SOYAL®
ACCESS & INDUSTRIAL CONTROL

Operation Manual
Enterprise Series HTTP Server

System Requirements

- Web Browser Setting Interface
- Cross-Platform Services does not limit to particular operating system, smartphone, or tablet
- Provide parameter setting, user data setting, event log query and direct control

SOYAL Website

Table of Contents

1. HTTP Server Introduction

1-1 / Main Features

- Easy setup via Smartphone, Tablet, and PC by entering IP address of the devices through web browser
- Controller communication setting and parameter setting
- Controller event log query
- Add, delete, and modify user data
- Remotely unlock door
- Manually and directly set access controller's time
- HTTP Server is compatible for SOYAL Enterprise Series and other series that is listen on separate manual such as SOYAL Industry Series (TCP), AR-716-E18 Ethernet module AR-727i-V3 and Converter AR-727-CM (refer to 'Operation Manual AR-727-CM HTTP Server')

HTTP Server Comparison Table

	Interface Menu	Enterprise Series	Industry Series (TCP) AR-727-CM-0804M AR-401-IO-0808R-U2	AR-727i-V3 (AR-716-E18 Ethernet module)	Converter AR-727-CM
1	Current State	V	V	V	V
2	Network Setting	V	V	V	V
3	**Controller Setting:** Event Log / User List / Controller Parameter / User Add/ Change / Timezone / Clock	V			
4	Login Password	V	V	V	V
5	**RS485 Setting:** Channel 1 Setting / Channel 2 Setting		V		V
6	**I/O Control Setting:** Direct Control IO 0~3 / Direct Control IO 4~7		V		

1-2 / Architecture Schematic Diagrams

PC

HUB

Enterprise Series
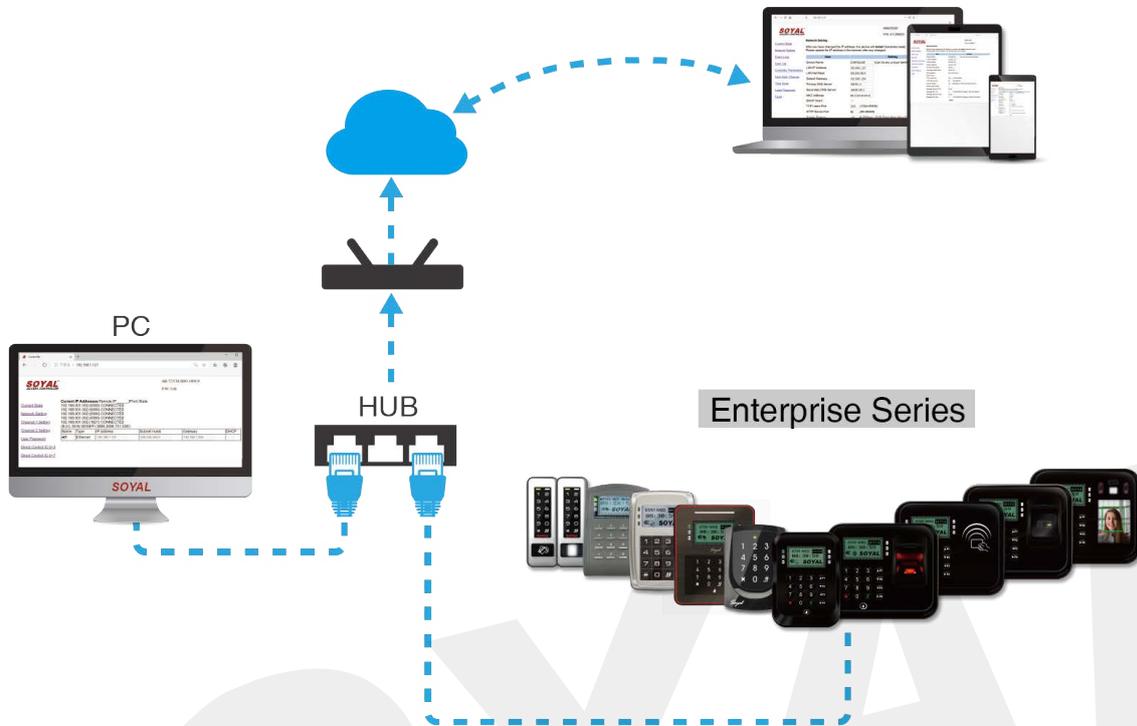
2. Interface Overview

2-1 / Log in HTTP Server page

2. Interface Overview

❶ Through PC, Tablet, or Smartphone web browser software/app, enter device IP Address and enter HTTP Server interface (default IP Address 192.168.1.127)

❷ When entering HTTP Server page required to enter ID and Password. Default ID: SuperAdm / Password: 721568 which can also be found on serial no. sticker that include on the packaging.
(For older version, default ID: admin / password: admin)

❸ Device Model no. and Firmware Version
After logged in, on the top right side will show the controller's model no. including the firmware version

2-2 / Device Connection Status

❶ After logged in, the first menu that will automatically show Current State of controller's IP Address

2-3 / Network Setting

❶ Click 'Network Setting' on the left side menu

❷ **Device Name :** Rename network device, could be used to differentiate between one device and another

❸ **LAN IP Address :** Enter IP address designated for the device of the intranet. Default setting is 192.168.1.127

❹ **LAN Net Mask :** Subnet Mask of the intranet

❺ **Default Gateway :** Default gateway of the intranet. if there is Internet connection access, this IP address must point to the router or the gateway provided by the ISP

❻ **Primary DNS Server :** Domain Name Server 1

❼ **Secondary DNS Server :** Domain Name Server 2

8 MAC Address : Network physical address (this field cannot be changed). Each TCP/IP device has designated MAC address that could be found on the serial number sticker

AR-727-E
EHR05276005 → Product serial number
13.57.043A7B → MAC Address
ID:SuperAdm
PWD:721568
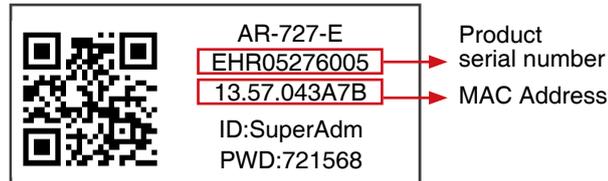
9 DHCP Client : Ticking this feature will enable dynamic host protocol which means devices will automatically obtain IP address without manually typing and assigned device to a designated IP address. Enabling this feature is not recommended in case Client could not communicate with Server and it will cause a disconnection.

10 TCP Listen Port : Communication control port, connection to 701 Software enter 1621, connection to Mobile APP enter 1601.

11 HTTP Server Port : Web browser service port, it can be change if there is information security consideration but should not have the same TCP Port with 701Server connection to devices which is 1621 For Example: changing into 9680, to enter the HTTP Server you need to enter IP address followed with Port.

Q 192.168.1.127:9680

SOYAL
ACCESS CONTROLLER

AR837E/EF
F/W: 4.3 191023

12 Socket Timeout : Handshake timeout detection, default value 120seconds, if there is no data will be offline.

13 Node ID (Device ID) : Controller's node ID, node ID setting in HTTP Server must correspond to 701 Software otherwise data could not be transmitted.Step no. 14-16 is designated for third party system integration to choose between one way hosting and two way hosting of Event Logs. If there is no requirement for this, please enter Message Server IP as 0.0.0.0 and Message Port as 0 for both 1st and 2nd Reference document:

Active Push Communication free acknowledgement (8031)

A simply integration of retrieving transaction log from access controller and send it to the HOST. It is mostly used in NVR/DVR system for integration with CCTV surveillance camera, by showing the transaction log data for OSD (On Screen Display). SOYAL provides total two ports in total to work as a redundant port to keep system running when one of the ports fails.

Operation Mode:

HOST
(THIRD PARTY SYSTEM)

AUTO SEND
TRANSACTION LOG

SOYAL
Enterprise Series Controller /
Serial-to-Ethernet Server
with I/O Module

Host

Message port: 8031

Technical Document

Reader

Have log?

YES → Send log (text form) → Get log (text form) — **Host**

NO → Send keep alive → Get
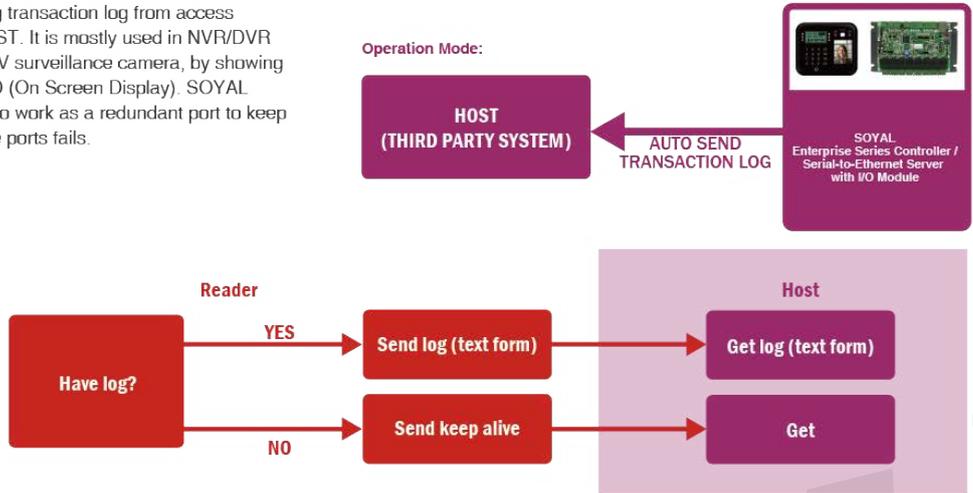
Active Push Communication required acknowledgement (8033)

Same method and function with one way hosting except two way hosting offer safest way when receiving data from SOYAL access controller. it required acknowledgement from HOST (third party) when transferring data to make sure there is no missing log, data, or message transferred.

Operation Mode:

HOST
(THIRD PARTY SYSTEM)

AUTO SEND
TRANSACTION LOG

SOYAL
Enterprise Series Controller /
Serial-to-Ethernet Server
with I/O Module

Host

Message port: 8033

Technical Document

Reader

Have log?

YES → Send log (hex form) → Send Accept / Deny — **Host**

NO → Send keep alive → Get

Delete the oldest log command 0x37 → ACK — **Reader**
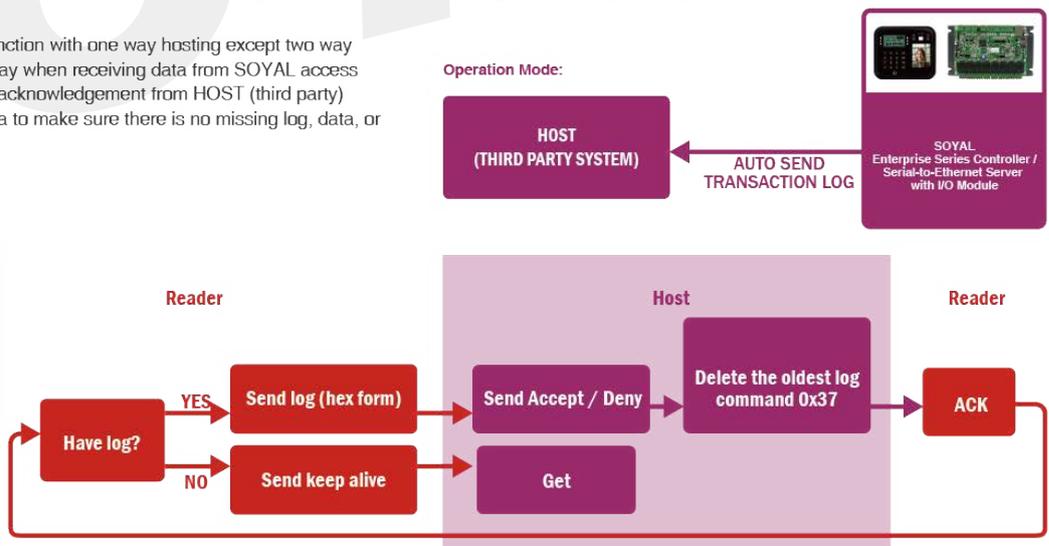
*Delete the oldest log command 0x37:
When the third-party system receives LOG, it will send 37H command to confirm that the message has been well received and delete the LOG message stored in the card reader that has been obtained

2. Interface Overview

14 Message Server IP 1st : Transfer event log to one of the Server's first IP address , active sending event logs to the designated server

15 Message Port 1st : Automatically send last event message port.

We offer two options:

8031 --> one way hosting, event log format is TEXT mode

8033 --> two way hosting, required acknowledgement in order to send the next event log, event format is HEX mode

16 Message Server IP 2nd : Transfer event log to one of the Server's second IP address, active sending event logs to the designated server

17 Message Port 2nd : Automatically send last event message port.

We offer two options:

8031 --> one way hosting, event log format is TEXT mode

8033 --> two way hosting, required acknowledgement in order to send the next event log, event format is HEX mode

18 Update : Press Update button to save changed.

2-4 / Event Log

1 Click 'Event Log' on the left side menu to query and monitor daily transaction record of access controller in the system

2 Selection page of records list
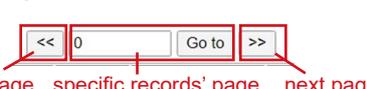
Previous page   specific records' page   next page

3 Total records stored on the controller's memory

4 Index: Events in sequence

5 YY'MM/DD: Event log date recorded in year/month/day format

6 Time: Event log time recorded in hours/minutes/seconds

7 Address: User Address

8 Display (Alias): User Address's display name or alias on LCD access controller

9 Access Detail: Message code with description

10 Card UID: Card number

11 Door: Door name of the access

12 When query Event Logs, click 'Refresh' button in order for browser to show latest event logs recorded.

2-5／ User Lists

① Click the 'User List' on the left side menu to query all user data stored on the controller

② Start From: show the first user address range from the search Example start from 199 then press 'Enter' it will show user list from user address 199, 200, … 213 (one page shows maximum 14 user address)

<< : previous page   /   >> : next page

③ Address: User address in sequence

④ Display (Alias): User Address's display name or alias on LCD access controller
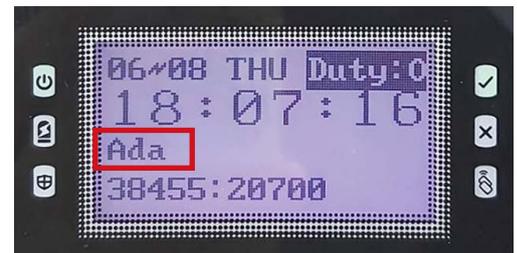
⑤ Access Mode: Assigned access mode for each user will be displayed as Invalid/ Card Only/Card or PIN/Card and PIN

⑥ Card UID: Card number

Note: Enterprise Series Controller could control both controller and Wiegand access reader connected to it. That way, below step will provide the display of controller (main controller/master controller) and reader (slave reader).

2. Interface Overview

7 Ma : Main in short is a setup for Main Controller's access.

　　　(Y=access permitted / N=access prohibited)

8 Zone: Main controller's access time zone

　　　(refer to 2-8 for more detail regarding time zone setting)

9 WG: setup for Slave Reader's access

10 Zone: Slave Reader's access timezone

11 Expiry: Date limit of user access

2-6 / Controller Parameters

1 Click 'Controller Parameters' on the left side menu to query and monitor daily transaction record of access controller in the system

2 Door Number(1~255) :

You can set door number for Main Controller and Slave Reader. This is usually required a setting when you established door group setting and implement anti-passback on your system where the exit and entrance is required to present access.

3 Master Code (6 Digital) :

Master code or programming code is a six digits code that is used to access programming mode (default value 123456)

4 Four digits arming code, enter arming code to enable arming mode

5 Door Relay Time (0~600,601~609 for 0.1~0.9 Sec) :

After the access identification is accepted (normal access), relay is triggered to release door. Door Relay Time indicated how long does it takes for relay to be opened.

- Output continuously (latch mode) enter 0
- Lock release after a specific time (pulse mode)
  601~609 = 0.1~0.9 sec
  1~600 = 1~600seconds

  ※Suggestion: 15 seconds for magnetic lock and electric bolt lock; 0.2 seconds for electric strike and cabinet lock.

  Set door relay time is available for both Main Controller and Slave Reader

6 Alarm Relay Time (0~600 Sec) :

Alarm output time until it stopped triggering.

- Output continuously enter 0 (alarm keep triggering until next actions for example close door, press push button, or swipe valid card)
- Alarm stop triggering after specific time 1~600 = 1~600 seconds

7 Door Close Delay (Sec) :

Door will be locked after specific time. If time is reached and door is not closed, will trigger alarm as door open too long (under arming mode).
Door close delay range 1~600 = 1~600 seconds
Set door close delay is available for both Main Controller and Slave Reader

8 Force Alarm :

Enabling this function will trigger alarm under force open situation

9 Serial Port (RS485-I) :

RS485 communication setting options: Lift Controller, Controller/PC, Display Panel, Printer.

(Default value: Controller/PC)

Controller/PC ⌄
LIFT Controller
Controller/PC
Display Panel
Printer
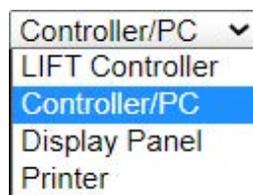
10 PIN Access :

Access identification via PIN can choose between two options:

M4: User Address(5) + PIN Code(4)

M8 mode: PIN Code(4) Only

For example:

User Address 250 with PIN 4879

Under M4 mode: enter 00250 4879

Under M8 Mode: enter 4879

2. Interface Overview

11 Door Status : Show the current status of the Main Controller

12 Open Door (Main/WG) :

Remotely open or close door of Main Controller and Slave Reader

Options to choose: Pulse (Auto Close), Latch (Always Open), Close

After done selecting the options, click 'Active'

13 Update : Press Update button to save changed.

2-7 / User Add / Change

1 Click 'User Add / Change' on the left side menu to add, delete, or modify user data

2 User Address :

To start modifying user data, enter designated user address and click 'Go to'

Previous page   specific records' page   next page

③ Display (Alias) :

User Address's display name or alias on LCD access controller

④ Access Mode :

Assigned access mode for each user will be displayed as Invalid/Card Only/Card or PIN/Card and PIN

⑤ Guard User :

Tick the box if designated user is a Guard User. Access with Guard identification will not release lock but will be recorded on the event log.

⑥ PIN Code :

Four digit access PIN, can be modified from 4~8 digits refer to command 42* for keypad access controller and menu (3) Parameters (1) > (9) PIN & UID format > User PIN length range

Step **⑦** **⑧** is card UID setting :

⑦ Card UID (__:xx)WG32(5:5) / u64(7~10:8) :

Site code, first 5 digit UID WG5:5 or HEX 4~7/64Bit

⑧ Card UID (xx:__)WG32(5:5) / u64(7~10:8) :

Card Code, last 5 digit UID WG5:5 or HEX 0~3/64Bit

Step **⑨** **⑩** **⑪** **⑫** is Time Zone setting to set user access on specific time zone for Main Controller and Slave Reader. Time Zone settings please refer to 2-8.

2. Interface Overview

9 Main Door Access :

Enabling access time zone for Main Controller

10 Time Zone :

Set access time zone for Main Controller, 0=free zone or set between 1-62 if access time zone is set on manual part 2-8

11 WG Door Access : Enabling access time zone for Slave Reader

12 Time Zone :

Set access time zone for Slave Reader, 0=free zone or set between 1-62 if access time zone is set on manual part 2-8

13 User Level(0~3) :

User access level options between 0~3. User Level must be correspond to Time Zone Level and Door Group Level to confirm access identification required by user.

The reason is that we use Level Comparison Function to realize;

In "Card and PIN" Access Mode, the User Card can access the door with Card Only if its level is higher than both Time Zone Level and Door Group Level; the User Card can access the door with Card and PIN if its level is equal to both Time Zone Level and Door Group Level; can't access the door if its level is lower than Time Zone Level or Door Group Level.

Level Comparison Rule Chart

User Level	Time Zone Level	Door Group Level	Access Mode
1	0	0	Card Only
1	1	0	Card and PIN
1	0	1	Card and PIN
1	1	1	Card and PIN
1	0	2	Cannot access
1	2	0	Cannot access

Level Comparison Chart for the example

User Level	Time Zone Level	Door Group Level	Access Mode
02	00< User level 02	Group 001: level 01 < User level 02	Card Only
02	00< User level 02	Group 002: level 02 = User level 02	Card+ Pin+#

Step ⑭ ⑮ ⑯ is Date Limit setting to allow access only in between start day and expiry day.

⑭ Access Date Limit : Allowing user access in between date limit by ticking the box

⑮ Start Day (YY-MM-DD) : User starting date to have access

⑯ Expiry Day (YY-MM-DD) : User last date to have access

⑰ Update : Press Update button to save changed.

2-8／ Time Zone

① Click 'Time Zone' on the left side menu to set time zone in a week.

② Level :

Time zone level differentiate between 0~3, User with higher level index number is allowed to access those time zones or door groups with lower level index numbers. (3 is the highest authority)

③ Link to :

Setting a set of time zone that could link to other time zone for compound setting. 0=free access, 64=END (no linking to other timezone)

④ Holiday :

Access time zone setting is for daily basis, if required to activate particular time zone on holiday edit, please tick the box. Holiday edit can be set on 701Client software.

2. Interface Overview

Step ❺ ❻ ❼ ❽ ❾ is a setup for Time Zone in a weekday (Sun-Sat)

Note: setting time zone control period must be in 00:00~23:59 format.

Conditions:

- If there is a gap in between, please separate the time zone into two different zone.
- If it time zone setting exceed midnight, please separate the time zone into two different zone (refer to example of zone 3 & zone 4).

Example of correct setting:

Weekday	Zone 1 (open for public time)		Zone 2	Zone 3	Zone 4
SUN	08:00-12:00		13:00-17:00	00:00-00:00	00:00-00:00
MON	08:00-12:00		13:00-17:00	22:00-23:59	00:00-07:00
TUE	08:00-12:00		13:00-17:00	22:00-23:59	00:00-07:00
WED	08:00-12:00		13:00-17:00	22:00-23:59	00:00-07:00
THU	08:00-12:00	12:00-13:00 access is prohibited, does not required to create zone (gap)	13:00-17:00	22:00-23:59	00:00-07:00
FRI	08:00-12:00		13:00-17:00	22:00-23:59	00:00-07:00
SAT	08:00-12:00		13:00-17:00	00:00-00:00	00:00-00:00
Holiday	V (allow)				
Link	End		Zone 1 (incl. access to Zone 2+ Zone 1)	Zone 2 (incl. access to Zone 3 + Zone 2 + Zone 1)	Zone 3 (incl. access to Zone 4 + Zone 3+ Zone 2 + Zone 1)

❺ Weekday : Weekday options

❻ Hour : Starting Hour

❼ Minute : Starting Minute

❽ Hour : Ending Hour

❾ Minute : Ending Minute

❿ Update : Press Update button to save changed.

2-9 / Change Login Password

1 Select 'User Password'

2 New Password : Enter new password (there's capital letter differentiation)

3 Password Again : Retype the new password

4 Update : Press Update button to save changed.

2-10 / Clock Setting

1 Click 'Clock' on the left side menu to manually change clock of the controller

2 Year : 2 digit, example: 2021 enter 21

3 Month : 2 digit

4 Day: 2 digit

5 Hour : 2 digit, 24H format

6 Min : 2 digit

7 Second : 2 digit

8 Press Update button to save changed.

3. Reference

3-1 ／ FAQ

- Why IP readers show offline, but you can enter to its webpage settings?

- How to change IP Address for LCD Screen of EV5 Series Controller?

- Why IP readers always show online/offline alternately and not all transaction log can be received timely?

3-2 ／ YouTube Videos

- 《SOYAL APP & WEB》E Series Controller Http Browser Steps