Knowledge Base

KB – LTK28xx Access Controller (NVMSv3)

Text: Jimmy Wang

This reading material is for internal training purposes. For all legal warnings and instructions, please refer to the official access control user manual.
Please visit our LTS website for more information. Link

c UL us LISTED #E485225

Roughly, you can think about the Access Control category separate to 4 levels.

1.	Doorbell	support ring/notify from the mobile app, but not support unlock door.
2.	Intercom	support ring/notify & unlock 1 door from the mobile app.
3.	Multiple doors Controller 28xx	support 2/4 doors unlock locally (not support remotely, no mobile app)
4.	XVMS Server Software/Solutions	Integrate multiple controllers (up to 8) and support mobile app unlock.

This KB only describe the #3, Access Controller 28xx

2 Doors / 4 Doors Access Controller

LTK2802 Access Control for 2 Doors

LTK2804 Access Control for 4 Doors

LTK2802
Access Control for 2 Doors

LTK2804
Access Control for 4 Doors

Before the Installation

- Please always read the official user manual.
- Access Control software supports Windows PC only.
- Require Internet connection for the Time Sync
- LTK Series only support Mifare Card.
- **PC NVMSv3** Support up to 16 Controllers
- For security reason, no remotely unlock features.

Reading Guide

First, the Hardware, then the Software

Warnings Follow these safeguards to prevent serious injury or death.

Cautions Follow these precautions to prevent potential injury or material damage.

All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region. Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value. Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard. Please make sure that the power has been disconnected before you wire, install or dismantle the device. When the product is installed on wall or ceiling, the device shall be firmly fixed. If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center. If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Installer License Requirements for Business environments:
Low Voltage Installation – C7 License
Fire Alarm – C10 License
Your State/City license requirements may vary.
Please note, LTS is not responsible for any issues related to installer license requirements.

California

Low Voltage Specialty License Types:

Low-Voltage Systems C-7

Electrical Contractor
(includes Fire Alarm installations) C-10

Fire Protection Contractor C-16

Lock and Security Equipment Contractor C-28

Solar C-46

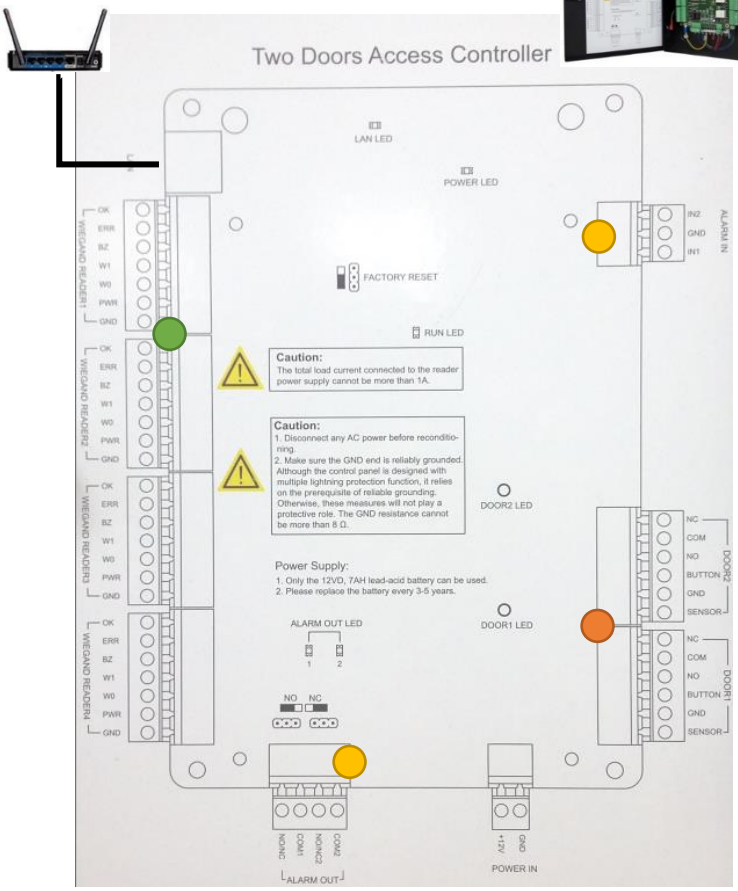
Controller Interface:

(Important) Open the side panel. There is a labeled sticker. It indicated the correct responding position and usage.
If it is different from the user manual, the sticker label is the correct answer. Please check it carefully first.

Left side: Wiegand section.

Right side: Door Locks section

For the fire alarm Input / Output trigger.
(Upper right and bottom sections).
Please read the user manual for detail connection instruction.



> Note:
> Door locks power must run separately.
> Controller won't support any power for door locks.
> NO/NC and COM connections are nonpowered

For 2 Doors Access Controller:
Support up to 4 Wiegand with Anti-Bypass solution.

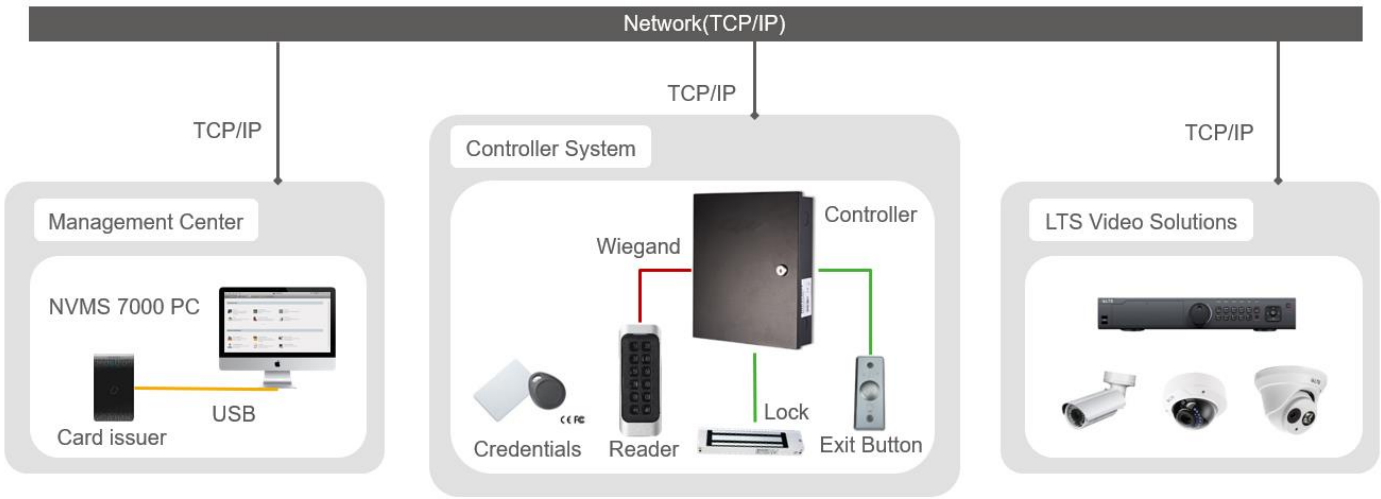
Control in or out by using the Wiegand reader to allow the access.
For example: W1, W2 for Door1. W3, W4 for Door2.

4 Doors Access Controller: Support up to 4 Wiegand readers.
Each Wiegand only supports to one designate door number.
For example: W1 for Door1. W2 for Door2. W3 for Door3. W4 for Door4

Structures

Internet Router ------ Main Network Switch ------ PC NVMSv3

+--------- LTS NVR / DVR
+--------- LTS IP Camera
+--------- LTK280x Access Controller Box
+--------- (Additional LTK280x Box, etc...)



2 Doors

Wiegand Reader 1 (Entry): For Door1
Wiegand Reader 3 (Entry): For Door2

Wiegand Reader uses 18/6 wires to be connected.

Regular Connection: (LTK2802)

Door Lock: (see Page 6)

Door lock device uses 18/2 wires to be connected.
Must Run door lock power separately.
Access Controller is NOT provided power to the door locks

NC	Door Lock Relay Output (Dry Contact)
COM	
NO	
BUTTON	Door Button Input
GND	Grounding
SENSOR	Door Magnetic detector

Exit Button: (see Page 6)

If Exit button is required, connect a wire (18/2) to the device.

4 Doors Access Connection: (LTK2804)

4 Doors connection diagram is
same as the 2 door Regular Exit button connection.

Anti-Passby Question:
Only 2 door can support the Anti-PassBy.
4 doors are not supported.

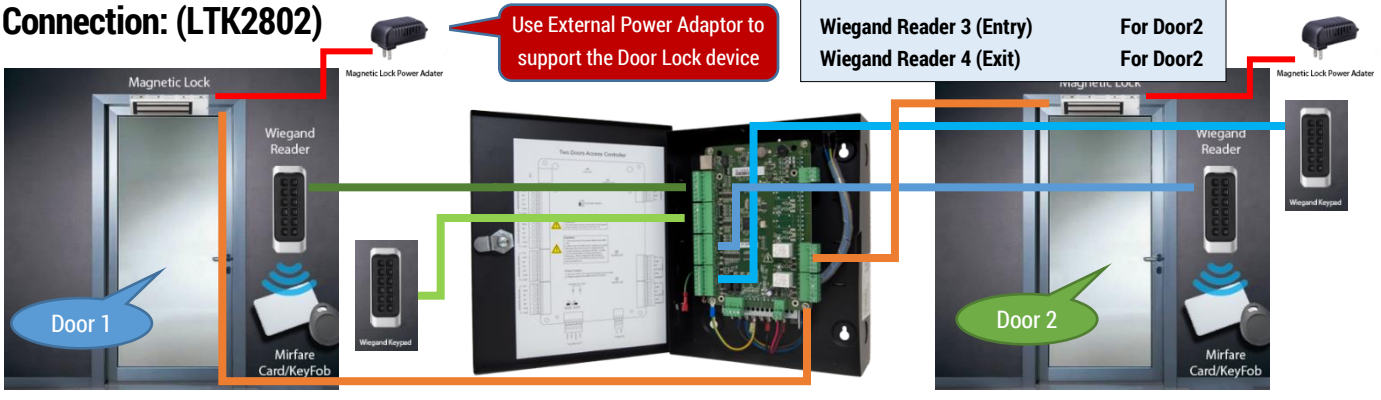
If you need Anti-Passby for 4 doors,
please purchase **Two Sets** of 2 door
access controller.

Wiegand Reader 1	**For Door1**
Wiegand Reader 3	**For Door2**
Wiegand Reader 5	**For Door3**
Wiegand Reader 7	**For Door4**

2 Doors Anti-Passback (see Appendix)

Connection: (LTK2802)

Wiegand Reader 1 (Entry)	**For Door1**
Wiegand Reader 2 (Exit)	**For Door1**
Wiegand Reader 3 (Entry)	**For Door2**
Wiegand Reader 4 (Exit)	**For Door2**



Wiegand Connection:

Please read the user manual. This diagrams below are for reference only.

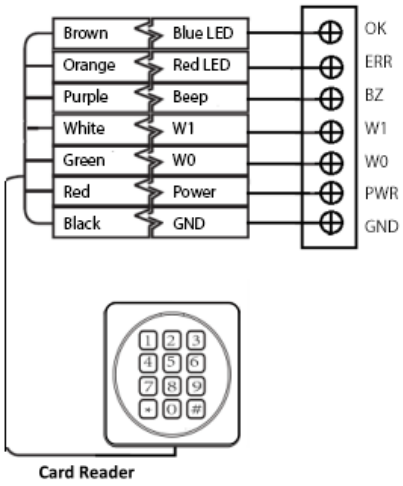
Standard Wigegand Protocol
4 Connections (very Minimum)

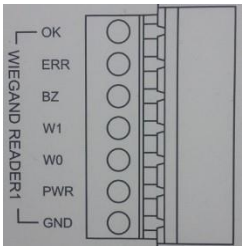
2 Power (DC 12V)
2 Data

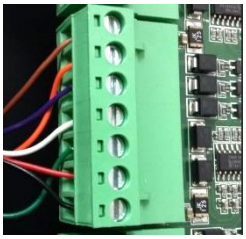
Wiegand 26 = 8 digit #
Wiegand 34 = 10 digit #

If the Controller is being used to control the LED and buzzer on the Wiegand card reader, then the OK/ERR/BZ ports need to be connected.

Simply said, if you run short of the wire, don't need to connect the ERR wire (18/6).







Some KB Info may be Old, please follow on the Actual Installation Document.

These are the responses based on the wire connected.

OK is connected:	Valid card is scanned, the indicator light shows Green.
ERR is connected:	Invalid card is scanned, the light will flash Red 3 times.
Beep is connected:	The valid card beep twice (be-be quickly), invalid card will beep 3 times slowly.

ATTENTION:

For the Newer Card Reader, there is no longer needs to adjust DIP switch. For all older model, Physical Dip Switches on the back of the readers need to be set prior to first use. If any changes need to be made to the DIP-Switches, the reader needs to be Power reset before the DIP-Switch changes are set properly.
For the older LTK1107M/MK, it requires DIP 5 is ON. Or, when you heard 4 beeps when scanning. Please turn DIP5 on.

Most DIP Switches 1- 8 are **OFF** position by default

Older Model (Newer No need)
Set 5,6 to ON for Wiegand Protocol
Set 7 to ON to Wiegand 26-bit Protocol
(Default OFF for Wiegand 34-bit Protocol)

SENSOR AREA

These four reader models are designed to support Wiegand 26-bit and 34-bit Protocols

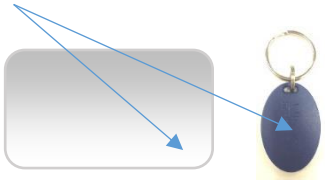
LTK1107M **LTK1107MK** **LTK1103M** **LTK1103MK**

How to manually input numbers?

Enter 8 Key numbers and Press # when finished.

How to find the card number?

123,45678 (26-bit 8 Key#; no comma)
1234567890 (34-bit 10 Key#)



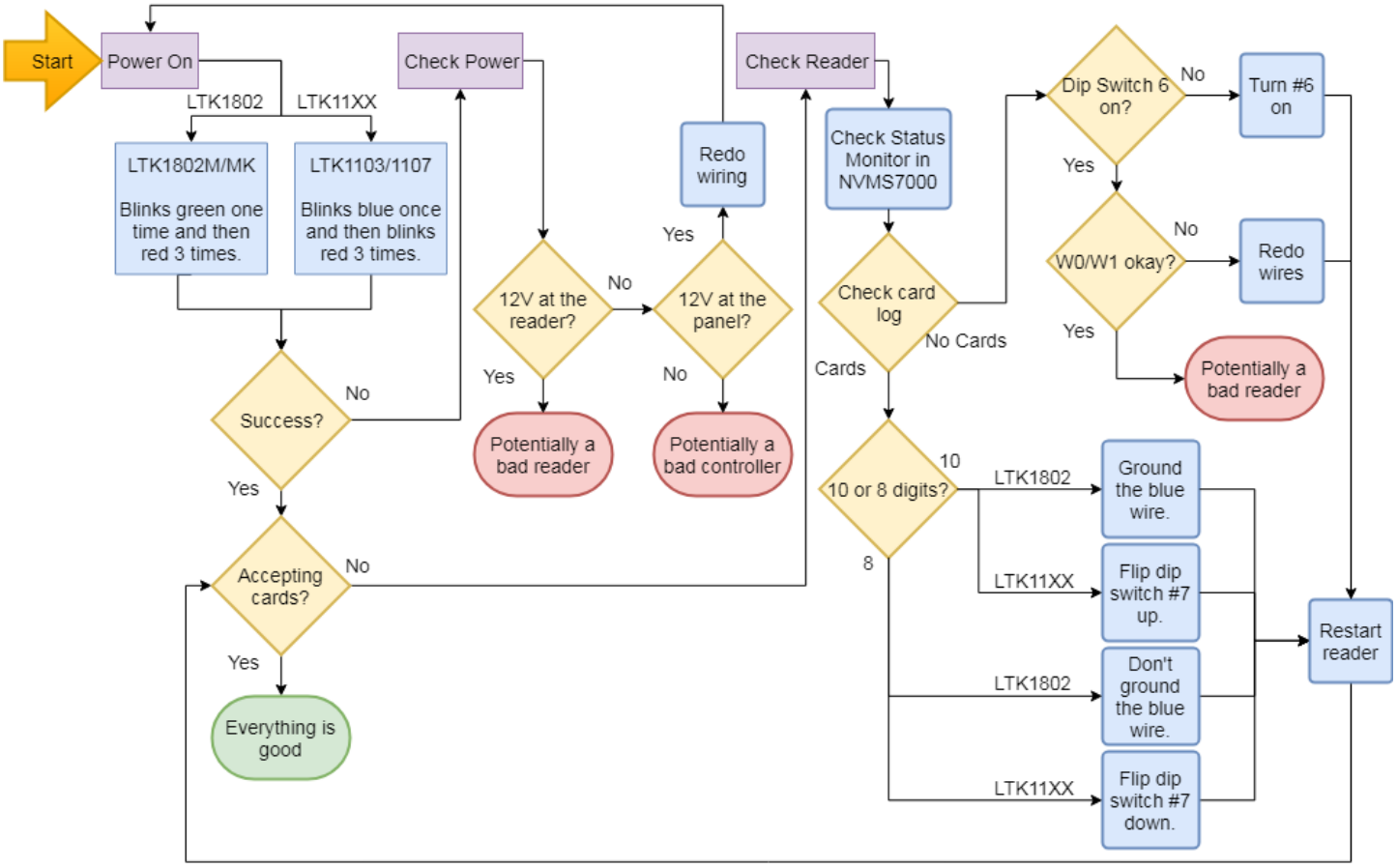
LTK1802M **LTK1802MK** (Wiegand 34-bit)

Economic Mifare Card Reader
LTK1802M
Sign In for Price
Card Reader
learn more

Economic Mifare Card Reader
LTK1802MK
Sign In for Price
Card reader with keypad
learn more

Connect the Blue cable to ground will switch from 34bit to 26bit (8 Keys)

Troubleshooting Flow Chart: Wiegand Card Reader

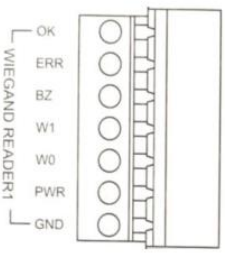


LTK1802MK

OK	Brown
ERR	Orange
BEEP	Purple
W1	White
W0	Green
12V	Red
GND	Black
26/34	Blue

(Optional)

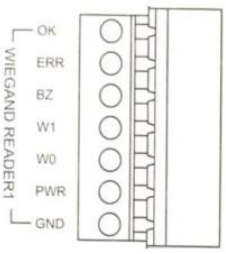
Grounding the Blue cable will switch Wiegand bits from 34 to 26.



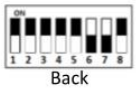
LTK1107MK

OK	Brown
ERR	Orange
BEEP	Purple
D1	White
D0	Green
12V	Red
GND	Black

(Optional)

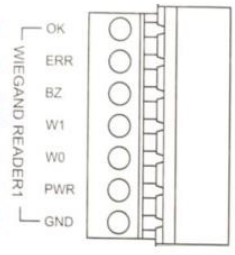


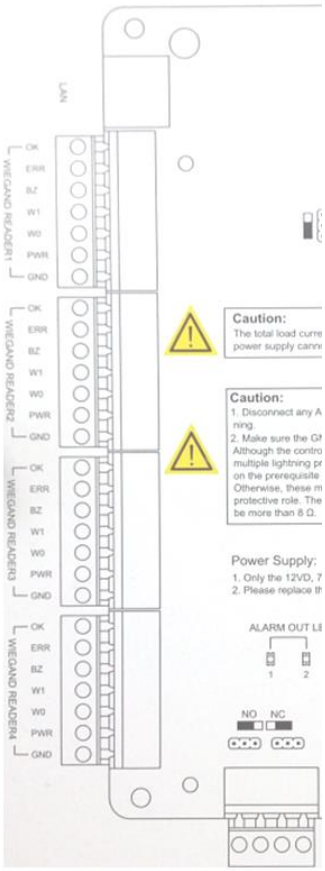
LTK1103MK



OK	Brown
ERR	Blue
BEEP	Yellow
W1	White
W0	Green
12V	Red
GND	Black

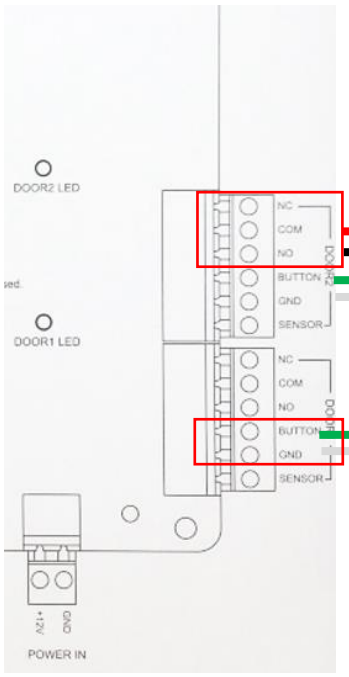
(Optional)

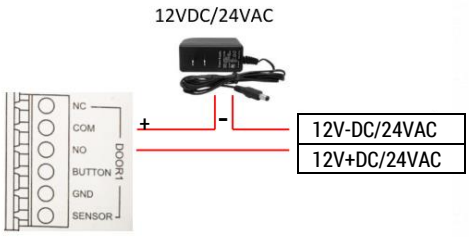




Door Lock Connection

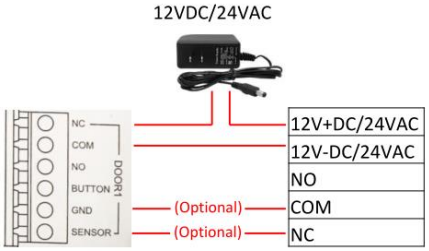
NO - Normally Open (**No Power**, door stays locked).
NC - Normally Closed (**Power** is required to keep the door locked).





LTKL101

Normally Open



LTK-600LB

Normally Closed

EXIT button

Green

White

No LED / No Power Needs
Exit Button

LTKB01

Green

White

LED / Sensor extra Power Needs
Exit Button

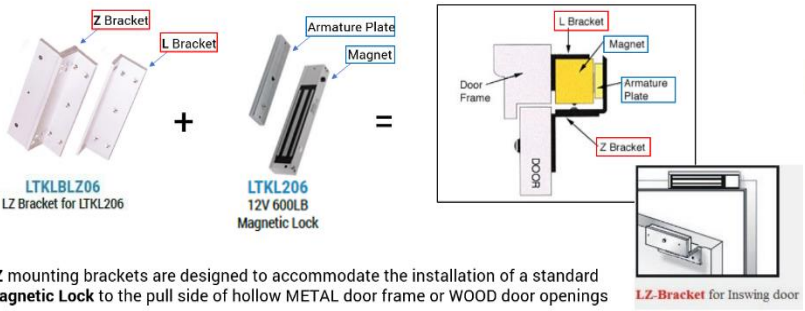
LTKB04

LTK-REB-1
No LED / No Power Needs

LTK-RT-1(Wireless)

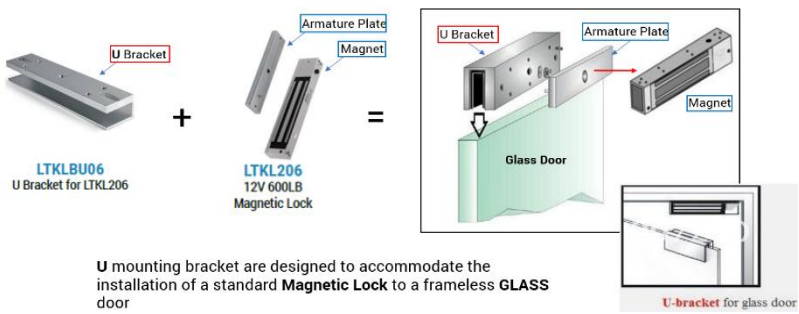
LTK-SREX-100

LTS LTKLBLZ06 - LZ Bracket for Magnetic Lock Application



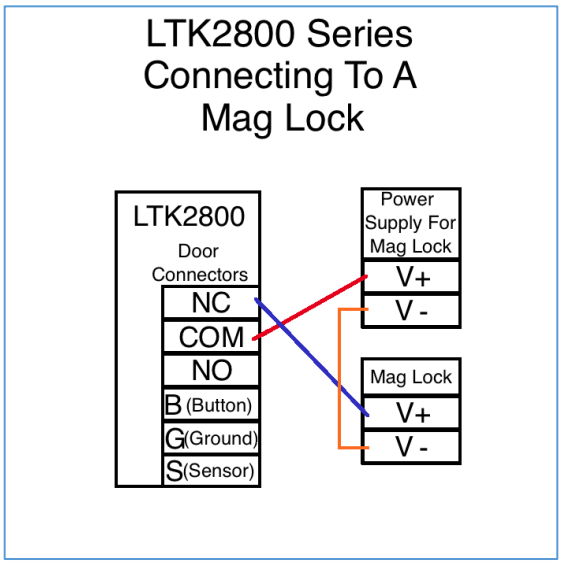
LZ mounting brackets are designed to accommodate the installation of a standard **Magnetic Lock** to the pull side of hollow METAL door frame or WOOD door openings

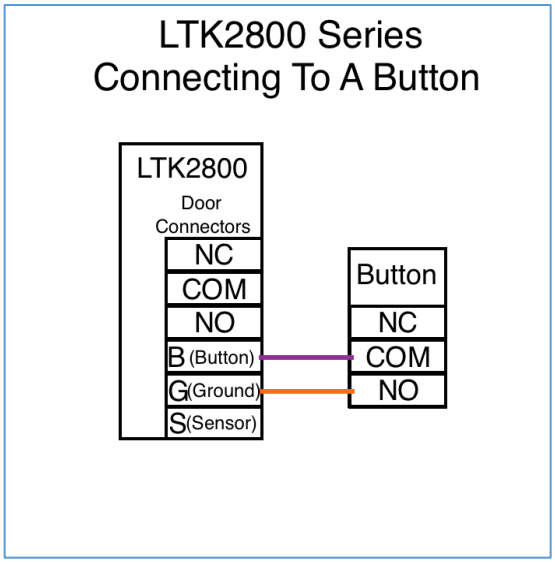
LTS LTKLBU06 - U Bracket for Magnetic Lock Application

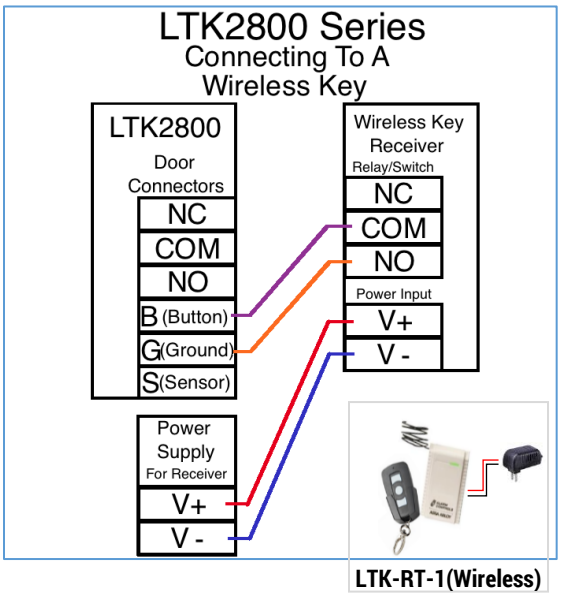


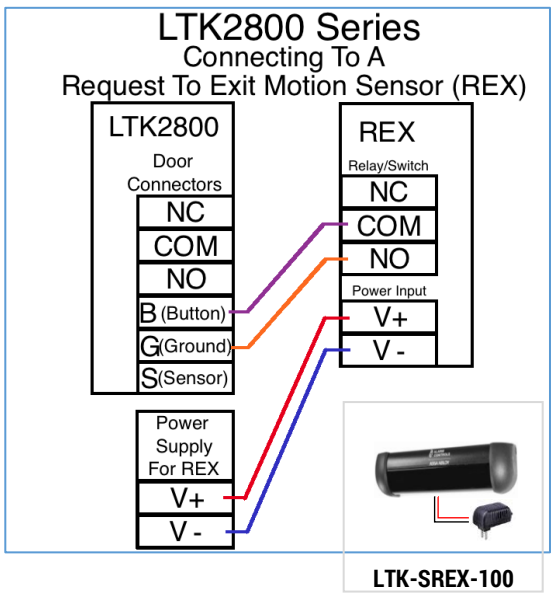
U mounting bracket are designed to accommodate the installation of a standard **Magnetic Lock** to a frameless **GLASS** door

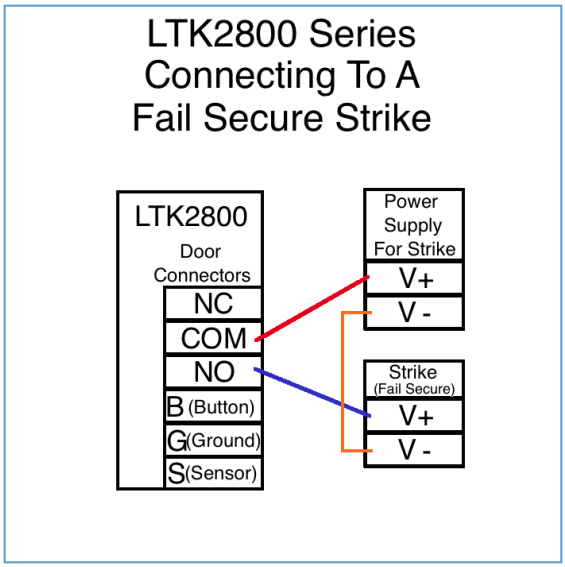
EXIT button Wire Diagram Example

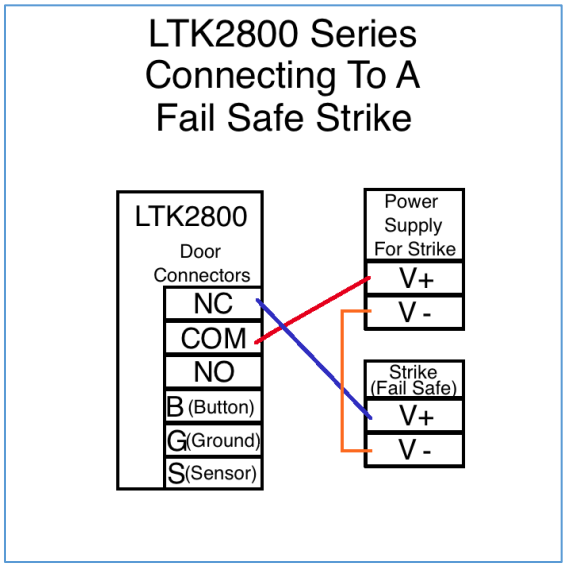












C – Door Wiring Connections

From James R's Note:

The Door Terminals on the Access Control Panel have 6 Connections.

N.C. =Normally Closed Circuit

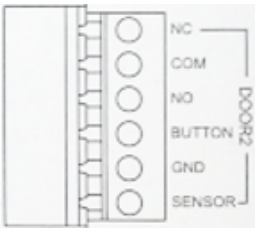
COM = Common

N.O. = Normally Open Circuit

B =Button

G =Ground

S = Sensor



* Strikes can use either the Normally Open Contact, or Normally Closed Contact, depending on the Strike. To determine whether a Strike should be connected to the N.O. contact or the N.C. contact, disconnect the Strike from any power and check to see if the Latch is released or locked. If the Strike is disconnected from power, and the Strike's Latch is released, then the Strike needs power to lock the Latch, and needs a Normally Closed Circuit (The Strike needs a closed circuit to provide power to lock the Latch). If the Strike is disconnected from power, and the Strike's Latch is locked, then the Strike does not need power to lock the Latch and needs a Normally Opened Circuit (The Strike needs an opened circuit to keep the Latch locked).

A button can be wired to the Door Terminal of the Access Control Unit, to allow the Door to be opened with the push of a button. For a 2 wired N.O. button, connect 1 wire to the B (Button) Terminal on the Door Terminal of the Access Control Unit, and connect 1 wire to the G (Ground) Terminal on the Door Terminal of the Access Control Unit.

For Buttons with more than 2 wires, consult with the button's packaging to determine what each of the colored wires is designated for. An Example is:

V+ = V+ Power for Button LED
V- = V- Power for Button LED
N.O. = Normally Open Button Connection
COM = Common Button Connection
N.C. = Normally Closed Button Connection

For a 5 wire button, COM will connect to the B (Button) Terminal on the Door Terminal of the Access Control Unit, and N.O. will connect to the G (Ground) Terminal on the Door Terminal of the Access Control Unit.

A Timed Button can be connected to the Power Loop of a Fail Safe Lock (Instead of connecting directly to the B & G Terminals of the Access Control Unit). This would be done by using a Timed Button's COM & N.C. connections and placing the button along the Power Loop, between the Fail Safe Lock and the Access Control Unit or Power Supply V-.

(Normal – The Non-Triggered state of the circuit)

V+ from the Power Supply always connects to COM Terminal on the Door Terminal of the Access Control Unit

V+ for a Mag Lock always connects to N.C. Terminal (Normally Closed Circuit) on the Door Terminal of the Access Control Unit

V+ for a Strike will connect to either N.C. (Normally Closed Circuit) or N.O. (Normally Open Circuit) depending on the Strike.

V- for a Mag Lock or Strike will always connect to V- from the Power Supply

i – Mag Lock
V+ from the Power Supply always connects to COM Terminal on the Door Terminal of the Access Control Unit.

N.C. Terminal (Normally Closed Circuit) on the Door Terminal of the Access Control Unit always connects to V+ on a Mag Lock.

V- on a Mag Lock will always connect to V- from the Power Supply to complete the circuit.

ii – Strike
V+ from the Power Supply always connects to COM Terminal on the Door Terminal of the Access Control Unit.

N.C. Terminal (Normally Closed Circuit) on the Door Terminal of the Access Control Unit will connect to V+ on a Strike IF it is a Fail Safe Strike.

N.O. Terminal (Normally Open Circuit) on the Door Terminal of the Access Control Unit will connect to V+ on a Strike IF it is a Fail Secure Strike.

V- on a Strike will always connect to V- from the Power Supply to complete the circuit.

Fail State – How the Door Locking Mechanism behaves when it is disconnected from Power.

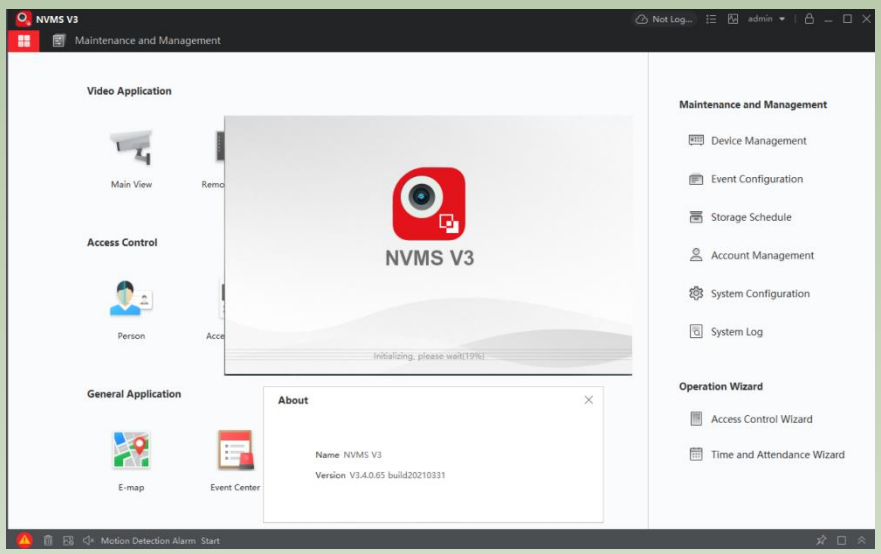
a – Fail Secure Strike
A Fail Secure Strike means when the Strike is disconnected from Power it is locked. This type of strike is wired as NO Normally Opened Circuit. It does not require Power to remain Locked, it requires power to open

b – Fail Safe Strike
A Fail Safe Strike means when the Strike is disconnected from Power it is unlocked. This type of strike is wired as NC Normally Closed Circuit. It requires Power to remain Locked.
[A Mag Lock is naturally Fail Safe]

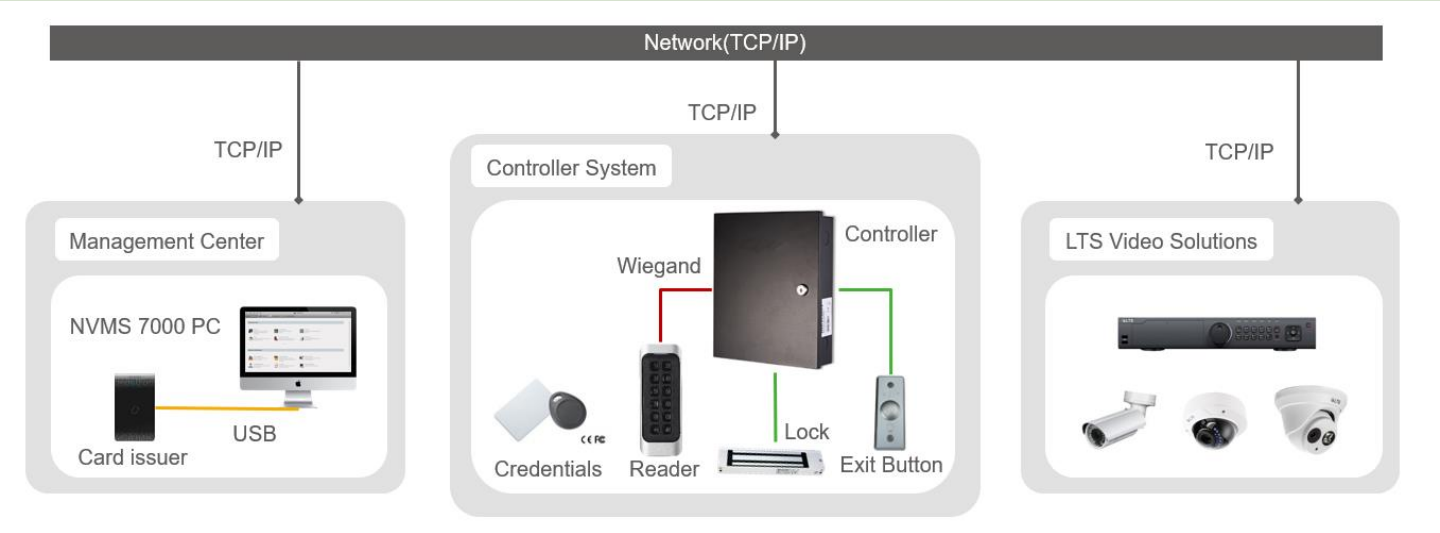
Software

Access Control Client Software:

NVMSv3



- **Max. 16 controllers / 64 doors**
- **Max. 10,000 users**
- **10,000 Cards**



Setup

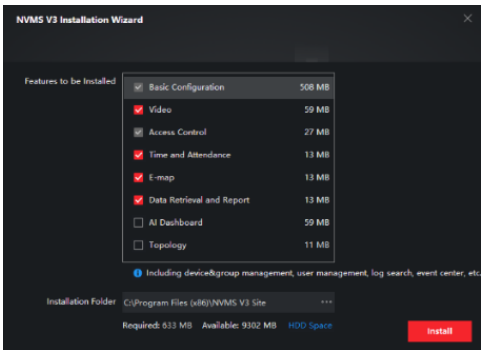
You can download the **NVMSv3** software from the LTS Website.
http://www.ltsecurityinc.com/downloads

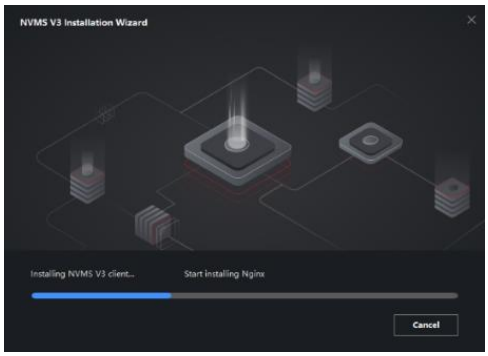
Installation is simple, please unzip it and the installation **Run as Administrator** is required.

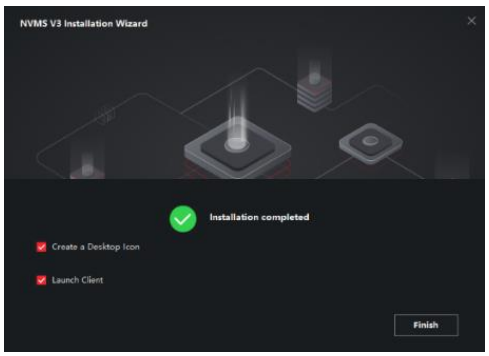
Topology is not necessary; you may remove it.

Client Software

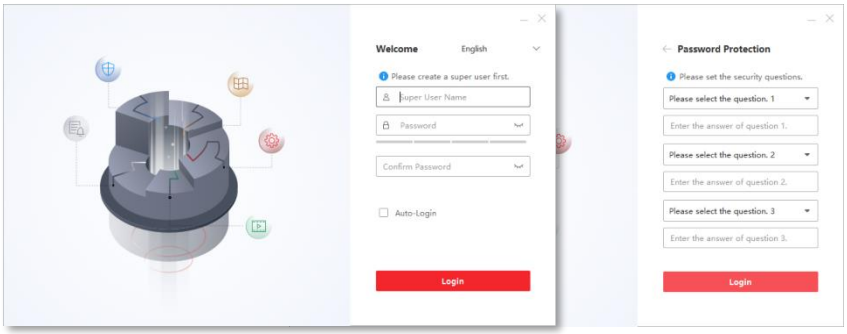
Software	Description	Version	Platform	Download
NVMS V3	Upgraded CMS client software	NVMS_V3_V3.4.0.65_20210331	Platinum Series	Windows







First Time Run / Super User



Note:
Please write down the super user password. LTS won't provide support for the Super User Password Reset (NVMS v3). For all others, please check the LTS Support Policy. Here

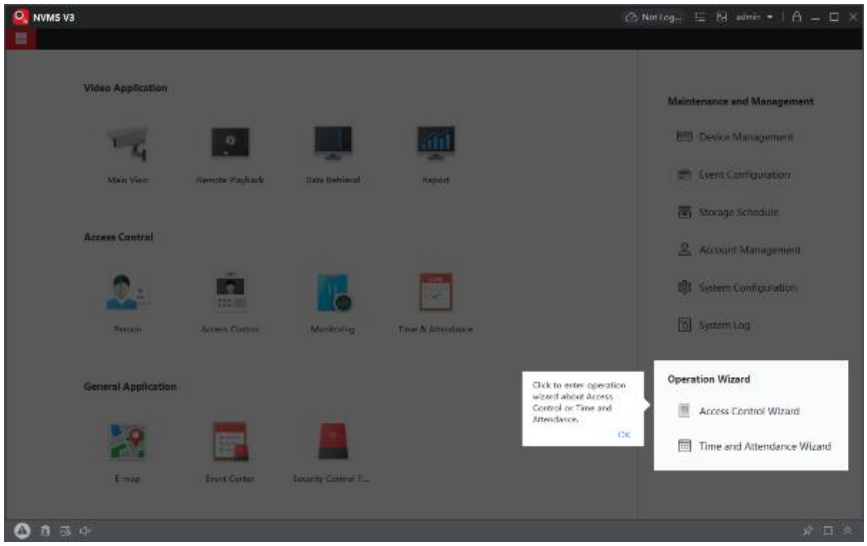
Troubleshoot:
Backup/Restore Configuration. (see Appendix E)

Super User is for the NVMSv3 account permission.

Create Super User Account, Password.
Enable Auto-Login (option; but Recommended)

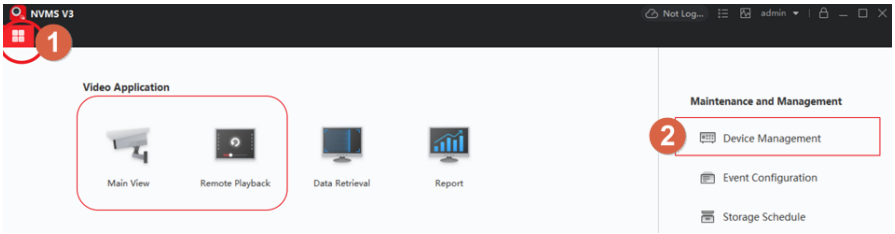
Next, the Introduction Wizard will pop up as below.

Click OK to skip it.



Device Management

1. Tap the upper-left Catalog button.
2. Click **Device Management**
3. Maximize to full screen is recommended.

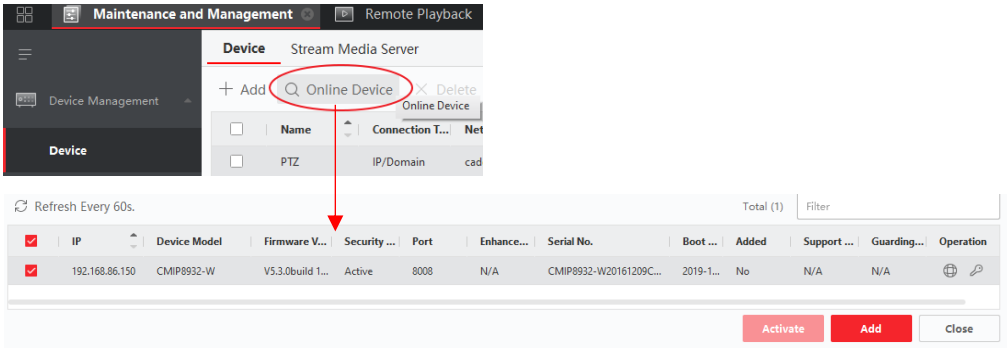


** IMPORTANT --- UPDATE THE FIRMWARE ** Please update the firmware before start everything! Backup Database always recommended. Factory default is also recommended.

Search Local Network Device

1. Make sure to allow the firewall first.
2. The bottom section will show up nearby devices from the local network.
3. Check the box, then click Add to the list.

4. If the Device is inactivated, please Activate first.
5. If you forgot the password, click the key icon.
6. Click the Global icon to modify the network IP.

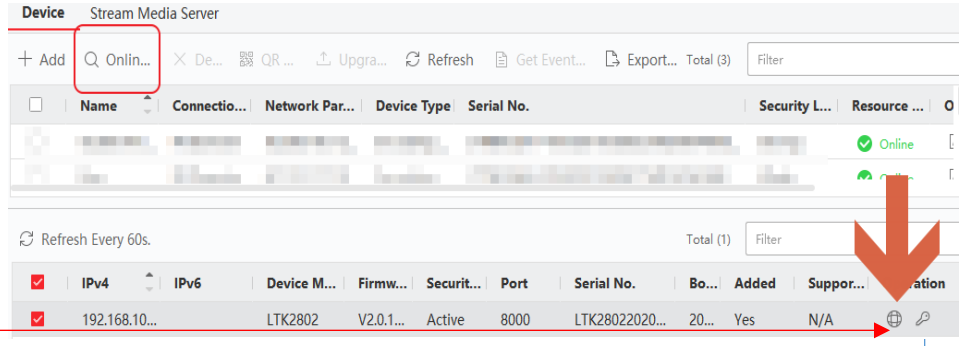


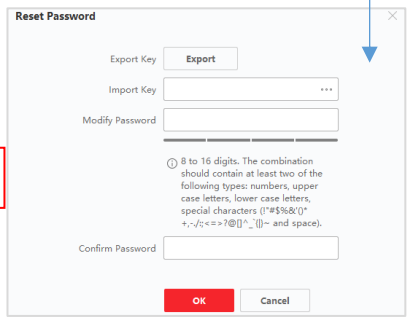
If you don't see anything from the Online Device search list. Please check your PC ip address first and make sure they are connecting to the same network.

Change Network IP Address

Click Global icon, to change the IP setting.

Note: Access Control and Intercom don't recommend use the DHCP IP address. because NVMSv3 will link to the wrong IP address and cause Arming issue.

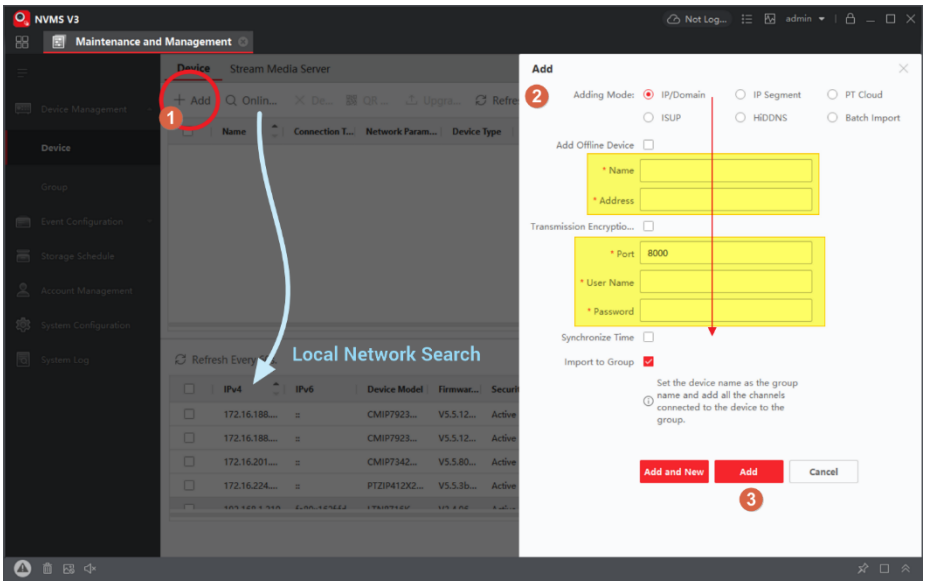




About Password Reset - https://ltsecurityinc.zendesk.com/hc/en-us/articles/360008093653--PC-Reset-Password-for-Platinum-IPC-NVR-DVR-

Adding Device

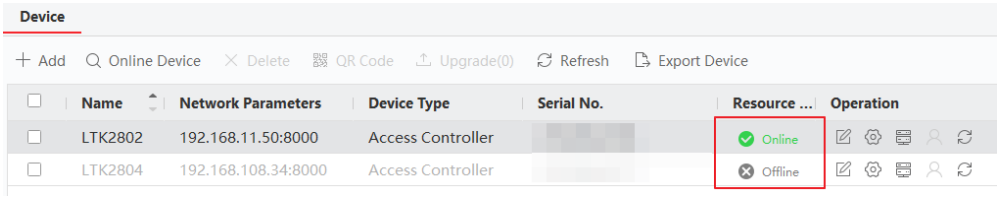
1. Click + Add, to create the new connection.
2. Select IP/Domain and fill up the yellow sections.
3. Click **Add** when finish.



*** Important ***
Please make an appropriate Name (aka nickname). It helps to label the controller if you have more than one. If it is not connected, please check the setting information again.

Note: Please always keep the minimal connections in the device management as possible. Because the NVMSv3 will check each device's location connectivity when offline.

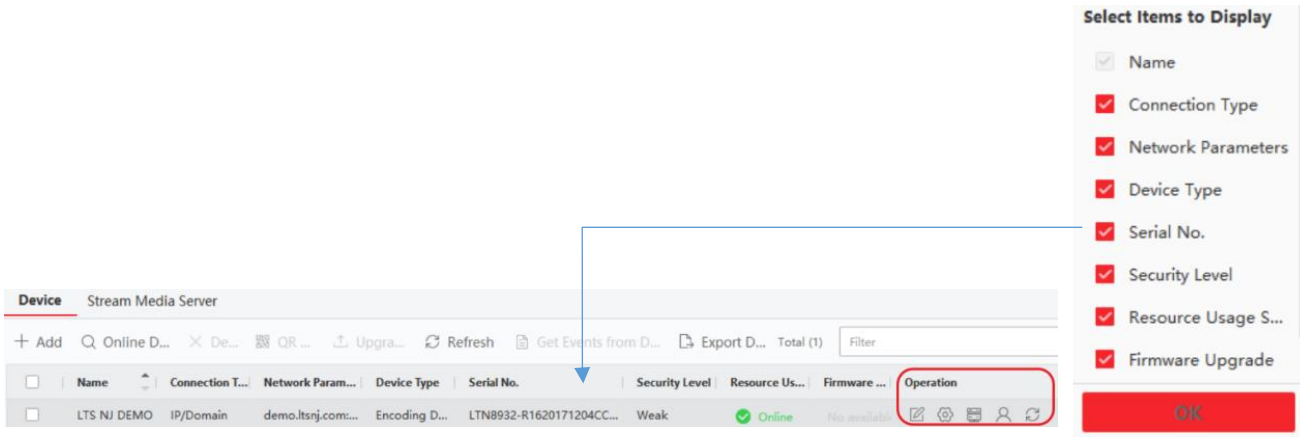
After connected, the Status will show Online



(Tips)

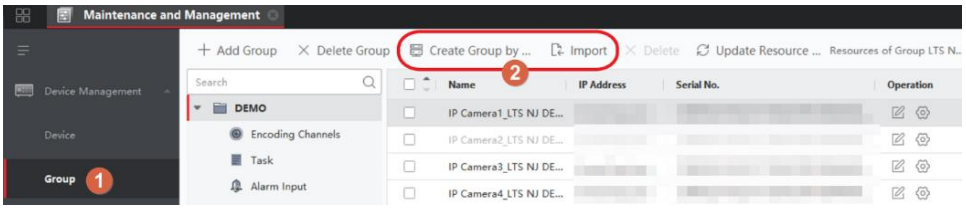
(Small Monitor) If you have a smaller monitor resolution, you may not be able to see the configuration button on the right side. Here is the trick on how to resolve this issue.

Move the Mouse on the column and Right-click the mouse button. The **Select Items to Display** will pop up.
For example, If you feel the Firmware Upgrade is useful. Remove it to reduce the column to save some space of view.



Group

What is the Group?
(Remember: No Group, No Doors)



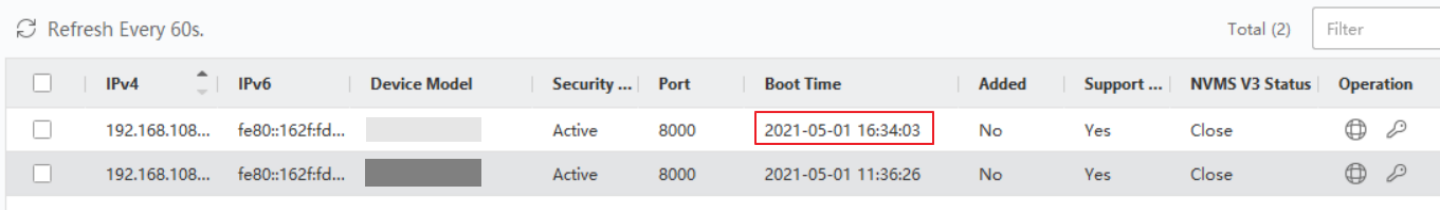
The Group is a folder for the Main View camera control or the Door Access in the Realtime event section. If you don't see this information in the real-time monitoring section. Please re-create it.

Create Group by the Device Name when you add the device fails, then it will not automatically create the Group folder. Use this function to add it back but make sure the device is online first.

For the Access Control, I recommend using the Create Group by the device name. Do Not use the **Import** button to merge with different Access Control devices/Doors together. Make the "Group" only contain the device as simple as possible. **(Will Discuss in the Programming Section)**

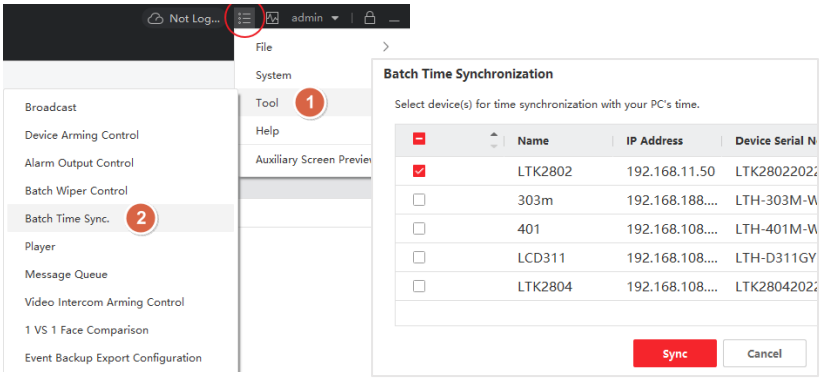
Time Sync

Device Time Accuracy is very important for Access Control. Please always make sure the device time is correct.
For the Access Control, you can verify that time from the device list. (28xx Boot time = Current Time; not apply for the intercom)



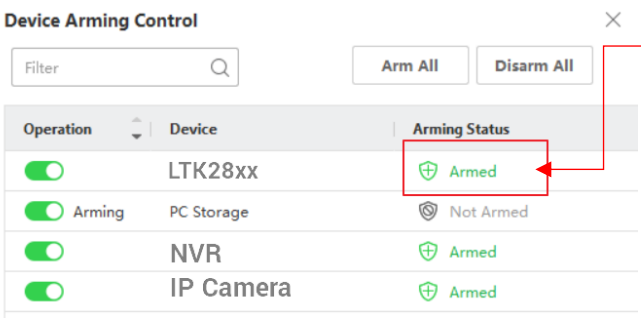
If you set up the TimeZone correctly, it will automatically sync with the Internet Time.

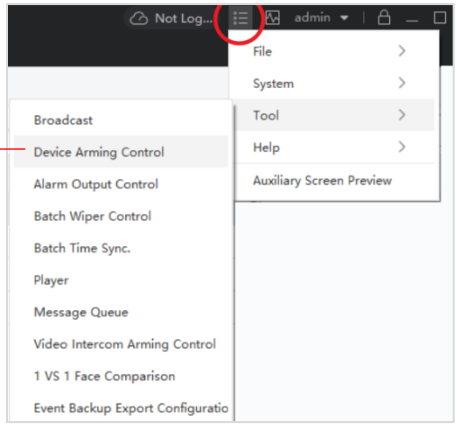
If you need to manually sync the time to the device, you can use the Batch Time Sync. It will copy **Current PC time** into the device.



Device Arming Control

Device Arming Control indicates the device is currently communicate with this NVMSv3. Please always make sure it is Armed.

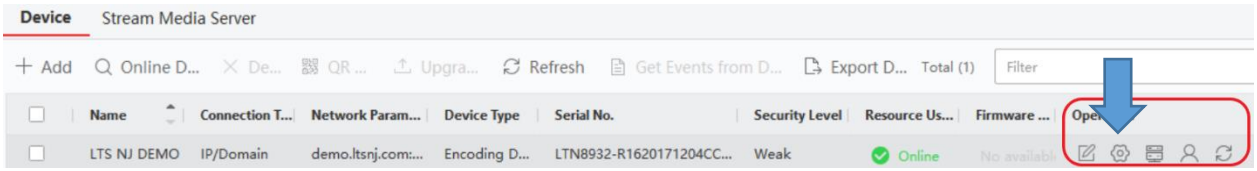




This is most important part to communicate in between PC to the Access Control device.
If not, the NVMSv3 will not get any feedback from the device.
That means – even the card to swipe to make the door open, but there will no card swiping record log in to this software.
Please always make sure connect the NVMSv3 and the device within the same network.
If you are using the VLAN or VPN environment, please make sure the port number is open and forward correctly.

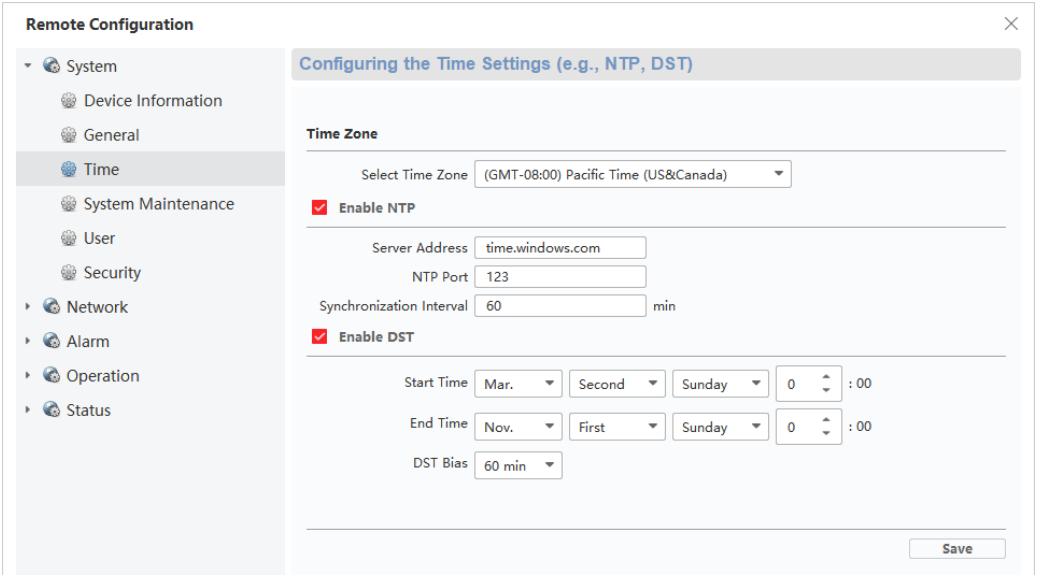
Change Setting in the Configuration

Check NTP Time Zone Setting in the configuration



Click the **Gear** icon (Configuration) button

System > Time



Troubleshooting:
if the Remote Configuration is not able to open, please make sure the Online Status is ready or the HTTP port (80) is open.
Usually, you shouldn't have this issue if you are the local network environment.

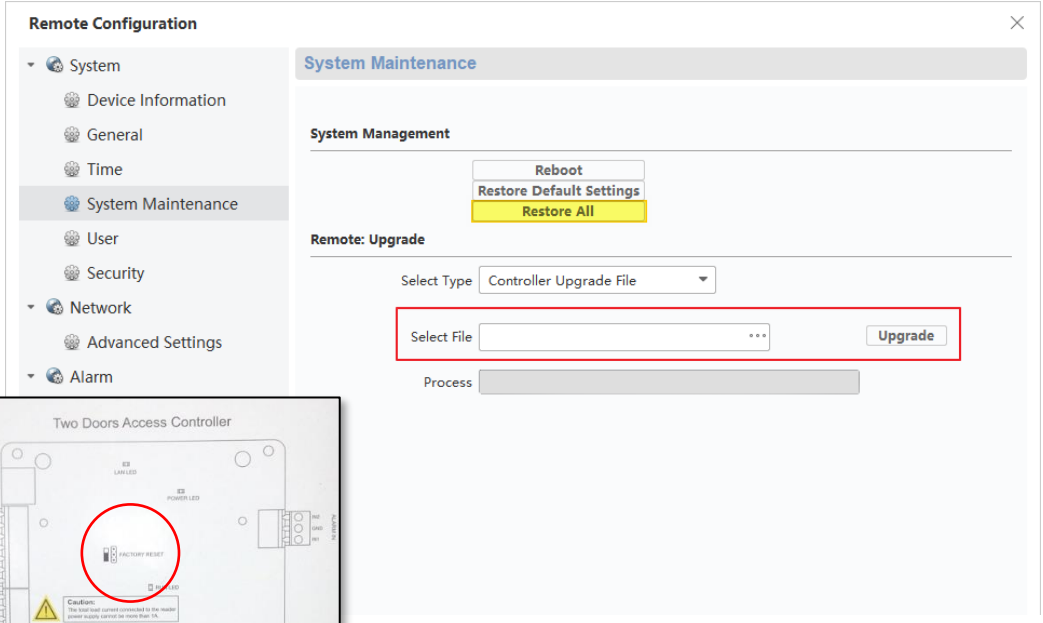
Maintaince (Factory Default)

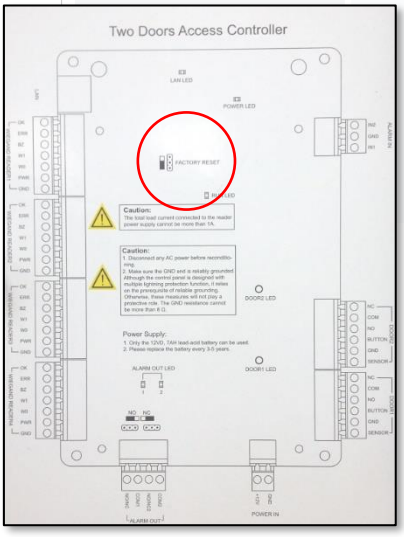
Go to Configuration button

** BACKUP DATA FIRST

System > System Maintenance

Restore All is the Factory Default





Hardware Reset:
Power down the device,
Short the jumper.

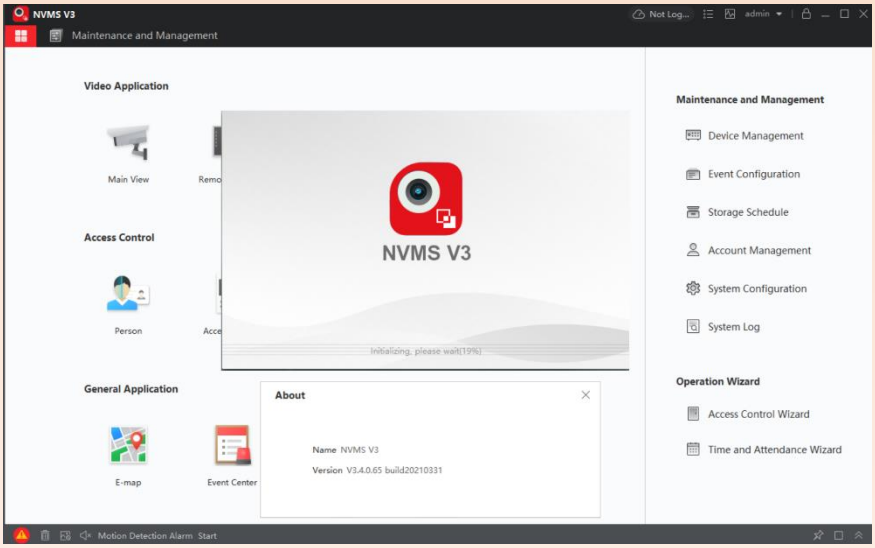
Power On
Will hear very Long Beep -----
Power Down.

Put the jumper back.

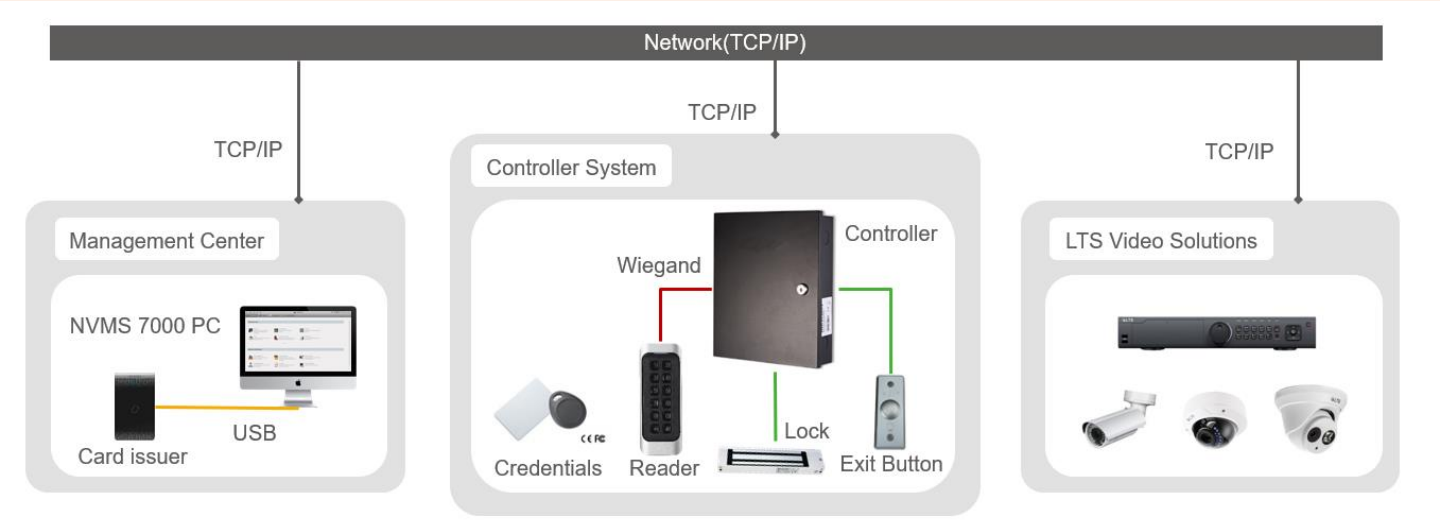
Programming

Access Control Client Software:

NVMSv3

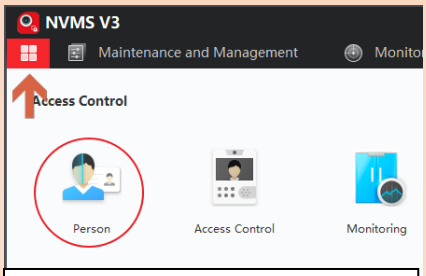


- **Max. 16 controllers / 64 doors**
- **Max. 10,000 users**
- **10,000 Cards**



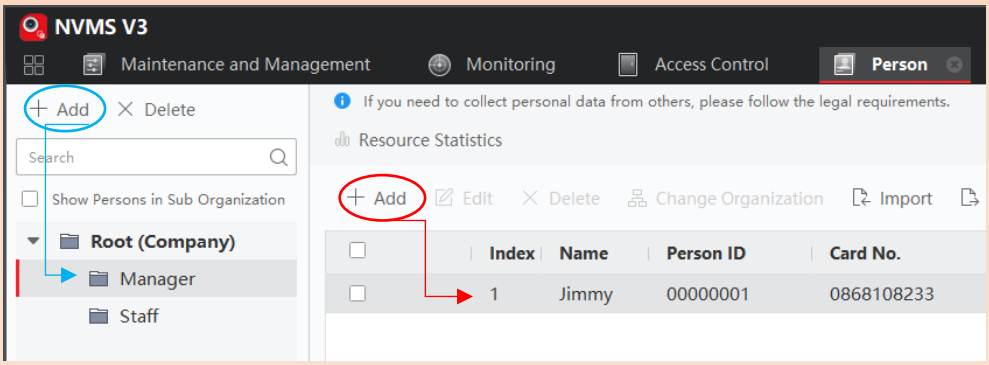
Add Card / Add Person (Person)

Menu > Person



(Important Note)

NVMv3 is designed for the "Single Company " Database, not for the multiple company. Please do not mix with different Access Control database locations together with. If you want to use different company database, please always Backup and Restore the database to switch in between.



Creating a clear understanding structure will help you to manage the database easier.

Please rename the Root structure to an appropriate name.
Click the root folder and click Add can create a department-level structure.
For Example: click on **"LTS"** > Add > give a department/group folder name "Manager".

(Note) recommend only create 1 level group folder structure.
Please don't create a group folder under another group folder.

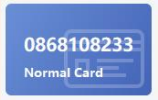
Click + Add to set up your first person.

1. **Add a person's name** first.
2. **Add Card.** Add the Mifare Tap Card

   or manual enter the card number become as the punch access number

   (number must be unique)

   i. Click + to Add
   ii. Click Settings
   iii. Click Card Reader
   iv. Select Remote Device OK
   v. Click Read and go to the device Tap the Card to scan it.

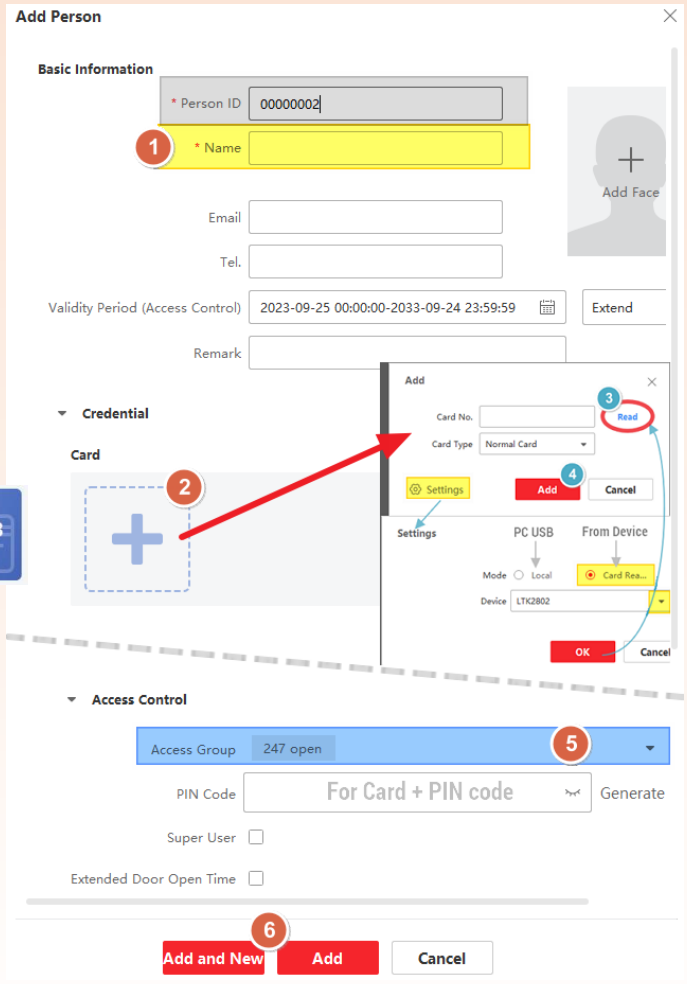


4. Click **Add** the card number.

5. Select Access Group (Option, you can do all together in the Access Group)

   If you can, please enter the Floor# and Room# for each person.

6. Complete Add.



Template (Time Template)

Not everyone got full schedule access.
That is the reason you need to schedule the Time Template.

By Default,
All-Day Authorized
is the full 24-7 allow-access schedule (no Holiday).

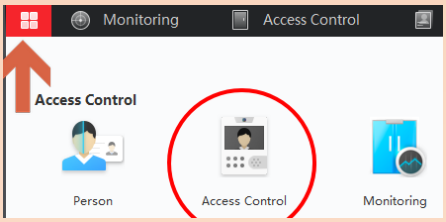
You also can define different **Allow-Access** time
for the management purpose.

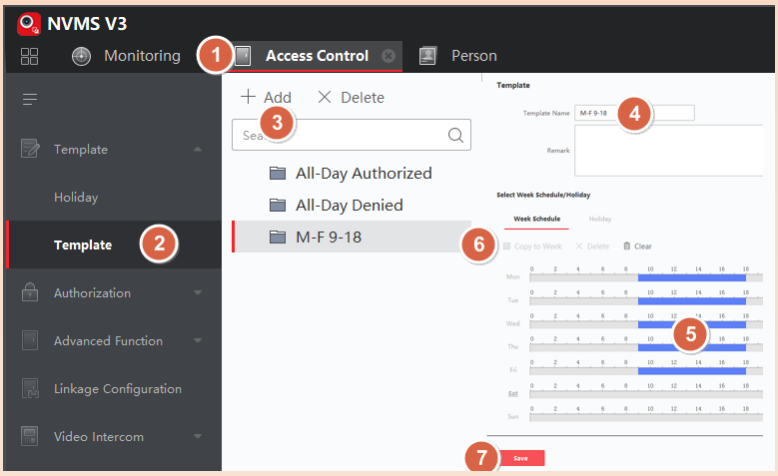
Follow Picture 1-7 Steps, should be simple.

#4 Please Provide an easy understanding Label.
for example: M-F 9-18

#5 The blue is allow, otherwise is not-allow.

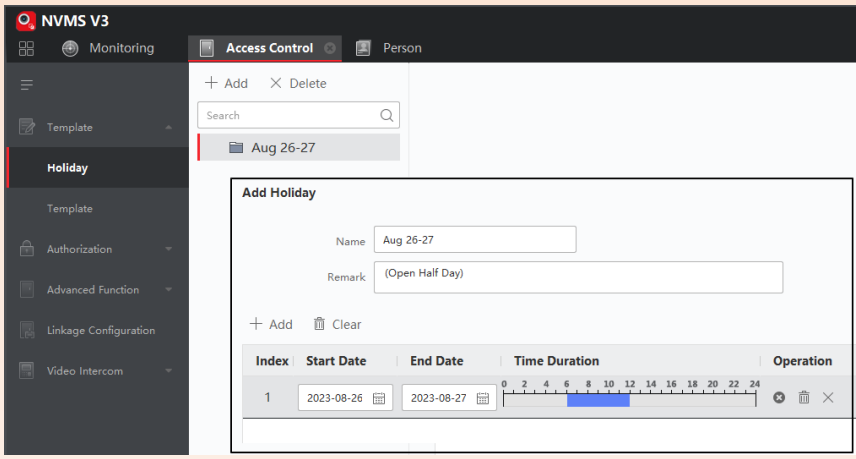
#6 after you copy to all weekdays,
Highlight Sat and press delete button.
It will clear out the Saturday.





Define Holiday

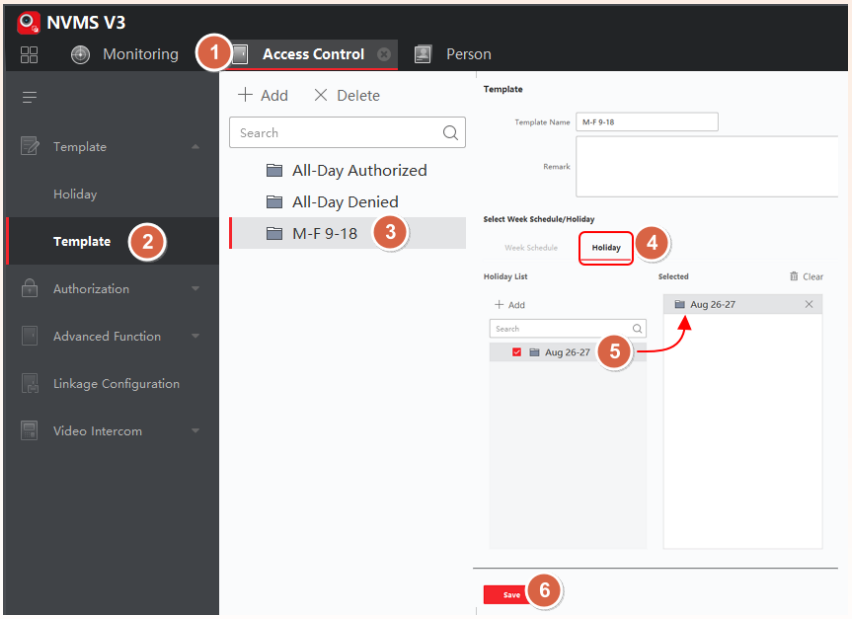
If you want allow/block special event such as Holiday, you also can define it.
If you didn't define the time period, it will treat it as block time.



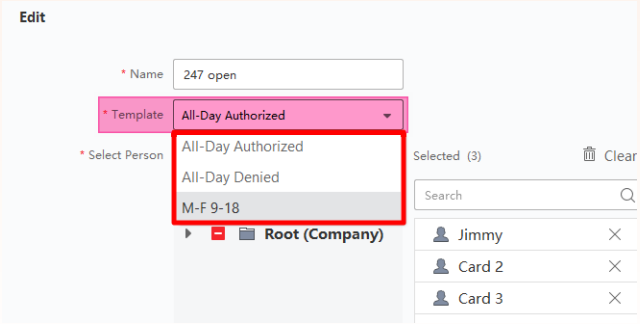
Then, you add it into your defined schedule.

For example,
Now, you should have

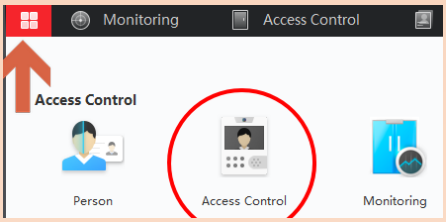
M-F 9-18 with Holiday	Allow to access Aug 26, Aug 27 (open half day)



Then you define the Access Group, please make sure to select the corresponding Time template. (See the next page)



Access Group (aka Permission)

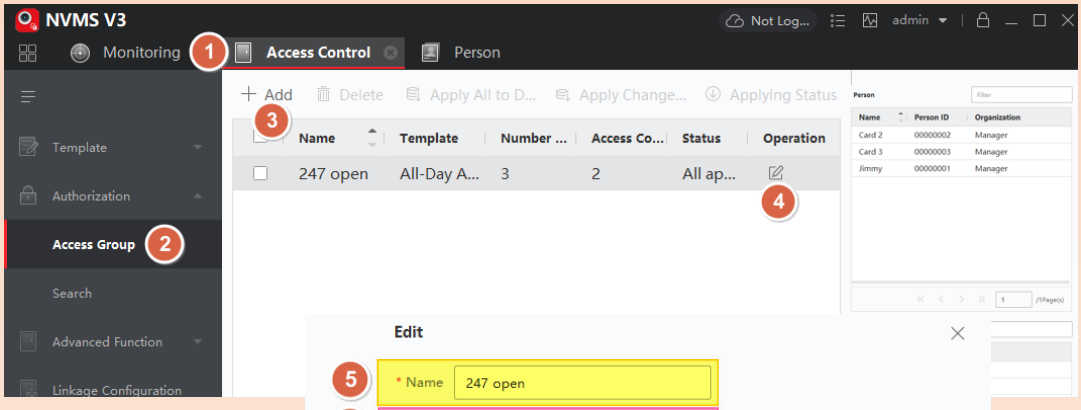


Access Group is the Door Access Permission.

You need to link the person with this Access Group, then you can tell which door is allowed to access with.

1. Open Access Control
2. Select Access Group

3. You can create a new, + Add
4. Or, you can modify the exist one.



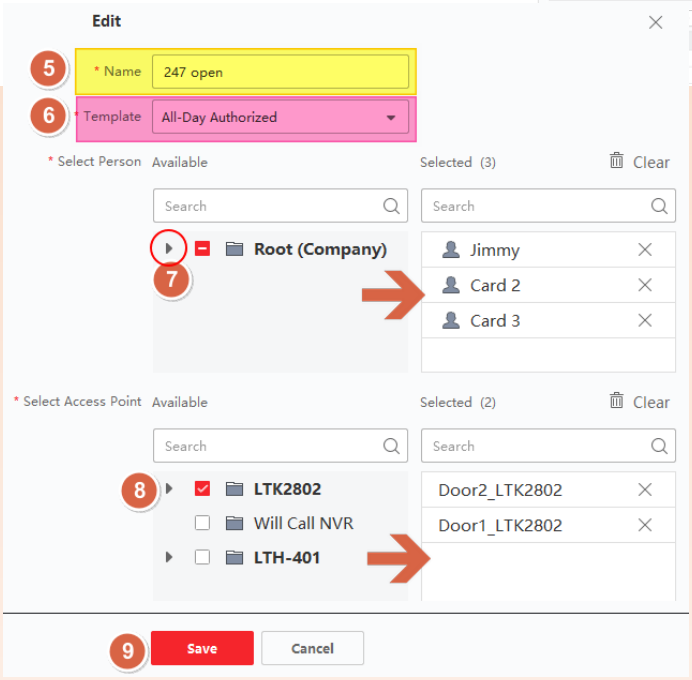
5. After the Panel shows up.
   please give an appropriate Name for this permission.
   For example: 247 Open

6. Time **Template**, please select allow-access Time (see prev. page)

7. Add Person to the Right panel.
   (Troubleshoot: if you see no name, please check the Person section. See page. 16)

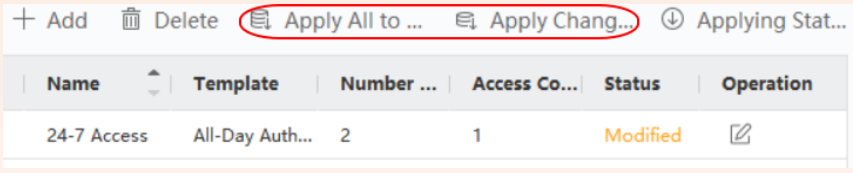
8. Add Door to the Right panel.
   (Troubleshoot: if you see no Door, please check the Device Management "Group")

9. **Save**



Now, we are almost done with the Person/Permission Programming.

You need to click **Apply** to the device.



There are two different kinds of applications.
Apply Changes – Only apply the Change section to the device.
Apply All to the device – Apply all settings (aka Manual Override) to the device, even all the data has already existed and same.

Congratulation, now you can Test the result.

Use the Facial to access or use the keycard to unlock it.

About how to rename the Door-name, please check the Appendix.

REMEMBER
Make sure there are **No Overlapping permissions.**
For example, if John has been allowed to open all doors in one permission, there is no reason for John to program only door 1 to open in another permission.
It is repetitive.

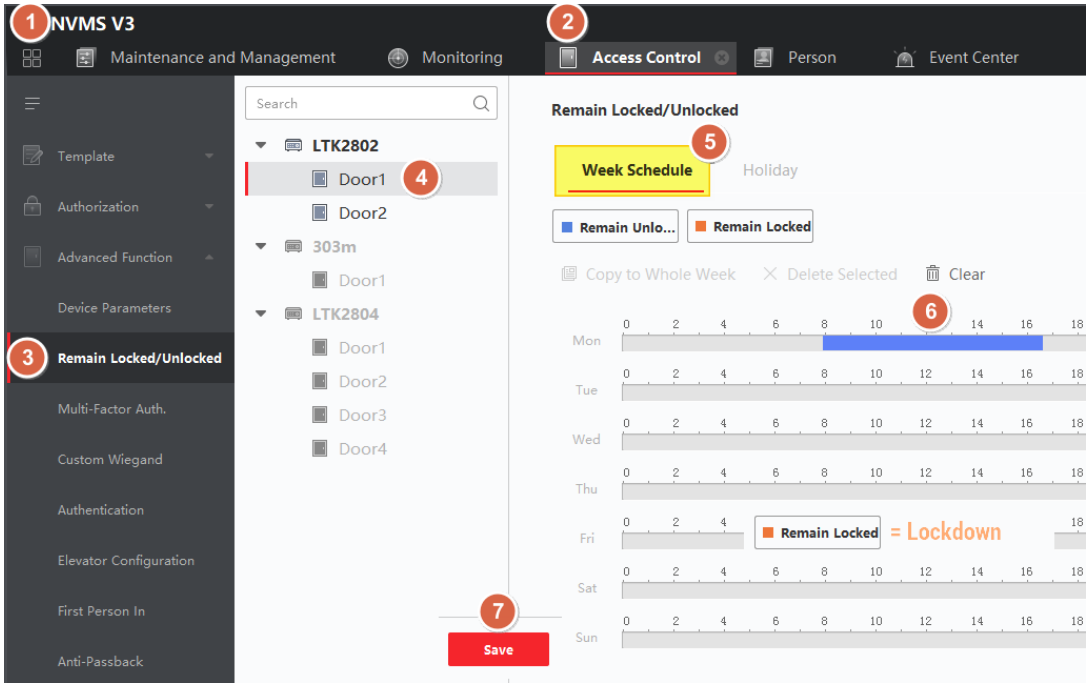
Advanced Function

Remain Unlocked

If you wish to automatically open the door by schedule, you can use the Remain Unlocked feature.

1. Main Menu
2. Access Control
3. Advanced Function
   Remain Locked/Unlocked
4. Select Door
5. Select by Week or by Holiday
6. Define the time action.
7. Save

Please be aware that, the remain locked = lockdown. That means even if you have the correct keycard, you are still not able to open the door.



Device Parameters

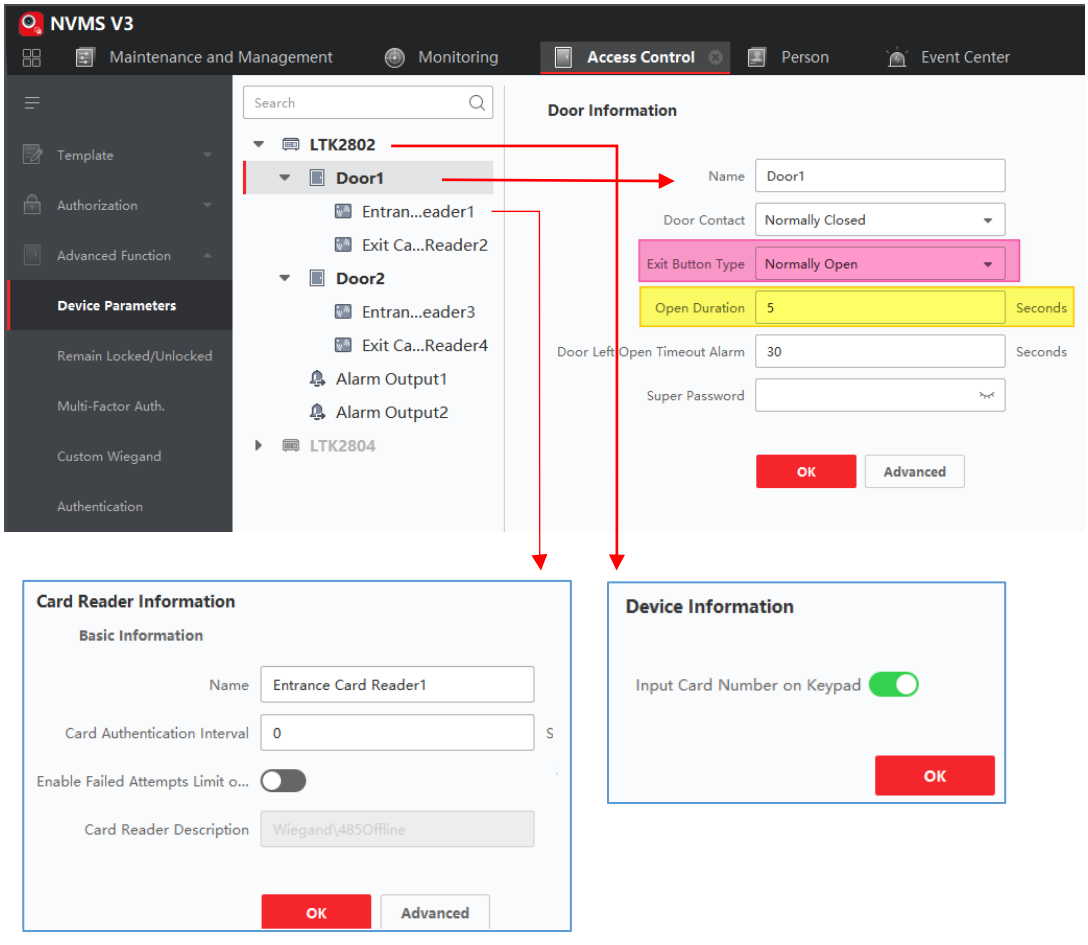
If you want to extend the open-Door duration, you can set up from here.

Open Duration – 5sec by default

Exit Button Type:
If you need to reverse the Exit button, you also can change the type from here.
NO (Normally Open) as default.

Door Contact (aka Door Sensor) –
if you have this, you can change the type from here.

Super Password can bypass any permission and grant access. Even the door is set to Remain Closed.



Other References:

Input Card Number on Keypad (ON)
if you don't allow to manually input the card number, you can set to OFF

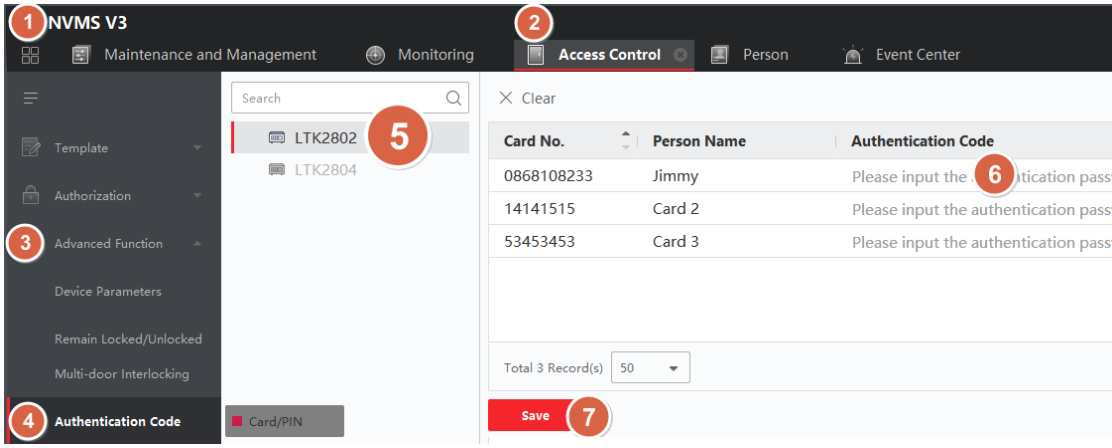
If you only allow swiping the card for few times, you can enable
Failed Attempts Limit….

Door Access Code mapping (Card/PIN)

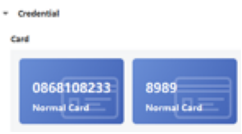
If you want to use Punching number to access, you can use this Authentication Code function. (aka Card/PIN)
What is the Card/PIN, will explain it later…

You need to match the real card number with this Punch code.

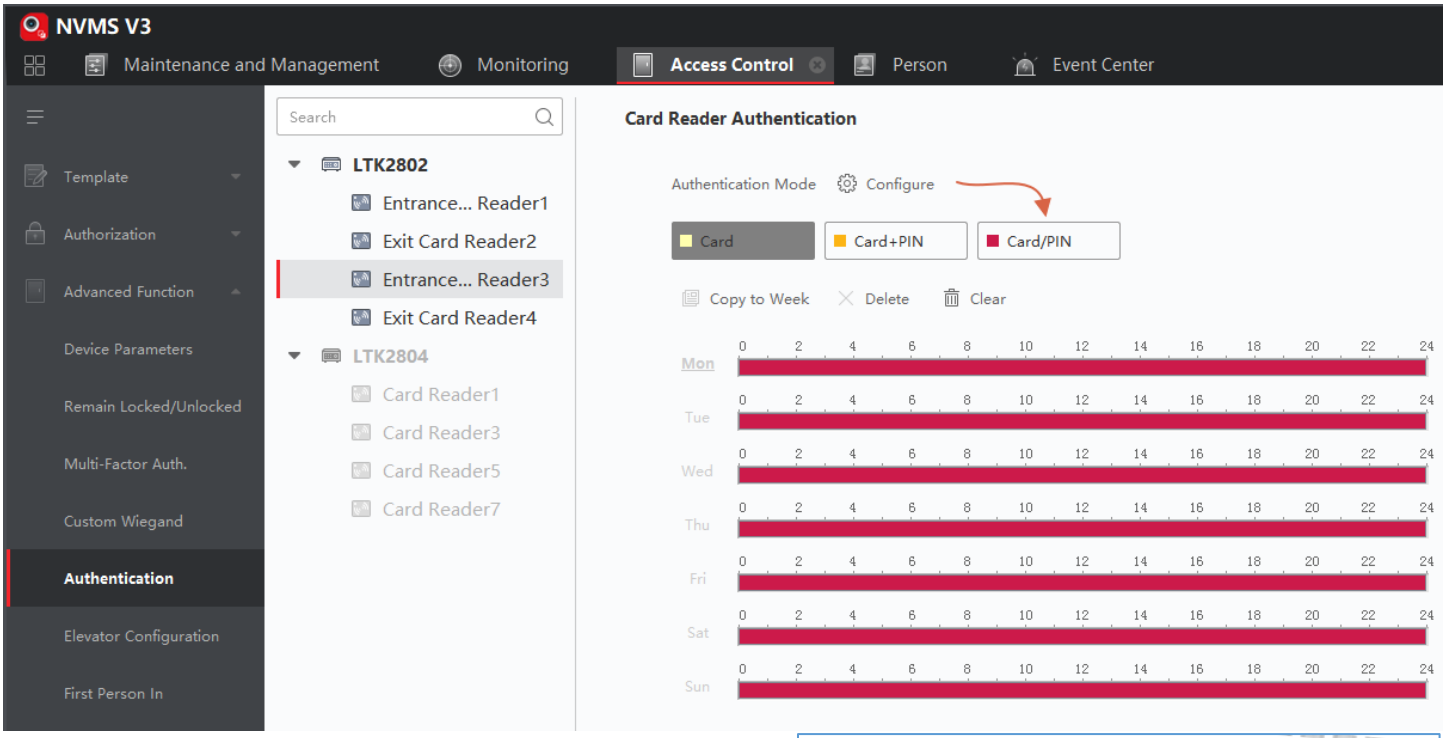
(5) is bigger, because it will refresh the list.
Please don't use Clear. It will erase all.



Here is another way which I **recommend**. Just going to assign a new Card (manual input) person as the punch number. It is easier and better to manage.

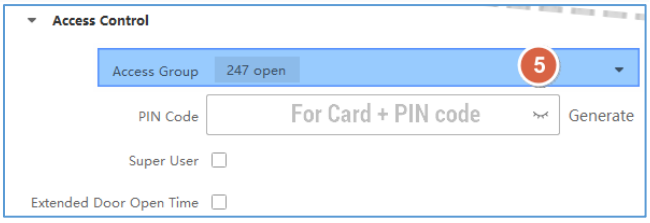


Card Reader Authentication Schedule



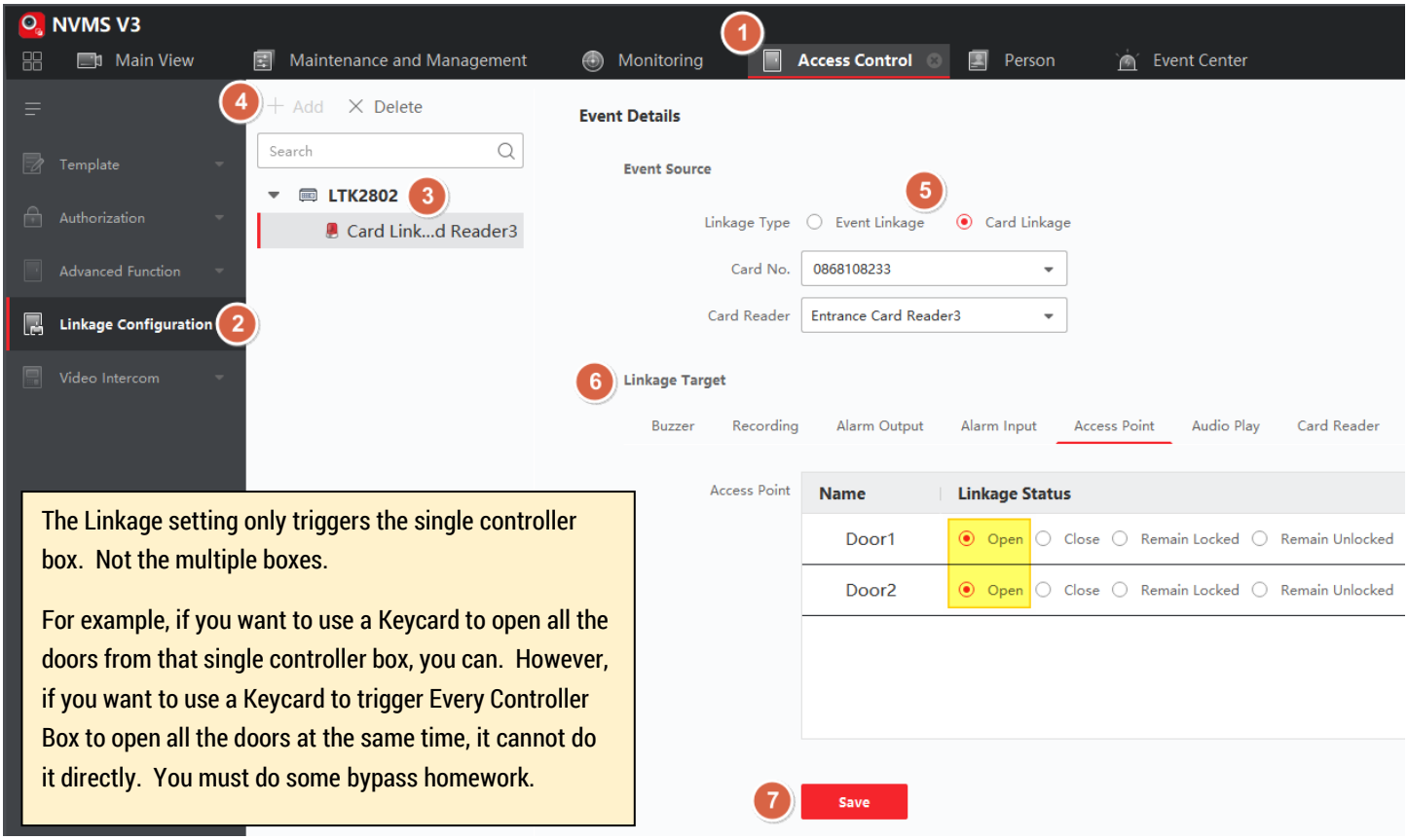
Understand what is the (Card + PIN) and (Card/PIN).

Card + PIN = Swipe Keycard first, then enter the Pin number.
Double Authentication. It will check for access.
(Full picture see Person section, Page 16)



Card/PIN = Swipe the Keycard or enter the Authentication Code to check for access.

Multiple Open Door Linkage Configuration (Support 2802 / 2804 only)



The Linkage setting only triggers the single controller box. Not the multiple boxes.

For example, if you want to use a Keycard to open all the doors from that single controller box, you can. However, if you want to use a Keycard to trigger Every Controller Box to open all the doors at the same time, it cannot do it directly. You must do some bypass homework.

The Linkage Configuration is designed for variation trigger purpose. **(Make sure upgrade NVMSv3 to 2023)**
It is only suitable for the 28xx devices, not for the Intercom 303 or 401 devices.

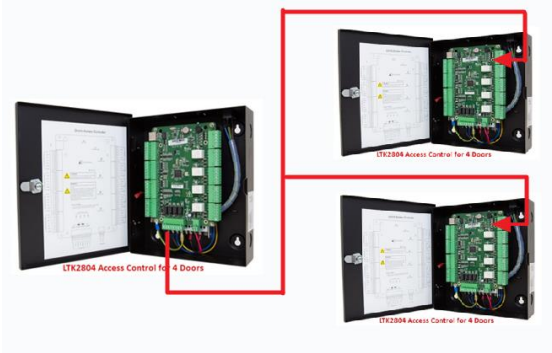
For example, when there is a fire-alarm input triggered. You can tell the controller box to open all the doors at the same time.

Follow the Step 1,2,3,4… **Make sure you selected the Device (3) before you click Add (4)**
Then, you should be able to Add the Linkage Event.
Remember, this section doesn't like many major modifications. If you try to change Event Type or you notice the setting can't be saved. Please Create a New one instead.

Open All Controller Doors Example

Keyword: you need to combine the Alarm Input Feature together.

For example, you setup the Card# from the Reader.
Linkage Target: you need at least Setup 3 actions.



1. Set the Access Point to open all doors for this controller box,

2. You also need to trigger the alarm output. And the alarm output wires is physically connected to another controller box alarm input.

3. Then, for the other controller box, you need to define when the alarm input has been triggered to open all the doors for this controller box.

Link Door to the Camera (or Link Event with Camera for the Log)

There are two different topics/things linking to the events.

1. Link the Door to a certain Camera.
   So, you can see who is calling and manually open the door for them.

2. Link the Event with Camera.
   Capture a picture when Unlock door is happened.
   So, you can search/link the Log to see who is accessing after.

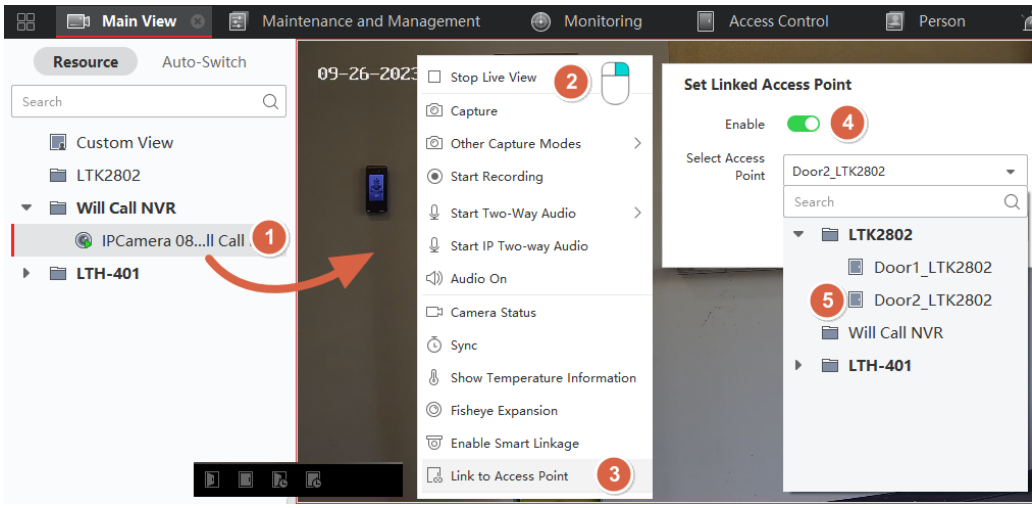
1. Open Door from Camera

1. Open the Main View, display a camera first.

2. Mouse Right click on top of the video
3. Select Link to Access Point.

4. Enable it
5. Select the Correspond Door.

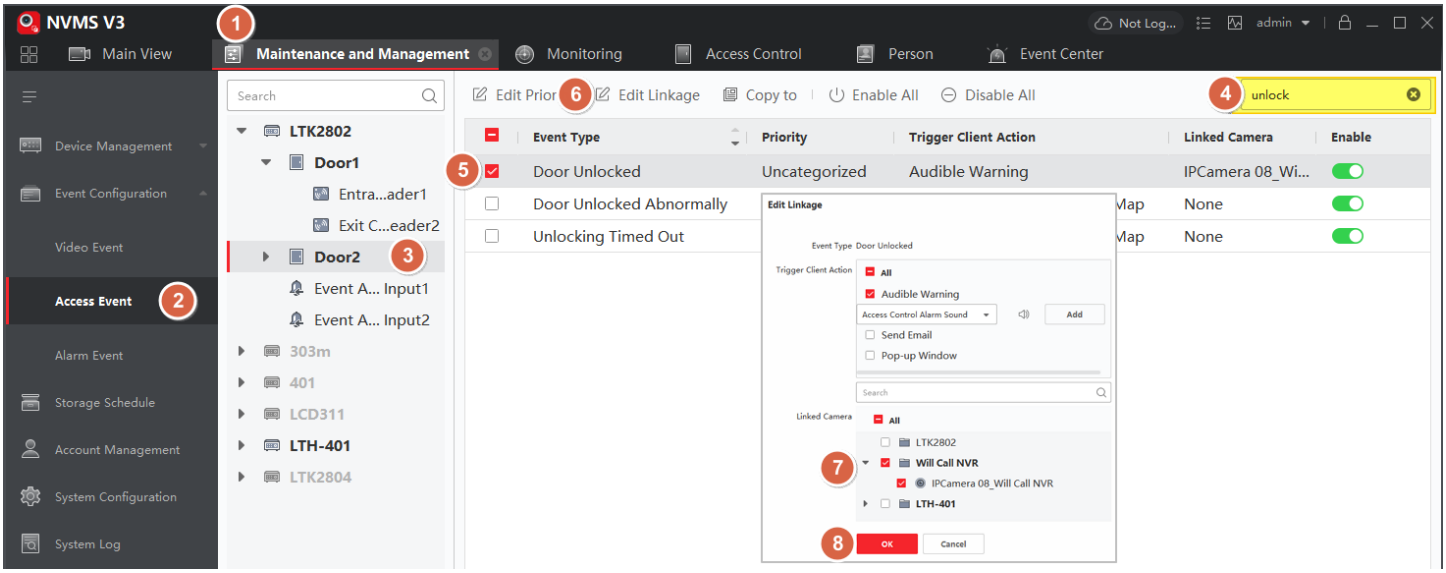
6. **After that,** make sure you **close** the video and re-open the video again.



7. Then, you should see couple door icons at the bottom bar.

2. Link the Event with Camera snapshot

Follow the picture steps first. (4) will help you faster locate the event you focus on. After you complete 1~8, the camera should be linked.

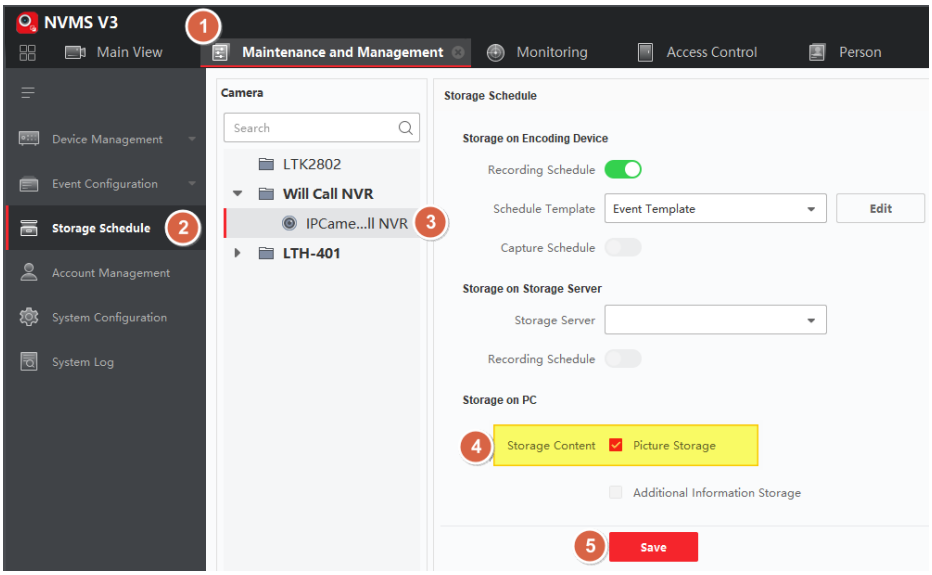


Enable Picture Storage

Follow the Steps from the Picture.

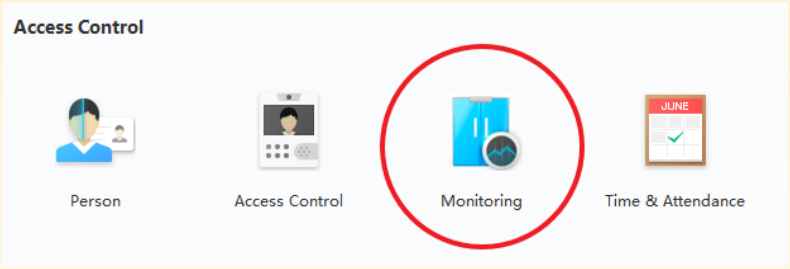
After it is set.

When the event is triggered, it will save an image to this PC and Log should be able to display the moment.



Monitoring (Realtime Monitoring)

Go to **MENU > Monitoring.**
You can Unlock/Lock the door from here.
Also, you can monitor who is/was currently access the device; or monitor which key card is accessing and thru which door.



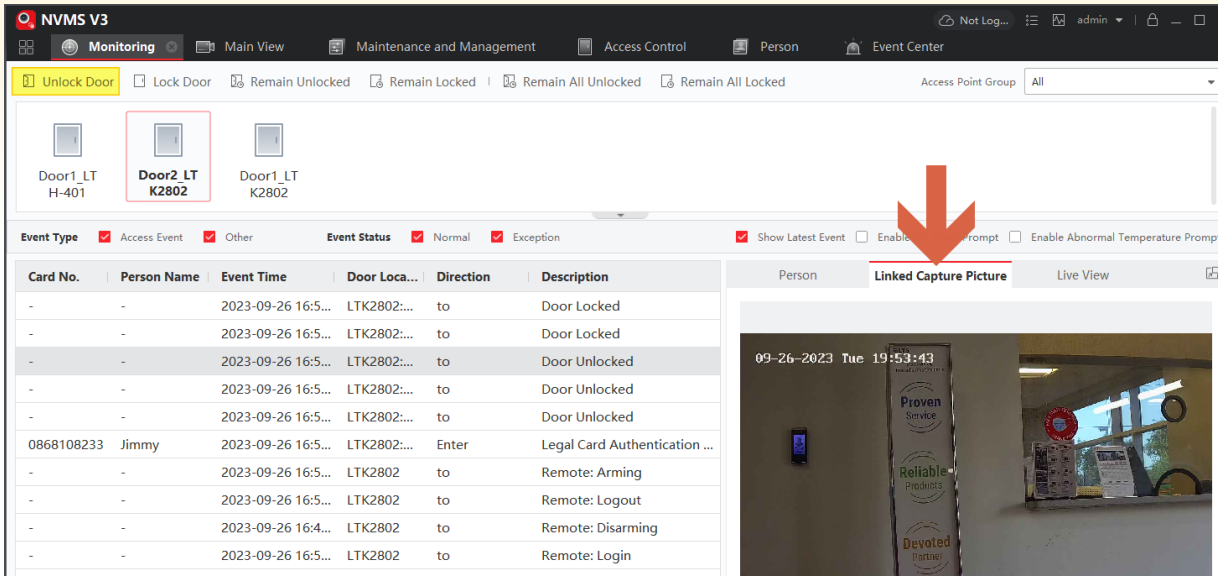
To Unlock Door:

Select Door first,
then click

Unlock Door at the top.

If you set up the Camera Link Event and Picture Storage.

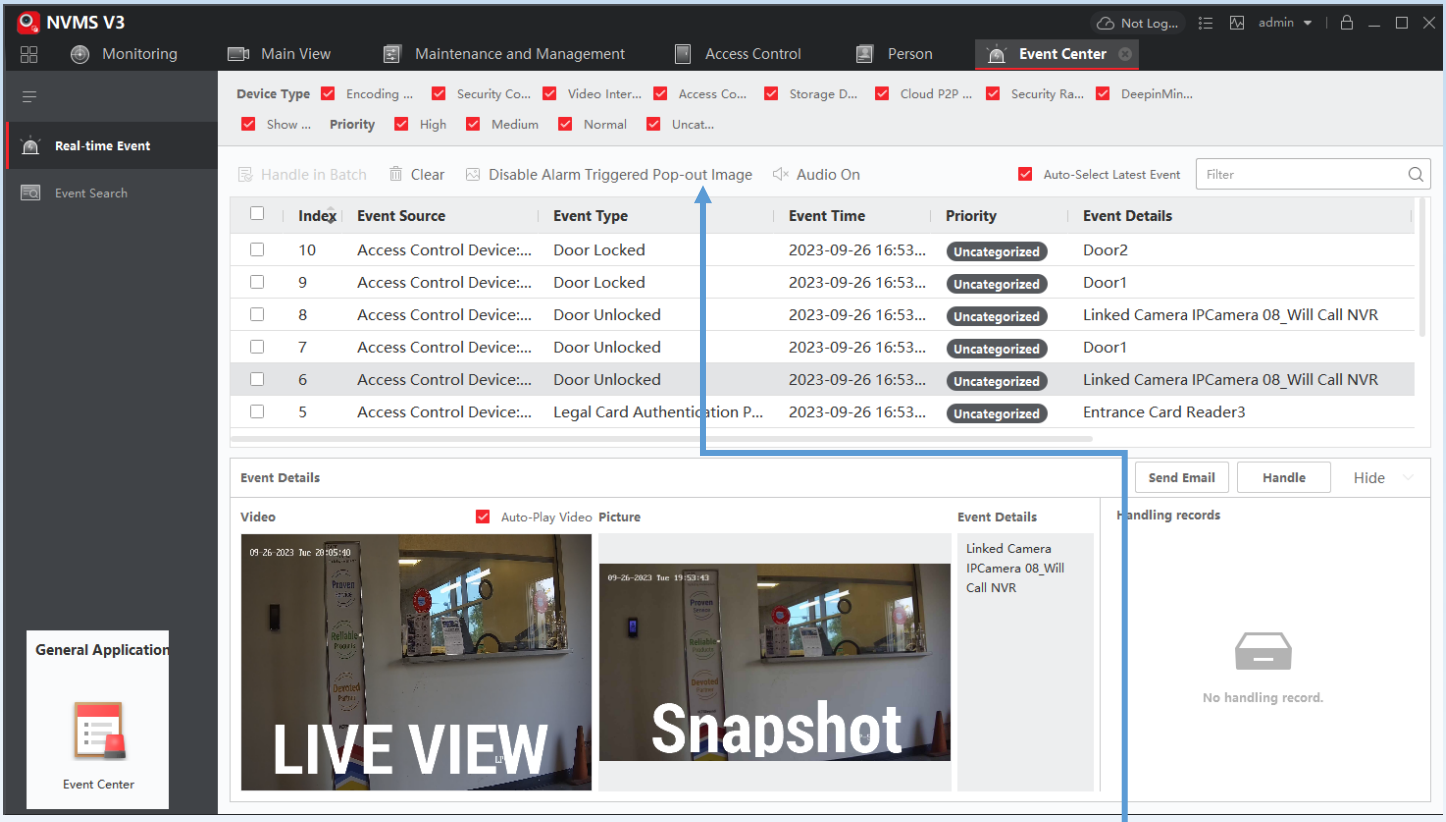
Then you should be able to see the snapshot took now.



Note: These logs will disappear after awhile or when you re-open the NVMSv3 will be trunked. You can use the Event Search to find out more details.

Event Center

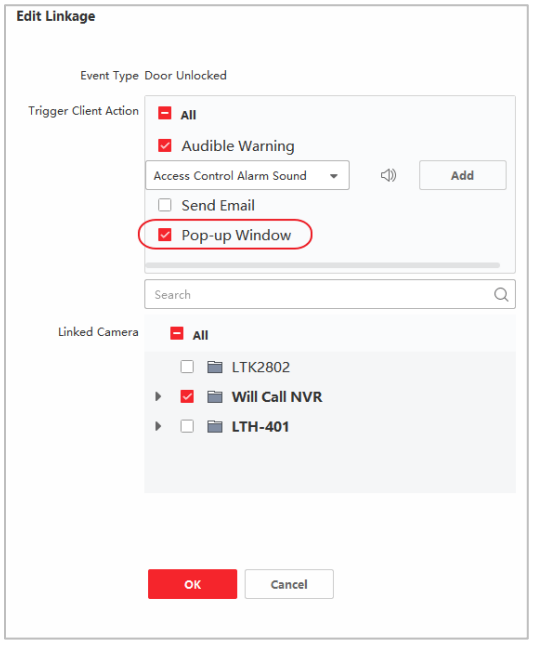
Real Time Event

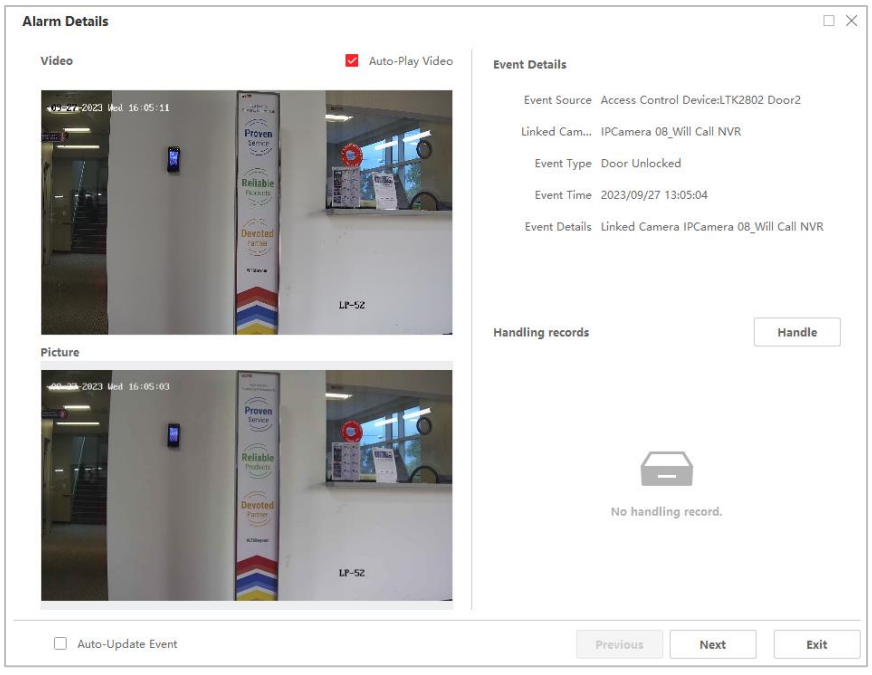


Event Center has two functions: Real time Event, Event Search.

The real-time event is pretty much the same as the monitoring. But mainly its more focus on the filter and more details to present the log.
You can use the filters at the top to narrow down the search Current Logs from here. Theoretically, this Realtime Event should contain more rows than the Monitoring windows.

Pop up Window

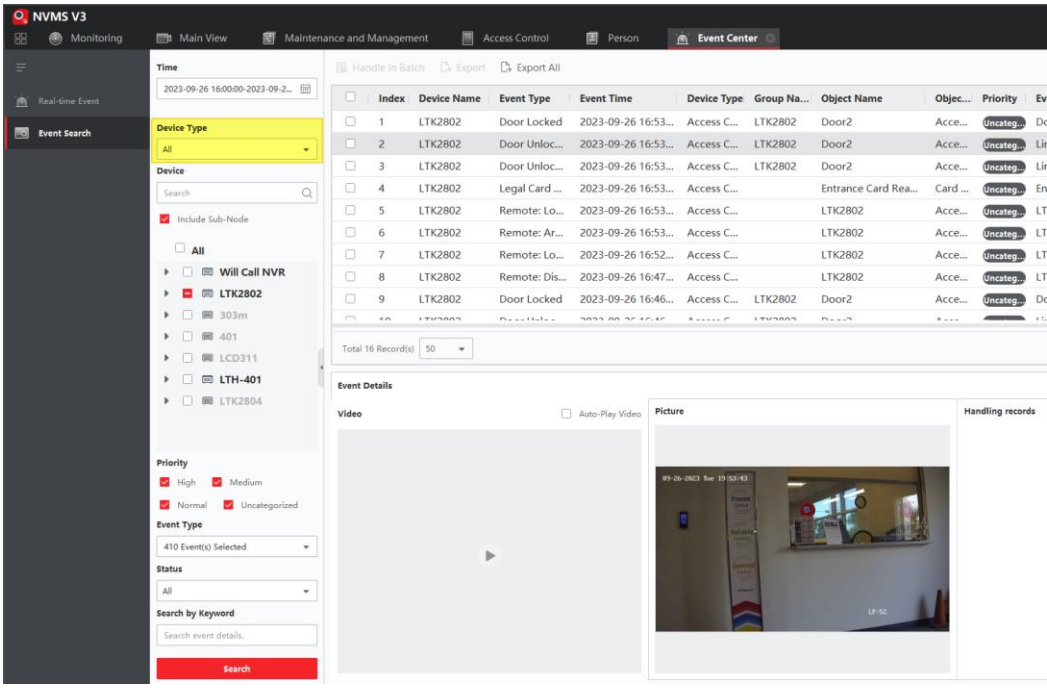




Event Search

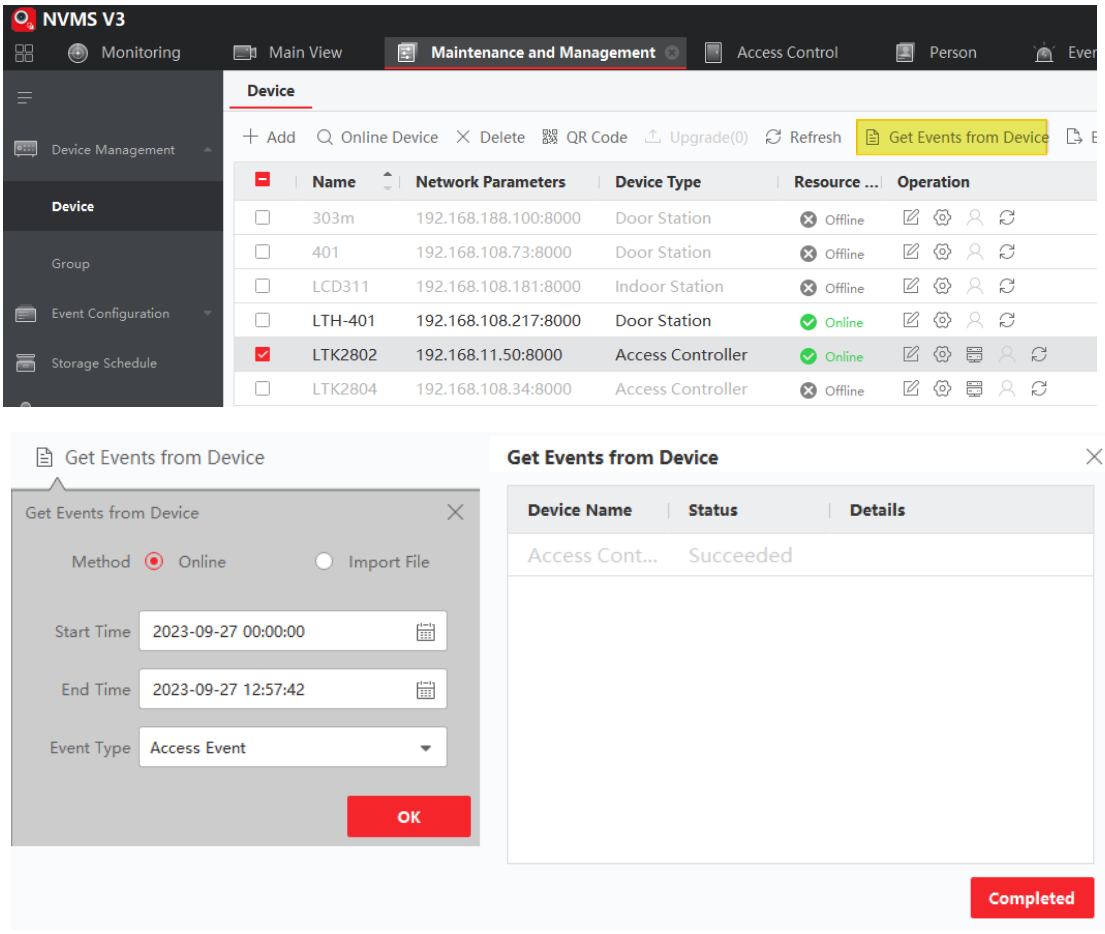
If you are looking for the card# search, please choose **Access Control**.

If you are looking for the linking Picture, please choose **ALL**



Re-Collect Data/Logs from the Controller

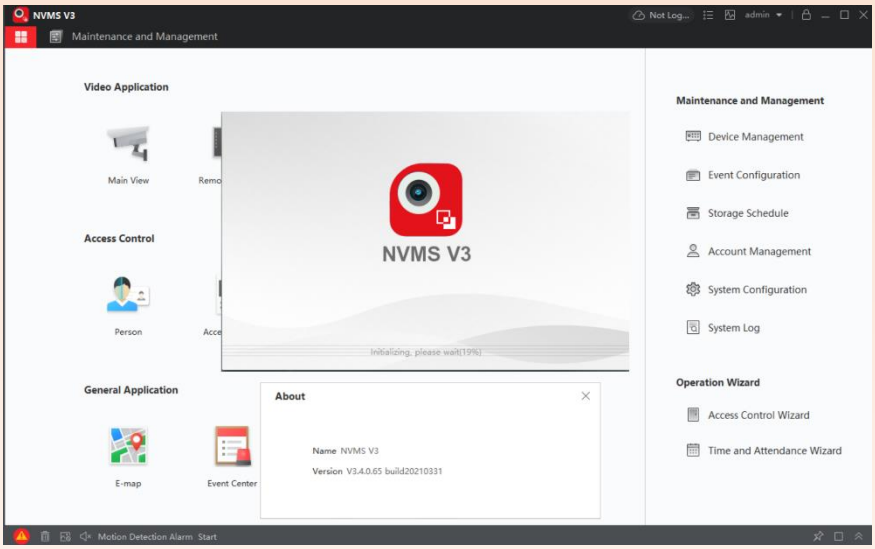
Normally, the NVMSv3 software will continue to monitor the controller box and all the transactions will be recorded in the PC. However, sometime if someone turns off the PC. Then you need to retrieve the log from the controller box.



BACKUP

Access Control Client Software:

NVMSv3



Backup Database

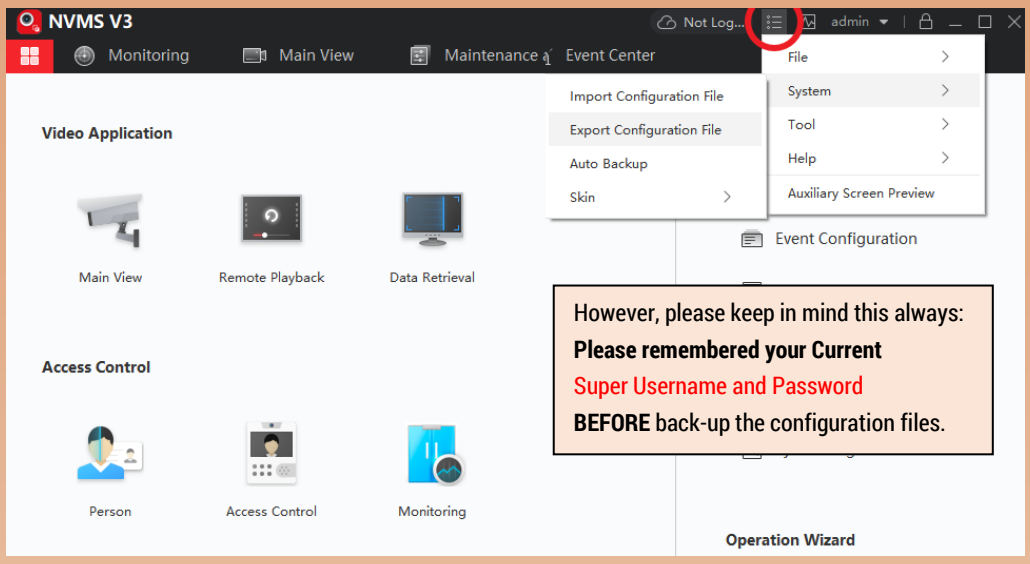
After you apply the access group to the controller box, it will remember this setting, but you will not be able to pull out of the controller. So it is very important for you to back up the database.

Export Configuration

Go to the Menu > System > Export Configuration

Select folder and setup a backup name.
That should do it.

The Config file should be a Zip file.

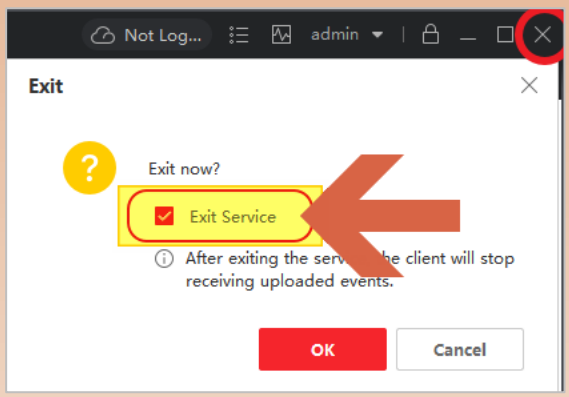


Import Configuration

WARNING : Import Configuration will overwrite/erase your current configuration file after restart.

Go to Menu > System > Import Configuration > Select File, OK

Now, you need to **Exit the NVMSv3** and run again to Load with the Restored Configuration. Make sure you select Exit Service. Otherwise, it won't work.

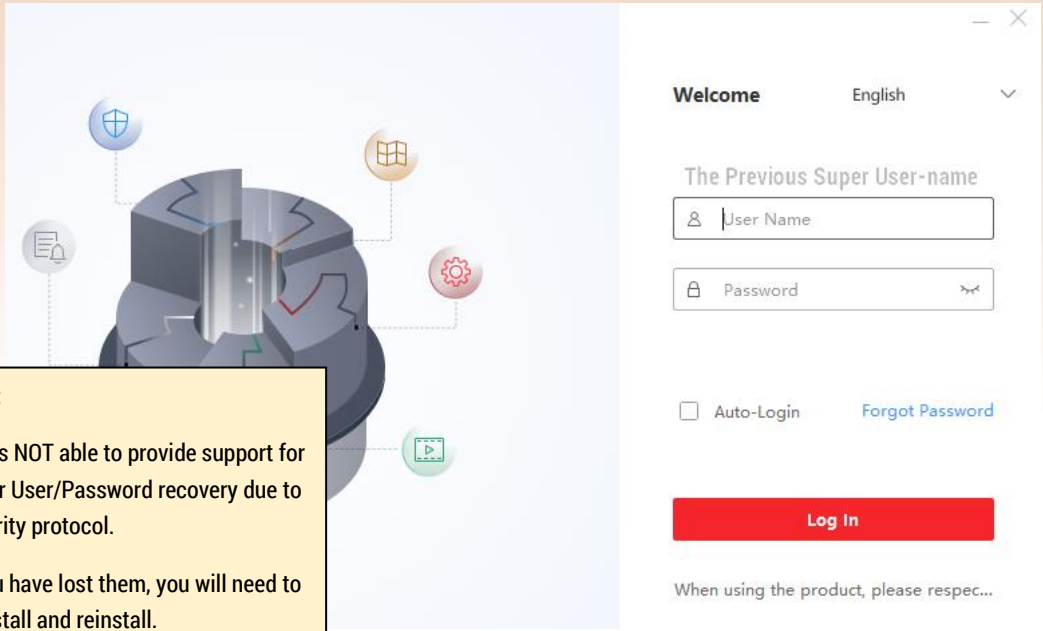


After restarting the NVMSv3, it should ask you to Login again.

Please enter the information from previous Configuration

Enter
Super User-name and Password
to Log in.

Then the NVMSv3 just like the way it was before.



Note:

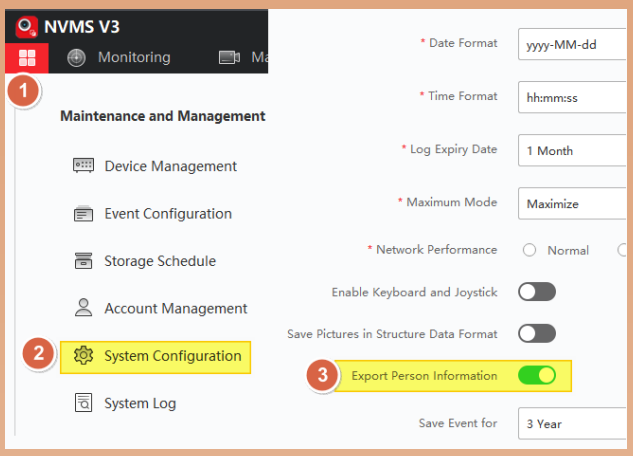
LTS is NOT able to provide support for Super User/Password recovery due to security protocol.

If you have lost them, you will need to uninstall and reinstall.

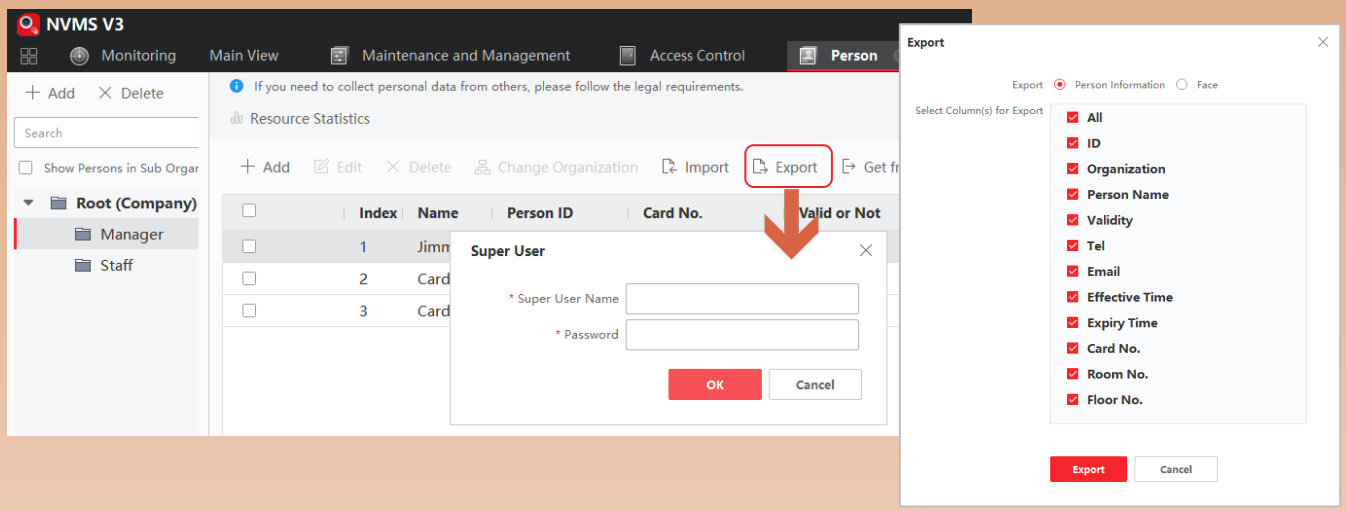
Export Person to an Excel file

If you can't find the **Export button**, please go to

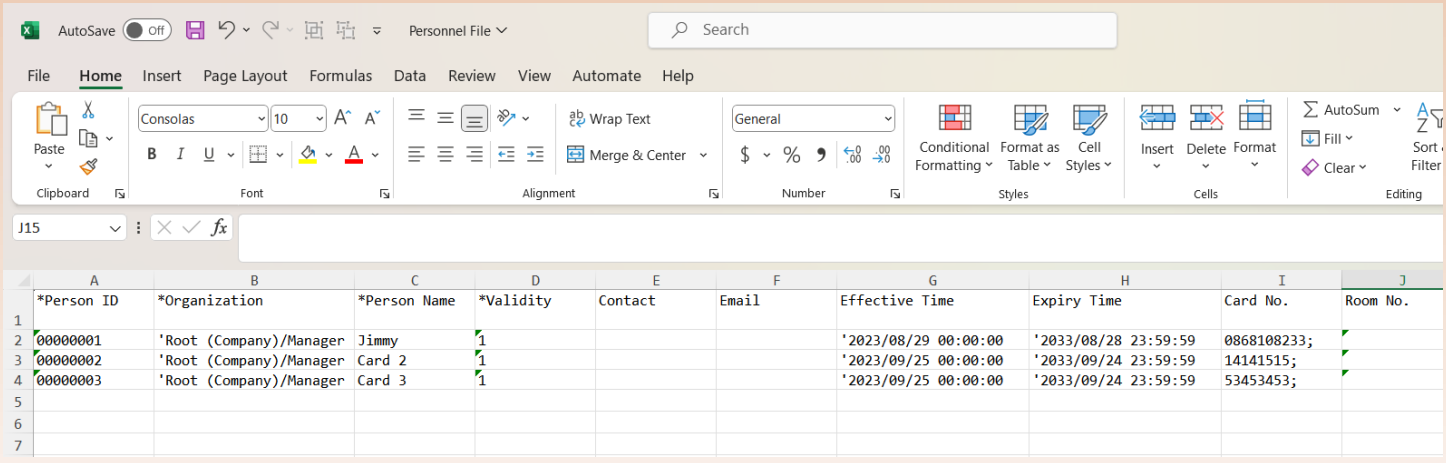
the System Configuration > turn on Export Person Information.



Steps



Example Excel file. Please remember the table format must be exactly same and Person ID and Card No CANNOT duplicated



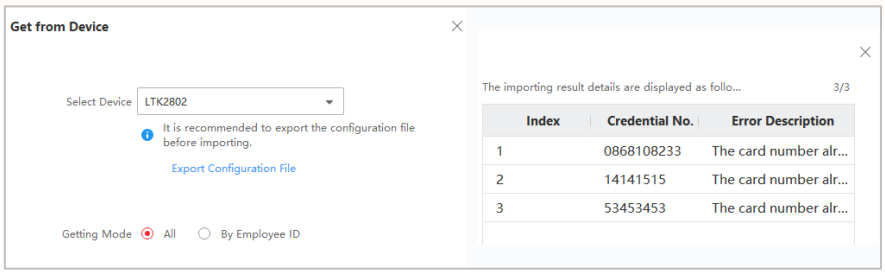
	A	B	C	D	E	F	G	H	I	J
1	*Person ID	*Organization	*Person Name	*Validity	Contact	Email	Effective Time	Expiry Time	Card No.	Room No.
2	00000001	'Root (Company)/Manager	Jimmy	1			'2023/08/29 00:00:00	'2033/08/28 23:59:59	0868108233;	
3	00000002	'Root (Company)/Manager	Card 2	1			'2023/09/25 00:00:00	'2033/09/24 23:59:59	14141515;	
4	00000003	'Root (Company)/Manager	Card 3	1			'2023/09/25 00:00:00	'2033/09/24 23:59:59	53453453;	
5										
6										
7										

Import Person from Excel

it will override your current exist person and it might break the Access Group. Please use it carefully.

Get from Device

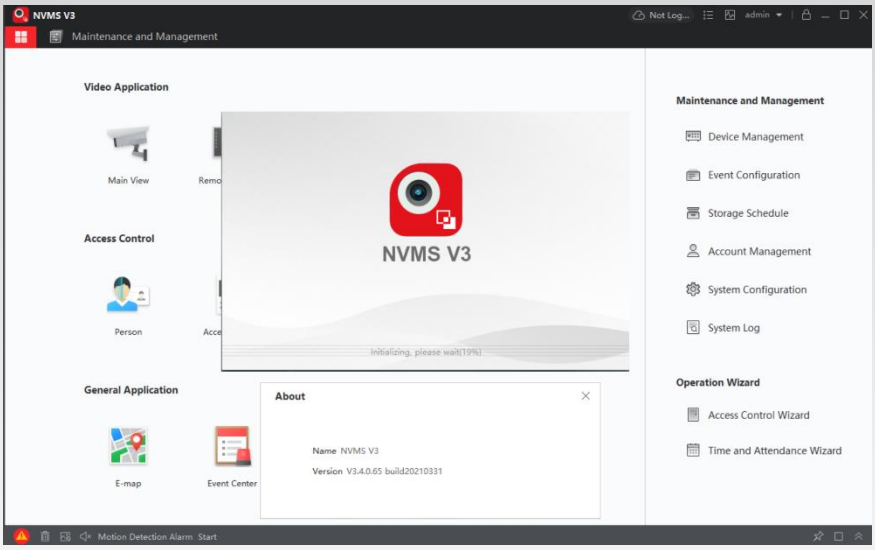
It will try Pull back Card# from the Controller and import it back to the Person database. If there is already an exist person, it will not be imported.



APPENDIX

Access Control Client Software:

NVMSv3

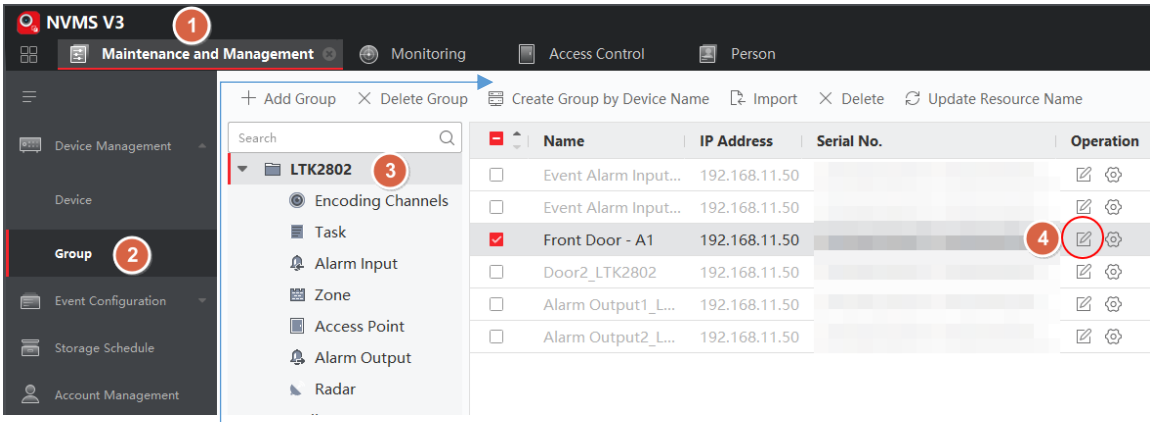


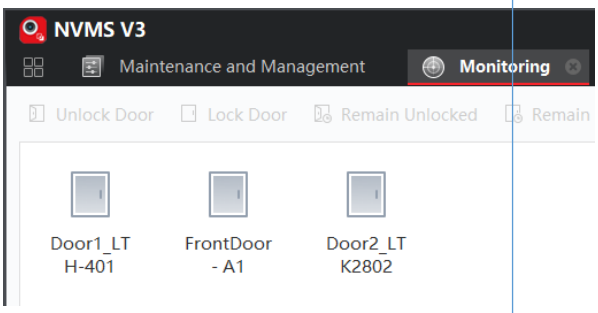
How to Rename the Door-name?

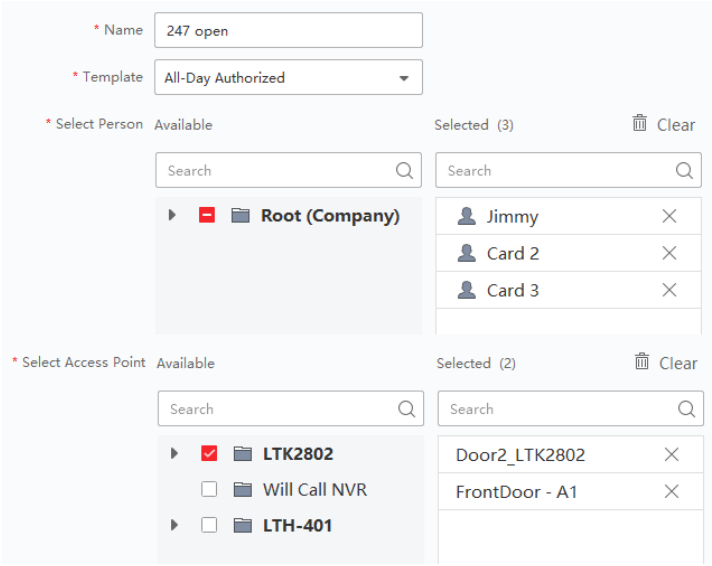
Most of the time, the User likes to see the corresponding Door-name.

You can change it from the Device Management > Group

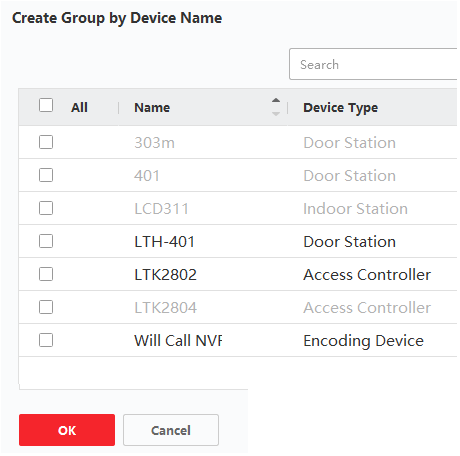
After you modify it, the Monitoring and Access Group will change the name also.







If you have the Device Group is not created, please use the **Create Group by Device Name** button.



Anti Passback (prevent same Keycard access Twice)

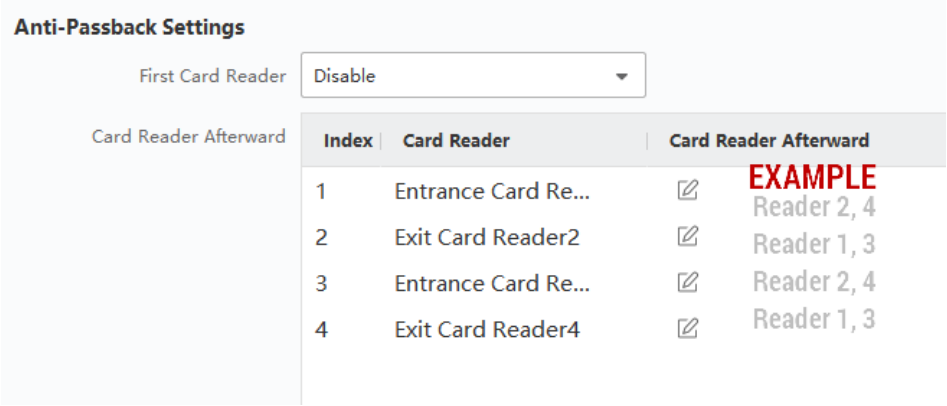
Anti Passback is designed for someone trying to access in the correct sign In and sign out.

In other words, if someone uses their keycard to access door 1 reader 1 (sign in).
The keycard will be registered in Used status.

If someone tries to use the same card to access Door 1 Reader 1 again, access will be denied.

Until the person tries to use the same keycard, Access Door 1 Reader 2 (for example) to Exit and sign out.

Release the keycard in Use status.
The keycard will then return-back to normal status.



Another word, if you exit without sign out, the key card will no longer work anymore.
Either you need to create a new keycard, or you have to wait for 1 day to reset or reboot the controller box.

Multi-Door Interlocking (aka Mantrap)

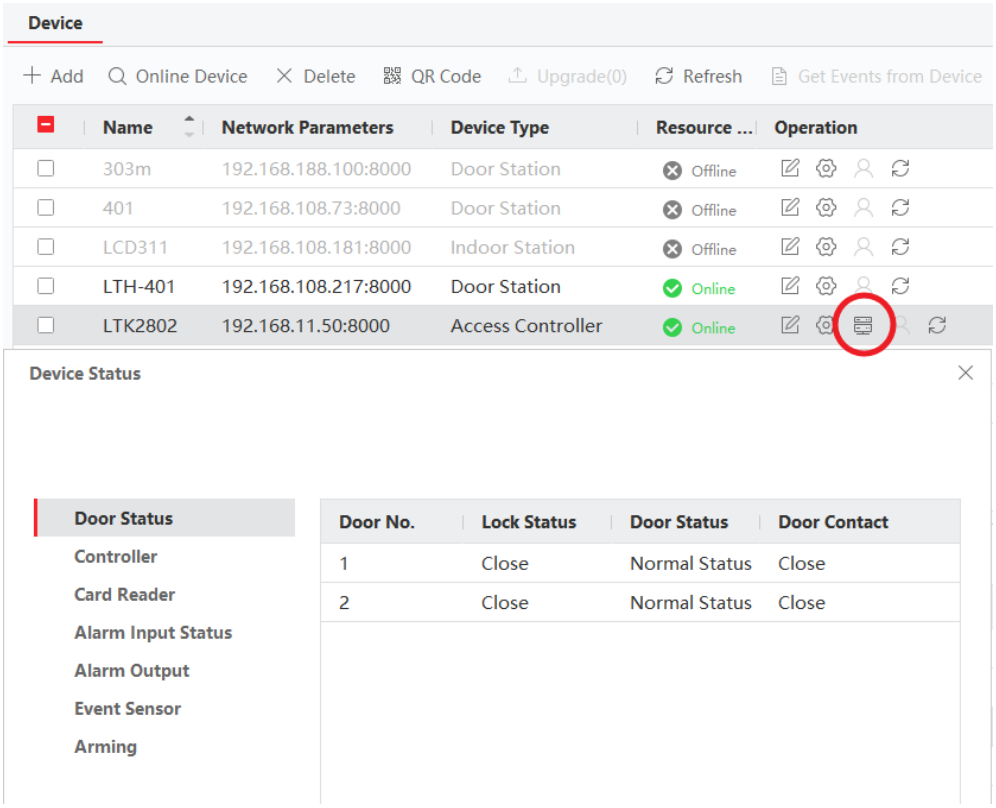
Multi Door Interlocking requires a specific Door Controller model to be supported.

As far as I know, we didn't carry that model.

Multi-Door Interlocking means that you must close a certain door first,

then you can open another door with a different reader.

Device Status



Event Backup Export Configuration from the NVMSv3