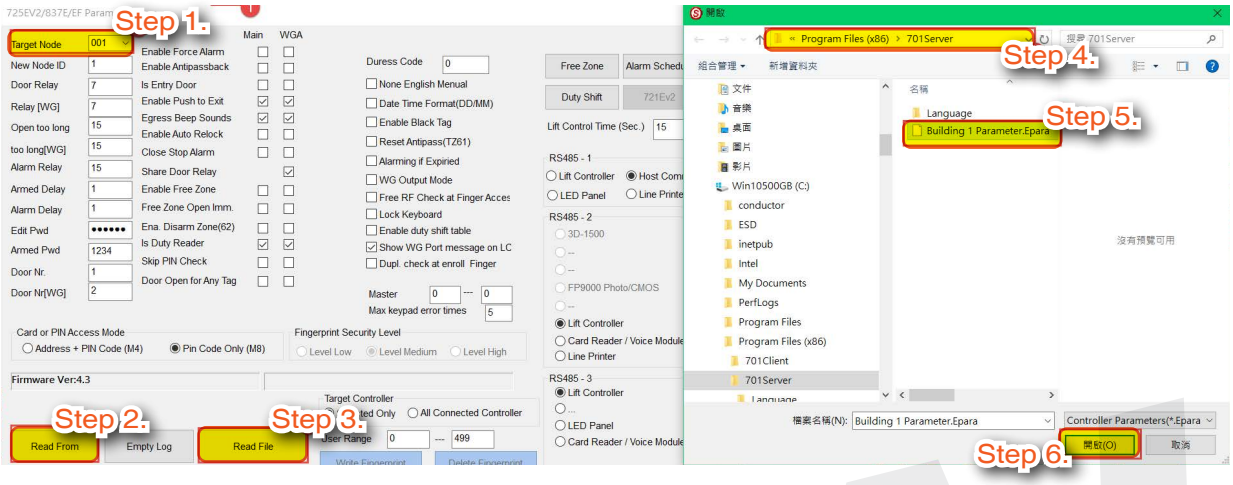
Step 5. Select path folder that you prefer to save the parameter setting

Step 6. Rename the parameter setting and remove the [*] symbol on the file name

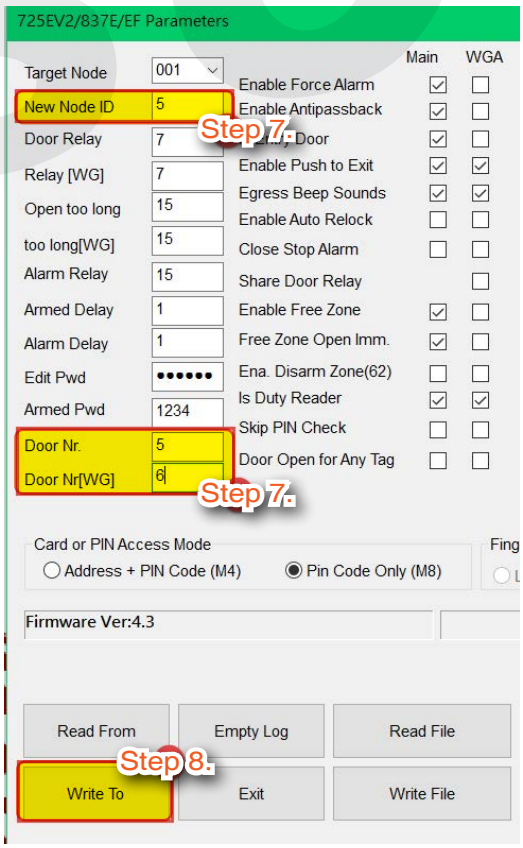
Step 7. Click [save] and your parameter setting is backed up

2. Save default setting and copy to multiple controller's

Create one default parameter setting for one controller and save it (copy), then write it (paste) to other controllers with the same setting. That way, you do not need to do the same process for many controllers with same setting.



Step 1. Select node ID of your new controller that you wish to paste the existed parameter setting
Step 2. Select [Read From] to read current parameter setting of controller
Step 3. Select [Read File] to read the saved parameter setting
Step 4. Select path folder that you prefer to read the parameter setting
Step 5. Select the parameter setting's file
Step 6. Click [open] and your parameter setting will be loaded on 701Server



Picture above is after loading (Read File) of saved parameter setting. You will notice that the parameter setting is difference than the default one. Before you directly write and save the parameter, please change:

Step 7. Input 'New Node ID', 'Door Nr.' And Door Nr [WG]' to differentiate one controller with another. This is because both three setting included on parameter setting BUT each unit controller must have different node ID, door no. and WG door no. this step does not applicable for AR-716-E16 as AR-716-E16 node ID is set up by DIPSWITCH and does not have RFID function on it so door no. and WG door no. does not exist.

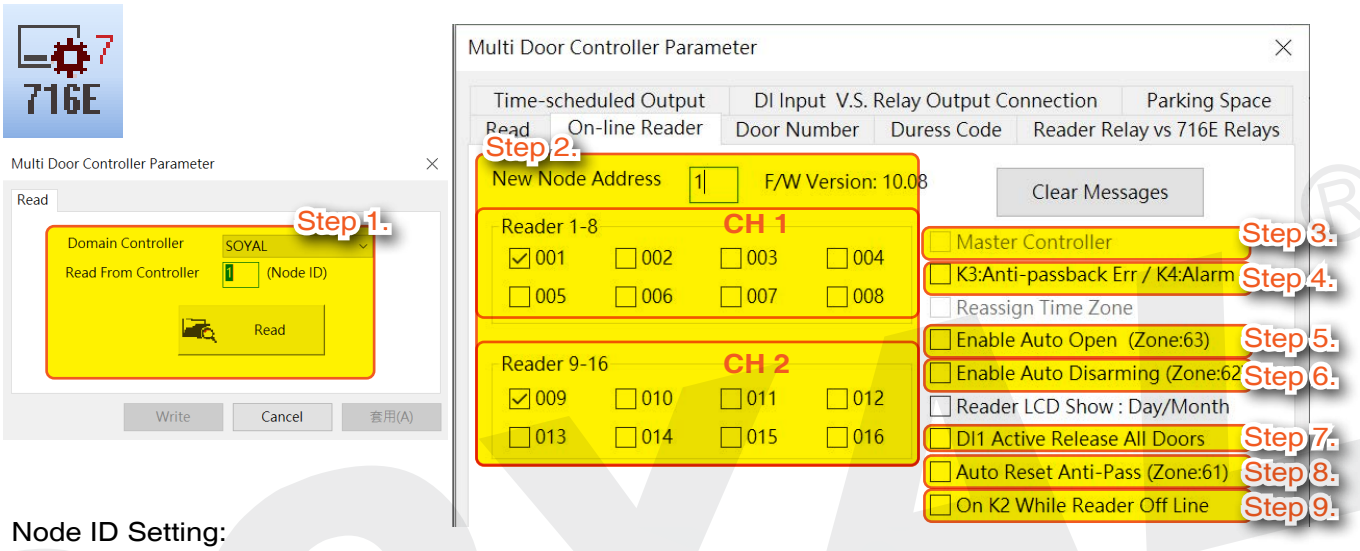
Step 8. Select [Write To] to save the new parameter setting

III. Parameter Setting Overview

8.1 Control Panel AR-716-E18 Parameter Setting

Control Panel AR-716-E18 built-in 4 digital input (DI1, DI2, DI3, DI4) and 4 relay output (K1, K2, K3, K4) that can be assign and set according to requirement and needs.
With expansion relay board AR-716-E-8I8O, it offer additional input and output total 8 digital input and 8 relay output.

• 8.1.1 On-line Reader Setting



Node ID Setting:

Step 1. Select Area and Node ID of the specified controller

Step 2. Select AR-716-E18 connected access controller, CH1: Node ID range 1-8 / CH2: Node ID range 9-16

Parameter Setting:

Step 3. If "K3: Anti-passback Err / K4: Alarm" option is ticked: when someone violates the anti-passback rule, K3 relay of AR-716E will be activated or when the alarm system is activated, K4 relay of AR-716E will be simultaneously activated as well.

Step 4. If "Enable Auto Open (Zone: 63)" option is ticked: enable auto open during the period of time zone 63. After time zone 63 is finished, the lock will be automatically locked again.

Step 5. If "Enable Auto Disarming (Zone: 62)" option is ticked, the selected access controller will automatically enter arming mode during the period of time zone 62. After time zone 62 is finished, the selected access controller will return its former state. That is, if the access controller is already in arming mode before time zone 62, nothing will change; in contrast, if the access controller is at the standby state before time zone 62, it will enter arming mode when time zone 62 begins, and return to the former standby state after time zone 62 is finished.

Step 6. If "DI1 Active Release All Doors" option is ticked: this option is mainly designed for emergency evacuation during fire event. When an alert signal like smoke detection is sent to DI1 of AR-716-E18, it can release all electric locks controlled by the access controllers connected with AR-716-E18 to facilitate the process of evacuation.

Step 7. If "Auto Reset Anti-pass (Zone: 61)" option is ticked: auto reset anti-pass-back function in time zone 61. When the user violates the anti-passback rule, user cannot get access anymore. Reset allows the user get access again at this time regardless of the violation of the anti-pass-back rule before. This function is suitable for limited lunch controller in which employee can only retrieve lunch once a day and auto restart to be function as usual for the next day.

Step 8. If "Auto Reset Anti-pass (Zone: 61)" option is ticked: auto reset anti-pass-back function in time zone 61. When the user violates the anti-passback rule, user cannot get access anymore. Reset allows the user get access again at this time regardless of the violation of the anti-pass-back rule before. This function is suitable for limited lunch controller in which employee can only retrieve lunch once a day and auto restart to be function as usual for the next day.

Step 9. If "On K2 While Reader Off Line" option is ticked: when any access controller connected to AR-716-E18 is disconnected, K2 relay of AR-716-E18 will be activated and a message will be sent to inform the administrator.

Step 9. Click "Write" button to save all settings.

Firmware Information:

This section will show current read controller's firmware version

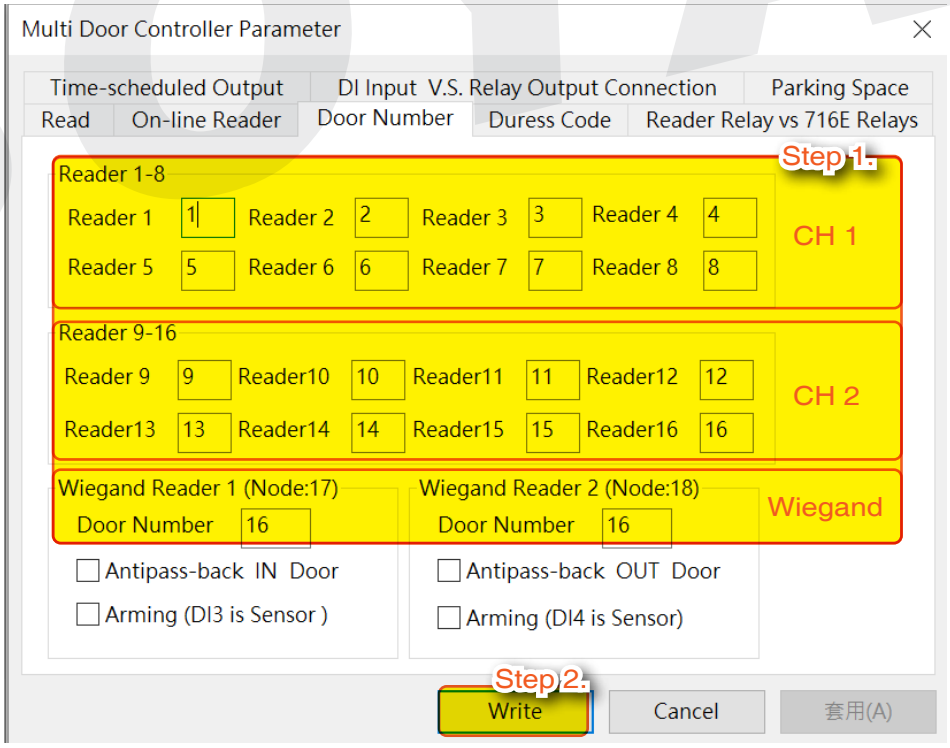
F/W Version: 10.08

• 8.1.2 Door Number Setting

Each door number represents a specific location. When event logs are sent to the computer, you can identify where the location is by the door number.

Physical Node ID: Node ID of the controller for connection with control panel or directly to PC, used for communication identification.

Logical Node ID: correspond to the name of the place and the identification of the entry/exit when editing the access door group to set the permission access for the user's access group, so that any controller wired to electric lock needs to specify the door number.



Step 1. Click "Door Number" and input the assign door number of each reader

Step 2. Click "Write" button to save all settings.

NOTE

There are two WG ports of AR-716-E18, and each port could connect with 1 WG access reader. The Node ID of the first WG reader is 17, and the Node ID of the second WG reader is 18. For Wiegand Reader setting, you can select the following functions:

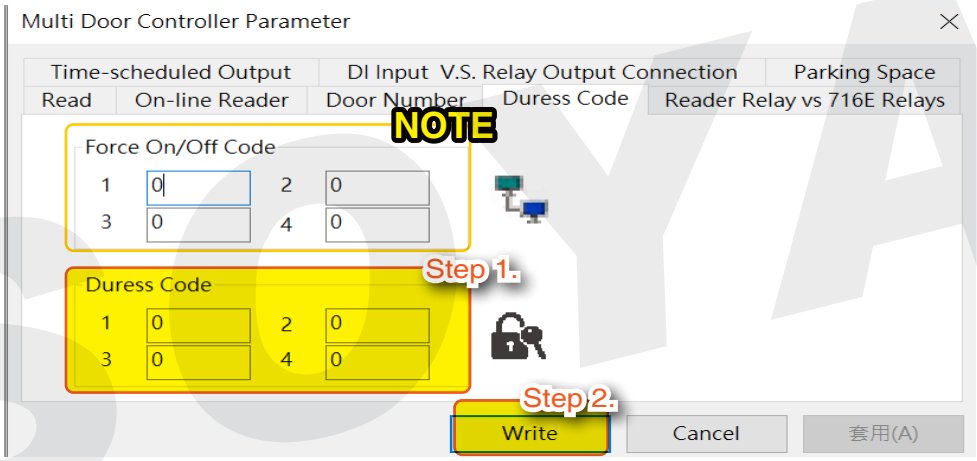
1. Anti-passback
2. DI3/DI4 of AR-716-E18 can act as a sensor for the WG readers.

More Details :

- FAQ : How to setup the door number ?

• 8.1.3 Duress Code

In the event that an assailant or robber ambush you at the entrance and force you to open the door or disarm the system, try to keep calm and input Duress code to open the door, which will simultaneously send a silent alert to the monitoring station or security guards.



Step 1. Enter 4 sets of 4-digit duress code.
If access controller has been set Duress Code before, access controller connected to the control panel AR-716-E18 must listen to the AR-716-E18 control, so there will be four sets of help codes.

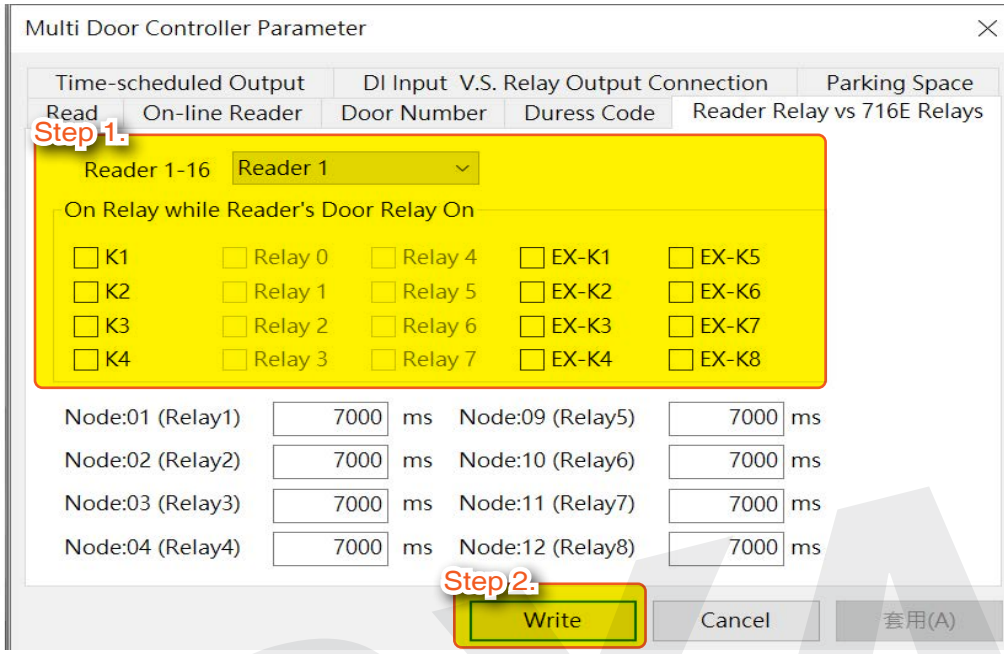
Step 2. Click "Write" button to save all settings.

NOTE

Force On/Off Code, which can be set as 4 sets of 4-digit code, used to control AR-716-E18 relay and corresponding AR-716-E-8I8O I/O Relay to control ON or OFF status of the I/O devices such as the rolling door, air-conditioning, alarm activation... etc.

• 8.1.4 Reader Relay vs 716E Relays

For security concerns, we can set the synchronization output of relays between the relay of the readers connected to AR-716-E18 and the 4 relays of AR-716-E18 (K-1 ~ K-4), as well as the action time how long these relays will be activated. With an additional extension relay board, AR-716-IO, there can be 8 more relays for further setting.



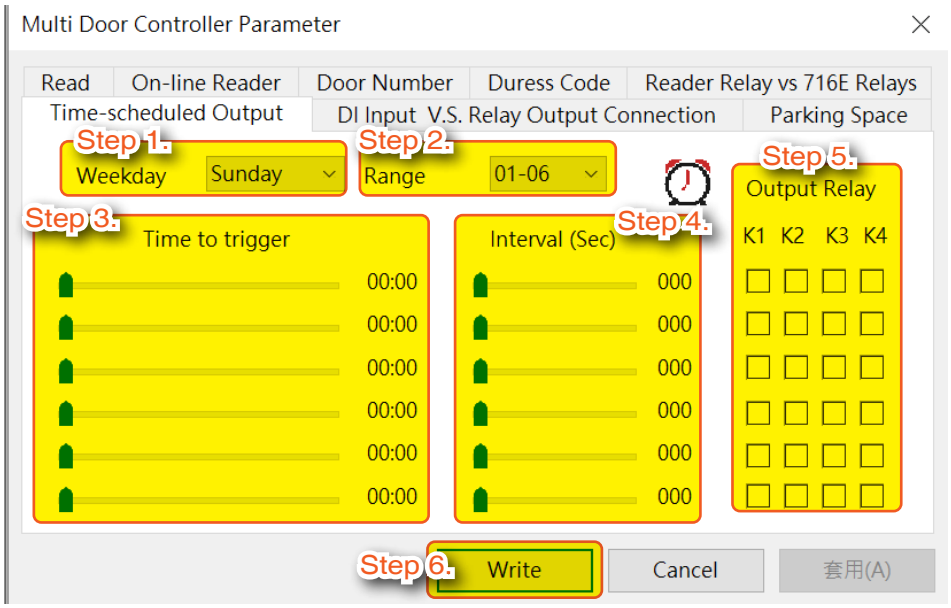
Step 1. Select the Node ID of the reader in "Reader 1-16" field and tick one or more relays between K-1 ~ K-4 to be simultaneously ON when reader's door relay is on.
EX-K1 until EX-K8 is setting that is available when AR-716-E18 is wired to I/O expansion board AR-716-E-8I8O

Step 2. Set the reader node ID 1-16 relay output time.

Step 3. Click "Write" button to save all settings.

• 8.1.5 Time-scheduled Output

You can set the time-scheduled output of designated relay of AR-716-E18 on designated time, weekday for specific interval (second). This function is mainly applied to alarm in the office or industrial automatic control.



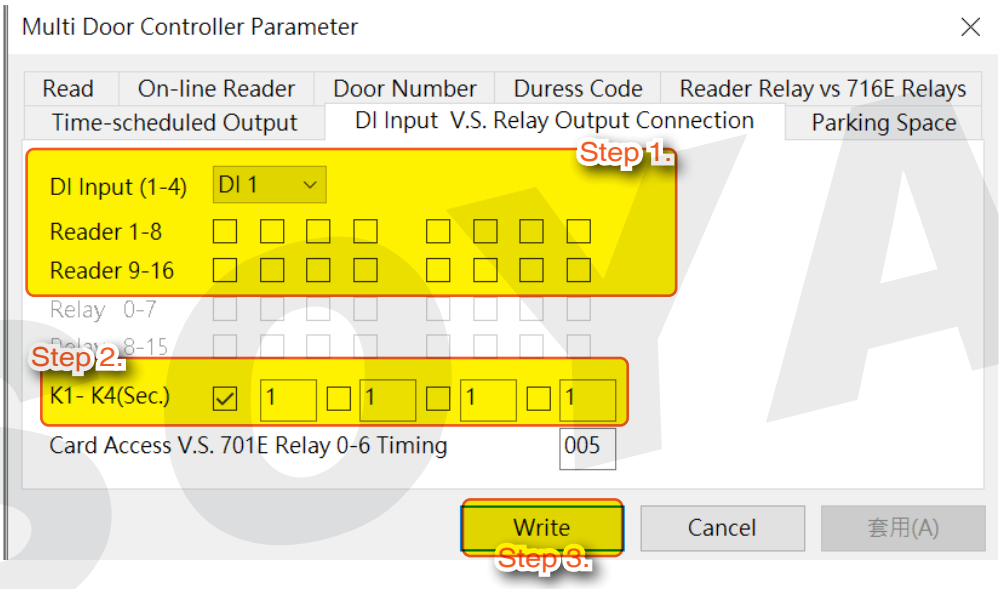
Step 1. Select a specific day in “Weekday” field
Step 2. Select the range of displayed data (6 groups at a time).
Step 3. Select "Time to trigger" , for example: 04:50 for the first group and 09:40 for the second group (by 24-hour clock).
Step 4. Select the activating interval, for example: 10 sec.
Step 5. Select relay for output.
Step 6. Click "Write" button to save all settings.

More Details :

- FAQ : How to set up “Time-scheduled Output” on AR-716E, and how to connect the alarm?

• 8.1.6 DI Input V.S. Relay Output Connection

The DI of AR-716E can be used to control relays and request to exit (RTE) buttons.



Step 1. Select one DI input from DI 1 ~ DI 4 and assign to reader
Step 2. Select one corresponding relay from K1 ~ K4 by ticking the box and input relay time.
For example K1 for DI1 and K2 for DI2 (please set all the relay time in the window when DI 1 is selected).

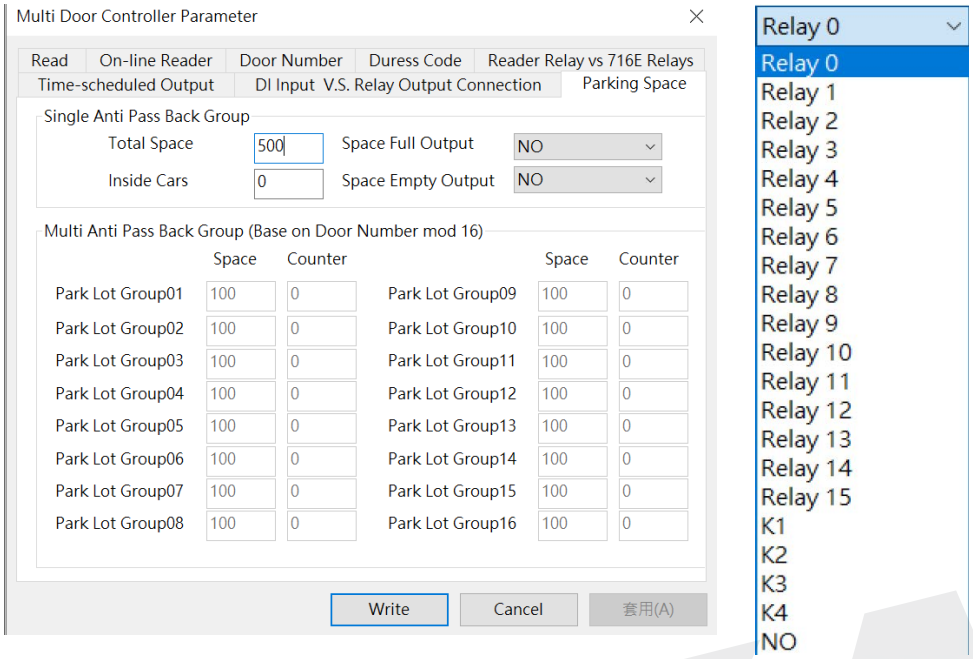
If you didn’ t select the corresponding relay, the relay of the access controller will be activated for the period of Door Relay Time (Electric Door relay Operate Time) which is set directly in program mode of this access controller.
Step 3. Click "Write" button to save all settings.

More Details :

- FAQ : AR-727H + AR-716E to set anti-passback, how to set alarm to be active when breach of anti-passback setting?
- FAQ : Reader Relay vs AR-716E Relay at 716E parameter.

• 8.1.7 Parking Space

This function is used for parking lot control, which can monitor the parking space status and output message to the designated device.



AR-716-E18 built-in parking space management and single/multi anti-passback group. At the same time, it has on-board function of external LED display integration to show current status of the parking lot.

Single Anti Pass Back Group:

Step 1. Total Space: set a number of total space of the parking lot

Step 2. Space Full Output: when the parking lot is totally full, K3 will be activated and send a message signal like "No Vacancy" to an external LED display.

Step 3. Inside Cars: get the current number of cars inside the parking lot

Step 4. Space Empty Output: when there is any parking space available in the parking lot, K4 will be activated and send a message signal like "Spaces Available" to an external LED display.

NOTE

Space Full Output/Space Empty Output selection:
Relay 0-15: relay of access controller Node ID 1-16
K1, K2, K3, K4: select activated relay output trigger from on-board relay AR-716-E18 between K1-K4
NO: there is no designated relay assigned for this action

Multi Anti Pass Back Group (Base on Door Number mod 16):
This function is used for Multi-Cars share One Parking Space, in which car is denied to enter when all spaces within the group are occupied.
Customized firmware required for AR-716-E18 to enable this function.

More Details :

- FAQ :How to edit user to access each door at different specific time zone on 716E?
- FAQ: How to enable AR-716E【Force On/Off Code】function?
- FAQ: How to setup anti-pass back function on wiegand reader and AR-727H which are under AR-716E?

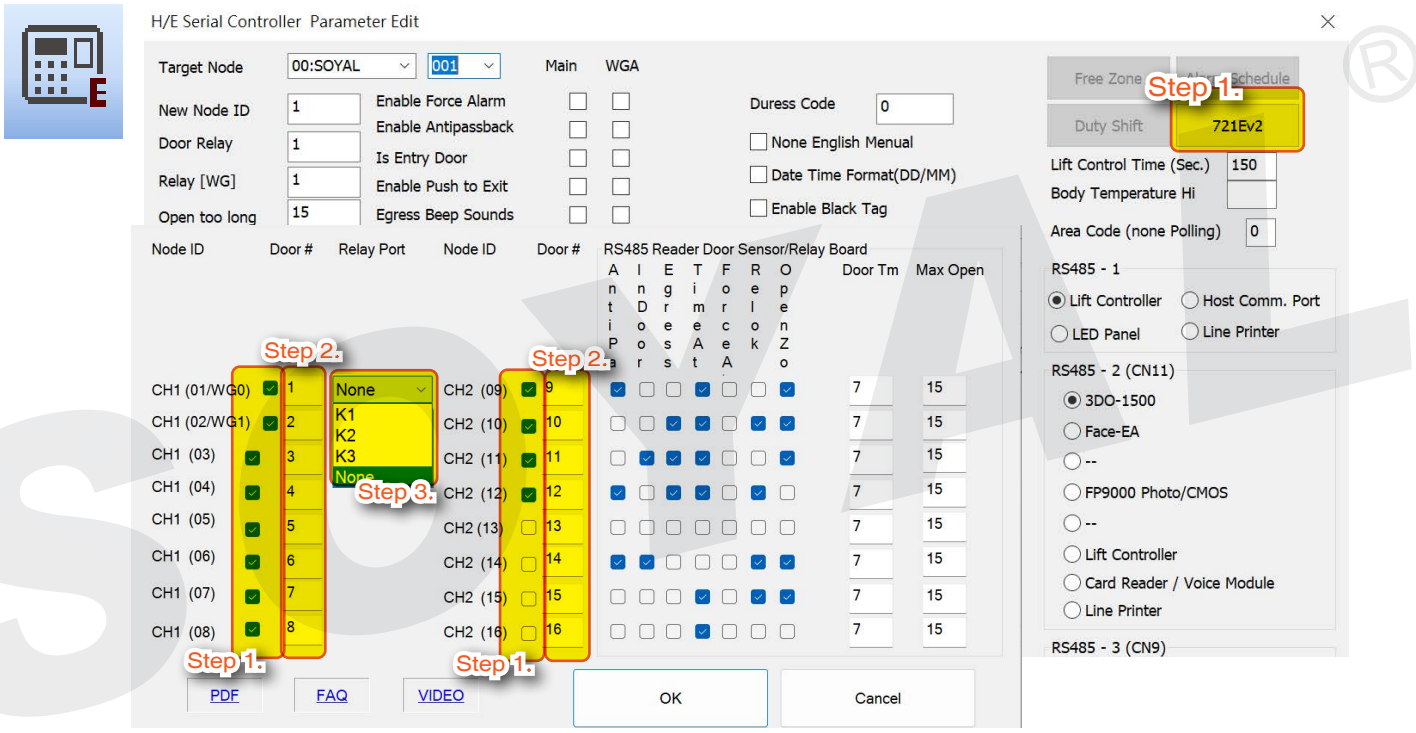
More Details :

- FAQ: Why swiping card on controller under AR-716E the event log shows card code 00000?
- FAQ: How to clear all messages which are saved in the controller?

8.2 Control Panel AR-716-E16 Parameter Setting

Control Panel AR-716-E16 built-in 3 relay output (K1, K2, K3) that can be assign and set according to requirement and needs.

• 8.2.1 Set the connected access controller Node ID

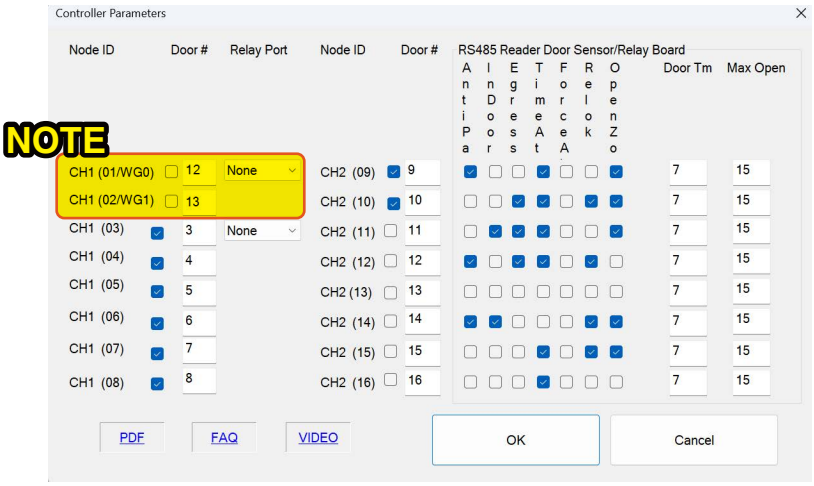


Step 1. Tick the connected access controller

- AR-716-E16 built-in 2 WG Port connection. If wiring plan to wire WG Port 0 and WG Port 1, for access controller please start from node ID 3.
  This is because WG Port 0, 1 and Node ID 1, 2 share the same Door Number
- Please refrain from ticking the connected Node ID if the controller is not connected.

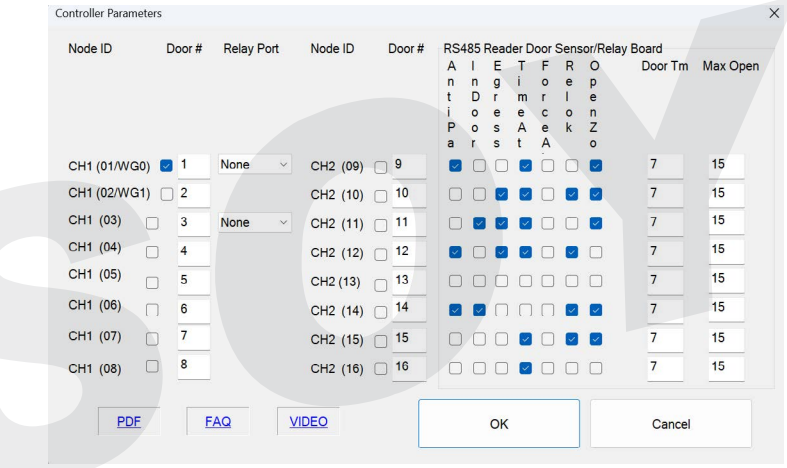
Example 1: WG Port wired to WG reader

NOTE wiring to WG reader does not required to tick the box



CH1	CH2	WG
	Node ID 9	WG0
	Node ID 10	WG1
Node ID 3	Node ID 11	
Node ID 4		
Node ID 5		
Node ID 6		
Node ID 7		
Node ID 8		

Example 2: WG Port does not wire to any WG reader



CH1	CH2	WG
Node ID 1	Node ID 9	
Node ID 2	Node ID 10	
Node ID 3	Node ID 11	
Node ID 4	Node ID 12	
Node ID 5	Node ID 13	
Node ID 6		
Node ID 7		
Node ID 8		

Step 2. Door #: enter Door Number

Step 3. Relay Port: Available for WG Port 0*, RS485 CH1 Node ID 3, and RS485 CH2 Node ID 9. This setting is to enable reader wired under AR-716-E16 to use on-board relay output instead of the access controller own relay.

K1/K2: the built-in relay of control panel to externally control the electric lock (if this function is selected, access controller's connection to electronic lock is disabled, and the electric lock is connected to the K1/K2 contact). It is suitable for public door access such as Gate & Back Door access to provide safer connection.

For example: Gate installed Node ID 3 use K1 contact and Back Door installed Node ID 9 use K2 contact.

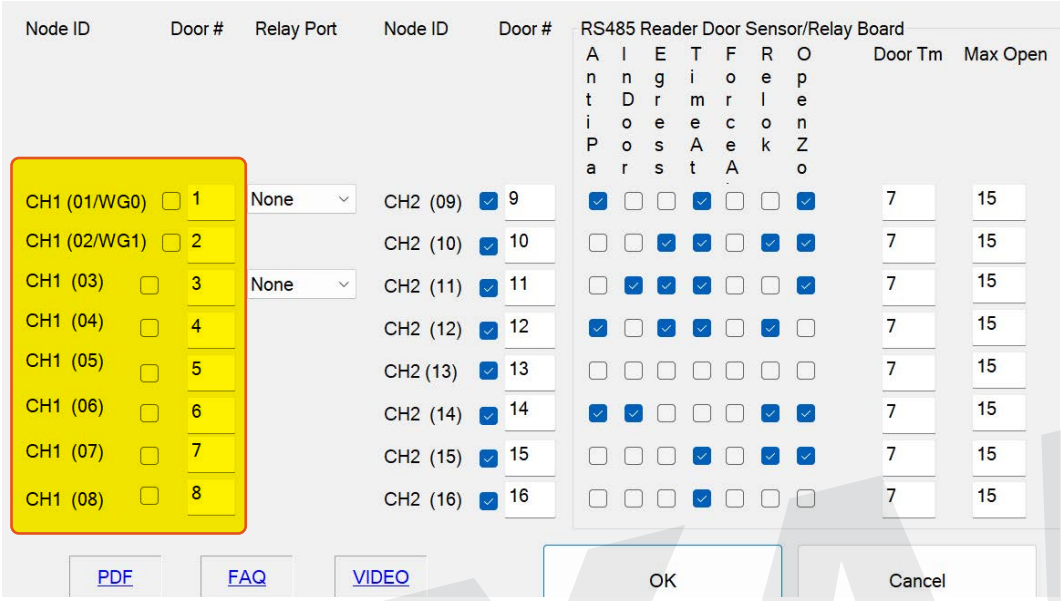
K3 : Public alarm

None: Use the access controller on-board relay to control the electric lock

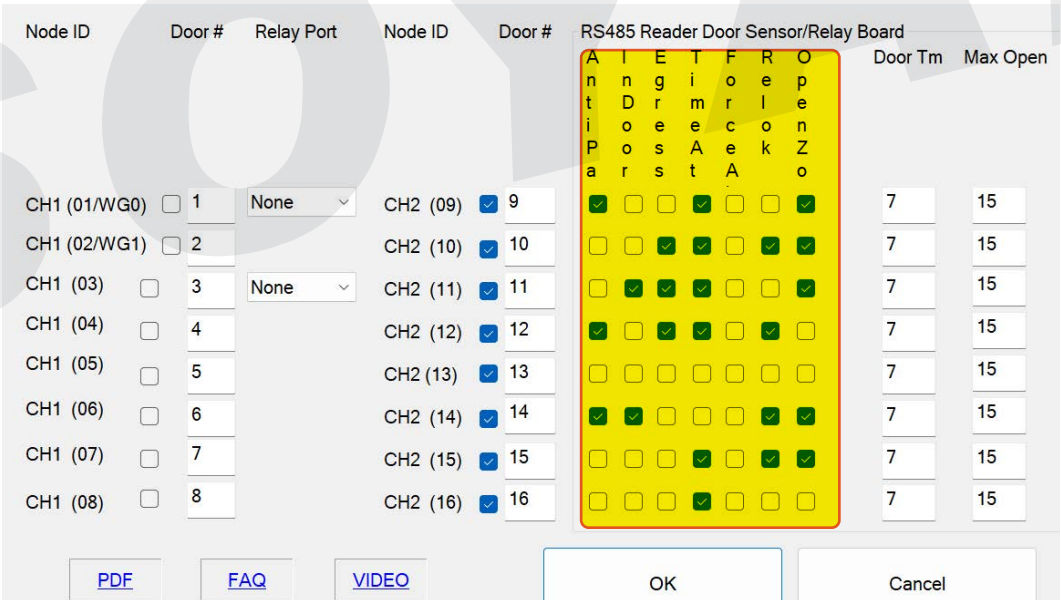
WG Port 0 Relay Port option is only for dual door interlocking with CH2 Node ID 9 (Node ID 9 controller must be activated dual-door interlocking function by inputting command 44)

• 8.2.2 High-Security Mode Settings

1. When CH1 is connected to the I/O expansion board, the selection for station numbers 01 to 08 must be unchecked.



2. Function Description



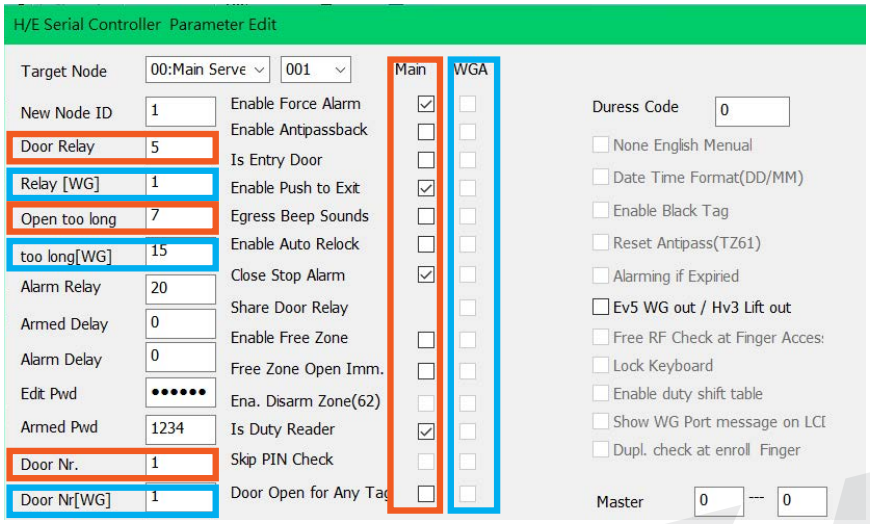
	701ServerSQL Screen Names	Function Description
1	Anitipa	Anti-pass-back
2	Indoor	Entry/Exit Reader
3	Egress	Exit by Push Button
4	TimeAt	Entry and Exit Access is recorded on Duty Report
5	ForceA	Enable force Open trigger alarm
6	Relok	Activate close door automatically lock (Auto-Relock)
7	OpenZo	Auto Open

• 8.2.3 Reader Setting

Partial AR-716-E16 Parameter Setting is divided into 'Main' & 'WG'

'Main' section is for AR-716-E16 as master controller and WG Port 0 reader

'WG' section is for WG Port 1 reader

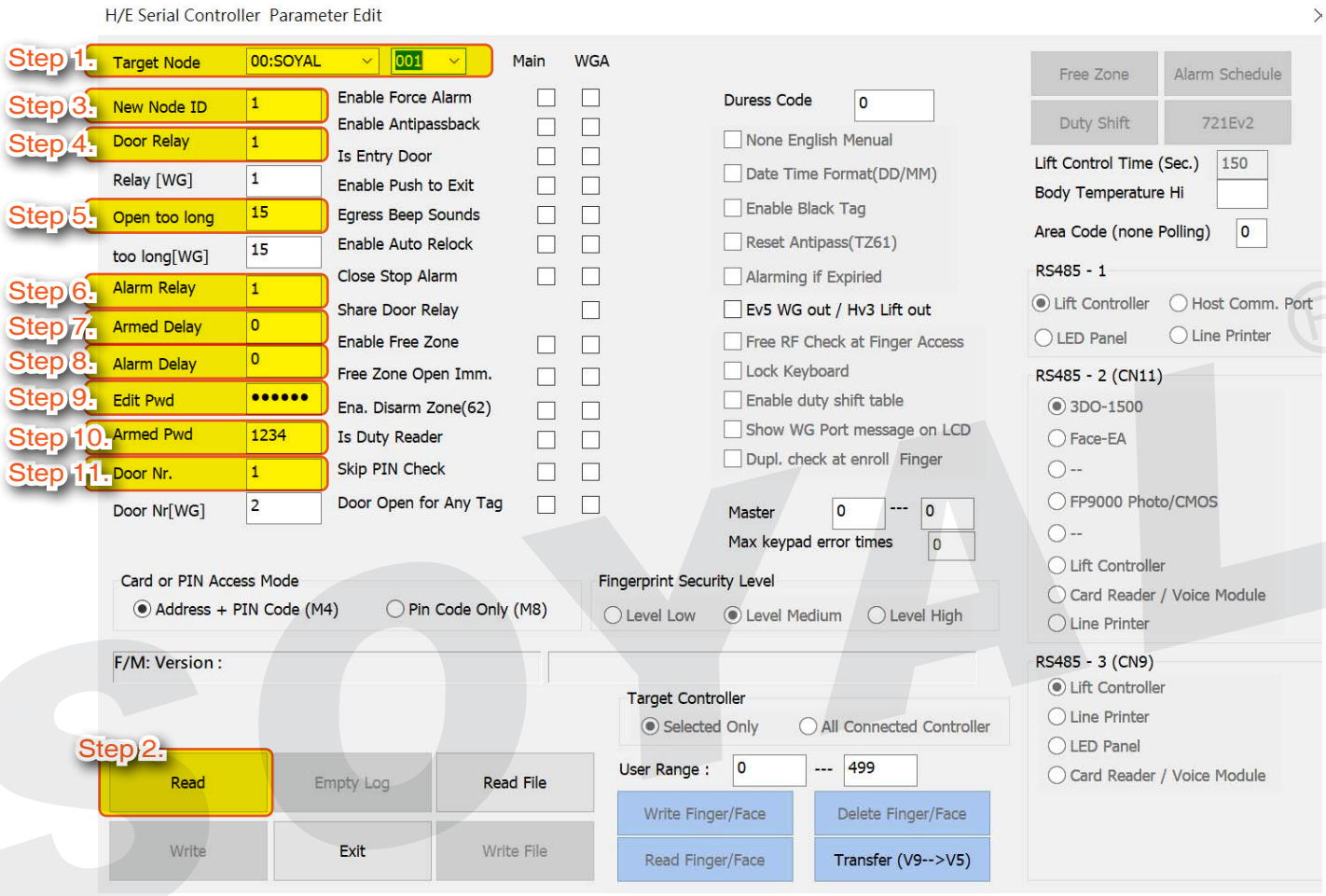


More Details :

- FAQ :How to enable Anti-Pass back function in-between multi-doors under 716E

8.3 Home Series (H Series) Controller Parameter Setting

The parameter setting of H Series is the same like in E Series but is limited to particular function than E Series controller. The unusable setting is disable and could not be set.



Step 1. **Target Node:** Select Area and Node ID of the specified controller

Step 2. **Read:** Read the current setting of the specified controller

Step 3. After the communication is successful, you can also modify the Node ID of this access controller in "**New Node ID**" field.

Step 4. **Door Relay:** Door Relay Time of the access controller, after access identification is successful, controller will trigger the relay to release lock and **how long the lock is being released to indicate door open is determined by Door Relay Time.**

The setting of Door Relay Time is based on what type of electric lock installed onsite.

Recommended setting:

1. Fail-Safe type of lock such as Electric Bolt Lock and Magnetic Lock is 15 seconds (recommended to combine with Auto Relock function)
2. Fail-Secure type of lock such as Electric Strike and Cabinet Lock is 0.2 seconds. Default value is 7 seconds.

Pulse setting (short-term release): range 001~600 seconds, if set as 01-0.9seconds enter 601~609

Latch setting (output continuously): enter 000

Step 5. **Open too long:** or also known as **Door Close Time or Door Open Waiting Time**. After the period of door relay time trigger relay and open the door, the door contact will start detecting the door status; however, sometimes the door is not be closed in time, so the door close time gives users a **buffer time (delay time) to close the door properly before the door contact starts detecting it as Door Open Too Long.**
For example: Default value of door open too long is 15 seconds (default), the door contact will start detecting after Door Relay Time (10 sec) + Door Close Time (15 sec), and the user should close the door properly within the total period (25 sec).
Note: Door Open Too Long will not be acknowledge if activating Auto Relock function, as door will relock immediately whenever door contact detect door is closed.
Default value is 15 seconds.

Step 6. **Alarm Relay:** When alarm event is triggered, alarm will output continuously for a period of time according to Alarm Relay Time.
Pulse setting (short-term release): range 001~600 seconds, if set as 01-0.9seconds enter 601~609
Latch setting (output continuously): enter 000
Default value is 15 seconds.

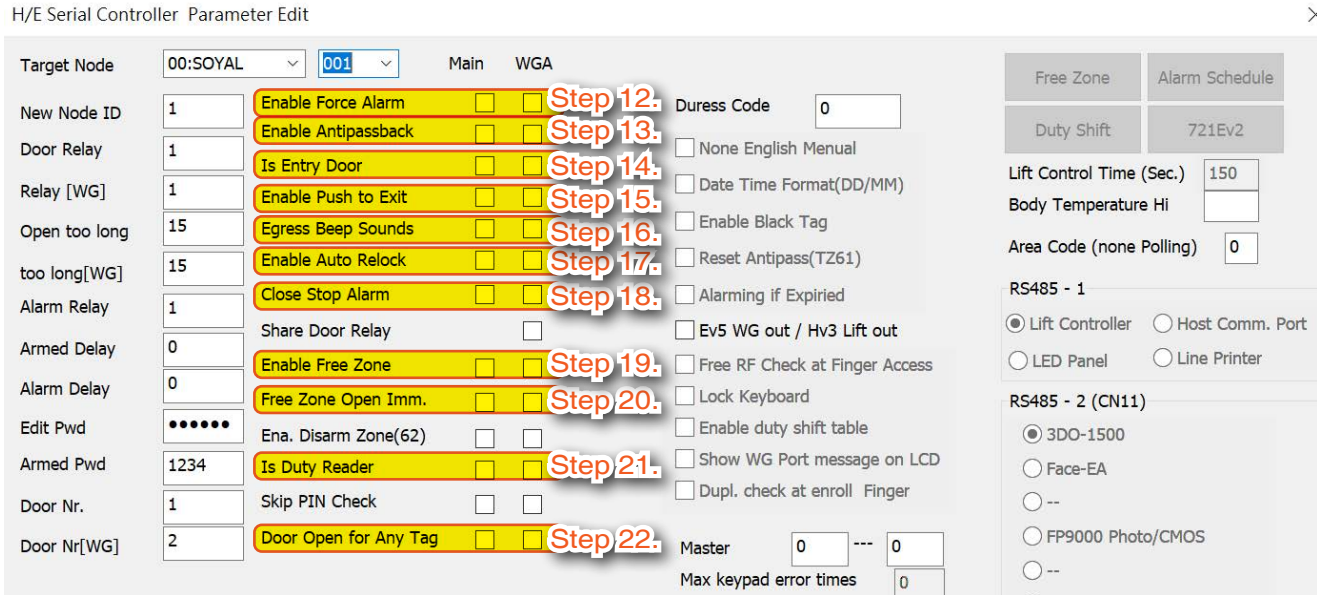
Step 7. **Armed Delay:** After activating Arming mode, access controller enter Arming mode after a period of **Arming Delay Time**, which gives users a buffer time to exit without triggering the alarm.
Default value is 1 second.

Step 8. **Alarm Delay:** Before Alarm Event is triggered, there is **a set of time period between conditions that triggered the alarm and the alarming event which is called Alarm Delay Time.** Alarm Delay Time gives users a buffer time to turn off the alarm before the beeper is sounding or an alarm signal is sent to the security guards.
Default value is 1 second.

Step 9. **Edit Pwd:** Master Code or Programming Code of the Access Controller can be changed from this field. Default Master Code is 123456.

Step 10. **Armed Pwd:** There are three method to enabling Arming Mode 1. Enter programming mode and exit programming mode by entering **# 2. Swipe Master Range card 3. **Enter Arming Password**. To enter the Arming Password there are two procedures:
1. Normal door open procedure + 4-digit Arming PWD + #
2. Without opening the door + 4-digit Arming PWD + Presenting a valid card
Default Arming Password is 1234.

Step 11. **Door Nr.:** Each door number of the controller can be changed according to the corresponding area or door number assigned. Access control system managed by PC will show specific door number on entry or exit record. Door number can be repeated and used in the same area but corresponding to the area and door itself.
Default value is 1.



Step 12. **Enable Force Alarm:** In the event that any door is opened without normal access like presenting a valid card from the outside or pressing the RTE button from the inside, it will cause a Force Open condition. This situation will trigger the Force Open Alarm if the access controller is under Arming mode.

Step 13. **Enable Antipassback:** If there is an external WG reader connected to this access controller, you can tick this option to enable the anti-passback rule.

Step 14. **Is Entry Door:** Determine door is exit or entry
If selecting controller for entry, check the "Is Entry Door" box
If selecting controller for exit, do not check "Is Entry Door" box, just left it unchecked

Step 15. Enable Push to Exit: Enable or disable exit door by Egress Button.
Default value is enabling for both Main and WG.

Step 16. Egress Beep Sounds: Enable or disable beeper sound when Egress is pressed.
Default value is enabling for both Main and WG.

Step 17. **Enable Auto Relock:** The electric lock will be only lockable after the period of Door Relay Time, so there might be a gap between closing the door and the door being actually locked. By **enabling the Auto Relock function which will let the door relock immediately whenever detecting the door is closed by the door contact.** This setting is suggested for fail-safe lock installation such as electric bolt and magnetic lock.

Step 18. **Close Stop Alarm**: There are three options to stop alarming event 1. Swipe valid card 2. Press egress button 3. Close door
When Close Stop Alarm function is checked, alarming event will stopped when door is closed or pressing egress button.
When this option is remain unchecked, alarming event will only stop when valid card is presented.
Default value is unchecked means alarm event will only stop when swiping valid card

Step 19. **Enable Free Zone**: This option is to enable or disable auto open zone (Timezone 63) function. Meanwhile, Auto open time zone setting refer to Step 43.

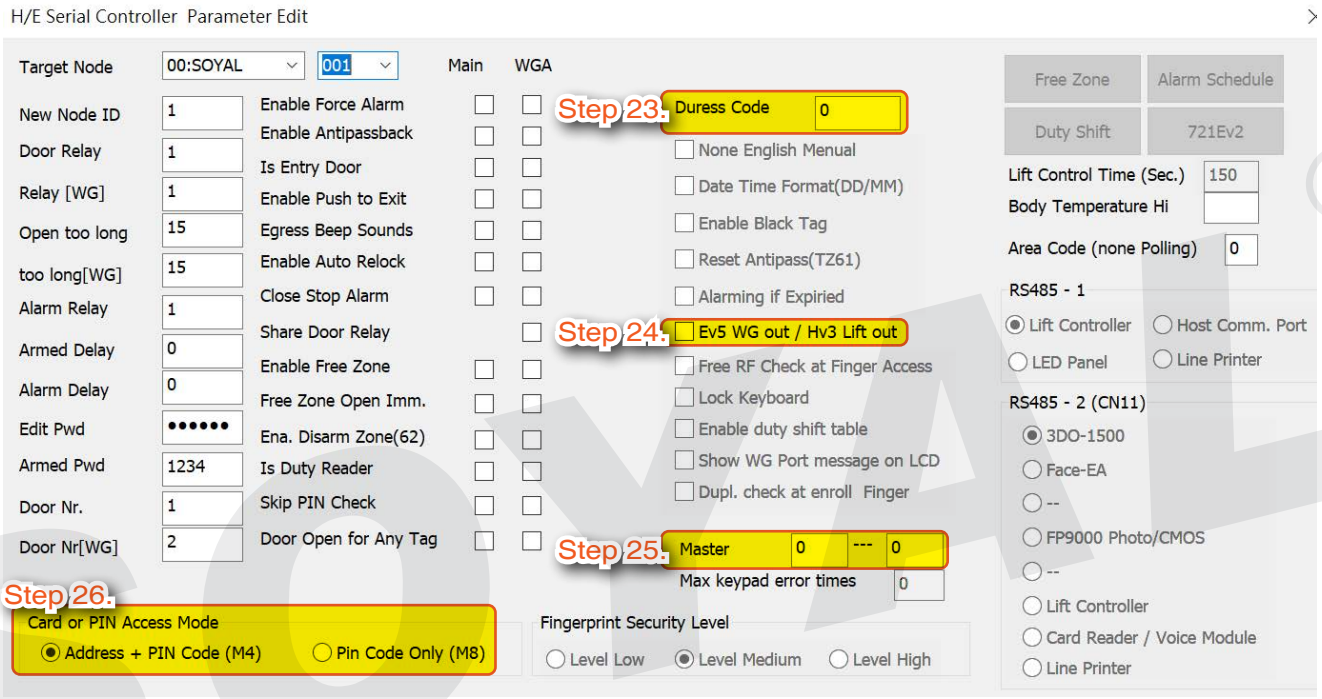
Complete method of Auto Open Zone Setting:

- E Series Controller : Auto Open Zone for all E/H-V5 series controller
- H Series Controller: Auto Open Zone for all H series controller and digital door lock AR-323D without keypad

Step 20. **Free Zone Open Imm.**: There are two ways to enable auto open timezone (Timezone 63):
1. When Auto-Time Zone begin, the door will be automatically open without presenting 1st valid Card.
2. **When Auto-Time Zone begin, the door don't automatically be opening till any one authorized user present a valid card to controller to open the door (Default Value)**
By enabling this function, it will enable auto open zoon when time has come.

Step 21. **Is Duty Reader:** Set controller and reader into Time Attendance device, when this option is checked, the event logs recorded will be integrated to the Time Attendance Report.
Default value is enabling for both Main and WG

Step 22. **Door Open for Any Tag:** Used for short-term activities or temporary events which enable door open whenever a card with the same frequency of the access controller is presented.



Step 23. **Duress Code:** In case an assailant or robber ambush at the entrance and force you to open the door or disarm the system, try to keep calm and input Duress code to open the door, which will simultaneously send a silent alert to the monitoring station or security guards.
Default value: 0 (not set)

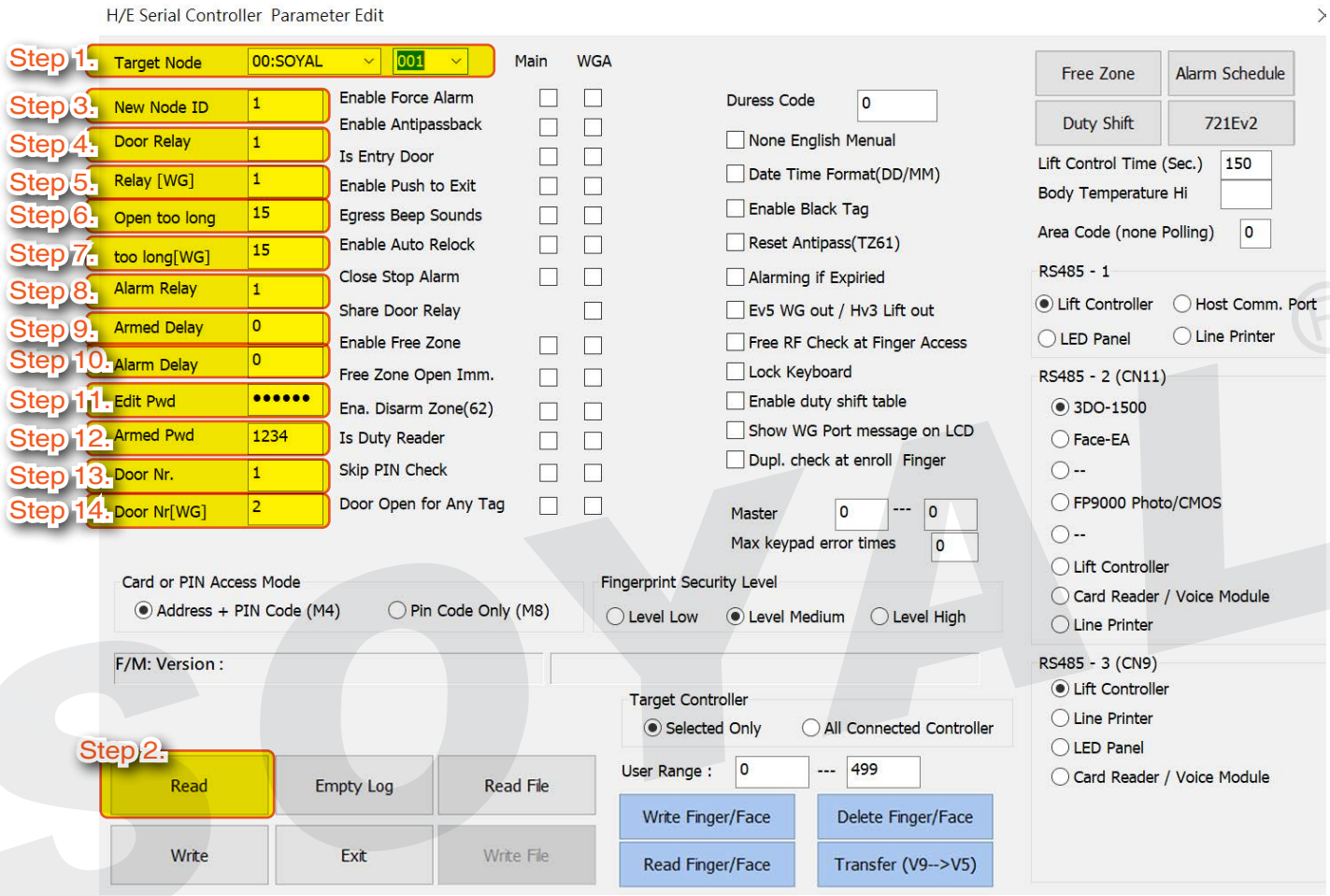
Step 24. **Ev5 WG out / Hv3 Lift out**: For E Series controller, check this option will enable controller **converted into a reader function** (convert duress and arming output into WG Mode WG0 Output and WG1 Output), for H series controller this check this function will **enable lift control function** (convert the alarm output terminal into lift control function)

Step 25. **Master Range:** Range of Master(Administration) user address to be set. Master user has authority to enter programming mode by swipe card + press #. For example if entering 1-5 means set user range 1-5 as Master/Admin.

Step 26. **Card or PIN Access Mode:** SOYAL offer three options of access mode
- Address + PIN Code (M4): Access by entering user address + PIN
- PIN Code Only (M8): Access by entering PIN only (Default)
M6: Standalone only, this option is not available for networking thus this option is not available in Software setting.

8.4 Enterprise Series (E Series) Controller Parameter Setting

Enterprise Series (E Series) Controller with connection to WG reader and second unit of egress, door sensor, and door lock function achieved dual-door controller feature. This means, E Series Controller eligible to edit parameter setting of its WG reader.



Step 1. **Target Node:** Select Area and Node ID of the specified controller

Step 2. **Read:** Read the current setting of the specified controller

Step 3. After the communication is successful, you can also modify the Node ID of this access controller in "**New Node ID**" field.

Step 4. **Door Relay:** Door Relay Time of the access controller, after access identification is successful, controller will trigger the relay to release lock and **how long the lock is being released to indicate door open is determined by Door Relay Time.**

The setting of Door Relay Time is based on what type of electric lock installed onsite.

Recommended setting:

1. Fail-Safe type of lock such as Electric Bolt Lock and Magnetic Lock is 15 seconds (recommended to combine with Auto Relock function)
2. Fail-Secure type of lock such as Electric Strike and Cabinet Lock is 0.2 seconds. Default value is 7 seconds.

Pulse setting (short-term release): range 001~600 seconds, if set as 01-0.9seconds enter 601~609

Latch setting (output continuously): enter 000

Step 5. **Relay [WG]:** Door Relay Time Setting for Wiegand Reader (only eligible for E Series controller's WG Reader and WG Port 1 under AR-716-E16)
Default value is 7 seconds.

Step 6. **Open too long:** or also known as **Door Close Time or Door Open Waiting Time**. After the period of door relay time trigger relay and open the door, the door contact will start detecting the door status; however, sometimes the door is not be closed in time, so the door close time gives users a **buffer time (delay time) to close the door properly before the door contact starts detecting it as Door Open Too Long.**
For example: Default value of door open too long is 15 seconds (default), the door contact will start detecting after Door Relay Time (10 sec) + Door Close Time (15 sec), and the user should close the door properly within the total period (25 sec).
Note: Door Open Too Long will not be acknowledge if activating Auto Relock function, as door will relock immediately whenever door contact detect door is closed.
Default value is 15 seconds.

Step 7. **too long[WG]:** Door Close Time for Wiegand Reader (only eligible for E Series controller's WG Reader and WG Port 1 under AR-716-E16)
Default value is 15 seconds.

Step 8. **Alarm Relay:** When alarm event is triggered, alarm will output continuously for a period of time according to Alarm Relay Time.
Pulse setting (short-term release): range 001~600 seconds, if set as 01-0.9seconds enter 601~609
Latch setting (output continuously): enter 000
Default value is 15 seconds.

Step 9. **Armed Delay:** After activating Arming mode, access controller enter Arming mode after a period of **Arming Delay Time**, which gives users a buffer time to exit without triggering the alarm.
Default value is 1 second.

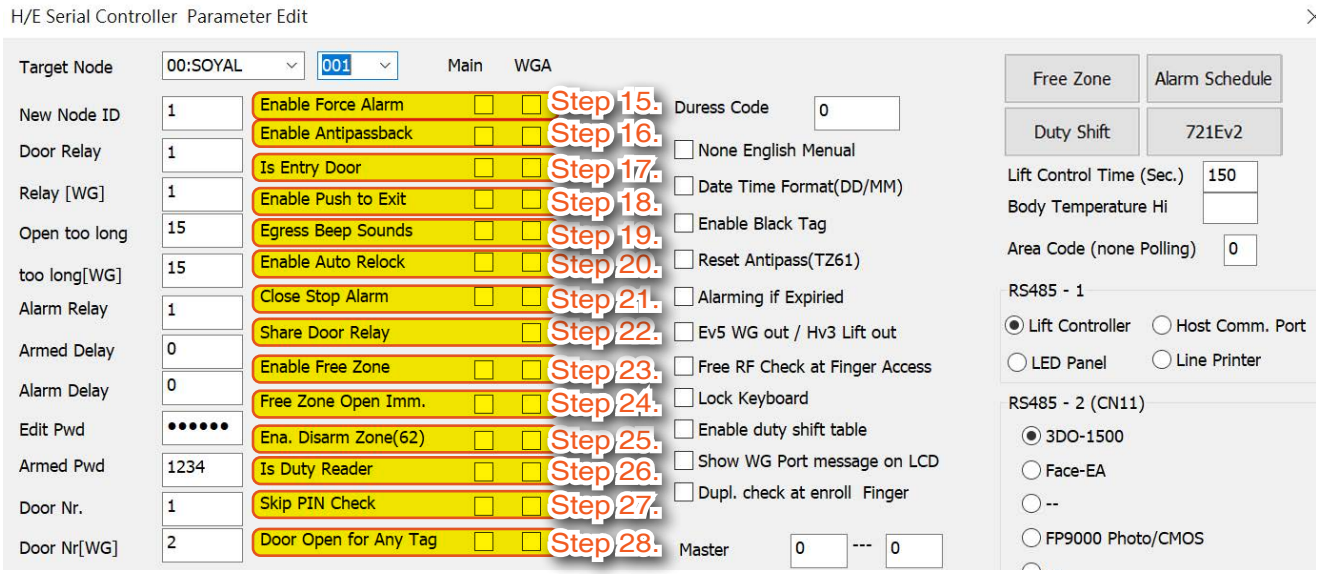
Step 10. **Alarm Delay:** Before Alarm Event is triggered, there is **a set of time period between conditions that triggered the alarm and the alarming event which is called Alarm Delay Time**. Alarm Delay Time gives users a buffer time to turn off the alarm before the beeper is sounding or an alarm signal is sent to the security guards.
Default value is 1 second.

Step 11. **Edit Pwd**: Master Code or Programming Code of the Access Controller can be changed from this field. Default Master Code is 123456.

Step 12. **Armed Pwd:** There are three method to enabling Arming Mode 1. Enter programming mode and exit programming mode by entering **# 2. Swipe Master Range card 3. **Enter Arming Password**.
To enter the Arming Password there are two procedures:
1. Normal door open procedure + 4-digit Arming PWD + #
2. Without opening the door + 4-digit Arming PWD + Presenting a valid card
Default Arming Password is 1234.

Step 13. **Door Nr.:** Each door number of the controller can be changed according to the corresponding area or door number assigned. Access control system managed by PC will show specific door number on entry or exit record. Door number can be repeated and used in the same area but corresponding to the area and door itself.
Default value is 1.

Step 14. **Door Nr. [WG]:** WG Door Number can be changed according to the corresponding Main access controller's area and door number. WG Door Number is only eligible for E Series controller's WG Reader and WG Port 1 under AR-716-E16.
Default value is 2.



Step 15. **Enable Force Alarm:** In the event that any door is opened without normal access like presenting a valid card from the outside or pressing the RTE button from the inside, it will cause a Force Open condition. This situation will trigger the Force Open Alarm if the access controller is under Arming mode.

Step 16. **Enable Antipassback:** If there is an external WG reader connected to this access controller, you can tick this option to enable the anti-passback rule.

Step 17. **Is Entry Door:** Determine door is exit or entry
If selecting controller for entry, check the "Is Entry Door" box
If selecting controller for exit, do not check "Is Entry Door" box, just left it unchecked

Step 18. **Enable Push to Exit:** Enable or disable exit door by Egress Button.
Default value is enabling for both Main and WG.

Step 19. **Egress Beep Sounds:** Enable or disable beeper sound when Egress is pressed.
Default value is enabling for both Main and WG.

Step 20. **Enable Auto Relock:** The electric lock will be only lockable after the period of Door Relay Time, so there might be a gap between closing the door and the door being actually locked. By **enabling the Auto Relock function which will let the door relock immediately whenever detecting the door is closed by the door contact**. This setting is suggested for fail-safe lock installation such as electric bolt and magnetic lock.

Step 21. **Close Stop Alarm:** There are three options to stop alarming event 1. Swipe valid card 2. Press egress button 3. Close door
When Close Stop Alarm function is checked, alarming event will stopped when door is closed or pressing egress button.
When this option is remain unchecked, alarming event will only stop when valid card is presented.
Default value is unchecked means alarm event will only stop when swiping valid card.

Step 22. **Share Door Relay:** if the WG reader and the access controller control the same one door, check this option (this setting is only available for WG).

Step 23. **Enable Free Zone:** This option is to enable or disable auto open zone (Timezone 63) function. Meanwhile, Auto open time zone setting refer to Step 43.

Complete method of Auto Open Zone Setting:

- E Series Controller : Auto Open Zone for all E/H-V5 series controller
- H Series Controller: Auto Open Zone for all H series controller and digital door lock AR-323D without keypad

Step 24. **Free Zone Open Imm.**: There are two ways to enable auto open timezone (Timezone 63):

1. When Auto-Time Zone begin, the door will be automatically open without presenting 1st valid Card.
2. **When Auto-Time Zone begin, the door don't automatically be opening till any one authorized user present a valid card to controller to open the door (Default Value)**

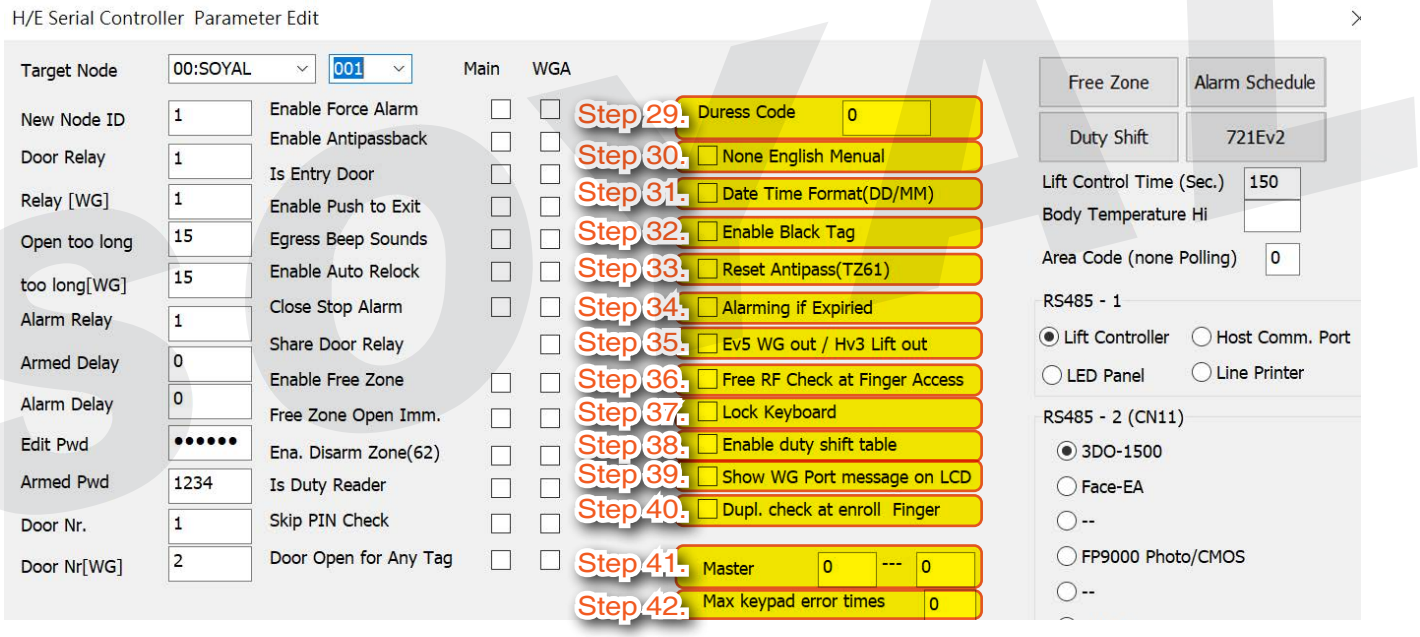
By enabling this function, it will enable auto open zoon when time has come.

Step 25. **Ena. Disarm Zone(62):** Timezone 62 is specifically assigned for controller' s autmomatically set as arming and disarming. The start time will automatically set controller into arming mode, and the end time will automatically set controller into disarming mode (standby mode). For example: set Timezone 62 as 08:00-12:00 means controller will enter arming mode at 08:00 and disarming at 12:00.

Step 26. **Is Duty Reader:** Set controller and reader into Time Attendance device, when this option is checked, the event logs recorded will be integrated to the Time Attendance Report.
Default value is enabling for both Main and WG.

Step 27. **Skip PIN Check:** For a system that has both controller and reader with keypad and no keypad, **user access mode set as "Card & PIN" could not enter PIN in no keypad controller/reader**. In this case, for no keypad controller or reader to omit enter PIN required to enable "Skip PIN Check" function.

Step 28. **Door Open for Any Tag:** Used for short-term activities or temporary events which enable door open whenever a card with the same frequency of the access controller is presented.



Step 29. **Duress Code:** In case an assailant or robber ambush at the entrance and force you to open the door or disarm the system, try to keep calm and input Duress code to open the door, which will simultaneously send a silent alert to the monitoring station or security guards.
Default value: 0 (not set)

Step 30. **None English Manual:** Setting for LCD access controller only, checking this setting will only display Chinese language manual (required power restart to apply this function).
Default Value: English Manual.

Step 31. **Date Time Format (DD/MM):** Setting for LCD access controller only, checking this option will change the Date Time format into DD/MM (required power restart to apply this function).
Default value: MM/YY.

Step 32. **Enable Black Tag:** Blacklisted designated card number to restrict access.
The designated card number is send to controller by protocol command via Commview Tools.

Step 33. **Reset Antipass(TZ61):** Timezone 61 is used to automatically reset anti-passback function. When the user violates the anti-pass-back rule, user could not have access anymore. Reset allows the user get access again at this time regardless of the violation of the anti-pass-back rule beforehand.

More Details :

- FAQ : How to use "Reset Anti-pass back" function of V5 series controllers to limit each staff to take one meal only during every meal interval section?

Step 34. **Alarming if Expired:** If any expired card is presented (exceed date limit), it will trigger an alarm.

More Details :

- FAQ : What is the purpose of option "Alarming if Expired" on Parameter Setting?

Step 35. **Ev5 WG out / Hv3 Lift out:** For E Series controller, check this option will enable controller **converted into a reader function** (convert duress and arming output into WG Mode WG0 Output and WG1 Output), for H series controller this check this function will **enable lift control function** (convert the alarm output terminal into lift control function)

Step 36. **Free RF Check at Finger Access:** Setting for Fingerprint access controller only, Check this option to make it unnecessary for access by card identification, only fingerprint can be used for access.

Step 37. **Lock Keyboard:** Check this option to lock keypad function, which also means access by PIN is illegible.

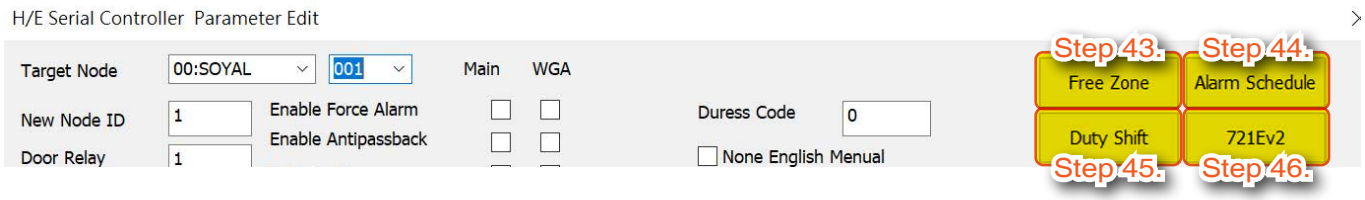
Step 38. **Enable duty shift table:** There are two methods to record Time Attendance 1. Base on Work Time (First and Last Records) 2. Depend on Duty Function Key.
For LCD access controller, it is built-in function key F1, F2, F3, and F4. Each of the function key can be pressed and set the Duty Shift manually (example: pressing F1 will interchange Duty ON and Break ON setting). Beside manually set the Duty Shift, management can set controller to change Duty Shift by enabling **"Enable duty shift table", then controller will automatically change Duty Shift according to the timetable set in Step 45.**

Step 39. **Show WG Port message on LCD:** Setting for LCD access controller only, show card number and reader event in access controller' s LCD.

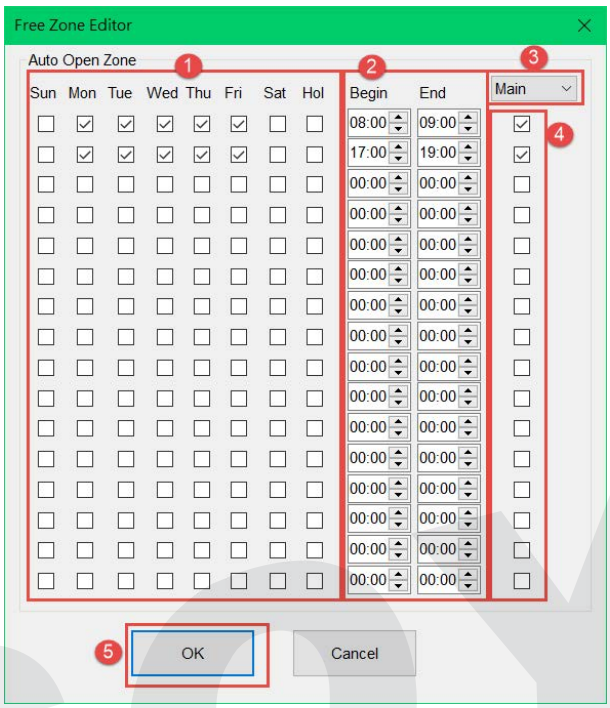
Step 40. **Dupl. check at enroll Finger:** Setting for Fingerprint LCD access controller only, check this setting whether the same fingerprint is existed (duplicated) and show the duplicated information in access controller' s LCD.

Step 41. **Master Range:** Range of Master(Administration) user address to be set. Master user has authority to enter programming mode by swipe card + press #. For example if entering 1-5 means set user range 1-5 as Master/Admin.

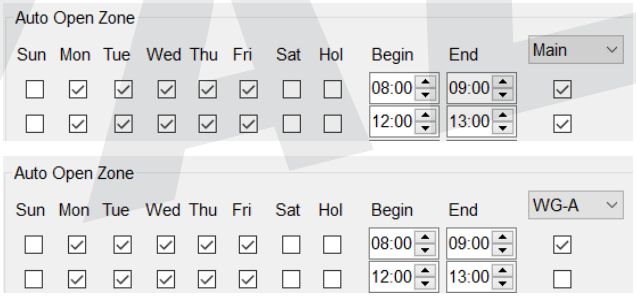
Step 42. **Max keypad error times:** Attempting access (invalid) for N times before controller' s locked itself from access and granted access again for a period of times. N can be set according to requirement.
Default Value: max keypad error is after attempting invalid access for 5 times.



Step 43. **Free Zone:** Set up to 16 free time zones for weekday, weekend, and holiday for Main access controller and WG. Must enable 'Enable Free Zone' function mentioned in Step 23



1. Select day to set auto open zone. Determining which date is categorized as Holiday, must be set separately in 701ClientSQL.
2. Select begin and end time (note: setting time exceed midnight must be set into two separate times. Example: 22:00-06:00 / Timezone 1 22:00-23:59 / Timezone 2 00:00-06:00
3. Select setting for target controller Main/WG (for control panel select WG-A for WG Port 0 and WG-B for WG Port 1).
4. Check the box for selected target controller. For example selecting Main for Timezone 1 and 2, meanwhile for WG-A is selecting only Timezone 1.



5. Select "OK" to save changed.

Complete method of Auto Open Zone Setting:

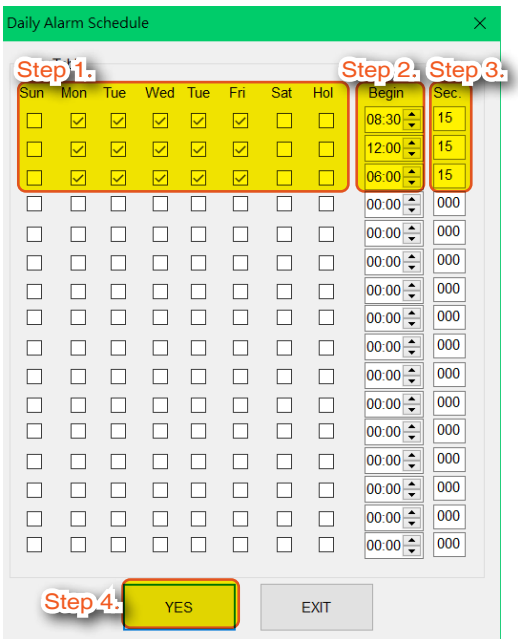
- E Series Controller : Auto Open Zone for all E/H-V5 series controller
- H Series Controller: Auto Open Zone for all H series controller and digital door lock AR-323D without keypad

More Details :

- FAQ : 881EF/EV, 829Ev5 and 725E-V2 free zone edit cannot set from 00:00~23:00. Why?
- FAQ : How to set Auto open door function on 829EV5/821EV5/881E/725EV2 series reader?

Step 44. **Alarm Schedule:**

Controller built-in bell timer function to ring the bell automatically according to time schedule set. This function is mainly applied to ring in the office, factory, and industrial automatic control. Alarm schedule is set for weekday, weekend, and holiday for Main access controller and WG. Note: Enabling this function will convert alarm output terminal into bell timer and required to set controller into Disarming Mode.

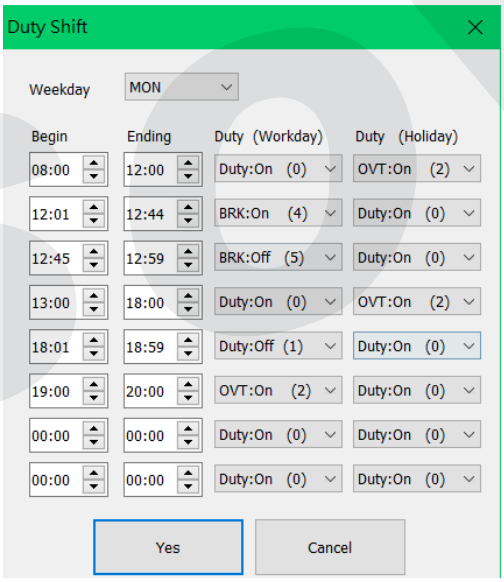


1. Select day to ring the bell schedule. Determining which date is categorized as Holiday, must be set separately in 701ClientSQL.
2. Select Begin time
3. Enter how long the bell will be activated. After the set timer bell will goes off.
   ※The recommended setting for the relay output time (in seconds) is 003 seconds or more to avoid having a too short output time that may result in incorrect triggering of external devices.
4. Select "YES to save changed.

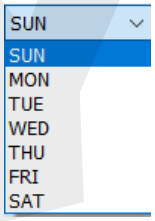
※Due to the changing dates each year, holidays must be reset and downloaded every six months.

Step 45. **Duty Shift:**

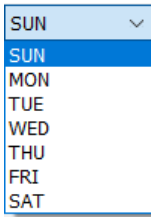
Duty shift will be automatically changed depend on the time setting. According to the shift time, the controller will show shift name (example: DUT ON, DUT OFF). Total of 8 Duty Shift available to set daily. Must 'Enable duty shift table' function in Step 38.



1. Weekday: Select day (range from SUN-SAT)



2. elect Begin and Ending time. Time must be set without overlapping End time and the next time's Start time. Correct example: 08:00-12:00 and 12:01-13:00
3. Select the Duty Shift for both Duty (Workday) & Duty (Holiday)



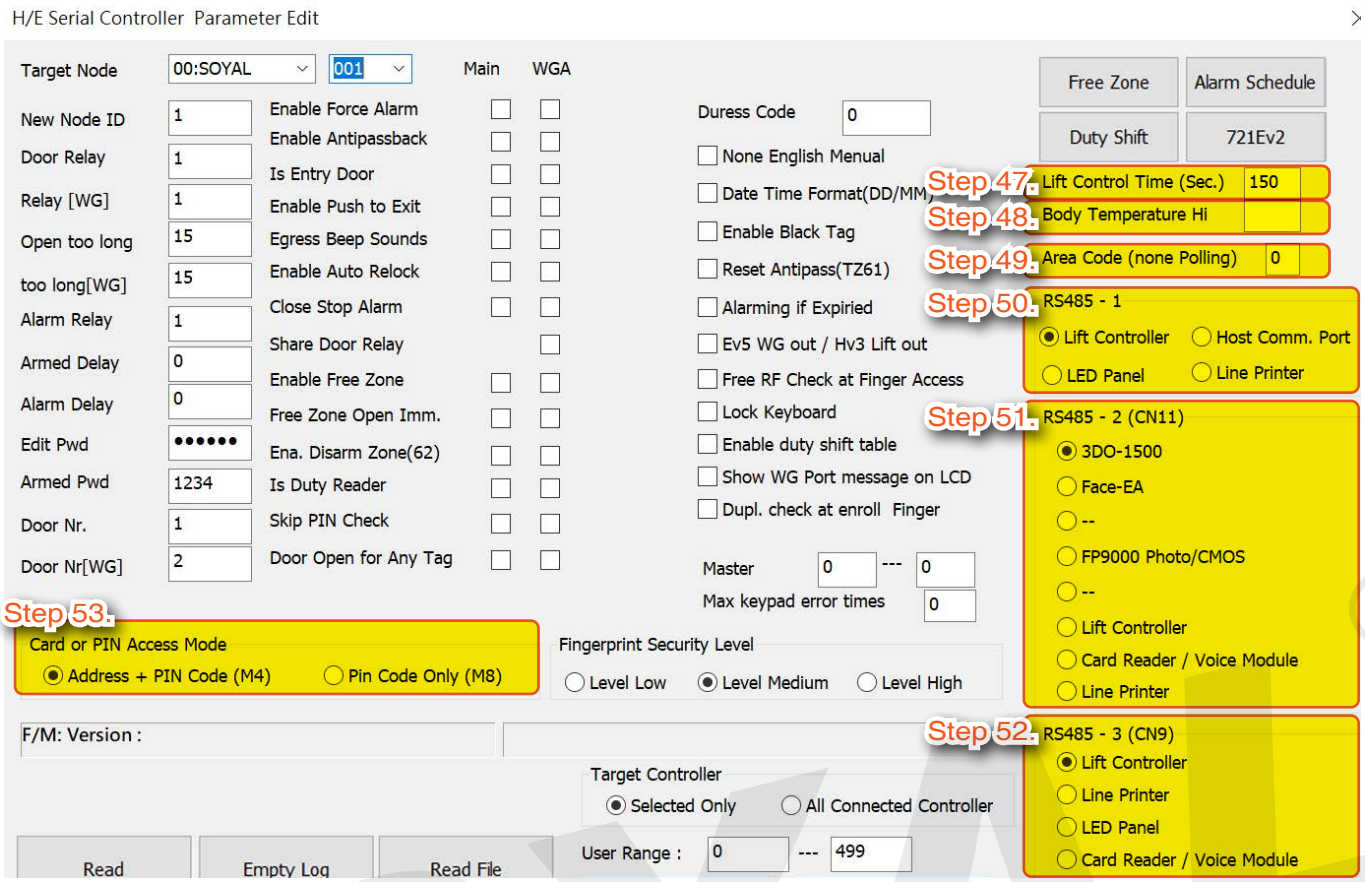
-Duty= working time
-OVT= overtime
-BRK= break time
-Go Out= doing job outside office
-Return= return to office after Go Out

Notes: If in weekday (SUN-SAT) selecting "Duty: On", on Holiday setting must set as "Ovt:ON"

4. Click "Yes" to save changed.

Step 46. **721Ev2:**

This setting is for control panel AR-716-E16 only, refer to 9.2 Control Panel AR-716-E16 Parameter Setting



Step 47. **Lift Control Time (Sec.):** When present card to access in access controller connected to lift control panel AR-401-IO-0016R, the relay output modules will trigger for specific seconds.

Step 48. **Body Temperature Hi:** For access controller equipped with Temperature Module, when controller sense user body temperature is higher than the limit, controller equipped with "high t emperature trigger alarm" function will trigger alarm.
Range: 36.50 – 39.00 (Default value: 36.50)

Step 49. **Area code (none Polling):** There are two ways to obtain transaction log from controller to software, Polling and Active Communication Mode. This setting is used when choosing Active Communication Mode, used to specify the assigned Area (Range 00-15, default value: 15).

More detail about implementing Active Communication Mode

- FAQ: How to improve the speed of receiving the message logs

Step 50. **RS485-1:** Controller wiring terminal CN6 is **RS485 Host communication**. Used mainly for connection to software. If controller communication to software using TCP/IP, RS485-1 setting can be allocated to lift controller, LED Panel, or Line Printer.
Default value: Host. Comm. Port

Step 51. **RS485-2:** Controller wiring terminal **CN11** mainly selected for Face and Fingerprint controller.
- 3DO-1500 is default value of white sensor module fingerprint controller AR-331-EF/AR-837-EF3DO
- Face-EA is default value of face controller AR-837-EA
- FP9000 Photo/CMOS is default value of red sensor fingerprint controller AR-837-EF9DO

For non-face and non-fingerprint controller, this terminal can be allocated for Lift Controller, Card Reader/Voice Module, and Line Printer

Step 52. **RS485-3:** Controller wiring terminal **CN9**, extra terminal for expansion feature that can be allocated for Lift Controller, Line Printer, LED Panel, and Card Reader/Voice Module.

NOTE

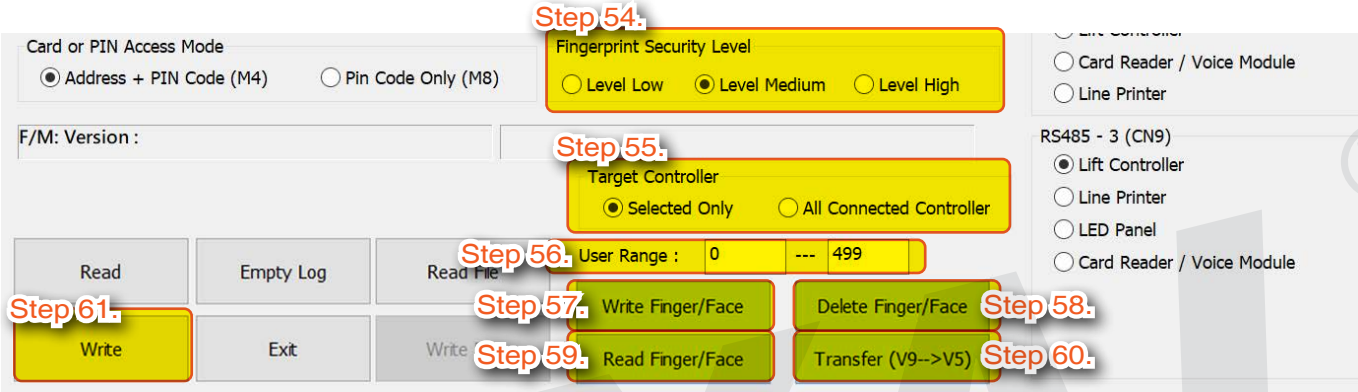
CN9 and CN11 built-in TTL interface. If required wiring to RS232/RS485 devices, SOYAL provides TTL to RS485 (AR-321L485) or TTL to RS232 (AR-321L232) converter

Step 53. **Card or PIN Access Mode:** SOYAL offer three options of access mode

- Address + PIN Code (M4): Access by entering user address + PIN

- PIN Code Only (M8): Access by entering PIN only (Default)

M6: Standalone only, this option is not available for networking thus this option is not available in Software setting.



Step 54 ~ Step 60 **is eligible for fingerprint and face controller only.**

- Fingerprint and face data is separated and is different entity from user card data. The data can be found in C:\Program Files (x86)\701Server. **701ServerSQL provides read/write fingerprint and face data from PC to controller.**
- Data format:

  FPXXXXX.FP5 fingerprint red sensor module (9DO)

  FPXXXXX.FP3 fingerprint white sensor module (3DO)

  FPXXXXX.FxL face data

  XXXXX= 5 digit user address.
- Fingerprint data between red sensor and white sensor could not interchange data between one another.

More Details :

- FAQ : How to set up networking for fingerprint controller AR-837EF via 701 SERVER and download fingerprint data?
- FAQ : How to transfer data from one fingerprint device (331EF/837EF/881EF) to other fingerprint device?

Step 54. **Fingerprint Security Level:** Setting fingerprint/face controller's security level.

- Fingerprint: Available to set from Level Low, Level Medium, and Level High. Recommended setting for fingerprint/face controller’ s security level setting (default)

- Face: Available to set from Level Low and Level Medium. Level Low is setting for face controller AR-837-EA enabling access with face mask, Level Medium is default setting.

Step 55. **Target Controller:** Select target controller to be read/write fingerprint or face data.
- **Selected Only:** Only for one unit controller Node ID that is currently being edited the parameter setting (example: currently editing for Node ID 1, selecting 'Selected Only' will only read/write data from/to Node ID 1)
- **All Connected Controller:** Read and write fingerprint or face data from/to all connected controller in the system (example: currently editing for Node ID 1, but the whole system in 701ServerSQL has 3 other fingerprint controller with node ID 2, 3, and 4. Selecting 'All Connected Controller' will read/write data from/to Node ID 1-4)

Step 56. **User Range:** Select user range to read/write data

Step 57. **Write Finger/Face:** After selecting Target Controller and User Range, select "Write Finger/Face" to transfer data from PC to controller.
Note: selecting this action will overwrite the same user address of existed data in the controller.

Step 58. **Delete Finger/Face:** After selecting Target Controller and User Range, select "Delete Finger/Face" to delete data in the controller.
To delete finger/face data from PC, go to C:\Program Files (x86)\701Server > select the file to be deleted > delete.

Step 59. **Read Finger/Face:** After selecting Target Controller and User Range, select 'Read Finger/Face' to transfer data from controller to PC.
Note: selecting this action will overwrite the same user address of existed data in the PC.

Step 60. **Transfer (V9 V5):** This function is to convert oldest version of fingerprint controller V9 into the latest format V5 or what we known as Enterprise Series (E Series) Controller.
Note: It is recommended to register again in E controller rather than converting it directly to prevent damage to the fingerprint file)

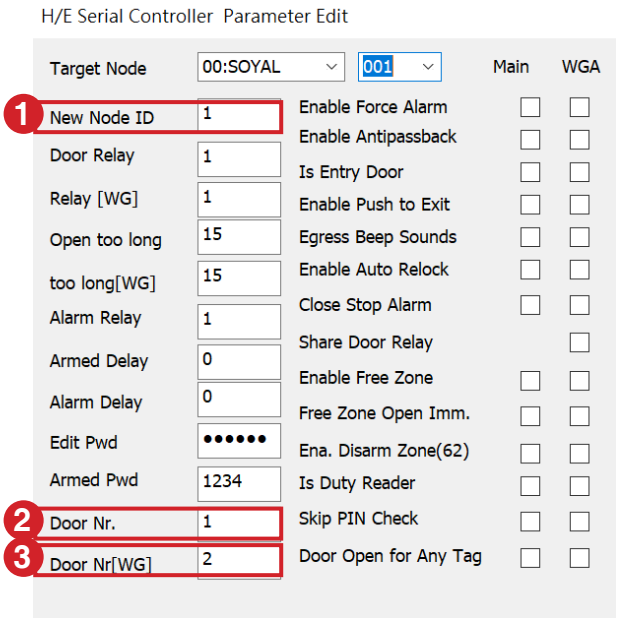
Step 61. **Write:** Write the current setting to saved changed new setting and effectively applied.

More detail about implementing Active Communication Mode

- FAQ: 701Server support Read and Write IP Based E Series Controller's parameter setting
- FAQ: How to use SOYAL E/V5 Controller for Lift Control?

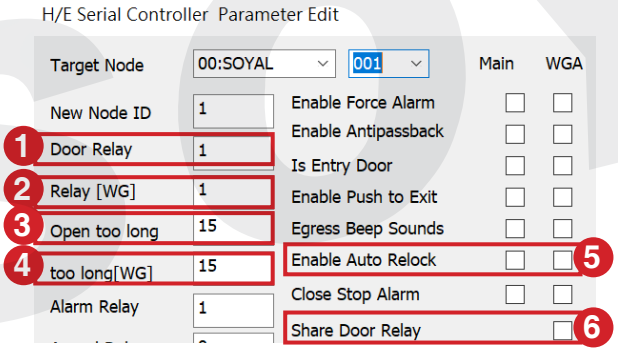
8.5 Parameter Setting by Functions

• 8.5.1 Node ID and Door Number



1. **New Node ID:** After the communication is successful, you can also modify the Node ID of this access controller in **"New Node ID"** field.
2. **Door Nr.:** Each door number of the controller can be changed according to the corresponding area or door number assigned. Access control system managed by PC will show specific door number on entry or exit record. Door number can be repeated and used in the same area but corresponding to the area and door itself. Default value is 1.
3. **Door Nr. [WG]:** WG Door Number can be changed according to the corresponding Main access controller's area and door number. WG Door Number is only eligible for E Series controller's WG Reader and WG Port 1 under AR-716-E16. Default value is 2.

• 8.5.2 Door Relay Setting



1. **Door Relay:** Door Relay Time of the access controller, after access identification is successful, controller will trigger the relay to release lock and **how long the lock is being released to indicate door open is determined by Door Relay Time.**
   The setting of Door Relay Time is based on what type of electric lock installed onsite.
   Recommended setting:
   1. Fail-Safe type of lock such as Electric Bolt Lock and Magnetic Lock is 15 seconds (recommended to combine with Auto Relock function)
   2. Fail-Secure type of lock such as Electric Strike and Cabinet Lock is 0.2 seconds. Default value is 7 seconds.

   Pulse setting (short-term release): range 001~600 seconds, if set as 01-0.9seconds enter 601~609

   Latch setting (output continuously): enter 000

2 **Relay [WG]:** Door Relay Time Setting for Wiegand Reader (only eligible for E Series controller's WG Reader and WG Port 1 under AR-716-E16) Default value is 7 seconds.

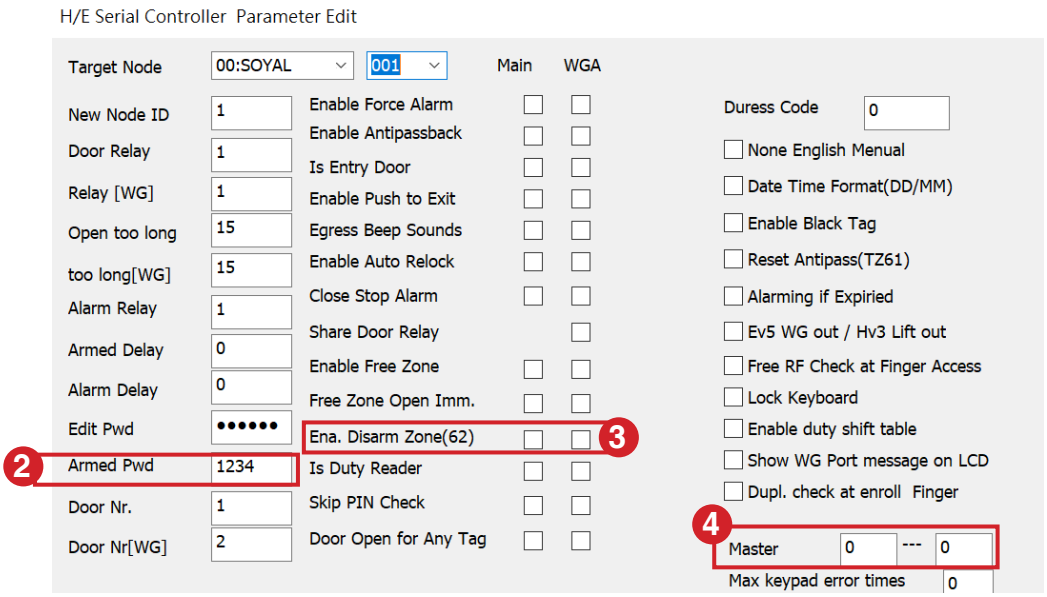
3 **Open too long:** or also known as **Door Close Time or Door Open Waiting Time**. After the period of door relay time trigger relay and open the door, the door contact will start detecting the door status; however, sometimes the door is not be closed in time, so the door close time gives users a **buffer time (delay time) to close the door properly before the door contact starts detecting it as Door Open Too Long.**
For example: Default value of door open too long is 15 seconds (default), the door contact will start detecting after Door Relay Time (10 sec) + Door Close Time (15 sec), and the user should close the door properly within the total period (25 sec).
Note: Door Open Too Long will not be acknowledge if activating Auto Relock function, as door will relock immediately whenever door contact detect door is closed. Default value is 15 seconds.

4 **too long[WG]:** Door Close Time for Wiegand Reader (only eligible for E Series controller's WG Reader and WG Port 1 under AR-716-E16) Default value is 15 seconds.

5 **Enable Auto Relock:** The electric lock will be only lockable after the period of Door Relay Time, so there might be a gap between closing the door and the door being actually locked. By **enabling the Auto Relock function which will let the door relock immediately whenever detecting the door is closed by the door contact**. This setting is suggested for fail-safe lock installation such as electric bolt and magnetic lock.

6 **Close Stop Alarm:** There are three options to stop alarming event 1. Swipe valid card 2. Press egress button 3. Close door
When Close Stop Alarm function is checked, alarming event will stopped when door is closed or pressing egress button.
When this option is remain unchecked, alarming event will only stop when valid card is presented.
Default value is unchecked means alarm event will only stop when swiping valid card.

• 8.5.3 Arming & Disarming



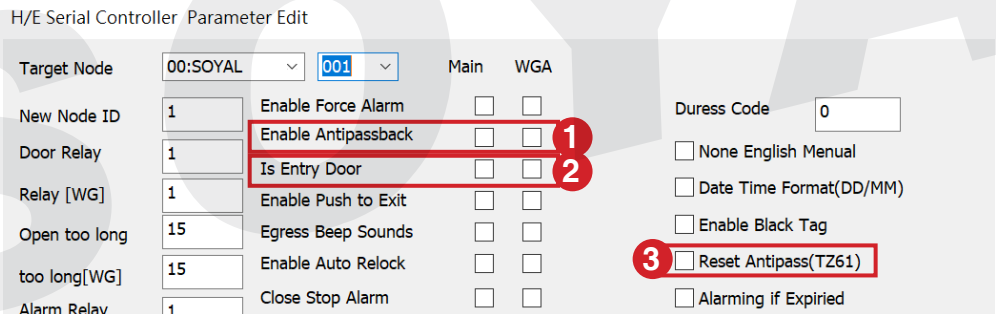
1 **Armed Delay:** After activating Arming mode, access controller enter Arming mode after a period of **Arming Delay Time**, which gives users a buffer time to exit without triggering the alarm. Default value is 1 second.

2 **Armed Pwd:** There are three method to enabling Arming Mode 1. Enter programming mode and exit programming mode by entering **# 2. Swipe Master Range card 3. **Enter Arming Password**.
To enter the Arming Password there are two procedures:
1. Normal door open procedure + 4-digit Arming PWD + #
2. Without opening the door + 4-digit Arming PWD + Presenting a valid card
Default Arming Password is 1234.

3 **Ena. Disarm Zone(62):** Timezone 62 is specifically assigned for controller's autmomatically set as arming and disarming. The start time will automatically set controller into arming mode, and the end time will automatically set controller into disarming mode (standby mode). For example: set Timezone 62 as 08:00-12:00 means controller will enter arming mode at 08:00 and disarming at 12:00.

4 **Master Range:** Range of Master(Administration) user address to be set. Master user has authority to enter programming mode by swipe card + press #. For example if entering 1-5 means set user range 1-5 as Master/Admin.

• 8.5.4 Anti-passback

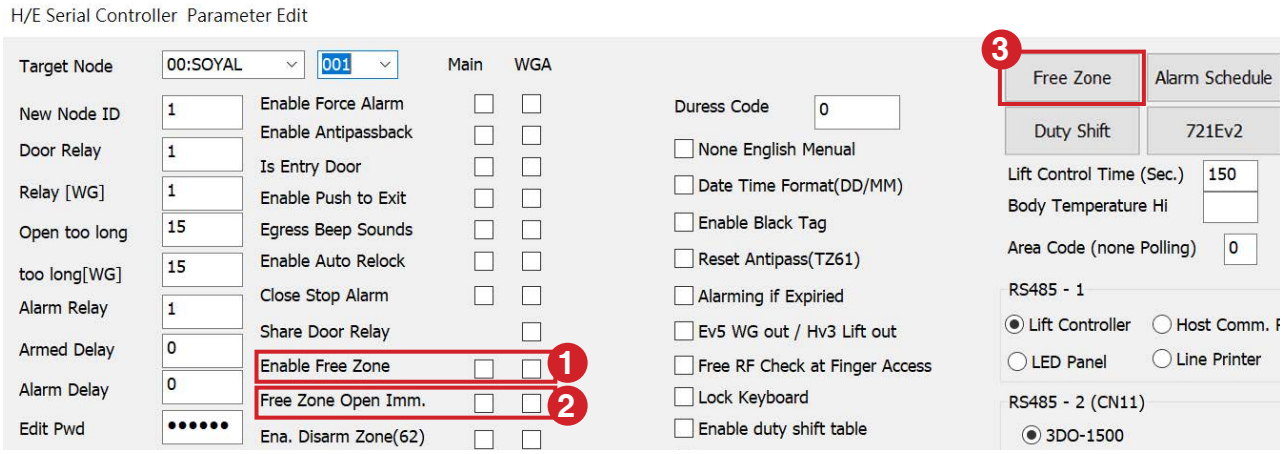


1 **Enable Antipassback:** If there is an external WG reader connected to this access controller, you can tick this option to enable the anti-passback rule.

2 **Is Entry Door:** Determine door is exit or entry
If selecting controller for entry, check the "Is Entry Door" box
If selecting controller for exit, do not check "Is Entry Door" box, just left it unchecked

3 **Reset Antipass(TZ61):** Timezone 61 is used to automatically reset anti-passback function. When the user violates the anti-pass-back rule, user could not have access anymore. Reset allows the user get access again at this time regardless of the violation of the anti-pass-back rule beforehand.

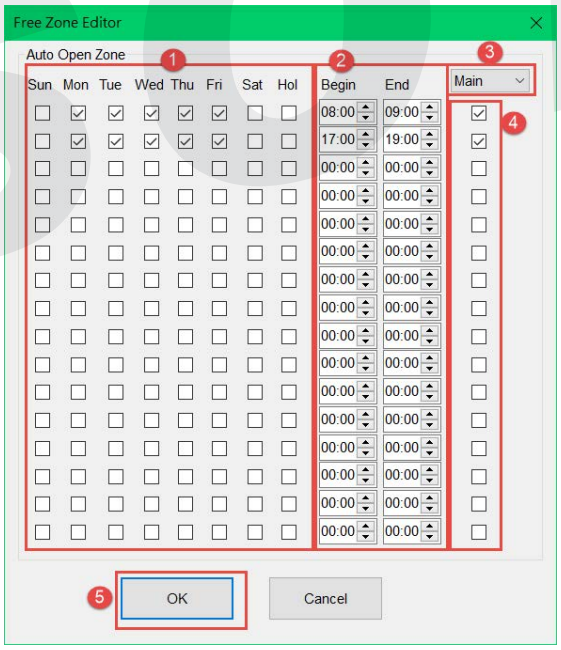
• 8.5.5 Arming & Disarming



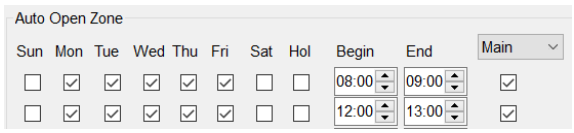
1 **Enable Free Zone:** This option is to enable or disable auto open zone (Timezone 63) function. Meanwhile, Auto open time zone setting refer to Step 43.

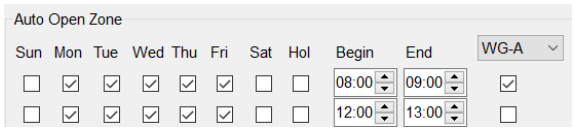
2 **Free Zone Open Imm.**: There are two ways to enable auto open timezone (Timezone 63):
1. When Auto-Time Zone begin, the door will be automatically open without presenting 1st valid Card.
2. **When Auto-Time Zone begin, the door don't automatically be opening till any one authorized user present a valid card to controller to open the door (Default Value)**
By enabling this function, it will enable auto open zoon when time has come.

3 **Free Zone:** Set up to 16 free time zones for weekday, weekend, and holiday for Main access controller and WG. Must enable 'Enable Free Zone' function mentioned in Step 23



1. Select day to set auto open zone. Determining which date is categorized as Holiday, must be set separately in 701ClientSQL.
2. Select begin and end time (note: setting time exceed midnight must be set into two separate times. Example: 22:00-06:00 / Timezone 1 22:00-23:59 / Timezone 2 00:00-06:00
3. Select setting for target controller Main/WG (for control panel select WG-A for WG Port 0 and WG-B for WG Port 1).
4. Check the box for selected target controller. For example selecting Main for Timezone 1 and 2, meanwhile for WG-A is selecting only Timezone 1.



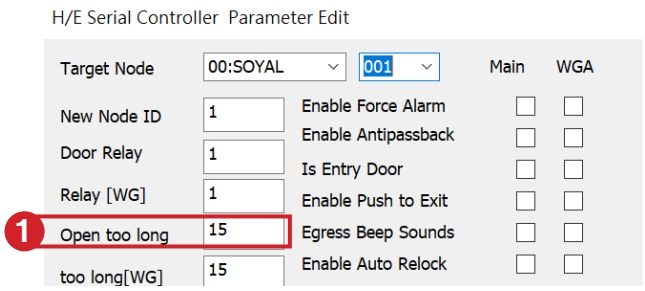


5. Select "OK" to save changed.

Complete method of Auto Open Zone Setting:

- E Series Controller : Auto Open Zone for all E/H-V5 series controller
- H Series Controller: Auto Open Zone for all H series controller and digital door lock AR-323D without keypad

• 8.5.6 Alarm Schedule

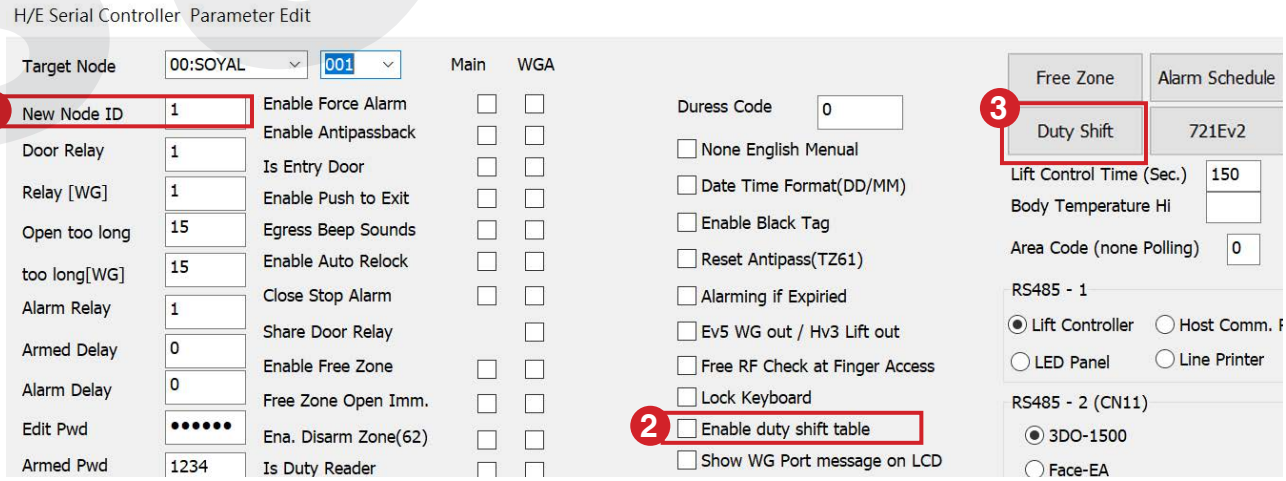


1 **Open too long:** or also known as **Door Close Time or Door Open Waiting Time**. After the period of door relay time trigger relay and open the door, the door contact will start detecting the door status; however, sometimes the door is not be closed in time, so the door close time gives users a **buffer time (delay time) to close the door properly before the door contact starts detecting it as Door Open Too Long.**

For example: Default value of door open too long is 15 seconds (default), the door contact will start detecting after Door Relay Time (10 sec) + Door Close Time (15 sec), and the user should close the door properly within the total period (25 sec).

Note: Door Open Too Long will not be acknowledge if activating Auto Relock function, as door will relock immediately whenever door contact detect door is closed.Default value is 15 seconds.

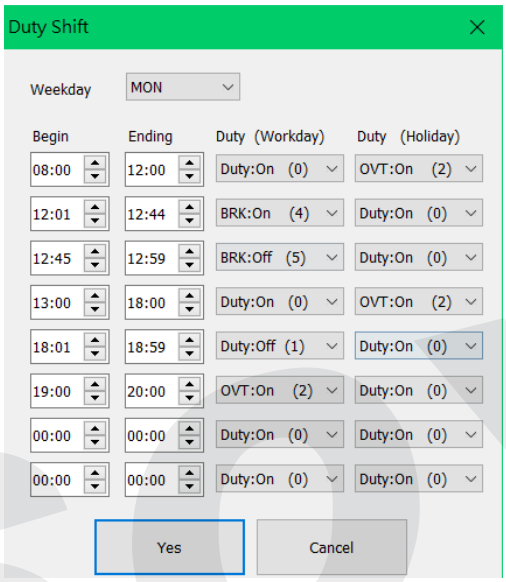
• 8.5.7 Duty Shift



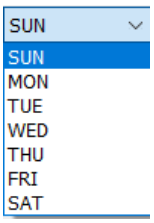
1 After the communication is successful, you can also modify the Node ID of this access controller in "**New Node ID**" field.

2 Enable duty shift table: There are two methods to record Time Attendance 1. Base on Work Time (First and Last Records) 2. Depend on Duty Function Key.
For LCD access controller, it is built-in function key F1, F2, F3, and F4. Each of the function key can be pressed and set the Duty Shift manually (example: pressing F1 will interchange Duty ON and Break ON setting). Beside manually set the Duty Shift, management can set controller to change Duty Shift by enabling **"Enable duty shift table", then controller will automatically change Duty Shift according to the timetable set in Step 45.**

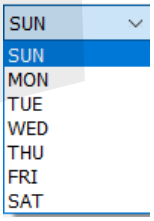
3 Duty Shift:
Duty shift will be automatically changed depend on the time setting. According to the shift time, the controller will show shift name (example: DUT ON, DUT OFF). Total of 8 Duty Shift available to set daily. Must 'Enable duty shift table' function in Step 38.



1. Weekday: Select day (range from SUN-SAT)



2. elect Begin and Ending time. Time must be set without overlapping End time and the next time's Start time. Correct example: 08:00-12:00 and 12:01-13:00
3. Select the Duty Shift for both Duty (Workday) & Duty (Holiday)

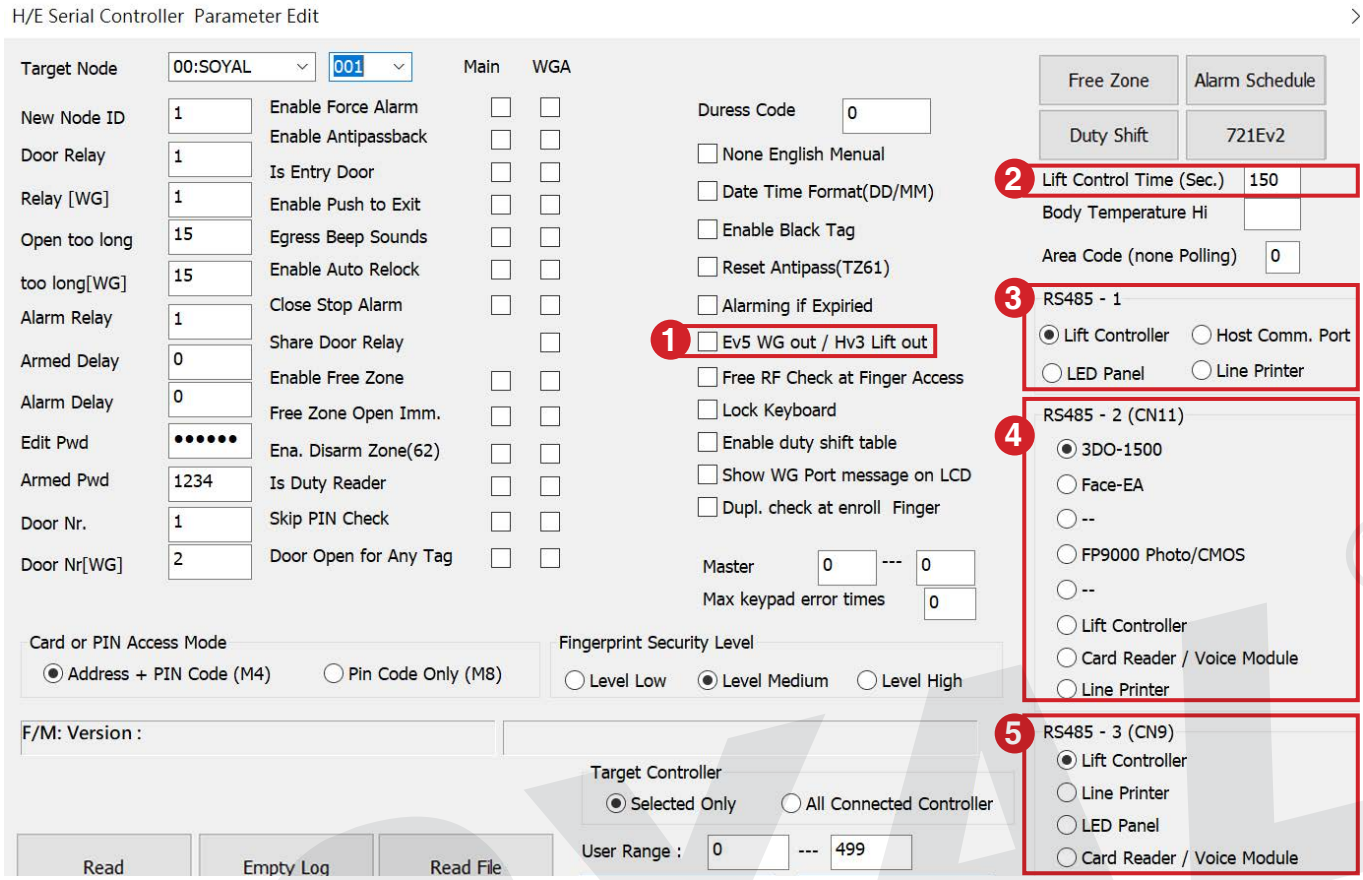


-Duty= working time
-OVT= overtime
-BRK= break time
-Go Out= doing job outside office
-Return= return to office after Go Out

Notes: If in weekday (SUN-SAT) selecting "Duty: On", on Holiday setting must set as "Ovt:ON"

4. Click "Yes" to save changed.

• 8.5.8 Lift Control



1 **Ev5 WG out / Hv3 Lift out:** For E Series controller, check this option will enable controller **converted into a reader function** (convert duress and arming output into WG Mode WG0 Output and WG1 Output), for H series controller this check this function will **enable lift control function** (convert the alarm output terminal into lift control function)

2 **Lift Control Time (Sec.):** When present card to access in access controller connected to lift control panel AR-401-IO-0016R, the relay output modules will trigger for specific seconds.

3 **RS485-1:** Controller wiring terminal CN6 is **RS485 Host communication**. Used mainly for connection to software. If controller communication to software using TCP/IP, RS485-1 setting can be allocated to lift controller, LED Panel, or Line Printer. Default value: Host. Comm. Port

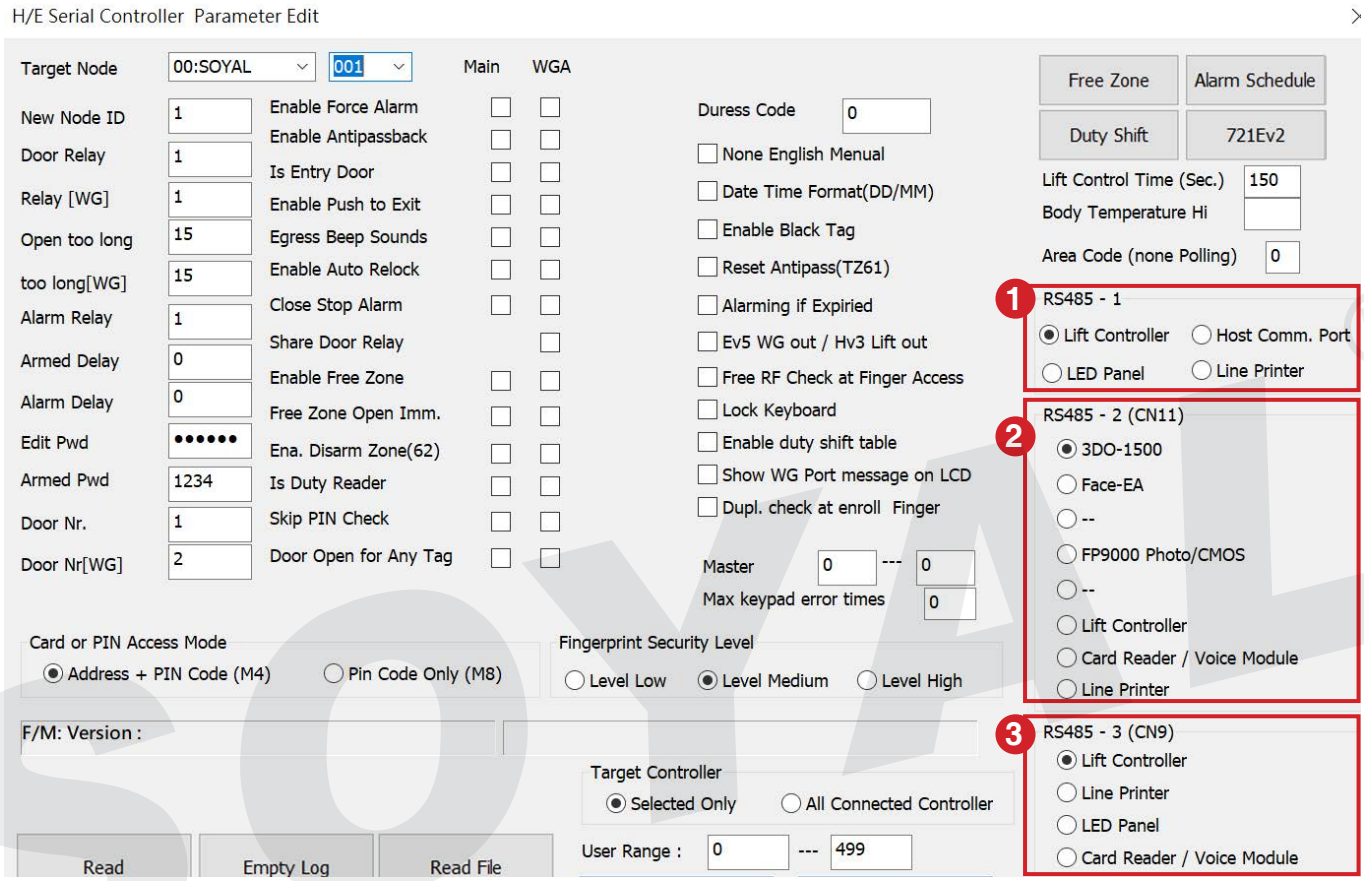
4 **RS485-2:** Controller wiring terminal **CN11** mainly selected for Face and Fingerprint controller.
- 3DO-1500 is default value of white sensor module fingerprint controller AR-331-EF/AR-837-EF3DO
- Face-EA is default value of face controller AR-837-EA
- FP9000 Photo/CMOS is default value of red sensor fingerprint controller AR-837-EF9DO For non-face and non-fingerprint controller, this terminal can be allocated for Lift Controller, Card Reader/Voice Module, and Line Printer

5 **RS485-3:** Controller wiring terminal **CN9**, extra terminal for expansion feature that can be allocated for Lift Controller, Line Printer, LED Panel, and Card Reader/Voice Module.

NOTE

CN9 and CN11 built-in TTL interface. If required wiring to RS232/RS485 devices, SOYAL provides TTL to RS485 (AR-321L485) or TTL to RS232 (AR-321L232) converter

• 8.5.9 RS485 & UART



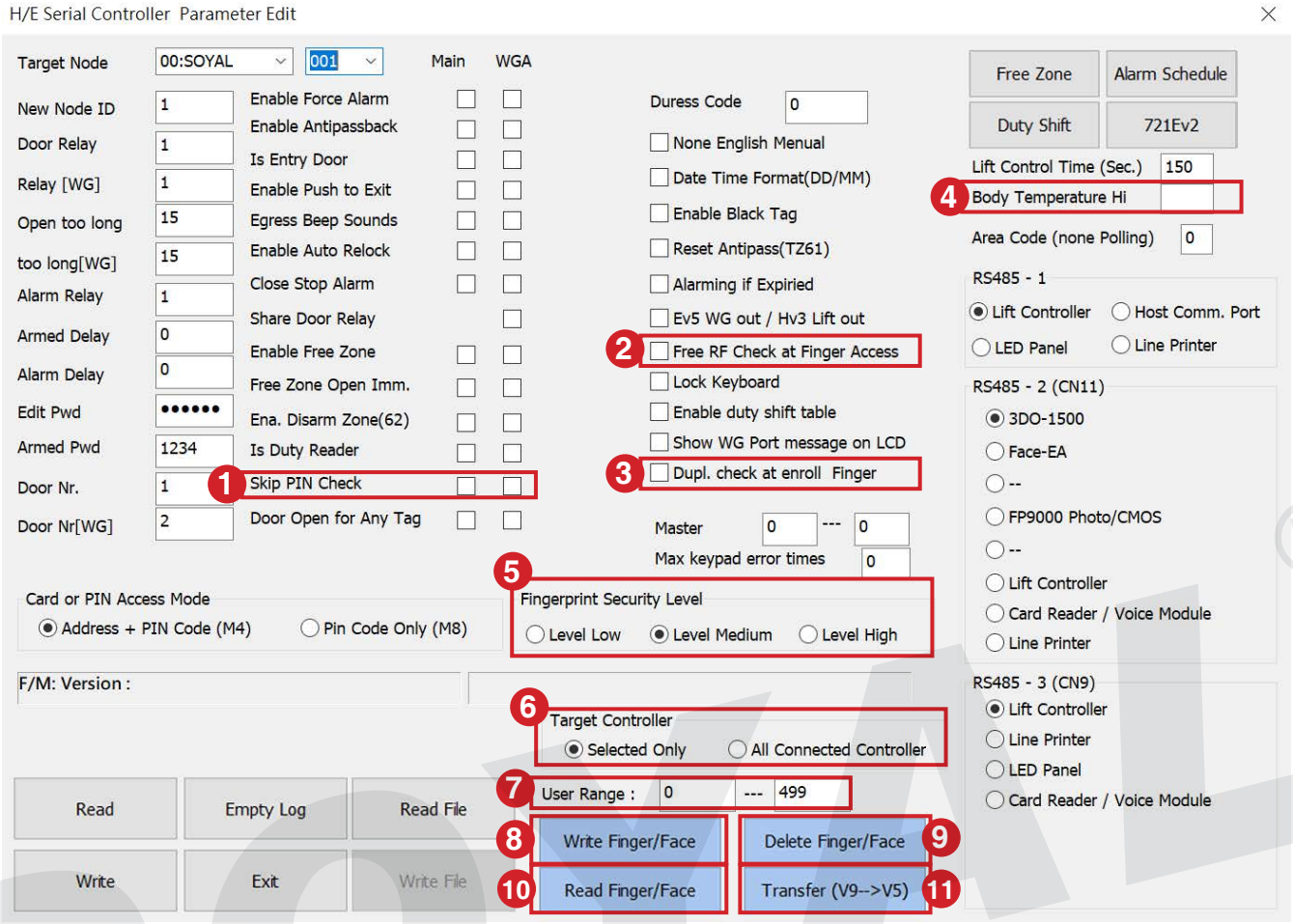
1 **RS485-1:** Controller wiring terminal CN6 is **RS485 Host communication**. Used mainly for connection to software. If controller communication to software using TCP/IP, RS485-1 setting can be allocated to lift controller, LED Panel, or Line Printer. Default value: Host. Comm. Port

2 **RS485-2:** Controller wiring terminal **CN11** mainly selected for Face and Fingerprint controller.

- 3DO-1500 is default value of white sensor module fingerprint controller AR-331-EF/ AR-837-EF3DO
- Face-EA is default value of face controller AR-837-EA
- FP9000 Photo/CMOS is default value of red sensor fingerprint controller AR-837-EF9DO For non-face and non-fingerprint controller, this terminal can be allocated for Lift Controller, Card Reader/Voice Module, and Line Printer

3 **RS485-3:** Controller wiring terminal **CN9**, extra terminal for expansion feature that can be allocated for Lift Controller, Line Printer, LED Panel, and Card Reader/Voice Module.

• 8.5.10 Fingerprint & Face Data



1 **Skip PIN Check:** For a system that has both controller and reader with keypad and no keypad, **user access mode set as "Card & PIN" could not enter PIN in no keypad controller/reader**. In this case, for no keypad controller or reader to omit enter PIN required to enable "Skip PIN Check" function.

2 **Free RF Check at Finger Access:** Setting for Fingerprint access controller only, Check this option to make it unnecessary for access by card identification, only fingerprint can be used for access.

3 **Dupl. check at enroll Finger:** Setting for Fingerprint LCD access controller only, check this setting whether the same fingerprint is existed (duplicated) and show the duplicated information in access controller's LCD.

4 **Body Temperature Hi:** For access controller equipped with Temperature Module, when controller sense user body temperature is higher than the limit, controller equipped with "high t emperature trigger alarm" function will trigger alarm. Range: 36.50 – 39.00 (Default value: 36.50)

5 **Fingerprint Security Level:** Setting fingerprint/face controller's security level.
- Fingerprint: Available to set from Level Low, Level Medium, and Level High. Recommended setting for fingerprint/face controller' s security level setting (default)
- Face: Available to set from Level Low and Level Medium. Level Low is setting for face controller AR-837-EA enabling access with face mask, Level Medium is default setting.

6 **Target Controller:** Select target controller to be read/write fingerprint or face data.

- Selected Only: Only for one unit controller Node ID that is currently being edited the parameter setting (example: currently editing for Node ID 1, selecting "Selected Only" will only read/write data from/to Node ID 1)

- All Connected Controller: Read and write fingerprint or face data from/to all connected controller in the system (example: currently editing for Node ID 1, but the whole system in 701ServerSQL has 3 other fingerprint controller with node ID 2, 3, and 4. Selecting "All Connected Controller " will read/write data from/to Node ID 1-4)

7 **User Range:** Select user range to read/write data

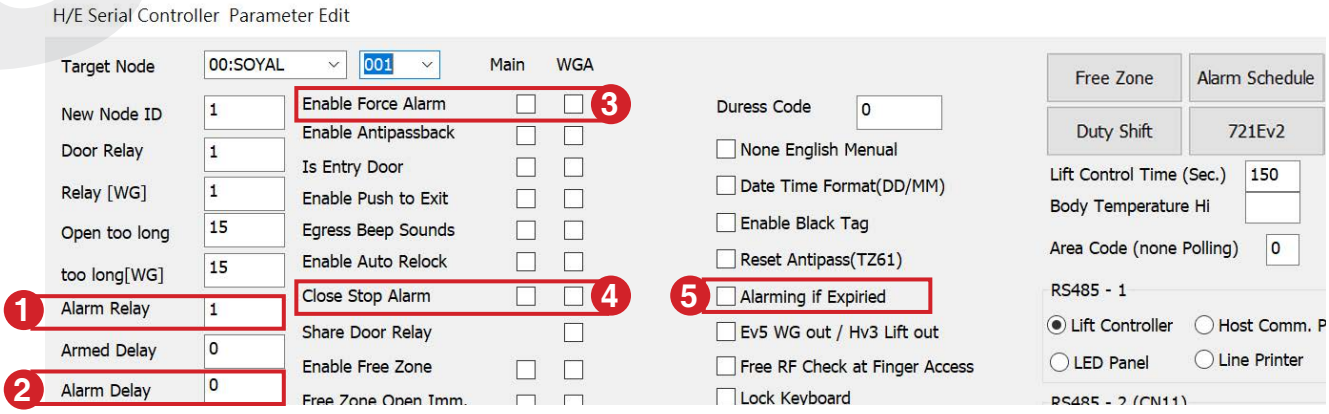
8 **Write Finger/Face:** After selecting Target Controller and User Range, select "Write Finger/Face" to transfer data from PC to controller.
Note: selecting this action will overwrite the same user address of existed data in the controller.

9 **Delete Finger/Face:** After selecting Target Controller and User Range, select "Delete Finger/Face" to delete data in the controller. To delete finger/face data from PC, go to C:\Program Files (x86)\701Server > select the file to bedeleted > delete.

10 **Read Finger/Face:** After selecting Target Controller and User Range, select 'Read Finger/Face' to transfer data from controller to PC.
Note: selecting this action will overwrite the same user address of existed data in the PC.

11 **Transfer (V9 V5):** This function is to convert oldest version of fingerprint controller V9 into the latest format V5 or what we known as Enterprise Series (E Series) Controller.
Note: It is recommended to register again in E controller rather than converting it directly to prevent damage to the fingerprint file)

• 8.5.11 Alarm Event



1 **Alarm Relay:** When alarm event is triggered, alarm will output continuously for a period of time according to Alarm Relay Time.
Pulse setting (short-term release): range 001~600 seconds, if set as 01-0.9seconds enter 601~609
Latch setting (output continuously): enter 000
Default value is 15 seconds.

2 **Alarm Delay:** Before Alarm Event is triggered, there is **a set of time period between conditions that triggered the alarm and the alarming event which is called Alarm Delay Time**. Alarm Delay Time gives users a buffer time to turn off the alarm before the beeper is sounding or an alarm signal is sent to the security guards. Default value is 1 second.

3 **Enable Force Alarm:** In the event that any door is opened without normal access like presenting a valid card from the outside or pressing the RTE button from the inside, it will cause a Force Open condition. This situation will trigger the Force Open Alarm if the access controller is under Arming mode.

4 **Close Stop Alarm:** There are three options to stop alarming event 1. Swipe valid card 2. Press egress button 3. Close door

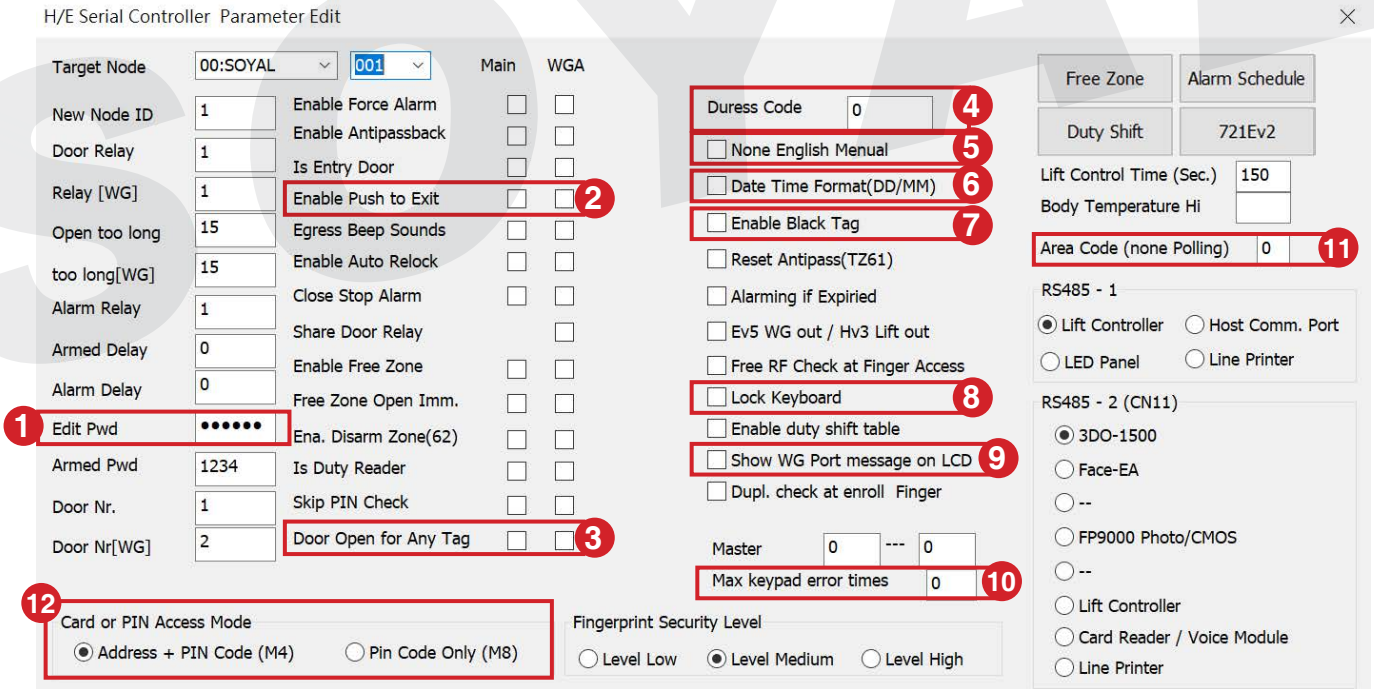
When Close Stop Alarm function is checked, alarming event will stopped when door is closed or pressing egress button.

When this option is remain unchecked, alarming event will only stop when valid card is presented.

Default value is unchecked means alarm event will only stop when swiping valid card.

5 **Alarming if Expired:** If any expired card is presented (exceed date limit), it will trigger an alarm.

• 8.5.12 Others



1. **Edit Pwd**: Master Code or Programming Code of the Access Controller can be changed from this field. Default Master Code is 123456.

2. **Enable Push to Exit:** Enable or disable exit door by Egress Button. Default value is enabling for both Main and WG.

3. **Door Open for Any Tag:** Used for short-term activities or temporary events which enable door open whenever a card with the same frequency of the access controller is presented.

4. **Duress Code:** In case an assailant or robber ambush at the entrance and force you to open the door or disarm the system, try to keep calm and input Duress code to open the door, which will simultaneously send a silent alert to the monitoring station or security guards.
   Default value: 0 (not set)

5. **None English Manual:** Setting for LCD access controller only, checking this setting will only display Chinese language manual (required power restart to apply this function).
   Default Value: English Manual.

6. **Date Time Format (DD/MM):** Setting for LCD access controller only, checking this option will change the Date Time format into DD/MM (required power restart to apply this function).
   Default value: MM/YY.

7. **Enable Black Tag:** Blacklisted designated card number to restrict access. The designated card number is send to controller by protocol command via Commview Tools.

8. **Lock Keyboard:** Check this option to lock keypad function, which also means access by PIN is illegible.

9. **Show WG Port message on LCD:** Setting for LCD access controller only, show card number and reader event in access controller's LCD.

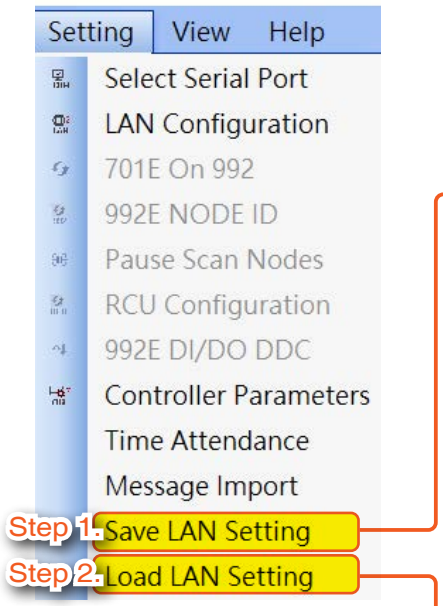
10. **Max keypad error times:** Attempting access (invalid) for N times before controller's locked itself from access and granted access again for a period of times. N can be set according to requirement.
    Default Value: max keypad error is after attempting invalid access for 5 times.

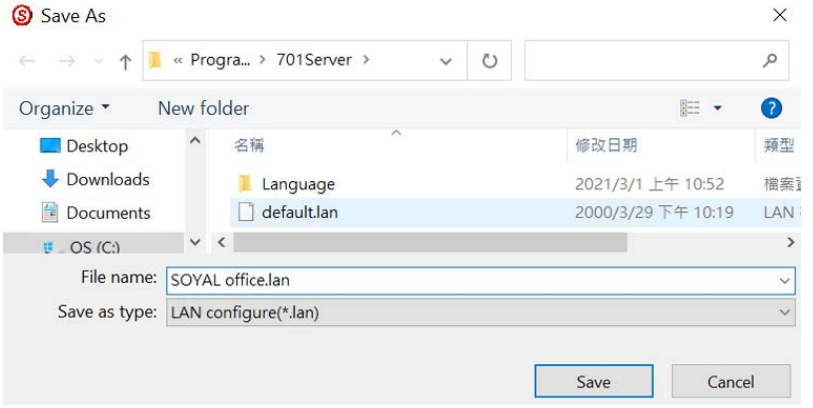
11. **Area code (none Polling):** There are two ways to obtain transaction log from controller to software, Polling and Active Communication Mode. This setting is used when choosing Active Communication Mode, used to specify the assigned Area (Range 00-15, default value: 15).

12. **Card or PIN Access Mode:** SOYAL offer three options of access mode
    - **Address + PIN Code (M4)**: Access by entering user address + PIN
    - **PIN Code Only (M8)**: Access by entering PIN only (Default)
    M6: Standalone only, this option is not available for networking thus this option is not available in Software setting.

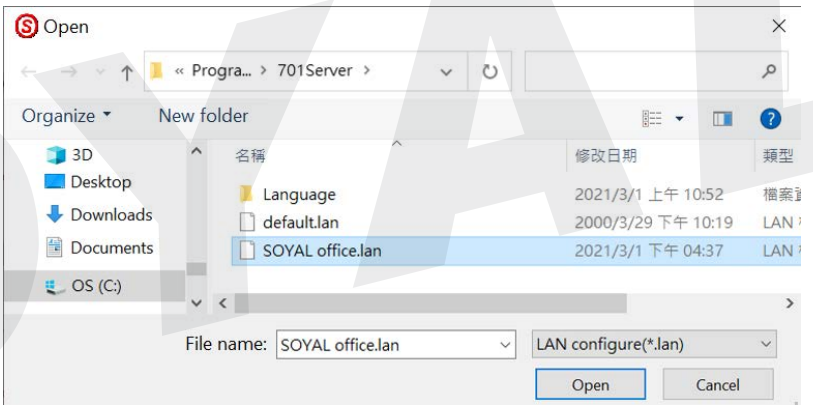
9. Backup and Restore LAN Setting

Switching from old PC to new PC required to migrate the data saved on 701ServerSQL and 701ClientSQL. It is required to backup from old PC and restore to new PC.





Step 1. Backup LAN Setting
Select the location to save the file (must be accessible to make restore easier; ex: save to desktop)



Step 2. Restore LAN Setting
Select file

NOTE

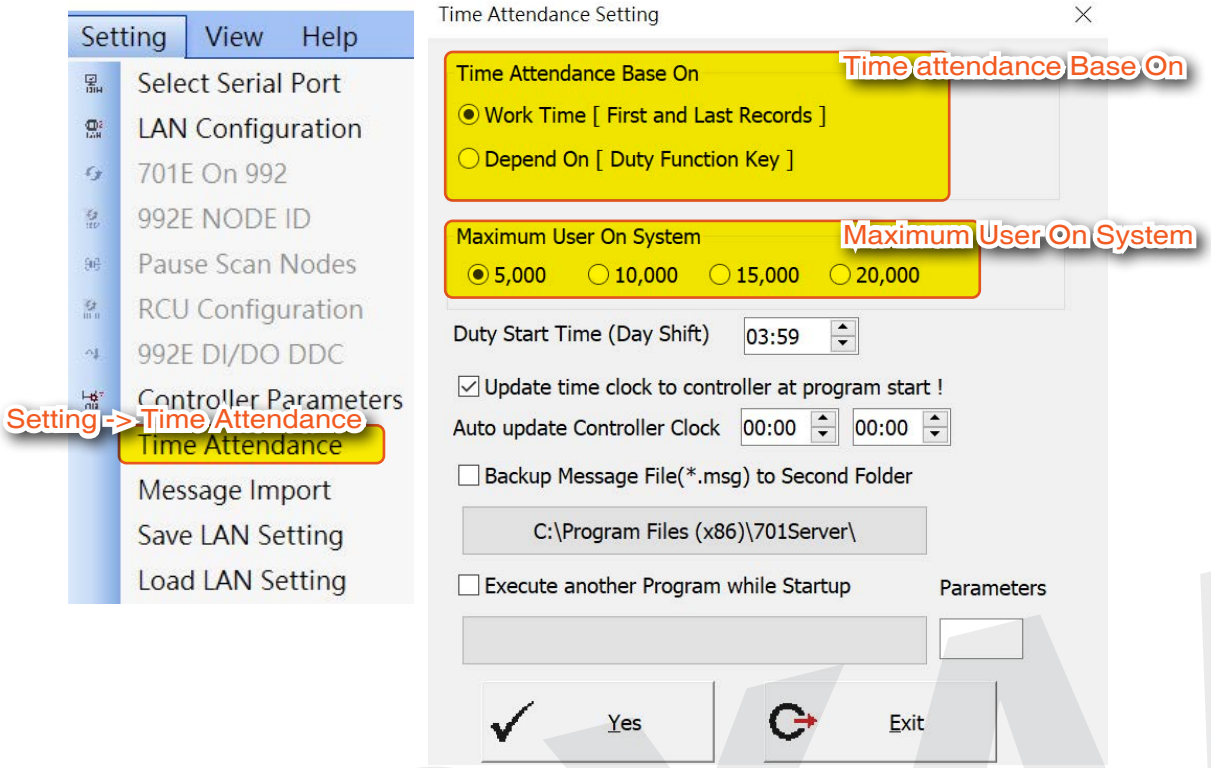
Software before 8.3 versions, you can't save the data and to save the LAN setting record, you can only take picture or take note and manually do the set up again.

More Details :

- FAQ : Backup and Restore 701 Server and Client from old PC to new PC

10. Attendance Recording Methods and Importing Message Files

10.1. Time Attendance Setting



Time Attendance : Click **Setting** -> **Time Attendance** to open "Time Attendance Setting" window.

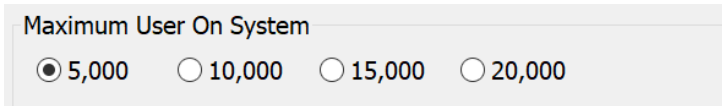
Time attendance Base On : you can decide how the time and attendance is reported from the two choices:

Work Time [First and Last Records]: The first record and last records will be integrated into the time attendance report.

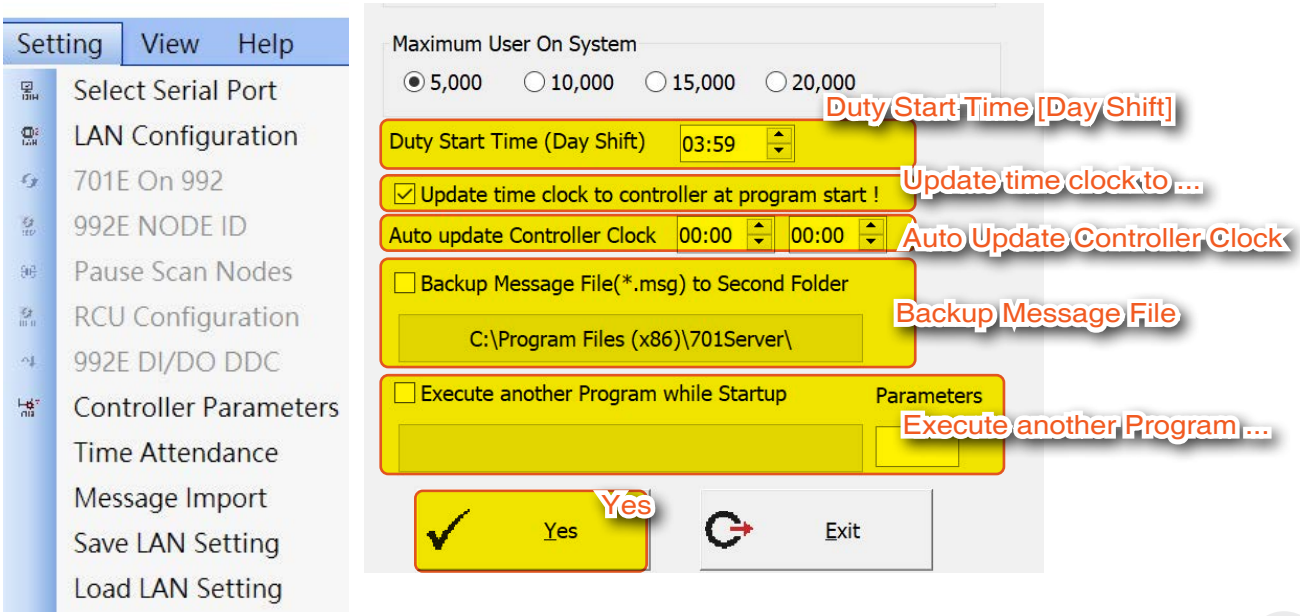
Depend On [Duty Function Key]: records are integrated into the tome attendance report according the shift name shown on the LCD panel ofthe access controller, for example: "Duty: 0,Duty: F; OVT: 0, OVT: F" .

Maximum User On System: select the user capacity, default value is 5000.

*While modifying the user capacity, please synchronize to the hardware of controller (hardware modification please refer to each controller' s manual). H series controller could select 5000 only, E series controller could select 5000/10000/15000, option 20000 is only for specific version.



Maximum User On System	5,000	10,000/15,000	20,000
Applicable Models	- H Series Controllers - Mixed Use of H&E Series Controllers	- E Series Controllers - Connected to H Series Controllers under Multi-door Controllers	Available only for Database Mode and Specific Software



Duty Start Time [Day Shift]: designate the beginning time of day shift, the records will be accumulated as the same day before time to start time, the default duty start time is 03:59, it is restricted to set after 00:00.

*Please remind that the software do not support multi-shift configuration exceeded one day, the setting of multi-shift in one day please refer to 701ClientSQL manual – Paragraph 4.6.

Update time clock to controller at program start: Synchronize the time of the computer and the controller whenever 701Server is launched or at the midnight(00:00).

Auto Update Controller Clock: you can designate two daily time sets to automatically synchronize the time of the computer and the controller.

Backup Message File: When there is inbound and outbound messaging, it can be additionally backed up to a designated path to ensure that messages are not lost due to accidental deletion (applicable to both file base mode and database mode).

(※Please designate the folder path other than C: disk, or it maight be intervened by the anti-virus software and cause error of the time attendance report.)

• For file base mode/Database mode message file import/export settings, please refer to >> Paragraph 4. Frequently Asked Questions - Q3. How to convert old data from file base to database?

• For the best approach to integrating third-party platforms with access control systems, please refer to >>11.2 Four Ways of Event Sharing

(It can directly receive all messages from 701ServerSQL, seamlessly integrating with the access control system without the need for development.)

Execute another Program while Startup: you can designate the second program to be automatically launched as long as 701Server is being launched. We normally execute 701Client as the another program.

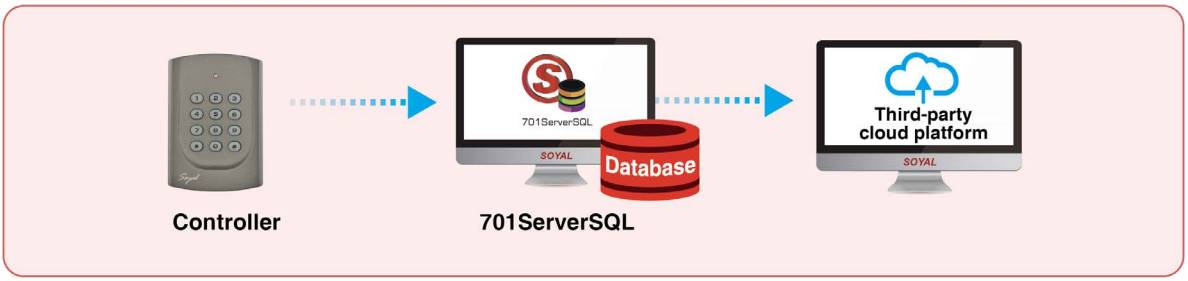
Yes : Click "Yes" button to save all settings.

More Details :

- FAQ : E serial controller, why cannot add more than 4999 users?
- FAQ : How to automatically backup daily transaction message file to second folder?
- FAQ : How to backup the transaction message from 701Server automatically?
- FAQ : Why can’ t I set up user number after 4999 at User card Edit of 701Client ?

10.2. Four Ways of Event Sharing

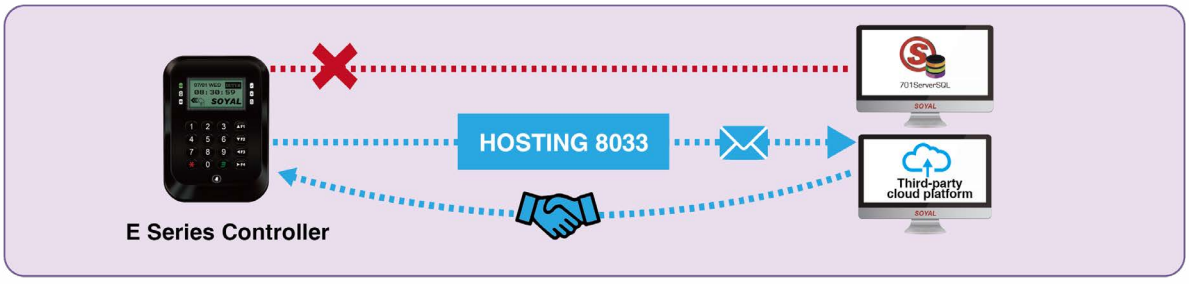
1. When 701ServerSQL receives a message, it actively forwards it.
Detailed setup instructions, please refer to>> Paragraph 11.2.1 701ServerSQL message forwarding to third-party



2. 701ClientSQL converts messages into text files either at scheduled intervals or in real-time, which can be extracted by third-party software.
Detailed setup instructions, please refer to>>
FAQ : How to Enable Cross-system Integration to Get Soyal Controller Transaction Log?

3.The controller uploads text messages to the cloud immediately upon event occurrence, without waiting for confirmation.
Detailed setup instructions, please refer to>>
FAQ : How to Enable Cross-system Integration to Get Soyal Controller Transaction Log?

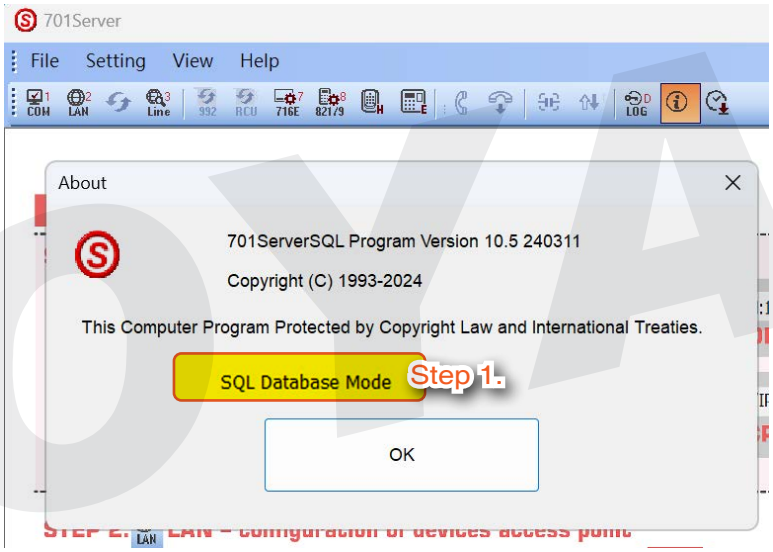
4.The controller uploads HEX messages to the cloud immediately upon event occurrence but requires confirmation before transmitting the next one.
Detailed setup instructions, please refer to>>
FAQ : How to Enable Cross-system Integration to Get Soyal Controller Transaction Log?



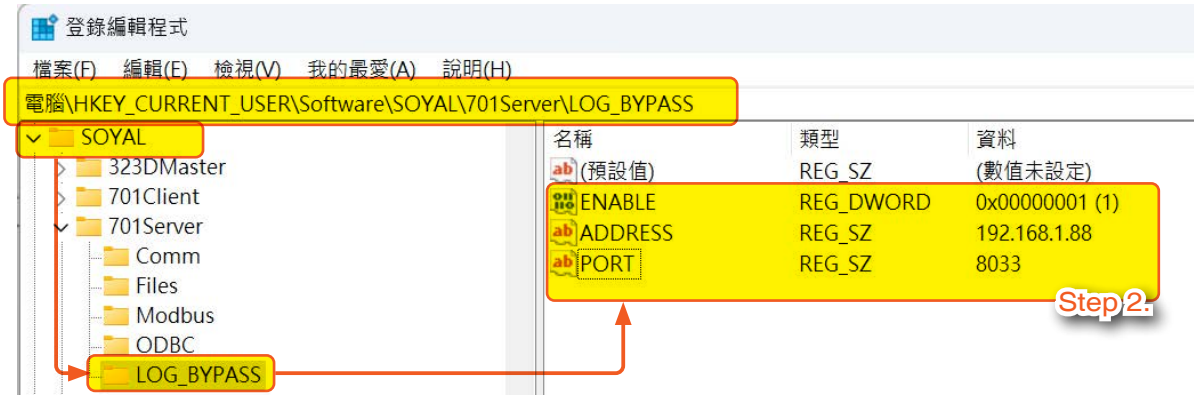
• 10.2.1 701ServerSQL message forwarding to third-party

Purpose: The new version of SOYAL 701ServerSQL software supports forwarding the latest records in real-time to a configured secondary server. After receiving response code 0X37 (fixed response code), it will proceed to forward the next record. This function is commonly used in attendance systems to obtain personnel entry and exit records, NVR/DVR systems to obtain access control records for display in surveillance videos, and other third-party platform integration applications.
Upon receiving a message, 701ServerSQL actively forwards it to a third-party. If the third-party platform cannot respond immediately, the system will temporarily store the message in the database, waiting to resend it once the third-party platform reconnects to ensure no message loss.

The steps to enable the "Enable event log bypass" feature mainly involve three steps, please refer to the following:



Step 1. Ensure that 701Server is in SQL Database Mode.



Step 2. In the registry editor (Regedit), navigate to the following path:
Computer\HKEY_CURRENT_USER\Software\SOYAL\701Server\LOG_BYPASS
Add the following three keys; we'll use the example of the second server IP: 192.168.1.88, Port: 8033, which is a fixed value.

Key Name	Data Type	Value	
ENABLE	REG_DWORD	1	0: Disable, 1:Enable
ADDRESS	REG_SZ	“192.168.1.88”	Remote Listen IP
PORT	REG_SZ	“8033”	Remote Listen Port

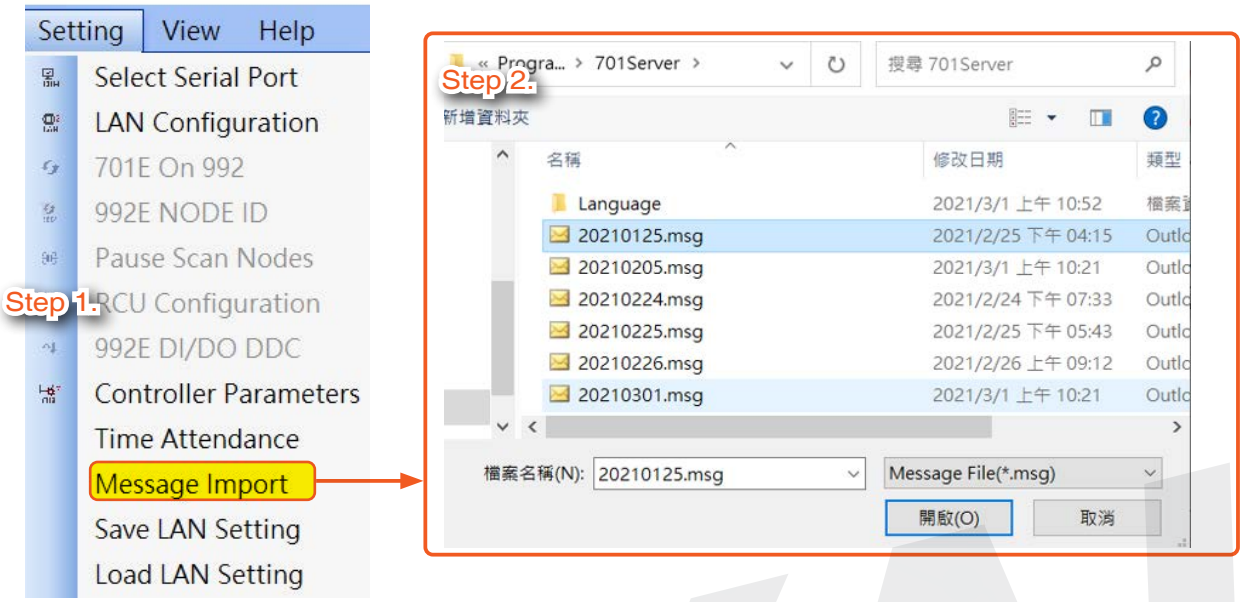
Step 3. After setting the parameters, the 701ServerSQL software must be restarted.
We use Packet Sender to simulate testing the reception of the latest record forwarded by 701ServerSQL to the second server path and returning response code 0X37.

Complete setup tutorial:

- 701ServerSQL Event Log Bypass Second Server Example

10.3. Message Import Setting

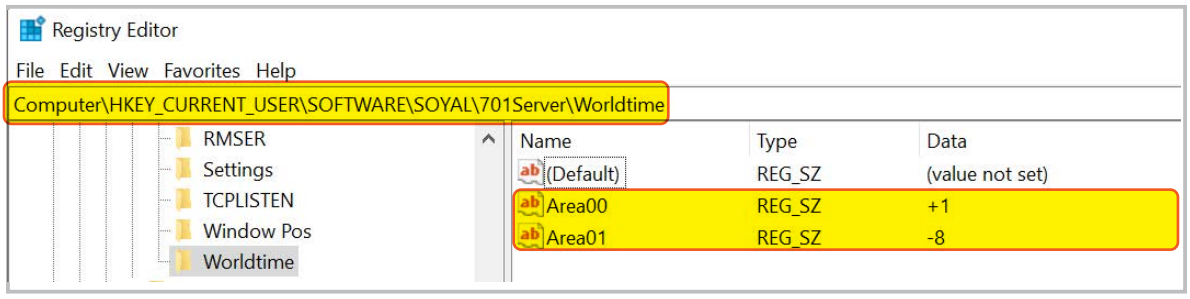
After backup and restore data from old PC to new PC, transaction record in .msg file format is required to do "Message Import" in order to generate daily duty .dut file again.



Step 1. Select Message Import
Step 2. Select the .msg file and click 'Open' to import.

10.4. Setting global time schedules for each regional controller

Supports independent time zone settings for Area00 to Area15, with the reference time based on the computer time of the running 701ServerSQL, in hourly increments.



NOTE

1. To create a time difference, you need to navigate to the "Worldtime" folder within the path of 701Server.
2. The type of time difference to create is a "**String Value**".
3. The time creation rule is based on the computer time of executing 701ServerSQL.
   If it is one hour later than the computer time of 701ServerSQL, it is represented as "+1".
   If it is 8 hours earlier, it is represented as "-8", and so on.

11. Appendix

11.1 User License Agreement - Third-Party Software

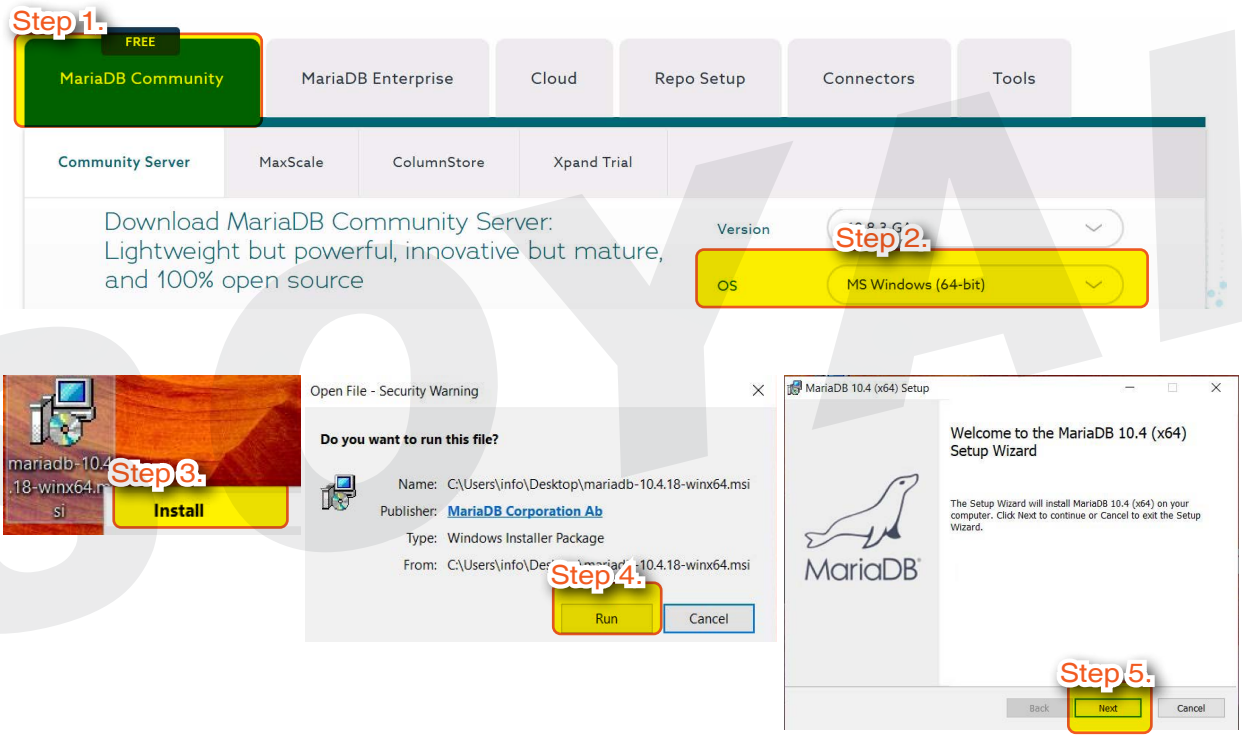
SOYAL software and products may be used in conjunction with other products or software and may include links to third-party software, interfaces, content, or data (hereinafter referred to as "Third-Party Software"). When using such "Third-Party Software," you must obtain authorization from the original manufacturer and comply with the terms and conditions provided by the software licensor, including their privacy policy. By accepting or using "Third-Party Software," you agree to abide by the applicable third-party terms. SOYAL makes no representations or warranties regarding the operation, suitability, or performance of "Third-Party Software." Additionally, SOYAL or its licensors shall not be held liable for any loss or damage arising from the inability to use, limited functionality, or removal of "Third-Party Software."

11.2 Installation Tutorial for MariaDB Database

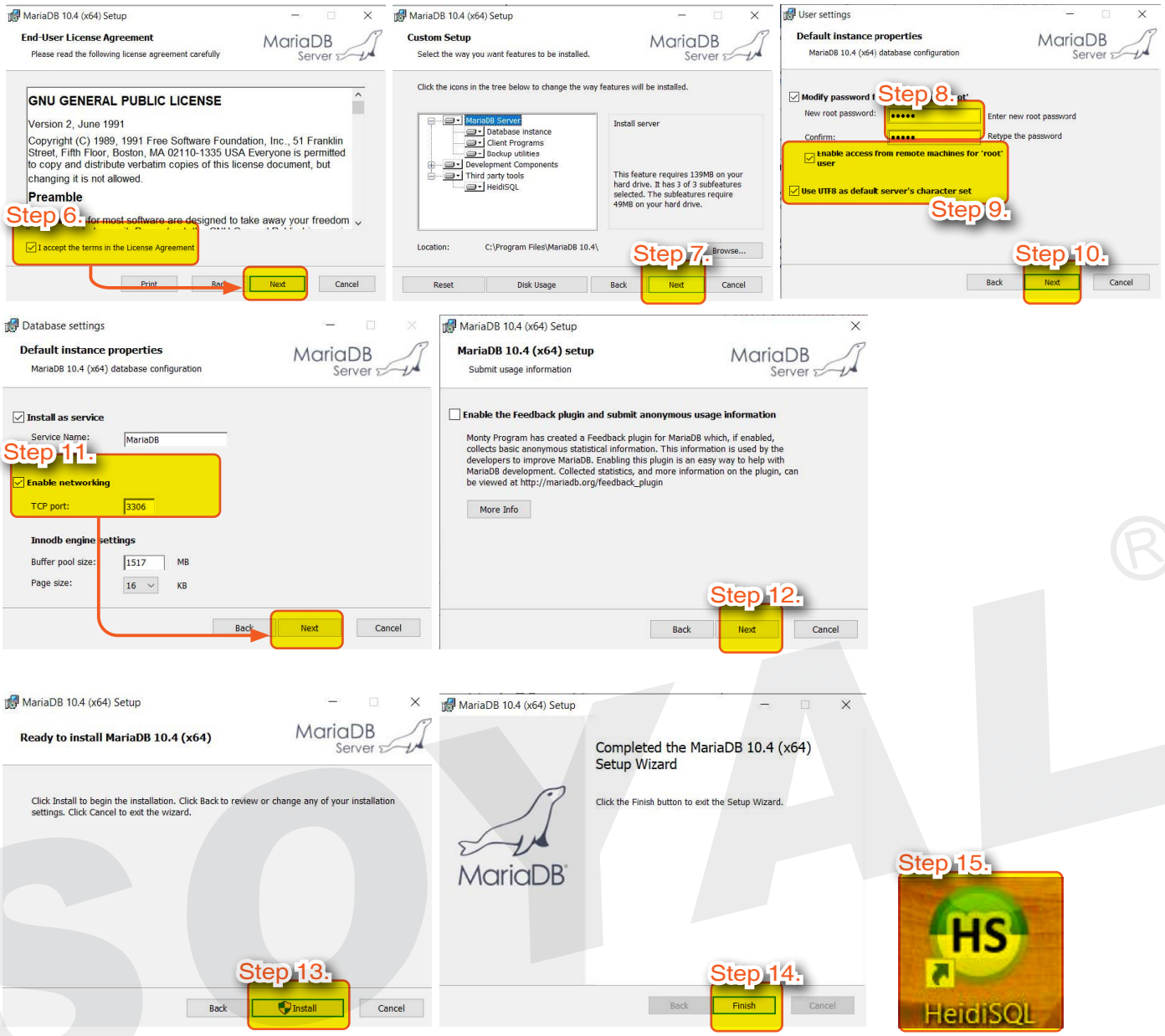
11.2.1 Installing MariaDB Database Software

NOTE

- Please choose Win32 or Win64 to download and install according to your operating system and download the version MariaDB version 10.3 and after
- This software can't be put in the SOYAL CD. Customers can only download it from the original website to meet the requirements of open source.
- Example we use mariadb-10.4.18-winx64.msi for installation steps demonstration



Step 1. Download the installation from database (using MariaDB as example, please download from MariaDB Official Website)
Step 2. Select 64-bit version and download
Step 3. Install MariaDB
Step 4. Select [Run]
Step 5. Select [Next]



Step 6. End-User License Agreement
Accept the License Agreement by ticking [I accept the terms in the License Agreement] and select [Next]

Step 7. Custom Setup Select [Next]

Step 8. Enter [New root password] and [Confirm] as admin. This password is used for connection to database, please do not forget this password.

Step 9. Then tick 'Enable access from remote machine for 'root' user' and 'User UTF8 as default server' s character set'

Step 10. Select [Next]

Step 11. Enter TCP Port '3306' (note: if you have installed other software that also required connection to database, please note the TCP Port value cannot have the same value as 701ServerSQL)

Step 12. Select 'Next'

Step 13. Select 'Install' to start installation of MariaDB

Step 14. Select 'Finish' to finish installation

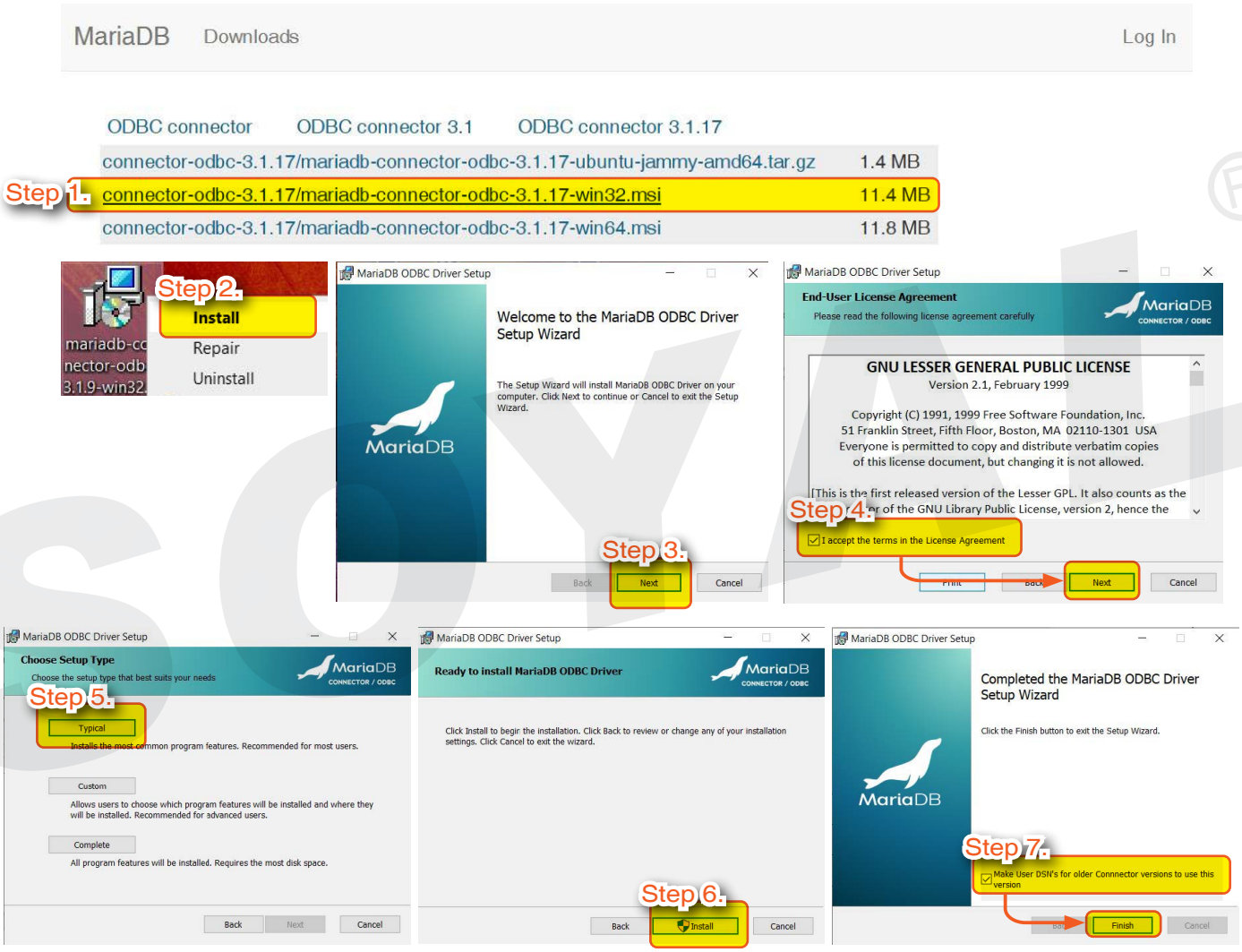
Step 15. When installing MariaDB, HeidiSQL will also be included as a bundle. That is why, on your desktop HeidiSQL shortcut is automatically created.

11.2.2 Installing MariaDB ODBC Connector

To establish connection between 701ServerSQL and 701Client SQL, ODBC Connector is required. 701 Software offer compatibility with Database Software such as MariaDB, MySQL, and SQLite. We will demonstrate using MariaDB as an example and the ODBC Connector of MariaDB is MariaDB Connector/ODBC

NOTE

- No matter what is your operation system either Win64 / Win32, please download ODBC Connector of Win32.
- This software can't be put in the SOYAL CD. Customers can only download it from the original website to meet the requirements of open source.
- Example we use mariadb-connector-odbc-3.1.17-win32.msi for installation steps demonstration



Step 1. Please download the 32-bit version of the installation from the database. (Using MariaDB as an example, please download it from the official website of MariaDB.)

Step 2. Install MariaDB Connector/ODBC

Step 3. Select 'Next'

Step 4. End-User License Agreement
Accept the License Agreement by ticking [I accept the terms in the License Agreement] and select [Next]

Step 5. Select [Typical]

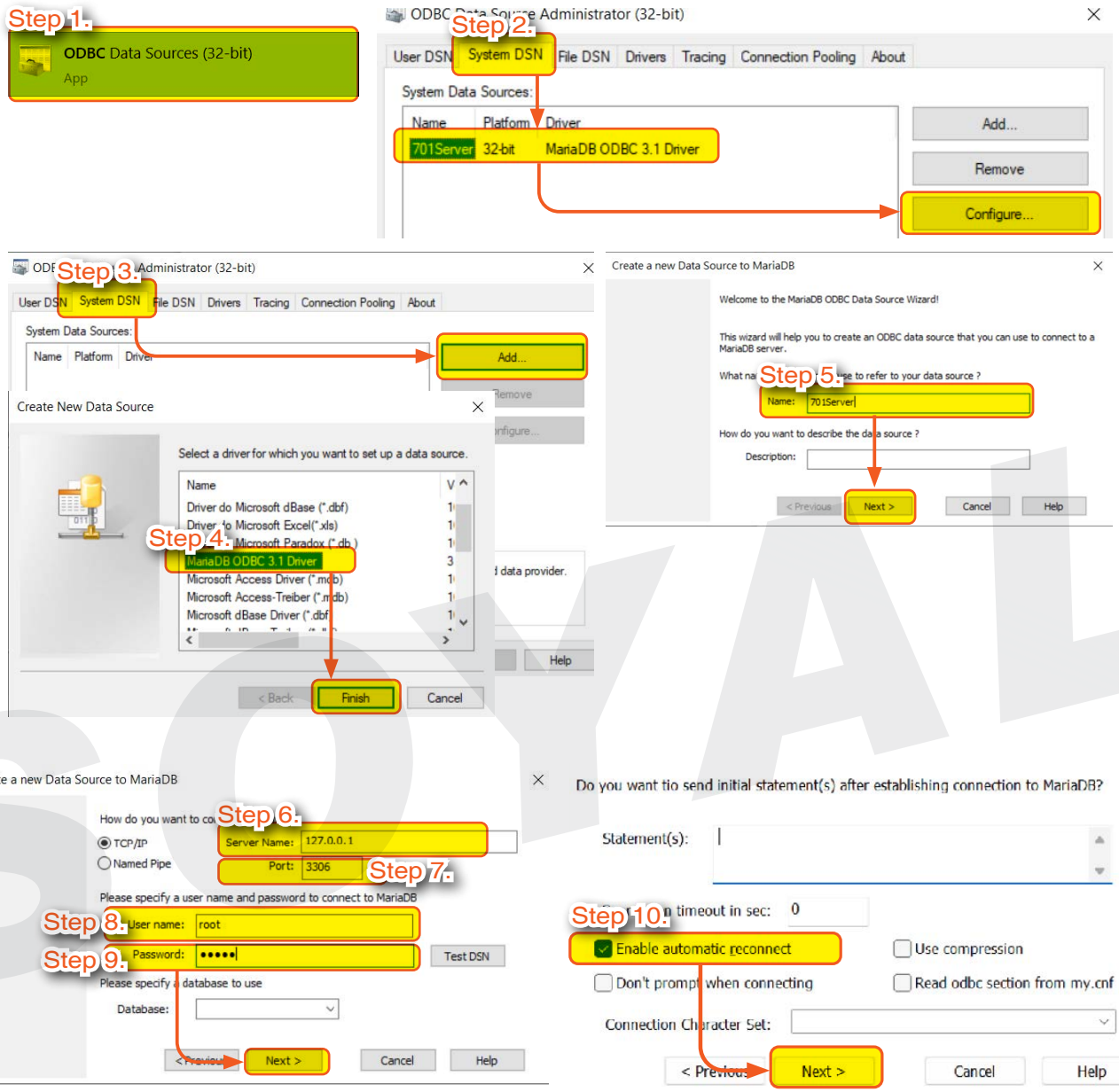
Step 6. Select [Install] to start installation of MariaDB Connector/ODBC

Step 7. Tick option [Make User DSN's for older Connector version to use this version] and click [Finish] to finish installation

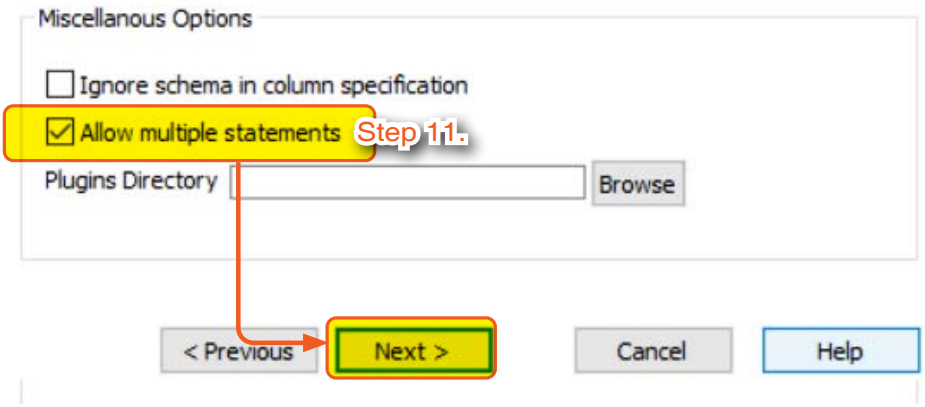
11.2.3 Setting Up MariaDB ODBC 32 DSN

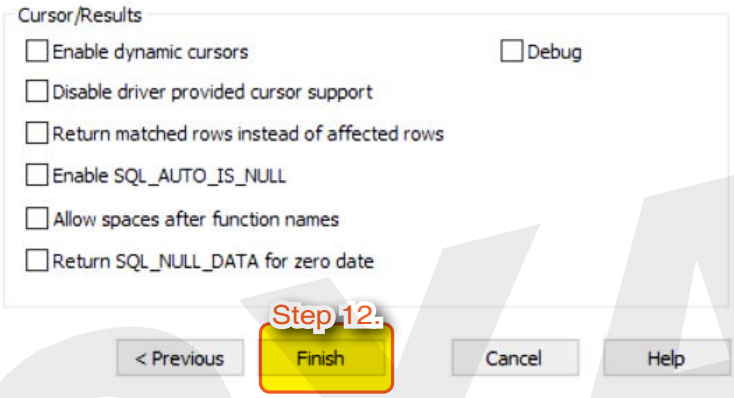
Setting up ODBC Connector will enabled connection between Remote Client A and B PC to the Main Server.

- Main Server Setting (192.168.1.79)



Step 1. Go to 'ODBC Data Sources (32-bit)'
Step 2. Select 701ServerSQL and select Configure
(Skip Step 3-Step 5 if connection to 701Server is established and directly to Step 6)
Step 3. If connection to 701Server is not establish yet, select Add
Step 4. Select 'MariaDB ODBC 3.1 Driver, Click [Finish]
Step 5. Enter [701Server] on Name field and select [Next]
Step 6. Server Name 127.0.0.1 (connection to Host PC)
Step 7. On Port setting enter [3306]
Step 8. Username enter [root]
Step 9. Password enter [admin] and select [Next]
Step 10. Tick [Enable automatic reconnect] then select Next





Step 11. Tick [Allow multiple statements] then select Next

Step 12. The next part does not required set up so click Click Next>until you the end of the page and click [Finish]

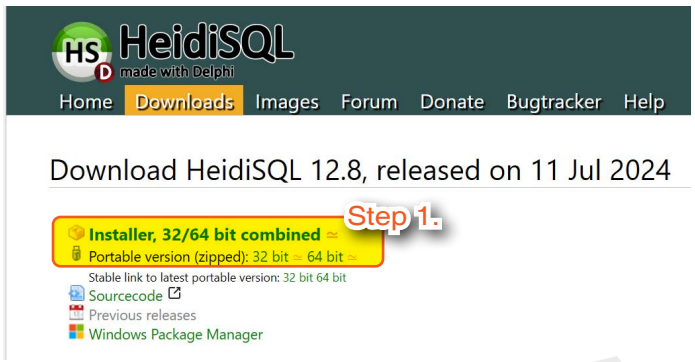
11.2.4 Installing HeidiSQL Tool

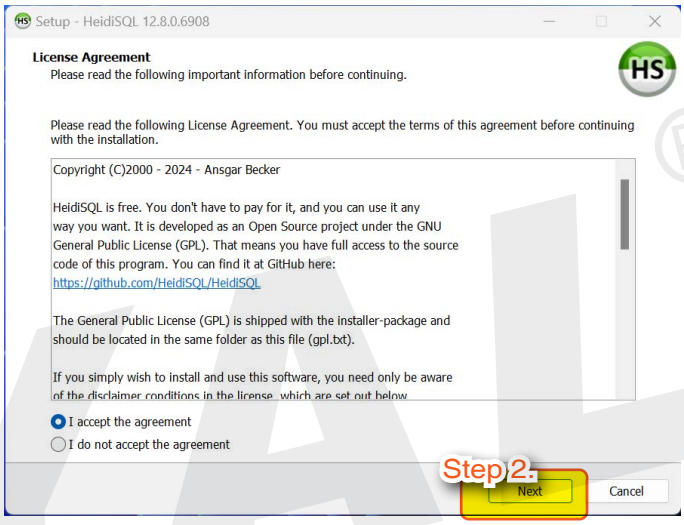
NOTE

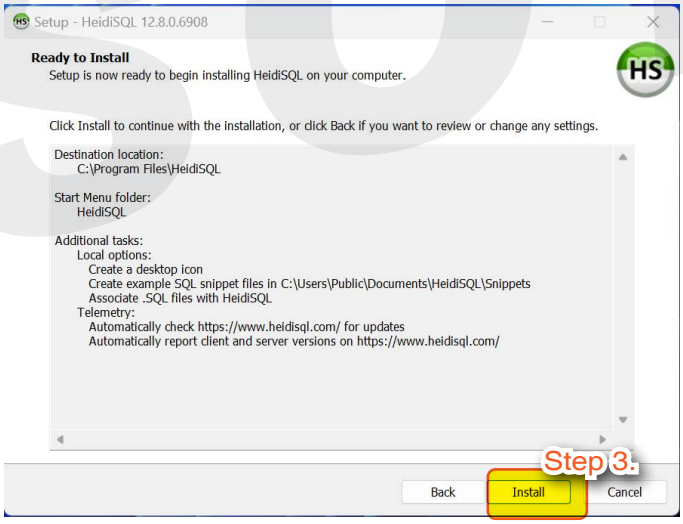
If the MariaDB database software is already installed, this step can be skipped.

When installing the MariaDB database software, the HeidiSQL tool will also be installed and can be found in the toolbar

Download link for the HeidiSQL tool, please download it from the official website of HeidiSQL. The following operations are based on version 12.8.







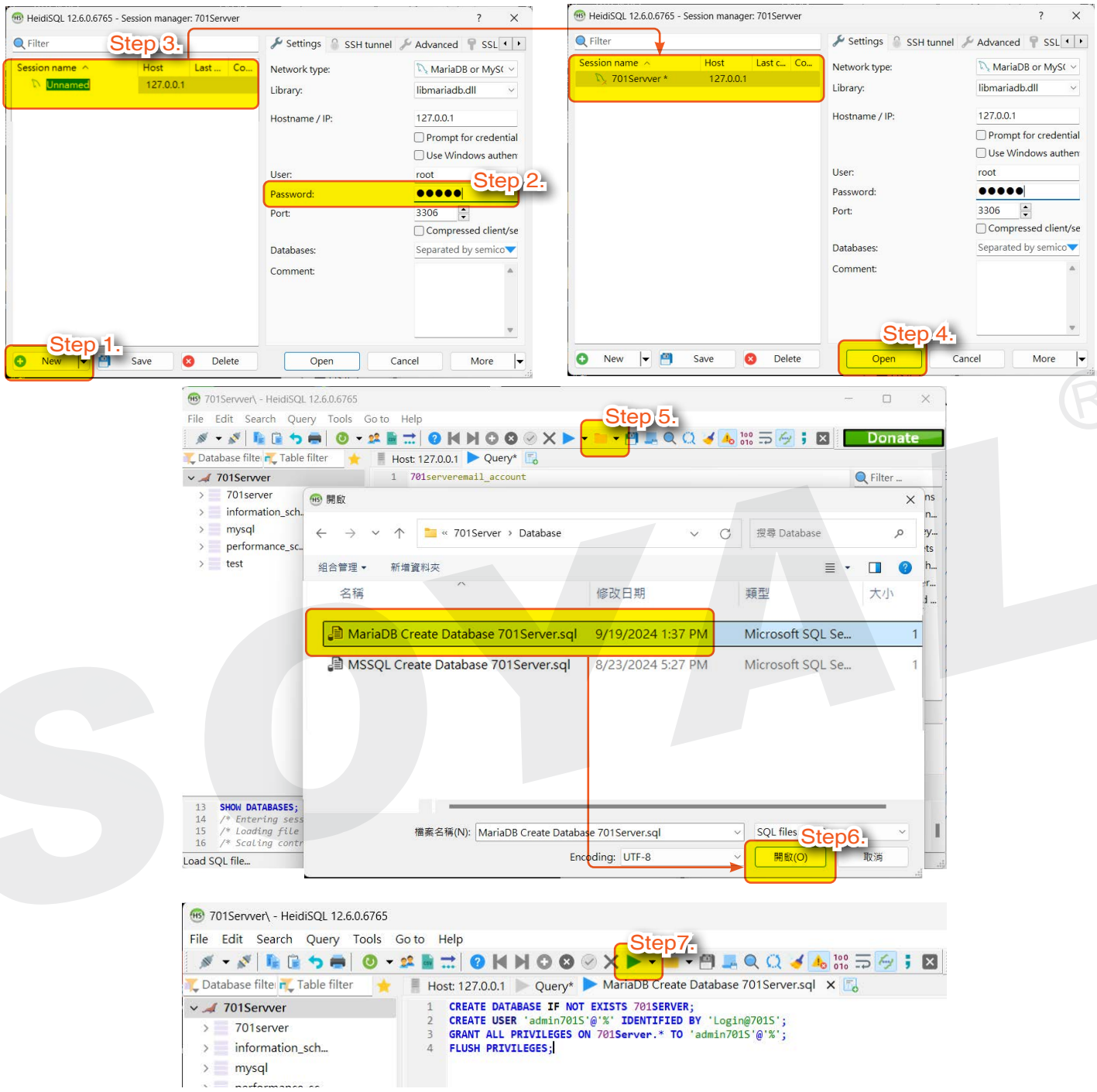
Step 1. Download the 64-bit version of the HeidiSQL installation file (please download it from the official website of HeidiSQL.)

Step 2. After executing the installation file, click [Run].

Step 3. Follow the prompts in the installation process to proceed to the next step, select the required features, and then click [Install].

Step 4. Click [Finish] to complete the installation.

11.2.5 Running HeidiSQL to Open T-SQL Script Files for Creating Database and User Login Permissions



Step 1. Launch [HeidiSQL] and click on [NEW].

Step 2. Enter the password in the Password field: admin (the password is the same as set during installation).

Step 3. Change the name from Unnamed to [701Server].

Step 4. Click [Open] to open the database.

Step 5. Click the [Open File] icon → In the path C:\Program Files (x86)\701Server\Database, select the file named MariaDB Create Database 701Server.sql.

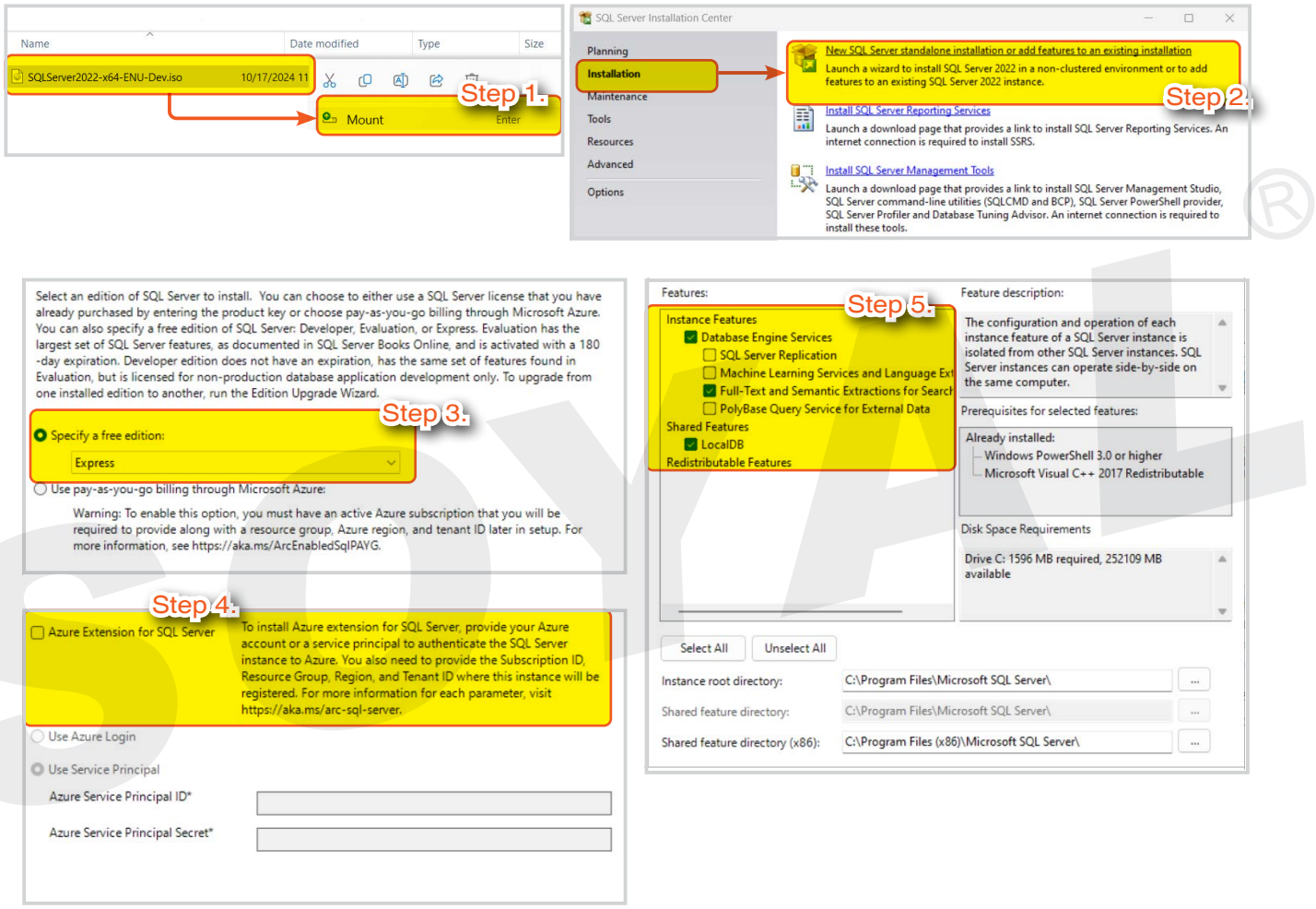
Step 6. Click [Open].

Step 7. Click [Execute]; after running the T-SQL statement, it will create the default users for 701ServerSQL: user: admin701S and password: Login@701S.

11.3 Installation Tutorial for MSSQL Database

11.3.1 Installing MSSQL Database Software

Download the MSSQL database software installation file (please download it from the official Microsoft website). The following operations are based on the SQL Express version.



Step 1. Right-click on SQLServer2022-x64-ENU-Dev.iso and mount it.

Step 2. Select [Installation] → Choose [New SQL Server standalone installation or add features to an existing installation].

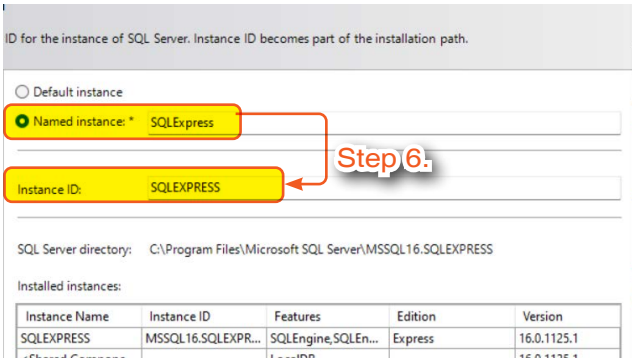
Step 3. Select [Specify a free edition] → In the dropdown menu, choose [Express].

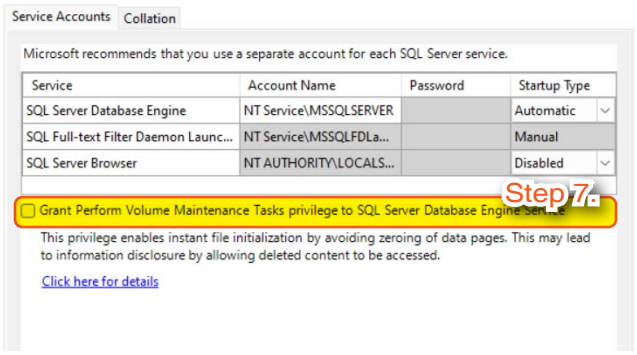
Step 4. If you do not have an Azure account, you can skip this step; uncheck the option.

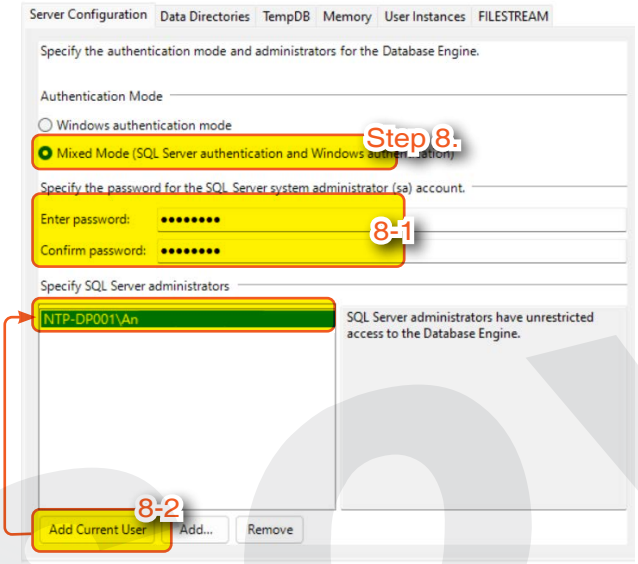
Step 5. SQL Express feature options:

When installing SQL Express, you do not need to select all features; generally, selecting the following three is sufficient:

- Database Engine Services
- Full-Text and Semantic Extractions for Search
- LocalDB







Step 6. Select Named Instance, enter: SQLExpress
For Instance ID, enter: SQLEXPRESS

Step 7. Do not check this option

Step 8. The installation mode must be set to [Mixed Mode].

8-1 The password field is for logging into the database as 'sa' in the future; you can enter: Soyal@sa8, which can be synchronized with the tutorial document and changed later if needed.

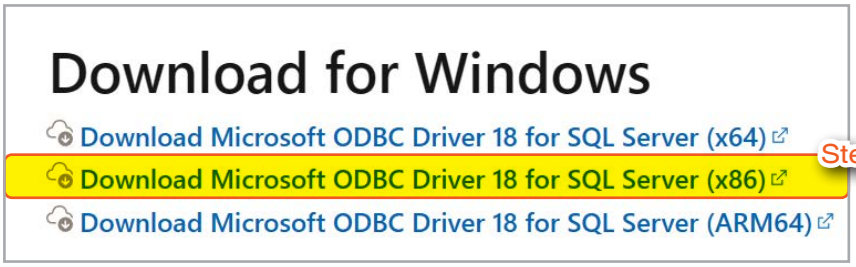
8-2 [Add current user] for easy local login.

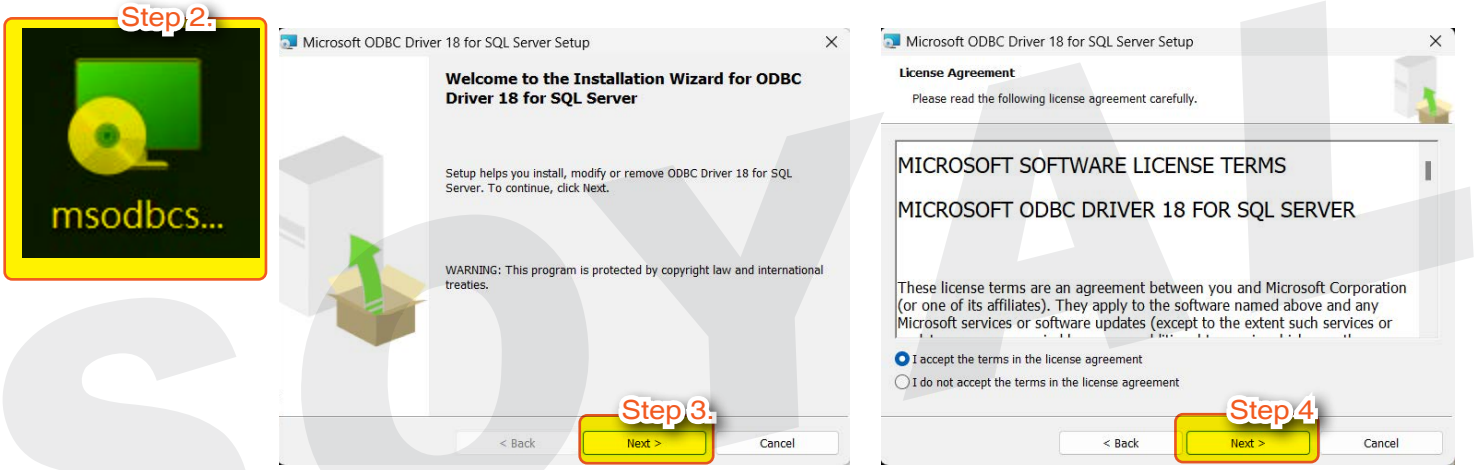
11.3.2 Installing MSSQL ODBC Connector

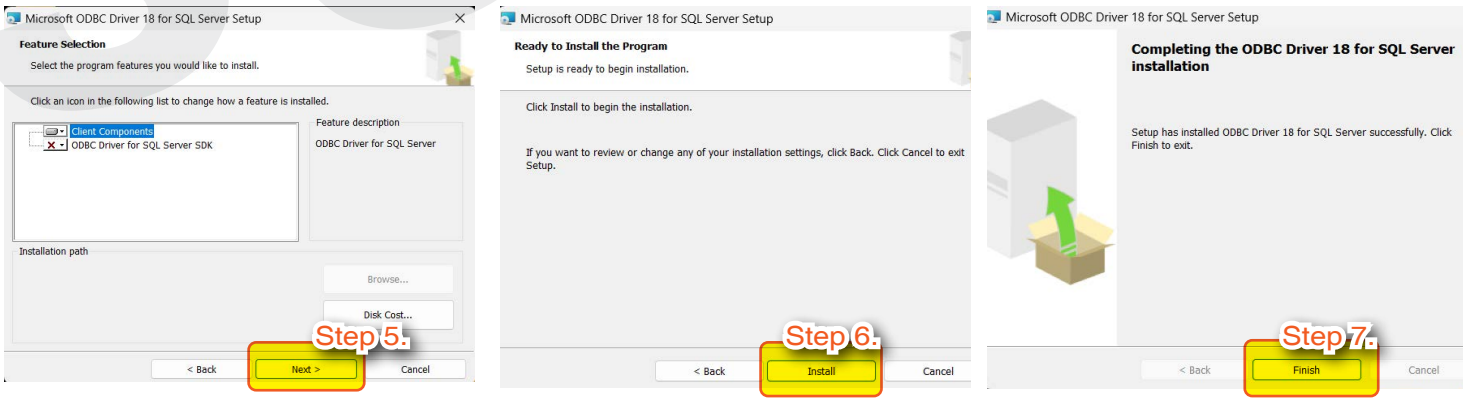
To establish communication connections for 701ServerSQL and 701ClientSQL, the ODBC Connector needs to be installed. The following operations use Microsoft ODBC Driver 18 for SQL Server (X86) as an example.

NOTE

- Regardless of whether the computer's operating system is Win32 or Win64, please download the X86 version of Microsoft ODBC Driver.
- Please download the software from the official website that meets your needs → Microsoft official website.

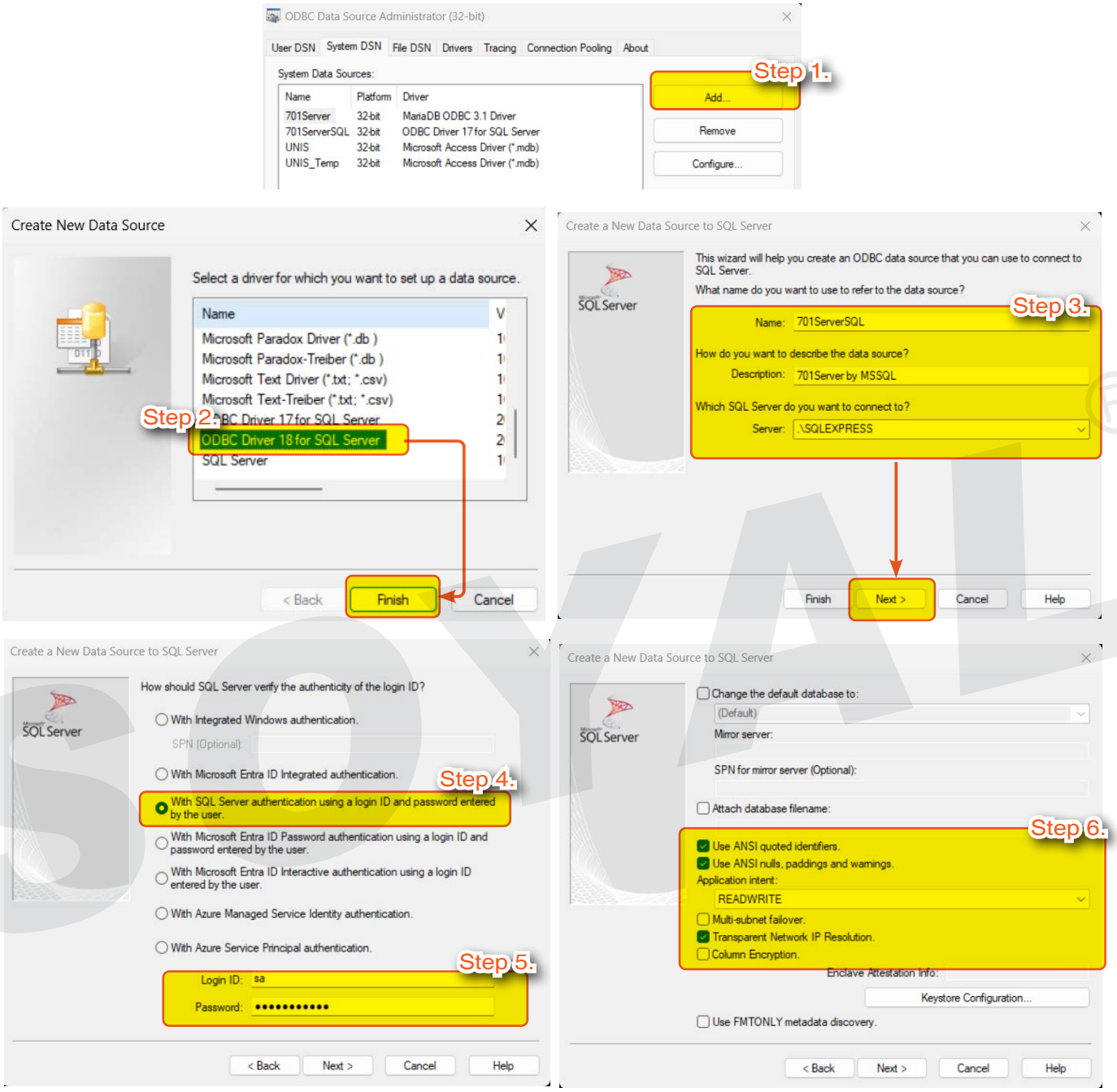






Step 1. Download the X86 version of the ODBC Connector installation file (please download it from the official Microsoft website).
Step 2. Install the ODBC Connector (software name: msodbcsql)
Step 3. Select [Next].
Step 4. Select [Next].
Step 5. Select [Next].
Step 6. Select [Install] to begin installing the ODBC Connector.
Step 7. Click [Finish] to complete the installation.

11.3.3 Setting Up MSSQL ODBC 32 DSN



Step 1. Click [Add]

Step 2. Select [ODBC Driver 18 for SQL Server], then click [Finish].

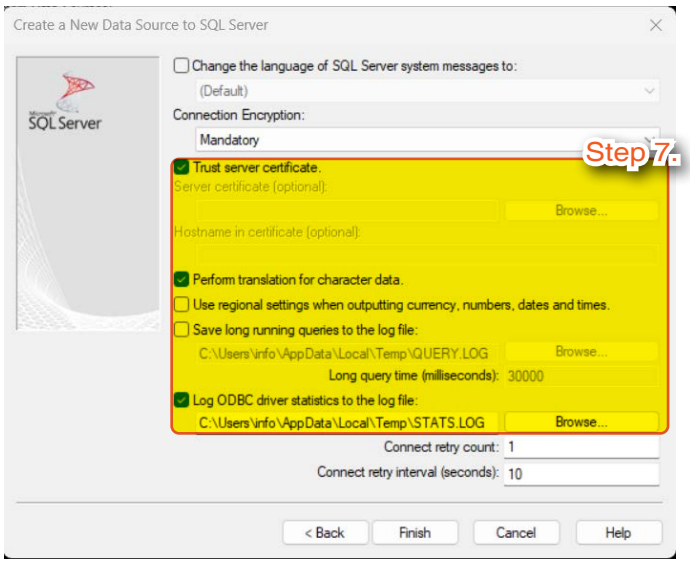
Step 3. Enter the Data Source Name and click Next after entering:

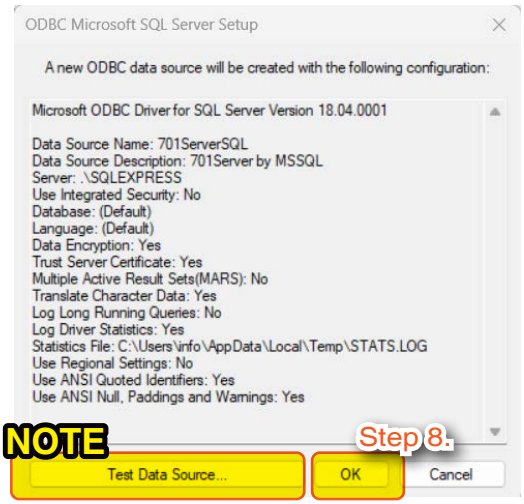
- Name must be: 701ServerSQL
- Description: 701Server by MSSQL
- Server: If it is a database host, enter .\SQLEXPRESS; if it is a remote computer, point to the host IP, entering the host IP here.

Step 4. Choose [With SQL Server authentication using a login ID and password entered by the user].

Step 5. Login ID: sa, Password: Soyal@sa8 (as set during SQL Express installation).

Step 6. Check options as shown in the image.





Step 7. Check options as shown in the image; note that you must check [Trust server certificate], as well as [Log ODBC driver statistics to log file].

Step 8. Configuration complete; click [OK].

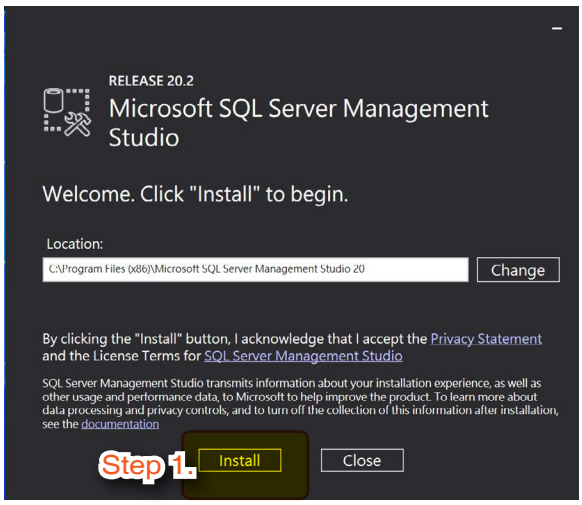
NOTE

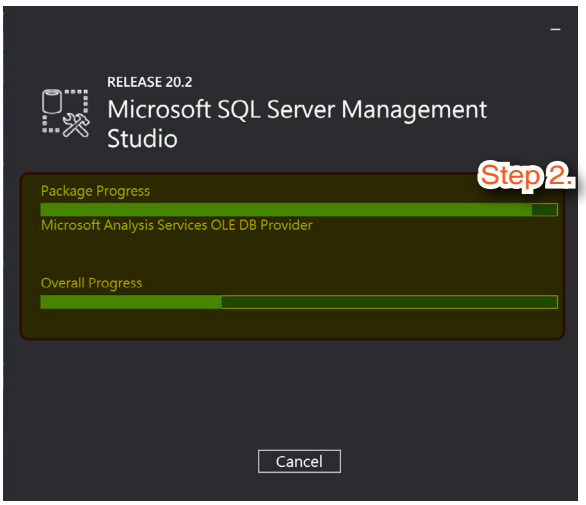
- You can click [Test Data Source] to verify if the configuration is correct.

11.3.4 Installing SSMS Tool

Download and install SQL Management Tools SSMS (please download it from the official Microsoft website).

After installing the MSSQL database software, you need to install SQL Management Tools SSMS in order to execute T-SQL statement files for creating the 701Server Database.



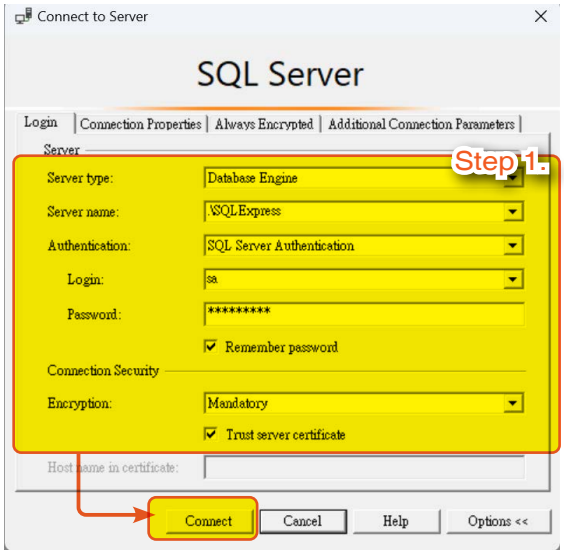


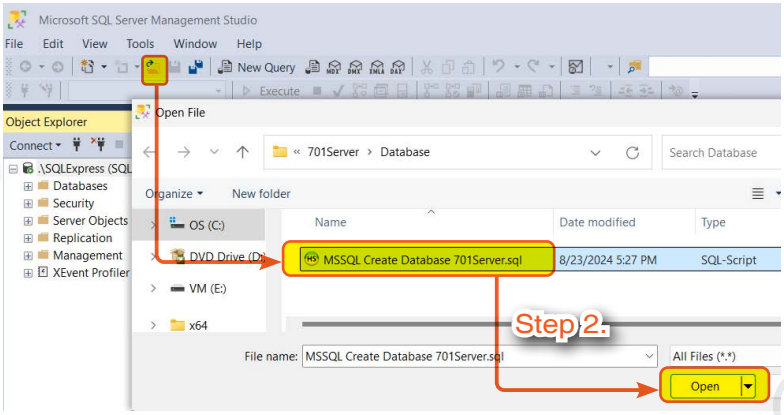
Step 1. Click [Install].

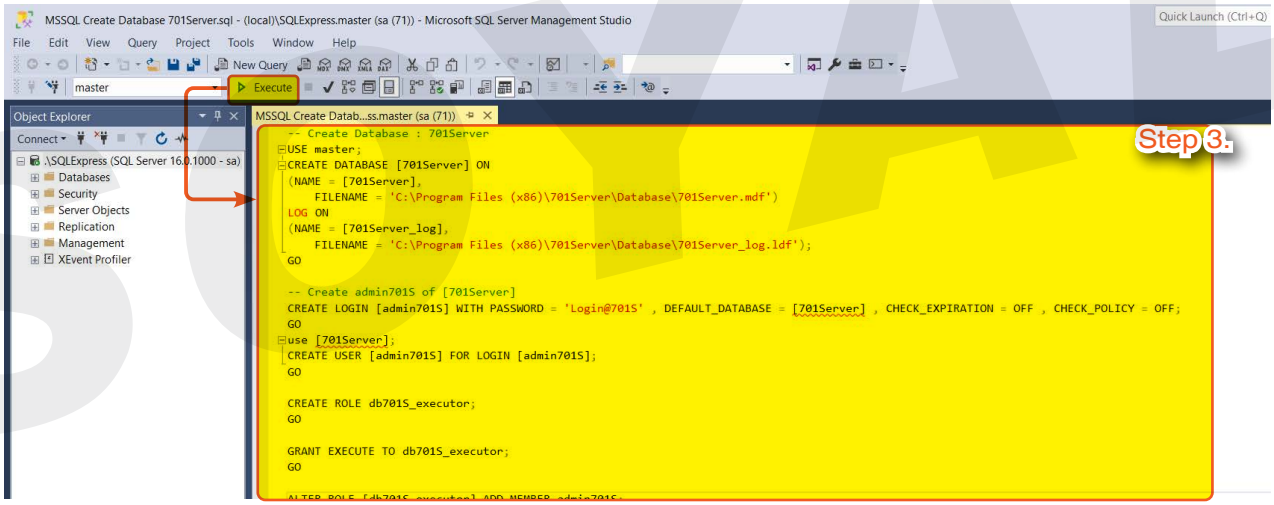
Step 2. Wait until the progress bar reaches 100% to complete the installation.

11.3.5 Running SSMS to Open T-SQL Script Files for Creating Database and User Login Permissions

Run SSMS to create the 701Server Database and user.







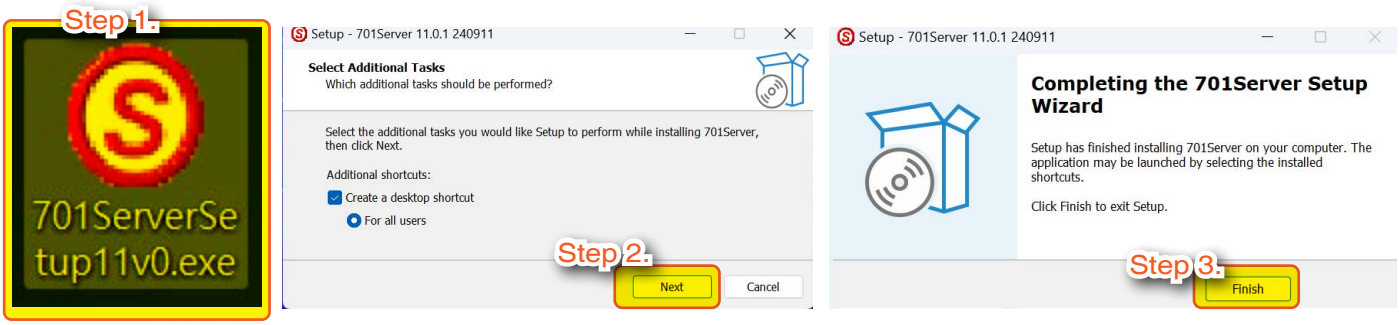
Step 1. Launch SSMS and log in to the SQL Server [.\SQLExpress].

- Server name : Select [.\SQLExpress] .
- Authentication : Choose [SQL Server Authentication].
- Login: sa, Password: Soyal@sa8 (as set during SQL Express installation) (※ remember to check "Remember password").
- Encryption: select [Mandatory] (※ ensure "Trust server certificate" is checked).

Step 2. Execute the MSSQL Create Database 701Server.sql by clicking the [Open File] icon → In the path C:\Program Files (x86)\701Server\Database, select the file named MSSQL Create Database 701Server.sql → click [Open].

Step 3. Click [Execute]; after running the T-SQL statement, it will create the default user for 701ServerSQL: admin701S and password: Login@701S.

11.4 Installing 701ServerSQL Version 11.X



Step 1. Double-click to start the installation.

Step 2. During the installation process, keep clicking [Next] until the installation is complete.

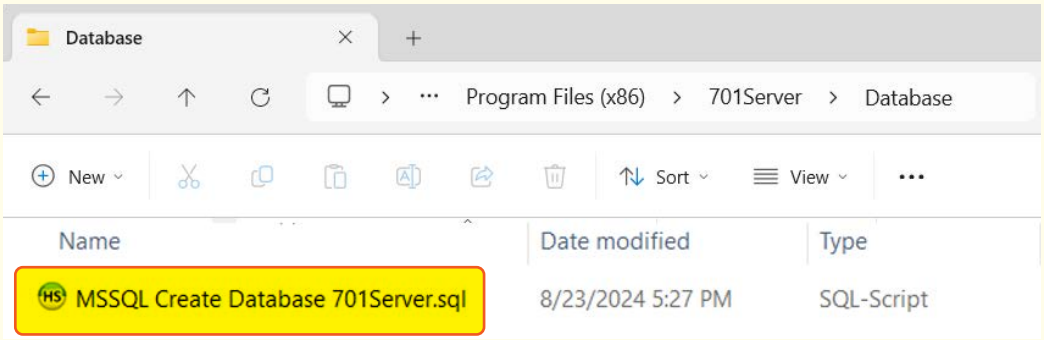
Step 3. Click [Finish] to complete the installation (a shortcut for 701ServerSQL will be automatically created on the desktop).

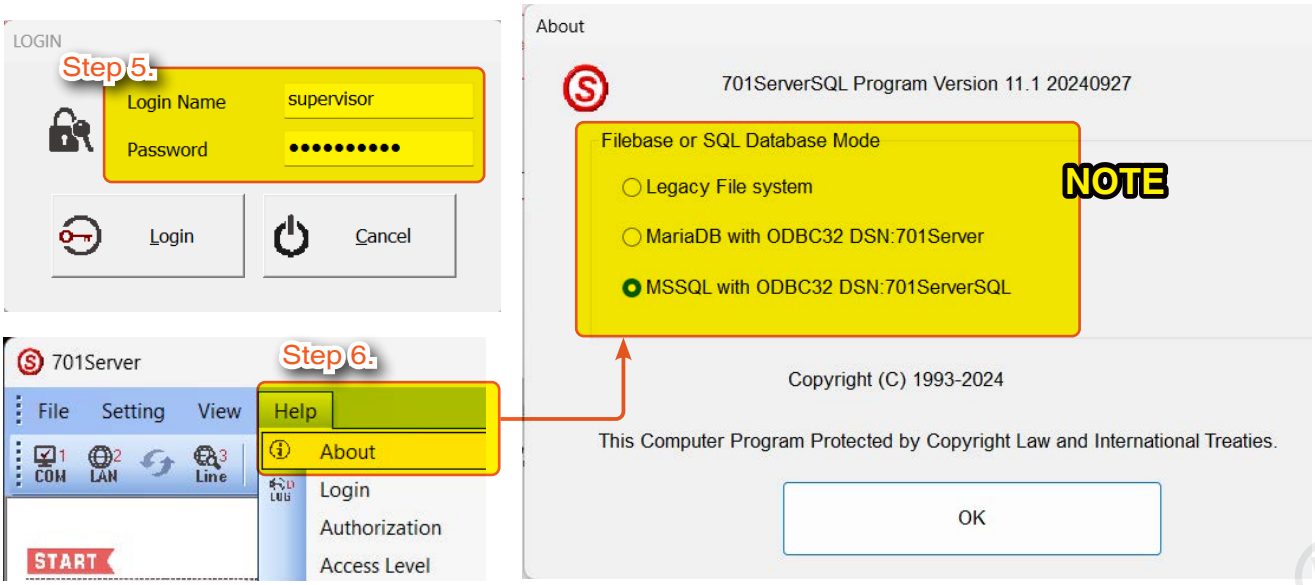
※ After installing the database version, do not run 701ServerSQL V11.X immediately; first, complete the steps to create users for 701ServerSQL and 701ClientSQL before running the software.

- For detailed steps on creating users in MariaDB, please refer to 11.2.5 Running HeidiSQL to Open T-SQL Script Files for Creating Database and User Login Permissions
- For detailed steps on creating users in MSSQL, please refer to 11.3.5 Running SSMS to Open T-SQL Script Files for Creating Database and User Login Permissions

NOTE

When installing 701ServerSQL version 11.x, it includes a T-SQL script file that can create the 701Server Database and login users. The T-SQL script file is located at: C:\Program Files (x86)\701Server\Database\MSSQL Create Database 701Server.sql.





Step 4. Run the software and enter the default username: supervisor and the default password: supervisor.

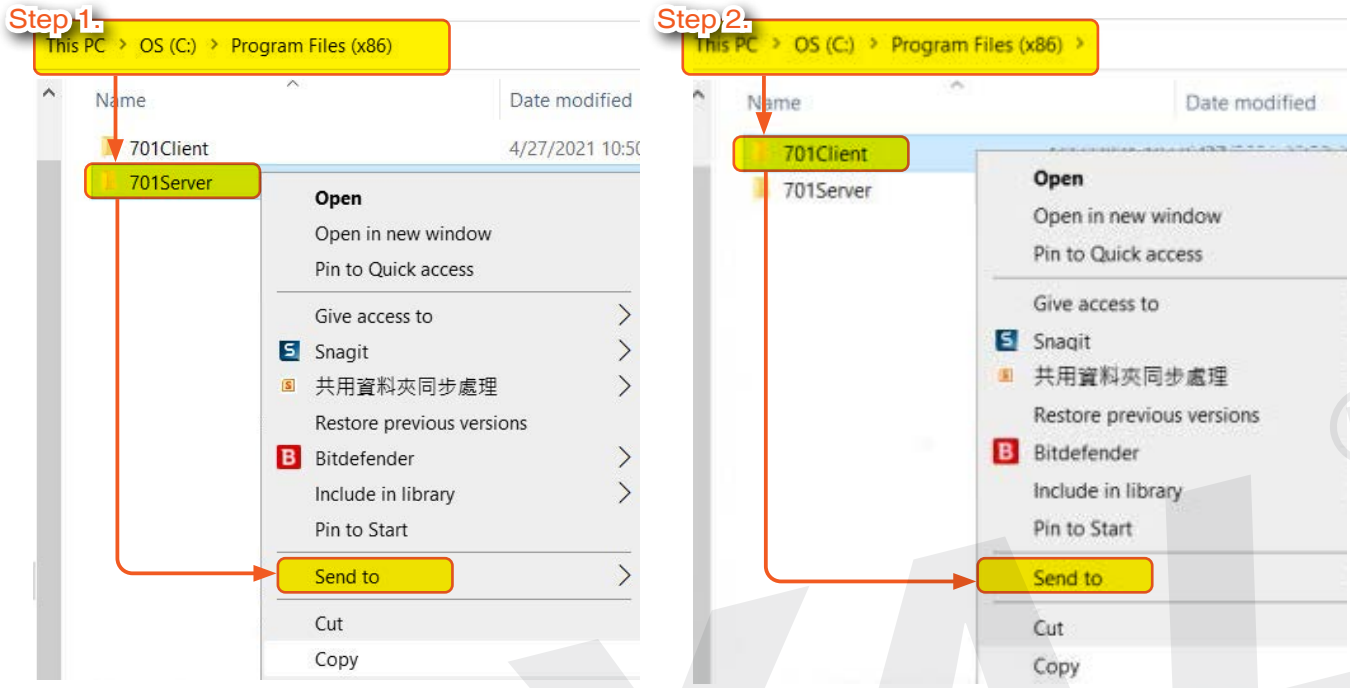
Step 5. Click on Help → About in the toolbar of 701ServerSQL; a pop-up About window will display three options, which can be selected as needed. (※ Note: Although there are three modes to choose from, once selected, they cannot be switched.)

NOTE

If the database ODBC DSN 32 is not installed/configured, the database options will be unavailable for selection.

11.5 Back Up DATA

Creating a back-up data is necessary to avoid data from lost during the upgrade especially for .msg files (transaction log) and user data (default.xx)



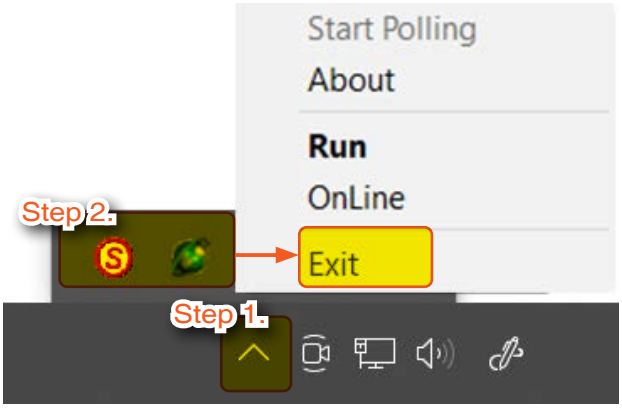
Step 1. Copy 701 Server folder and paste into Drive D, Desktop, or any hard drive that will be safely stored.
Step 2. Copy 701 Client folder and paste into Drive D, Desktop, or any hard drive that will be safely stored.

NOTE

- Full version about backup data could be found in the step-
  Backup and Restore 701 Server and Client from old PC to new PC
- When upgrading to Database Mode, the old data that is recorded on file system mode will still save under file system format. Once you upgrade into the database, all of old data will automatically transferred to database and cannot be converted back to file system data. For event log (msg files), you required to do 'Message Import' manually from 701ServerSQL to convert the data from file system into database format.
- If you want to preserve the old data under file system format, make a copy and stored in a safe place (refer to 2.3.3. BACK UP DATA)
- Data that is remain on file system base even after upgrade to database mode:
  1. time attendance report such as DUTY file
  2. lift and floor data
  3. fingerprint and face data
- Upgrade from Windows XP to Windows 10, all of the data must be copy and directly paste to C:\Program Files (x86)

Close 701 Software

Before uninstall and updating new software, make sure 701ServerSQL and 701ClientSQL is properly closed and not under running condition.



Step 1. Click [Show hidden icons] on the right bottom side of the desktop.
Step 2. You will see 701ServerSQL and 701ClientSQL software icon > right click > **Select Exit**

12. Reference document

FAQ

- how to Solve the trouble when the User Press Duress Code For Access on V5 Series Controller to Cause Error Time Attendan
- Solve 701ServerSQL maintain logged in status when Windows Server auto restart
- How to automatically change user access mode for different reader?
- What is “DI Loop2/3 Show Message” under 821E/829E Parameter setting?
- How to set up alarm event on AR-829E?
- How to set up AR-829E auto-shift function?
- How to set up door number on AR-821EF and AR- 829E?
- How to set up “door auto open” function on AR-829E?
- How to enable AR-829E “Auto Disarm(Zone:62)” function?
- AR-716E + 721H*2 the hardware installation is done, how to set software connection?
- How to solve 0xc000007b and mfc140u.dll problems when installing 701Server and 701Client?
- How to use Resources file to translate 701software to other languages
- How to Run 701Software with Different PC User Account?
- How to translate 701server/client from English to different language?
- How to export the 701Sever/Client registration file?
- 701Server, 701Client data sharing?
- In one site install 721H and 821EF-V5 and download the same user data to two reader at the same time, but the user is asked to only use FP access on 821EF-V5 , not use card , How to do it?
- The sensor of AR-821EFB/D-9000DO can't induct/identify fingerprint

Video

- 《701 Server》 Quick Start