

Quick User Guide



Optiview Access Control System



The Quick Guide is not intended to provide a full knowledge and training to installers at the job site. Installers are still assumed to have a good understanding and preferably a hands-on experience prior to installing an access control system and its peripheral devices associated to the main controller.

I. Installation and Wiring of Access Control Hardware

1. Installing Main Controller Device

You can install the controller device either:

- a. On a wall with a screw
- b. On a wall with DIN rail (for models CAS-2SC, CAS-4SC and CAS-4SAM).





Slave or Standalone Controller installed on a fixed wall

Please ensure that device mounting surface will able to hold 3 times as much as the total weight of the device, bracket and accessories. Measure each holes distance and position according at the back of the metal case of the device; drill holes in the wall according to the measured hole positions of the case. Embed expansion nuts and fix screws into the wall. Hang the device onto the screws and secure the case using all the four screws.



- 2. Wiring the Main Access Control Device
 - a. Access Control Schematic Diagram



Connect peripheral devices such as sub-controller (slave access controllers), card reader, and door lock control CAN Bus connection, Ethernet cable etc...

Note:

- Never plug/unplug wire when the power is ON.
- Make sure 120 AC wall outlet is actually grounded.
- Always refer to manual and schematic diagram when wiring peripheral devices.

1.1 Connecting Master Controller with Slave Controller

Access master controller and slave controllers can be interconnected using CAN (Controller Area Network) bus, as shown in Figure 2-4 below. Please refer to Table 2-1 for descriptions about wiring terminals, and refer to Table 2-2 for communication distance. Speed is set with dip switch. Please refer to -2.4 DIP Switch for details.





Table 2-1

Interface	Wiring Terminal	Description
CAN Bus	CANH	CAN Bus Communication
	CANL	

Table 2-2

Speed	Distance
50 kb/s	1968 feet
80 kb/s	1312 feet
100 kb/s	1312 feet
125 kb/s	656 feet

Interconnecting Master Controller and Slave Controller via CAN Bus



CAS-4SC 4-door Slave Controller



1.2 Basic Schematic Diagram to Interconnect Master Controller and Peripheral Devices

Every job environment, new or pre-existing switches and equipment including customer requirement is unique. This wiring quide is intended as a general instruction only. It may or may not be totally applicable to your own job application or installation. Refer to your equipment (request to exit buttons, Alarm input/output devices etc..) for proper wiring and pre-existing conditions of such which may be NC (normally close) or NO (normally open).



Connecting Card Reader or Keypad Using CAT6 Cable

Using CAT6 may always be good to use with access control. It is best to use at least 18-AWG cable or Access Control riser Note: (cable) when installing an Access Control System.

485 Reader



1.3 Wiring of External Alarm Input

Supports 8-channel external alarm input as shown below:



Interface	Wiring Terminal		Description
	ALM1 Alarm input port 1		
	GND	Alarm input port 1 and 2	
	ALM2	Alarm input port 2	
	ALM3	Alarm input port 3	
External	GND	Alarm input port 3 and 4	External alarm input ports connect smoke
Alarm	ALM4	Alarm input port 4	detector and IR detector etc
Input	ALM5	Alarm input port 5	
	GND	Alarm input port 5 and 6	
	ALM6	Alarm input port 6	
	ALM7	Alarm input port 7	
	GND	Alarm input port 7 and 8	
	ALM8	Alarm input port 8	

1.4 Wiring of External Alarm Output



Interface	Wiring Terminal	Description
External Alarm	OUT1+	External alarm output ports connect audible and visual siren
Output	OUT1-	etc

1.5 DIP Switch

Operate with DIP switch.											
			F	igure	2-12	2					
	0	N					[P			
	1	2	3	4	5	6	7	8			
● Uthe switch is at ON p	ositio	n, me	eanin	g 1.							
• The switch is at the b	ottom	, mea	aning	0.							
 1~8 are all 0; the syst 1~8 are all 1; the syst 1, 3, 5 and 7 are 1, whi 	em is em er ile oth	start nters ners a	ed no BOO are 0.	ormal T mo Afte	lly. ode a r rest	fter s art, t	tart. he sy	/stem i	restore	s facto	ory de

efaults. • 2, 4, 6 and 8 are 1, while others are 0. After restart, the system restores factory defaults,



Remote Management of Access Control System

Network configuration and programming outline:

- Remote management of Access Control via Optiview VMS or Internet browser. a.
- b. Network configuration of the Access Control
- Configuration of User account information c.
- d. Configuration of User rights
- e. Create and assign Access Level
- f. Create and assign time zone assignments.
- Integrate Access Control events to video cameras g.

1. Optiview VMS (An Integrated Video and Access Control Management Software)

1a. Initialize Access Control device



With Access Control integration

The default IP address:

- ٠ Main access controller is 192.168.1.109 (username: admin default password: 123456)
- Stand Alone series controller is 192.168.0.2 (username: admin default password: 123456). • Note that stand-alone access controllers do not have web page login. They can only be configured using Optiview VMS.

To restore factory default, go to page 6 "DIP Switch" and follow the settings of PINs as shown.

If you are setting the Master Access Control for the first time, you will need to "Initialize" the controller, which means you need to setup the following:

a. Using the "admin" as the username on the Web page login screen (if using a master controller) and set the "admin" password. You may combine upper case and lower-case letters, numbers and special characters.

🧲 🔿 👿 htt	p://192.168.1.109/	- 0	Search	▶ ☆☆☺
WEB SERVICE	× 📑			
File Edit View	Favorites Tools Help			
\$				**
				<u>^</u>
	Device Initialization			
	Username	admin		
	New Password	•••••		
		High		
	Password shall be at least 8	digits, and shall at least include two typ	es, including number,	
		letter and common character		
	Confirm Password	•••••		
	Pind Email			
	L) bild Effai			
		(It will be used to reset password. Pl	ease fill in or complete it timely	9
		Next		
			_	~

b. Configure the network address information based on your job site environment.

Access Maste	Access Master Controller					System Setup	Information	Lopout
					of the second se	eyen in beidp	and a state of the	and har
Vetwork Setting								
> TCPMP	Default Ethernet Card	Ethernet Card 1						
> Port	Ethomol Card	56 J. O. H. H						
> DDNS	Calefret Card	Ethernet Card 1 V						
> Register	MAC Address	14 . a7 . 8b . 42 . b7 . 00						
	Mode	 Static O DHCP 						
	IP Address	192 . 168 . 1 . 109						
Safety Mgmt.	Subnet Mask	255 , 255 , 0 , 0						
Date Setting	Default Gateway	192 , 168 , 1 , 1						
▶ User Mgmt.	Preferred DNS Server	8.8.8.8						
► Maintenance	Alternate DNS Server	8 , 8 , 4 , 4						
Config Mgmt.								
▶ Default		OK Refres	h Default					
► Upgrade								

1b. Install Optiview VMS

Install the Optiview VMS on your computer. Please refer to Optiview VMS manual on how to go through the process of installing the software on a Windows or MAC-based computer. You can download the software at: https://optiviewusa.com/product/optiview-vms-2018/



1c. Programming Stages to Configure Access Controller

- a. Device network setting: Date/time, TCP/IP, ports, P2P (if applicable), subnet mask and DNS (See Step# 1c.a below)
- b. Time Schedule Management (See Step# 1c.b at Page 9)
 - Create preferred time schedule (Time zone) time to open or close schedule period
- c. User Accounts Setup (See Step 1c.c at Page 10)
 - Create department or company name
 - Set the card type to be use by the system when reading cards: Decimal (10) or Hexadecimal (16)
 - Create Access Level
 - Create User accounts
 - Assign Department Name
- d. Customize Access Level. Create multiple Access Level to where certain employees are restricted to access doors on specific day and time.

Follow the detailed sequence of steps below:

1c.a Configure Device Network Settings

• Using Internet Explorer, log in to the Access Control Web login screen, then got o System Setup \rightarrow Network Settings.

Access Master Controller		Access Maste	r Controller			
Network Setting Note Note	Ethernet Card 1 V Ethernet Card 1 V 14 a7 8b 22 b7 00 State 0 HCP 192 168 1 109 255 255 0 0 192 168 1 109 256 285 0 0 192 168 1 109 265 285 0 0 192 168 1 109 264 8 8 8 8 8 8 8 8 8 8 8 0K Reltesh Detault	V Network Setting TCP/IP Put DDNS Register P2P Safety Mgmt. Date Setting User Mgmt.	Max Connection TCP Port UDP Port HTTP Port HTTPS Port	20 37777 37778 80 443 OK	(1~999) (1025-65) (1025-65) (1~65535) (1~65535) Relitesh	535) 535) C Enable Default

• Using Optiview VMS, set IP address.





• Set the Date and Time of the Access Controller

→ Modify Date/Time Using Internet Explorer

Access Maste	r Controller Access 0	control System Se	tup
 Network Setting TCP/IP Pot DDNS Register P2P HTTPS Safety Mgmt. Date Setting User Mgmt. Maintenance Config Mgmt. Default Upgrade 	Date Format Year Month Day Y Time Format 24-Hour system Y Date Separator Y System Time 2019 10 15 12 27 45 Sync with PC Date Setting Date Week Starting Time 2019 01 00 00 Ending Time 2019 01 00 00 00 00 00 00 10 Manual Update Port 123 (1 ~65535) Update Cycle 10 Min. (0 ~65535) Update Cycle OK Refresh Default Default <th></th> <th></th>		
 > DDNS > Register > P2P > HTTPS > Safety Mgmt. > Dats Setting > User Mgmt. > Maintenance > Config Mgmt. > Default > Upgrade 	Time Format 24-Hour system Date Separator		

→ Modify Date/Time Using Optiview VMS

	New A	Access Device CF	G +		(●●● ± ☆
Search Q	IP:	Device Model	l: Softwa	are version:	SN:	Up
▼ ♣ Default Group	192.168.1.109	ASC2204C-H	1.000.	0000.0.R	4A049C6PAZF7C56	
🗳 192.168.1.109-test			Build:2	2017-10-26		
Step 1	Network					
	ТСРЛР					
	Svstem		General 192.168.1.109-te	est		
Step 2	General	Account	Time Setup			
			TimeZone	GMT+08:00 -		
(,	Step Set d	3 ate/time	System Time	10-15-2019	12:40:27	Sync PC

1c.b <u>Time Schedule (Time Zone) Setup</u> The selected green bar specifies ON (allowed) and vice versa.





1c.c User Accounts Setup

1c.c1. Create Department or Company Name



1c.c2. Set Card Type

Set the card type to be use by the system when reading cards: Decimal (10) or Hexadecimal (16).



1c.c3. Create "Access Level"

Access Level is comprised of three setup process: creating door groups, assigning Time Zone (time schedule) and assigning door groups to user accounts.

Creating Door group.

Select doors for the Door Group. It may be from a single or multiple access controllers.





- → Click "ADD" to create a new group of doors. These doors can come from a single or multiple access controllers.
- ➔ Add name to Door Group
- → Assign "Time Zone" (time schedule) to the Door Group.
- → Select Doors to be included for the group.
- ➔ Click OK when done.
- Create User Accounts.

In User Management Interface as shown above,, click 🕮 to manually add user information.



Mandatory information must be filled up: User ID Name Department

Miscellaneous information can be manually enter, such as: Card No.: input card information by using card reader or manually typed in. Unlock password: used to unlock when password method is in use. Card password: used for card+password unlock Validity: default is 10 years

-	Ado	d User	×
Basic Info Fi	ngerprint Info Details		
User ID			
Name			
Department	: Default Department		
Card No.:		Card issuer 🔹	
Card Type	General Card		
Card Password			
Unlock Password		Image Size:0 ~ 120KB Upload Picture	
Number of Use			
Valid Time	: 2017/5/23 0:00:00	- 2027/5/23 23:59:59 - 3653	Days
Make sure reader	and card are in agreement.		
		Continue to Add Finish Car	ncel
Neter Cand Ne		ant ha dualizata	

Note: Card No. and User ID cannot be duplicate.

• Assigning User accounts to Access Level (sometimes called Door group)



a. Go back to "Access Level" menu



 Select user accounts to be assigned and permitted to access the Door group. User accounts may come from a single or multiple department/company. All User accounts selected will have an access to all the doors listed on Door Group.

	Ó	OPTIVIEW	Live View(1)	Access	+				•••• •	. 0 m –	0 X
	R.	Name:		TimeZone:	Ν	•	Search				
	Ē	Add Deb	te -								
Chest 1		Timecone				User Select					×
~		Holiday	All Day	02	÷ ŧ	Name:		Deers Group1			
	Click 2	Access Level		- 4		User List				1 d	£.
		First Card Unlock		L.							
		Multi-card Unlock Anti-passback Inter-door Lock Remote Ventification		Add User Accounts to Door Group	er Accounts r Group						
						Setault D	epartment%	Company1 -	User ID/N	arria Q	
						Add us of regi	er accou	tep 2 unts from the po user account list	Default De		

First Card Unlock – The reader will change to unlock mode when the first card is scanned.

Multi-card Unlock – a specific door can be unlocked <u>only</u> when specific users of a group all passed verification.

Anti-passback - The main purpose of an anti-pass back system is to prevent a card holder from passing their card to a second person to gain entry into the same controlled area.

InterDoor Lock – When one door is unlocked, other doors will be locked. If you want to unlock one door (under normal status), all of the other doors will be locked, otherwise you cannot unlock this door.

Remote verification - When a user scans the card, the admin will decide whether to unlock a door or not.

1c.d. Customized Restrictions to Access a Single or Multiple Doors

Create multiple Access Level to where certain employees are restricted to access doors on specific day and time. The steps cited below is based on the following assumptions: a single door, three work shifts and top management 24/7 access. This task is comprised of the following steps:

1c.d1 Create three different Time zone (Time Schedule). See Step# 1c.b on page 9 for other details to set up one.



Ż) op	riview	Devices	Access	New	Live View(3) Live View(2)	Live View(1)	Intercom	Device CFG	+		• 0	±\$%
R	A	dd Delete												
Ŀ				Timezone Det	ails									
		Open Door 9am-5pr	n 🖉 🗊											
			Ø Û		Name	Open Door	9am-5pm							
<u> </u>			Ø 🗊											
				Sun	0 1 	2 3	4 5 6 	7 8 9	10 11	12 13 14	15 16	17 18 19 	20 21 23	2 23 24
				Mon										*
				Tue										
				Wed										
				Thu										*
				Sat							mmum			#

1c.d2 Create three different Access Level (See step# 1c.c3 on page 10)

Ś) op	TIVIEW	Devices	Access	New
P.		Name:		TimeZone: All	
Ŀ		Add De	lete		
2			Timezone	Operation	
R		Staff Door1	Open Door 9am	Ø 2+ Ū	
		Door1 Mgmt	All Day	Ø Å Ū	
		Night Shift	Night Shift 7PM	Ø 2+ Ū	

1c.d3 Assign User Accounts (or Access Cards) to Access Level. See page 12

		Devices	Access								
R	Name:			TimeZone: All 💌 Search							
Ŀ	Add Delete										
2				Door G							
		Staff Door1	Open Door 9am	Ø & Ū	Name: Staff Door1 User Select ×						
		Door1 Mgmt	All Day	Ø & Ū 🚽							
		Night Shift	Night Shift 7PM	Ø 2+ Ū	Name:						
					User	List			Ū -I		
						User ID					
							Tester1 6013	Default Depart	Ū		