Quick User Guide

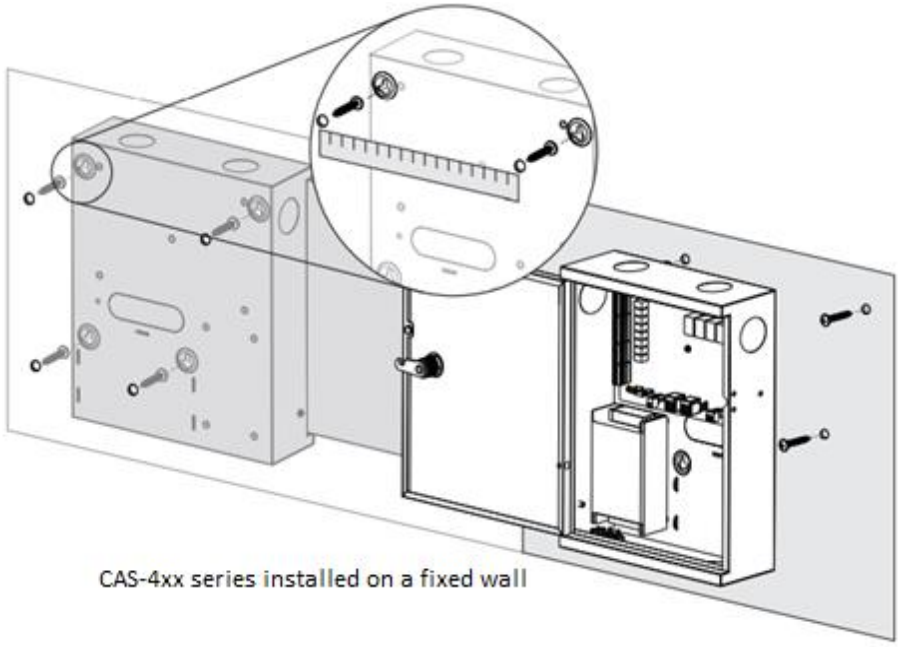
Optiview Access Control System

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

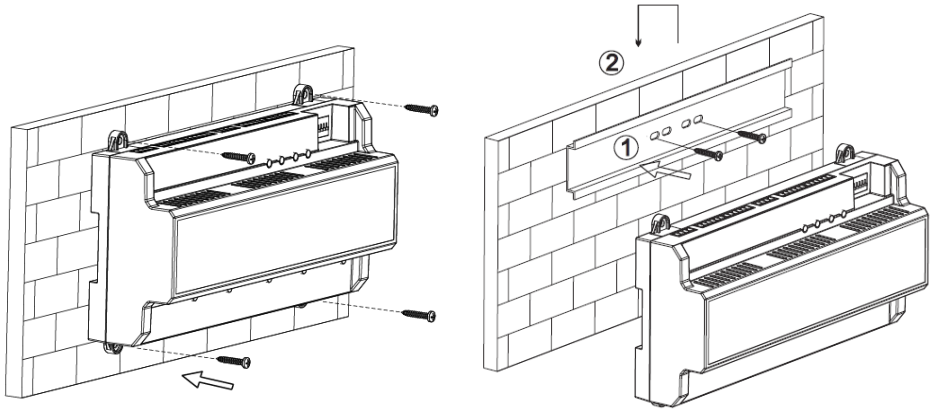
The Quick Guide is not intended to provide a full knowledge and training to installers at the job site. Installers are still assumed to have a good understanding and preferably a hands-on experience prior to installing an access control system and its peripheral devices associated to the main controller.

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).



CAS-4xx series installed on a fixed wall



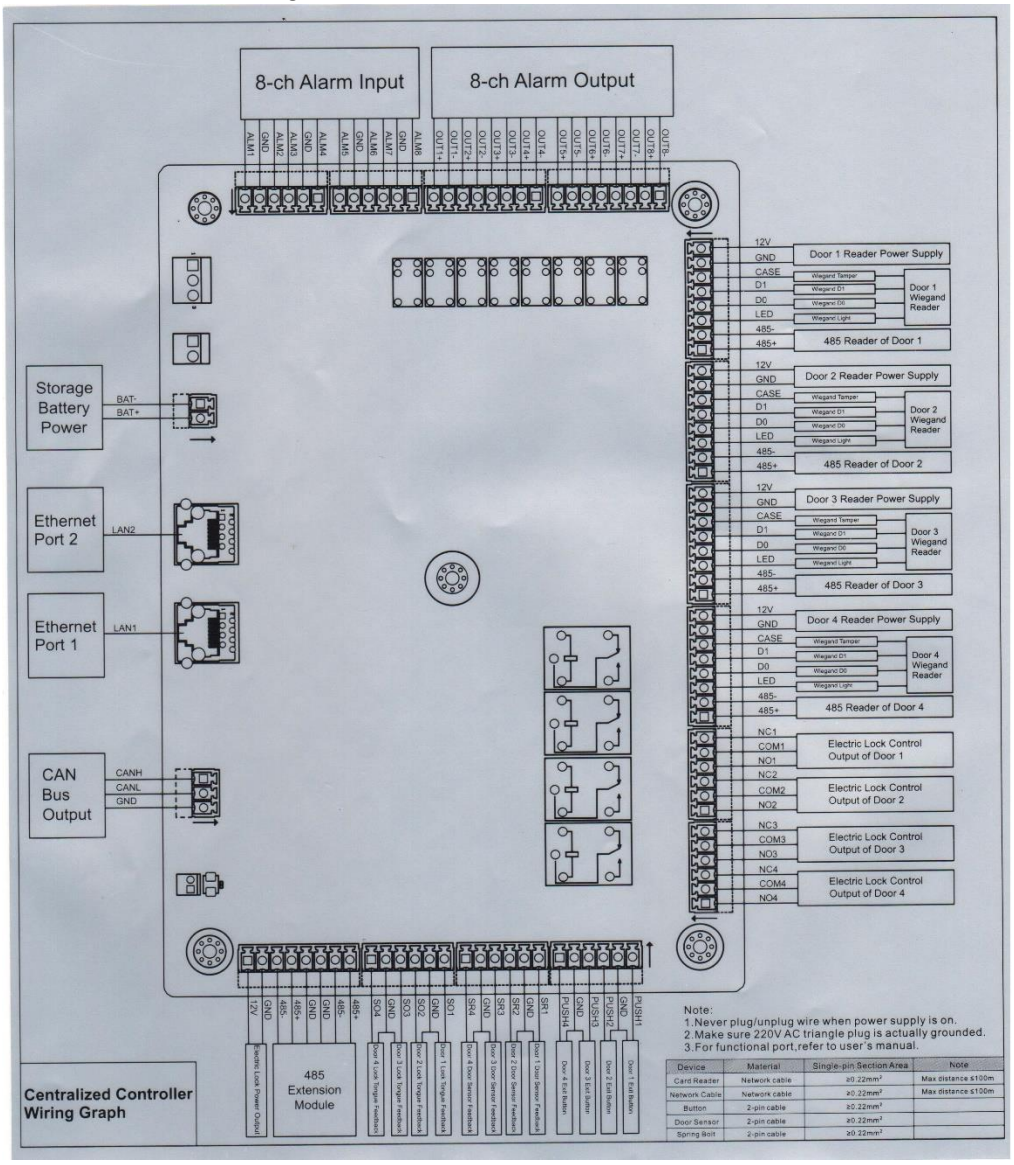
Fixed Wall Using DIN Rail

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.

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

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.

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

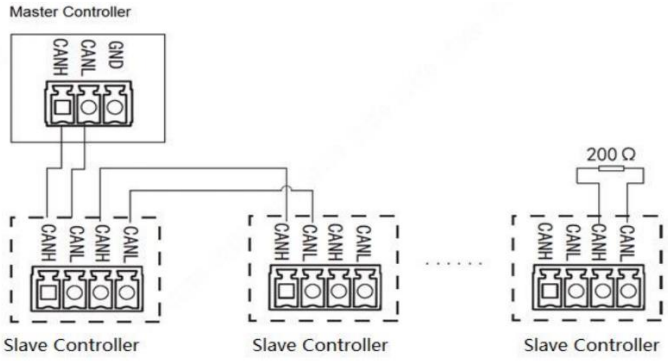


Figure 2-4

Table 2-1

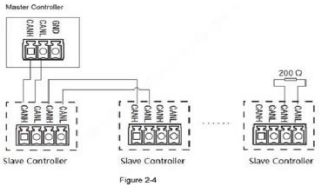
Interface	Wiring Terminal	Description
CAN Bus	CANH	CAN Bus Communication
	CANL	

Table 2-2

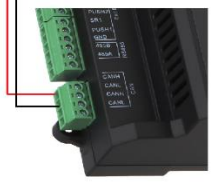
Speed	Distance
50 kb/s	1968 feet
80 kb/s	1312 feet
100 kb/s	1312 feet
125 kb/s	656 feet

Interconnecting Master Controller and Slave Controller via CAN Bus

Model#CAS-4MC 4-door Main Access Controller



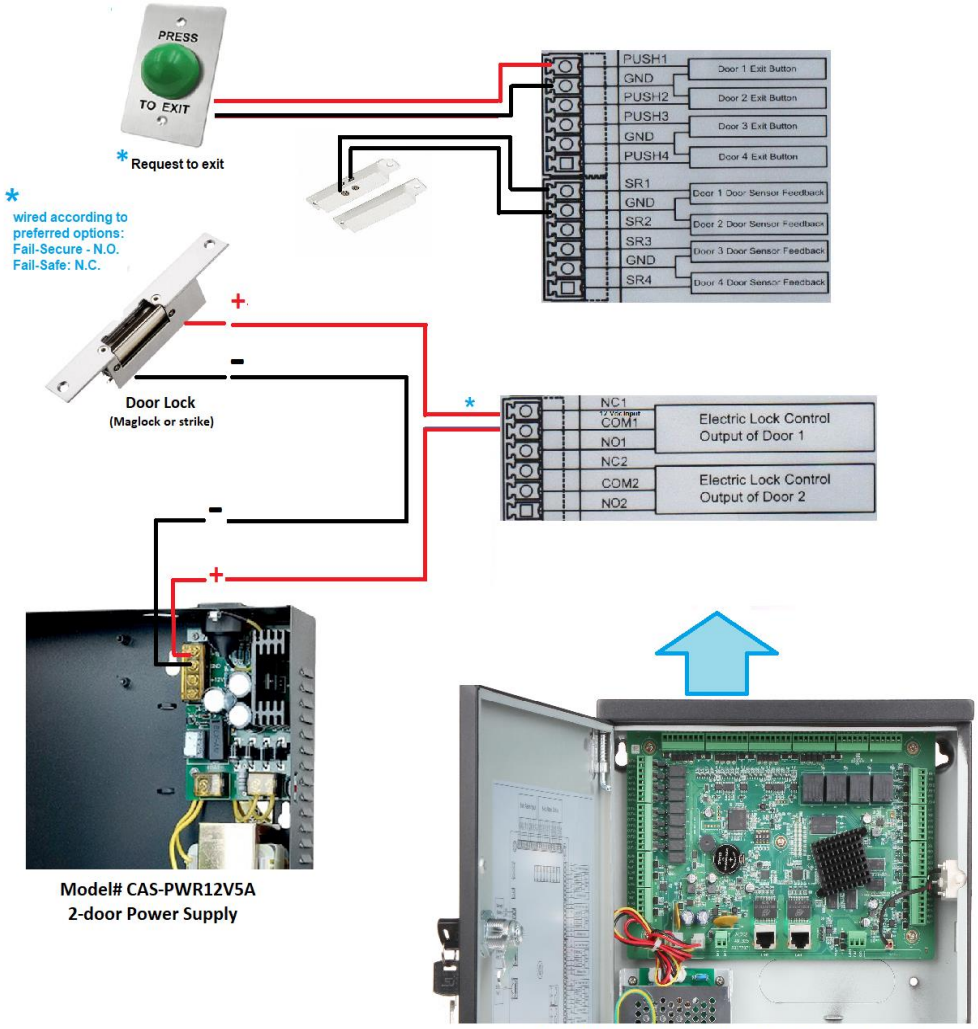
CAS-4SC 4-door Slave Controller



Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

1.2 Basic Schematic Diagram to Interconnect Master Controller and Peripheral Devices

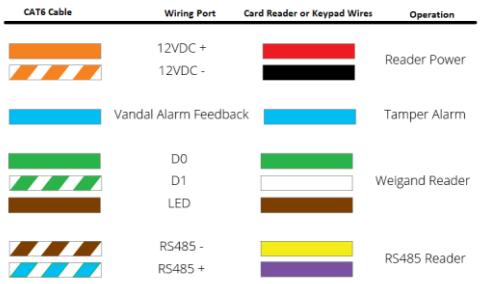
Every job environment, new or pre-existing switches and equipment including customer requirement is unique. This wiring guide is intended as a general instruction only. It may or may not be totally applicable to your own job application or installation. Refer to your equipment (request to exit buttons,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



Model# CAS-PWR12V5A
2-door Power Supply

Model#CAS-4MC 4-door Main Access Controller

Reader Type	Connection Mode	Length
485 Reader	CAT5e cable, 485	325 ft.
Wiegand Reader	CAT5e cable, Weigand	325 ft.



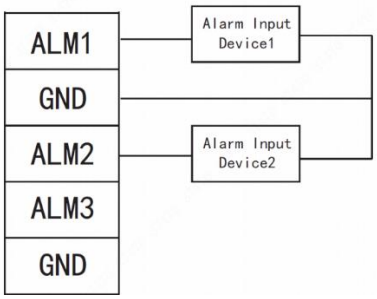
Connecting Card Reader or Keypad Using CAT6 Cable

Note: 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 (cable) when installing an Access Control System.

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

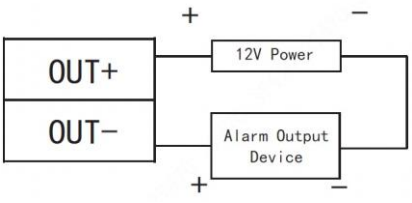
1.3 Wiring of External Alarm Input

Supports 8-channel external alarm input as shown below:

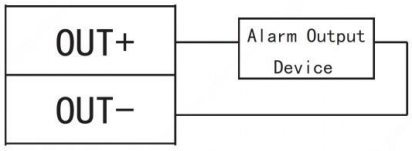


Interface	Wiring Terminal		Description
External Alarm Input	ALM1	Alarm input port 1	External alarm input ports connect smoke detector and IR detector etc..
	GND	Alarm input port 1 and 2	
	ALM2	Alarm input port 2	
	ALM3	Alarm input port 3	
	GND	Alarm input port 3 and 4	
	ALM4	Alarm input port 4	
	ALM5	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



or

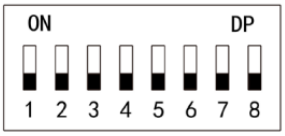


Interface	Wiring Terminal	Description
External Alarm Output	OUT1+	External alarm output ports connect audible and visual siren etc..
	OUT1-	

1.5 DIP Switch

Operate with DIP switch.

Figure 2-12



- the switch is at ON position, meaning 1.
- the switch is at the bottom, meaning 0.
- 1~8 are all 0; the system is started normally.
- 1~8 are all 1; the system enters BOOT mode after start.
- 1, 3, 5 and 7 are 1, while others are 0. After restart, the system restores factory defaults.
- 2, 4, 6 and 8 are 1, while others are 0. After restart, the system restores factory defaults,

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

II. Remote Management of Access Control System

Network configuration and programming outline:

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

Optiview Video Management Software (VMS)
With Access Control integration

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

1a. Initialize Access Control device

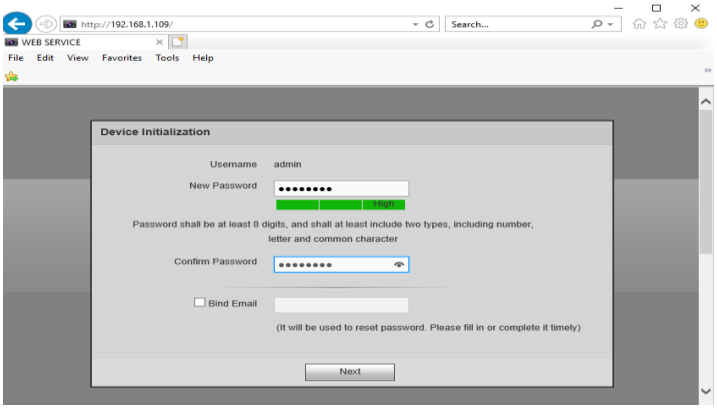
The default IP address:

- 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.

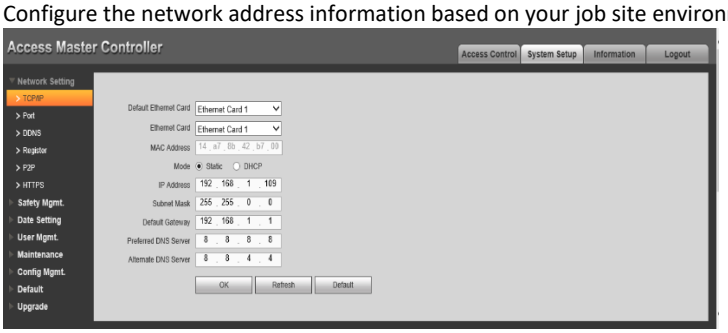
To restore factory default, go to page 6 "DIP Switch" and follow the settings of PINs as shown.

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.



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



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/

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

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

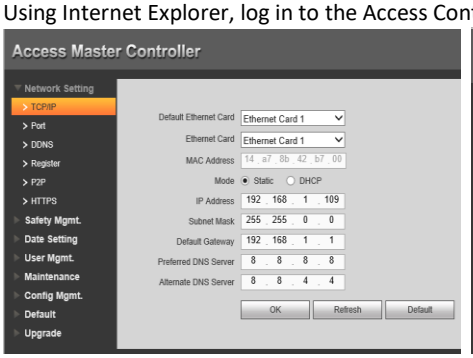
c. User Accounts Setup (See Step 1c.c at Page 10)
   - Create department or company name
   - Set the card type to be use by the system when reading cards: Decimal (10) or Hexadecimal (16)
   - Create Access Level
   - Create User accounts
   - Assign Department Name

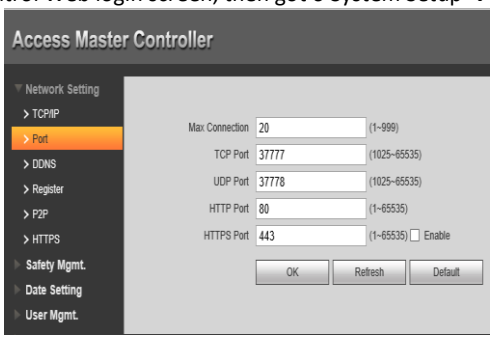
d. Customize Access Level. Create multiple Access Level to where certain employees are restricted to access doors on specific day and time.

Follow the detailed sequence of steps below:

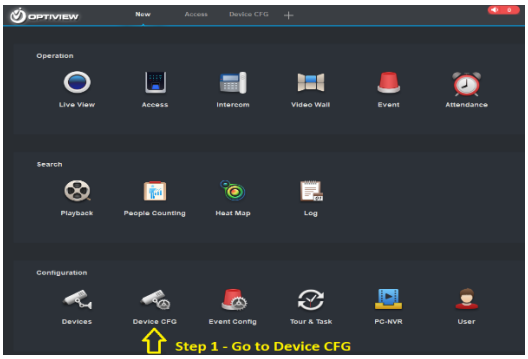
1c.a <u>Configure Device Network Settings</u>

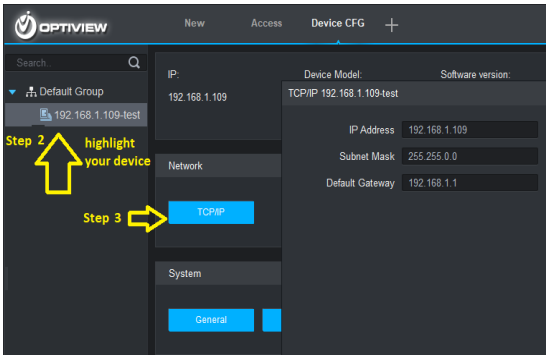
- Using Internet Explorer, log in to the Access Control Web login screen, then got o System Setup → Network Settings.





- Using Optiview VMS, set IP address.

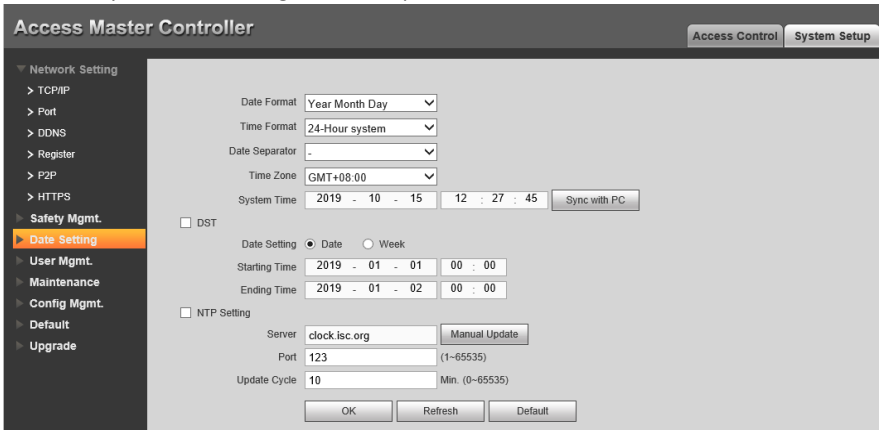




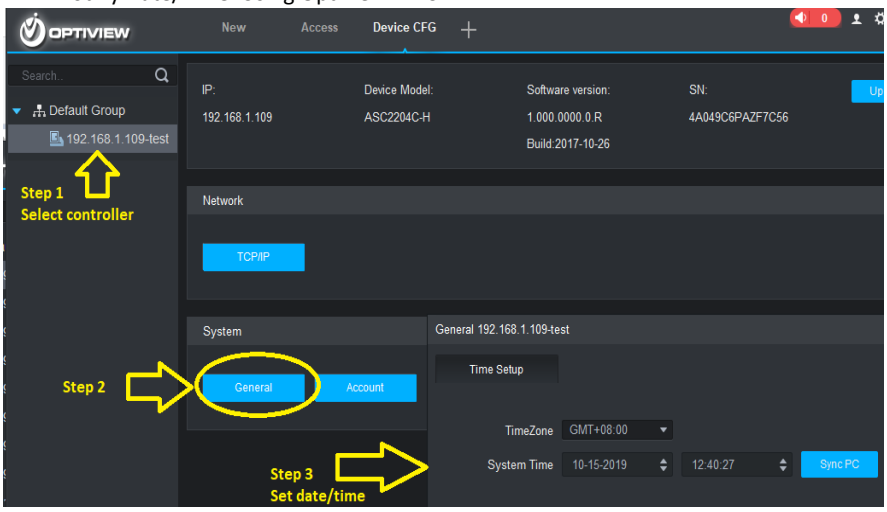
Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

- Set the Date and Time of the Access Controller

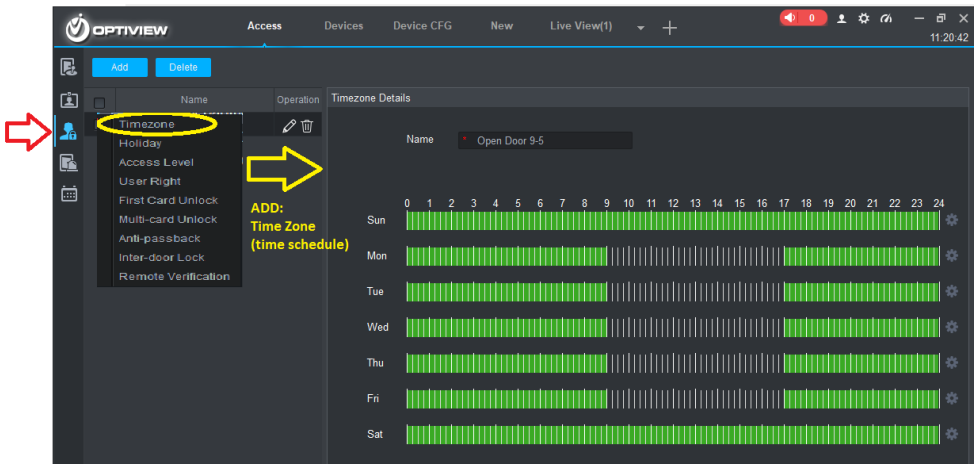
➔ Modify Date/Time Using Internet Explorer



➔ Modify Date/Time Using Optiview VMS



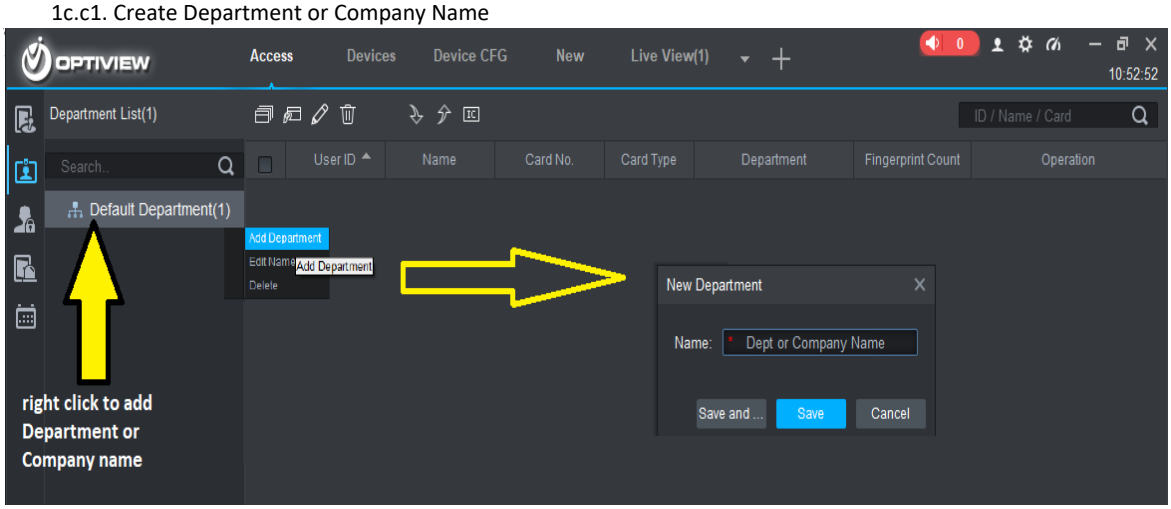
1c.b <u>Time Schedule (Time Zone) Setup</u> The selected green bar specifies ON (allowed) and vice versa.



Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

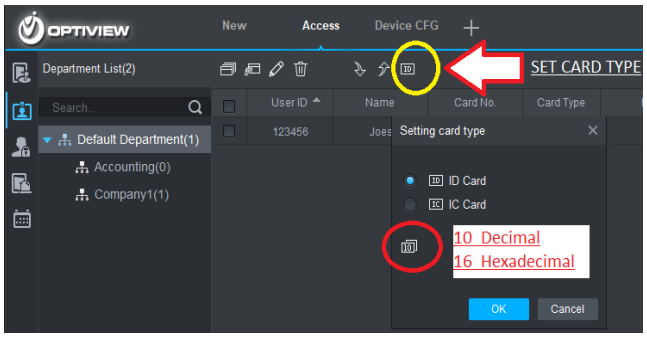
1c.c User Accounts Setup

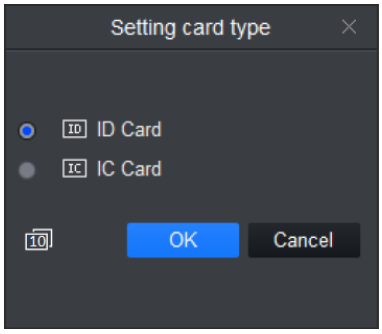
1c.c1. Create Department or Company Name



1c.c2. Set Card Type

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



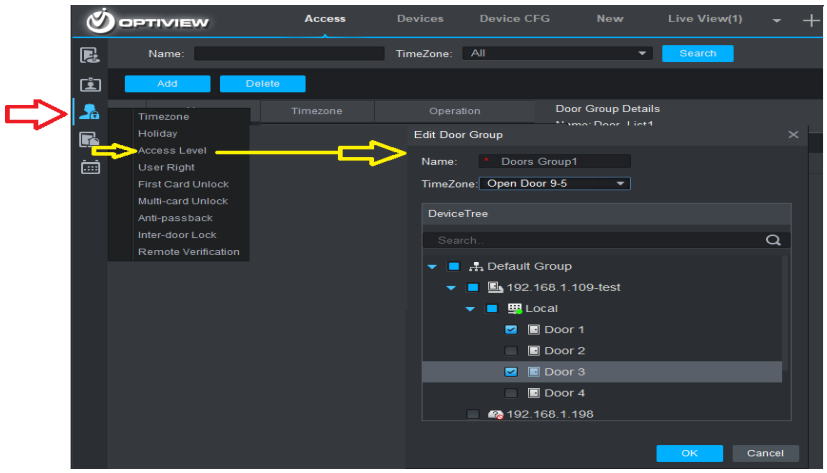


Recommended option: Use Decimal "10"

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.

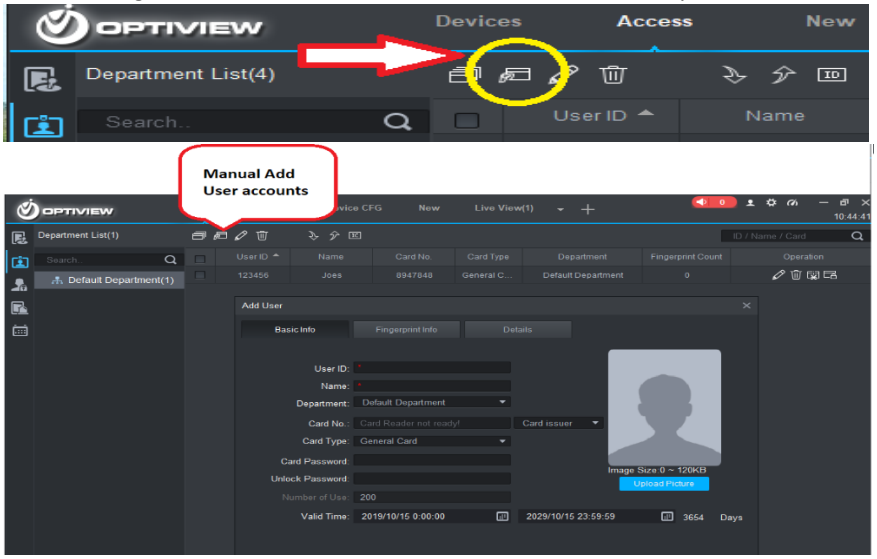


Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

➔ 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.

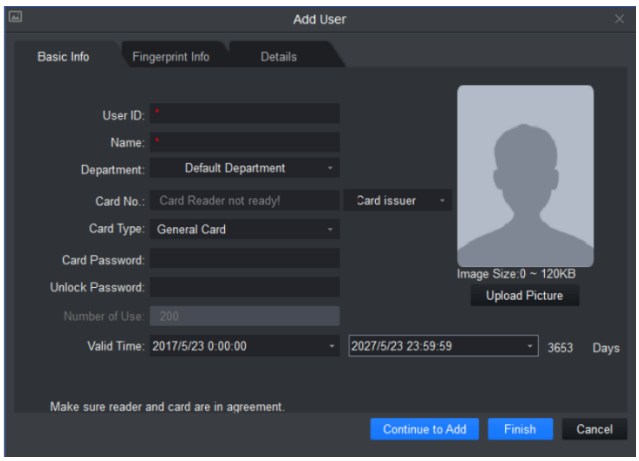
- Create User Accounts.

  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

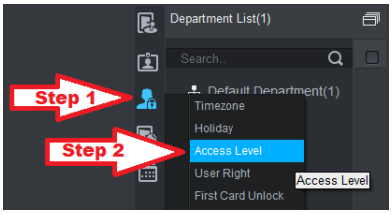


Note: Card No. and User ID cannot be duplicate.

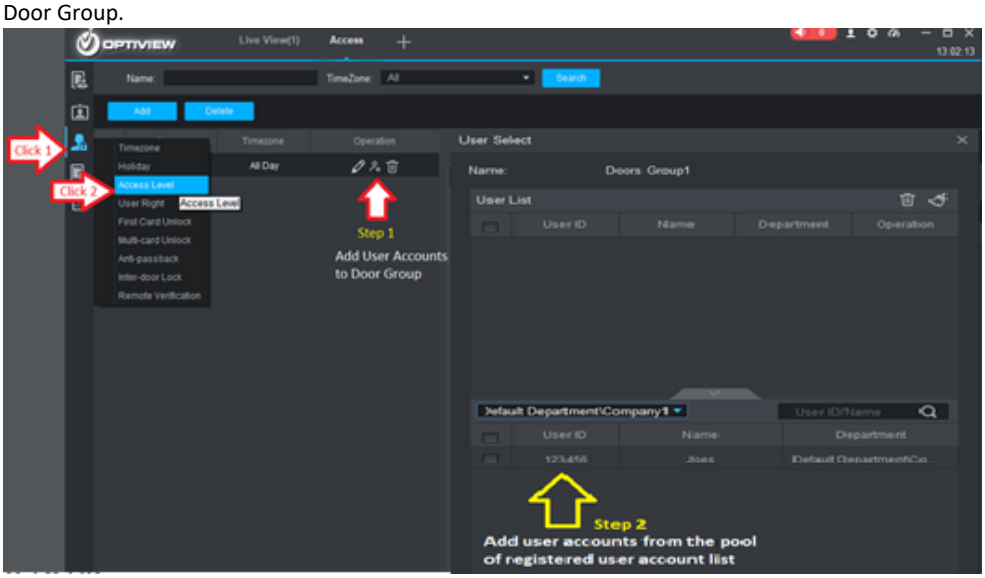
- Assigning User accounts to Access Level (sometimes called Door group)

Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020

a. Go back to “Access Level” menu



b. 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.



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 only 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.

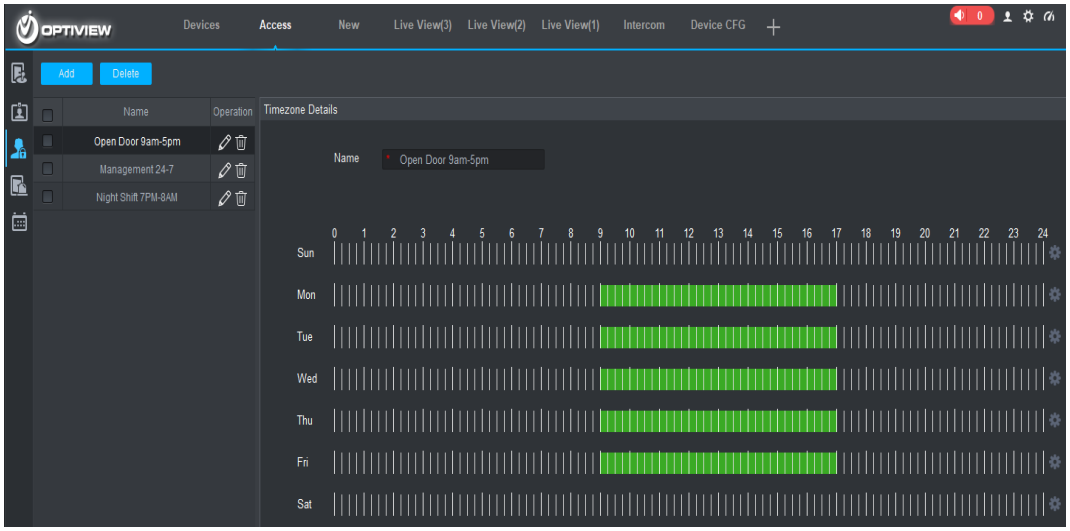
Remote verification – When a user scans the card, the admin will decide whether to unlock a door or not.

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

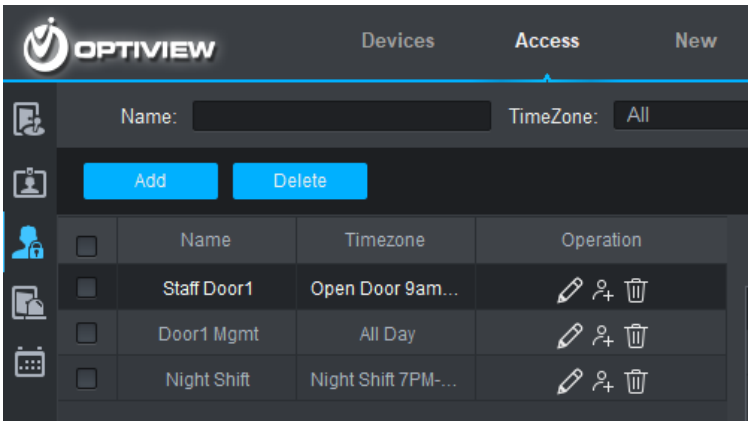
Create multiple Access Level to where certain employees are restricted to access doors on specific day and time. The steps cited below is based on the following assumptions: a single door, three work shifts and top management 24/7 access. This task is comprised of the following steps:

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

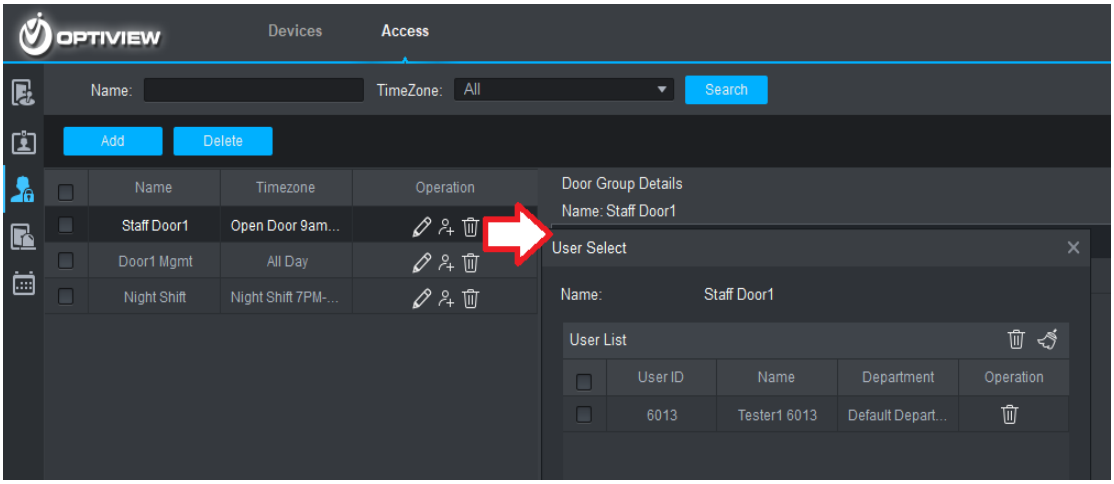
Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020



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



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



Created by: Jim B 10/01/2019
Last edited by: Jim B Date: 5/28/2020