

InfraSolution[®] Z-3001

Rack Access Control



User Manual



Simple. Flexible. Compact



Rack access control has become critically important for all data centers and server rooms.

InfraSolution Z-3001 access control solution not only meets the high level of rack access security but also supports POE to reduce the implementation time and expense of having electrical power cabling installed. Moreover, the compact Z-3001 control box is compatible to a variety of rack handle packages which allows the flexible and simple integration to different kinds of IT server racks.

**AUSTIN
HUGHES[®]**

Legal Information

First English printing, March 2025

Information in this document has been carefully checked for accuracy; however, no guarantee is given to the correctness of the contents. The information in this document is subject to change without notice. We are not liable for any injury or loss that results from the use of this equipment.

Safety Instructions

Please read all of these instructions carefully before you use the device. Save this manual for future reference.

- Unplug equipment before cleaning. Don't use liquid or spray detergent; use a moist cloth.
- Keep equipment away from excessive humidity and heat. Preferably, keep it in an air-conditioned environment with temperatures not exceeding 40° Celsius (104° Fahrenheit).
- When installing, place the equipment on a sturdy, level surface to prevent it from accidentally falling and causing damage to other equipment or injury to persons nearby.
- When the equipment is in an open position, do not cover, block or in any way obstruct the gap between it and the power supply. Proper air convection is necessary to keep it from overheating.
- Arrange the equipment's power cord in such a way that others won't trip or fall over it.
- If you are using a power cord that didn't ship with the equipment, ensure that it is rated for the voltage and current labelled on the equipment's electrical ratings label. The voltage rating on the cord should be higher than the one listed on the equipment's ratings label.
- Observe all precautions and warnings attached to the equipment.
- If you don't intend on using the equipment for a long time, disconnect it from the power outlet to prevent being damaged by transient over-voltage.
- Keep all liquids away from the equipment to minimize the risk of accidental spillage. Liquid spilled on to the power supply or on other hardware may cause damage, fire or electrical shock.
- Only qualified service personnel should open the chassis. Opening it yourself could damage the equipment and invalidate its warranty.
- If any part of the equipment becomes damaged or stops functioning, have it checked by qualified service personnel.

What the warranty does not cover

- Any product, on which the serial number has been defaced, modified or removed.
- Damage, deterioration or malfunction resulting from:
 - ☐ Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
 - ☐ Repair or attempted repair by anyone not authorized by us.
 - ☐ Any damage of the product due to shipment.
 - ☐ Removal or installation of the product.
 - ☐ Causes external to the product, such as electric power fluctuation or failure.
 - ☐ Use of supplies or parts not meeting our specifications.
 - ☐ Normal wear and tear.
 - ☐ Any other causes which does not relate to a product defect.
- Removal, installation, and set-up service charges.

Regulatory Notices Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in business, industrial and commercial environments.

Any changes or modifications made to this equipment may void the user's authority to operate this equipment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-position or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Notice : The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.

Contents

< Part. 1 > Hardware

1.1	Package Contents	P.1
1.2	Hardware Specification	P.2
1.3	Installation Diagram	P.3
1.4	Handle (Z-800P / Z-800M) Installation	P.4
1.5	Door Sensor Installation	P.15
1.6	Key Features	P.19
1.7	Meter (PDU) Level Setting	P.20
1.8	PDU Daisy Chain Connection	P.20
1.9	Expansion Fan Units Level Setting	P.21
1.10	Fan Daisy Chain Connection	P.21

< Part. 2 > Initial Installation and Configuration

2.1	Connecting the Z-3001 to a Power Source	P.22
2.2	Connecting the Z-3001 to a computer	P.23
2.3	Connecting the Z-3001 to your Network	P.24
2.4	Configuring the Z-3001	P.24

< Part. 3 > Using the Web Interface

3.1	Supported Web Browser	P.25
3.2	First Time login	P.25
3.3	Rack Access	P.27
3.4	Rack Power	P.30
3.5	Rack Airflow	P.33
3.6	Rack Sensor	P.35

< Part. 4 > System

4.1	Network	P.36
4.2	Date & Time	P.39
4.3	Authentication	P.40
4.4	Service	P.42
4.5	Notification	P.46
4.6	Maintenance	P.48

< Part 1 > Hardware

< 1.1 > Package Contents

Unpacking

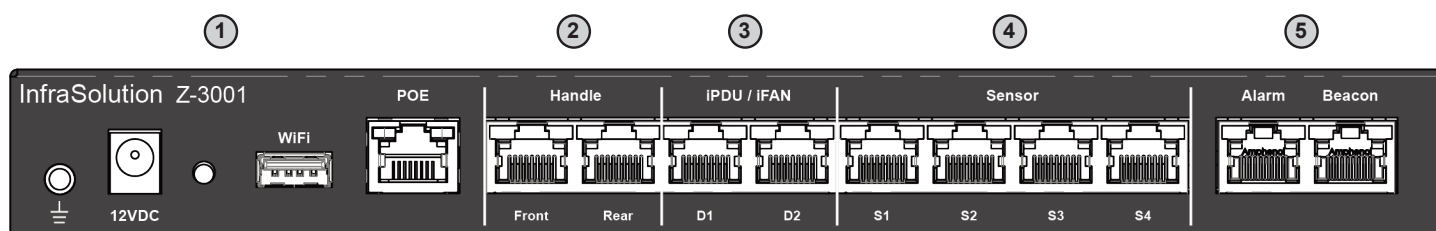
The equipment comes with the standard parts shown on the package contents. Check and make sure they are included and in good condition. If anything is missing, or damage, contact the supplier immediately.

Package Content

- InfraBox x 1
- Smartcard Handle x 2
- Door Sensor x 2
- SmartCard x 1
- Handle Key x 1
- Power adaptor x 1
- Mounting kit x 1
- Handle mounting screw set x 1



Intelligent Rack Access Control Solution



①

Network & Power Connection

- **PoE (Power over Ethernet) :**
Connect to PoE switch for network IP access & power.
- **USB WIFI Port :**
Optional WIFI kit connection
- **Alternative 12VDC :**
If PoE power connection unavailable

②

Smart Handle Connection

- **Z-700 smart access control package :**
Swing handles + door sensors + control panel(s)
or
- **Z-800 smart access control package :**
Handles + door sensors

③

iPDU & iFAN Connection

- **Intelligent PDU :**
1-Phase & 3-Phase PDUs
 - **Intelligent Fan :**
Door mount fan & 1U fan tray
- * iPDU and iFan support cascading up to 4 respectively

④

S1 / S2 / S3 / S4 – Sensor Connection

- **Temperature & Humidity Sensor :**
Low profile design with magnetic base to affix to rack
(2m or 4m)
- **Temperature Sensor :**
Low profile design with magnetic base to affix to rack
(2m or 4m)
- **Smoke Sensor :**
Once triggered, red LED lights up with continuous
beep sound (1m or 3m)
- **Shock Sensor :**
Alert the physical vibration on the rack (1m or 3m)
- **Water Sensor :**
Via 5M rope round the rack bottom, detect any fluid
leakage (3m)

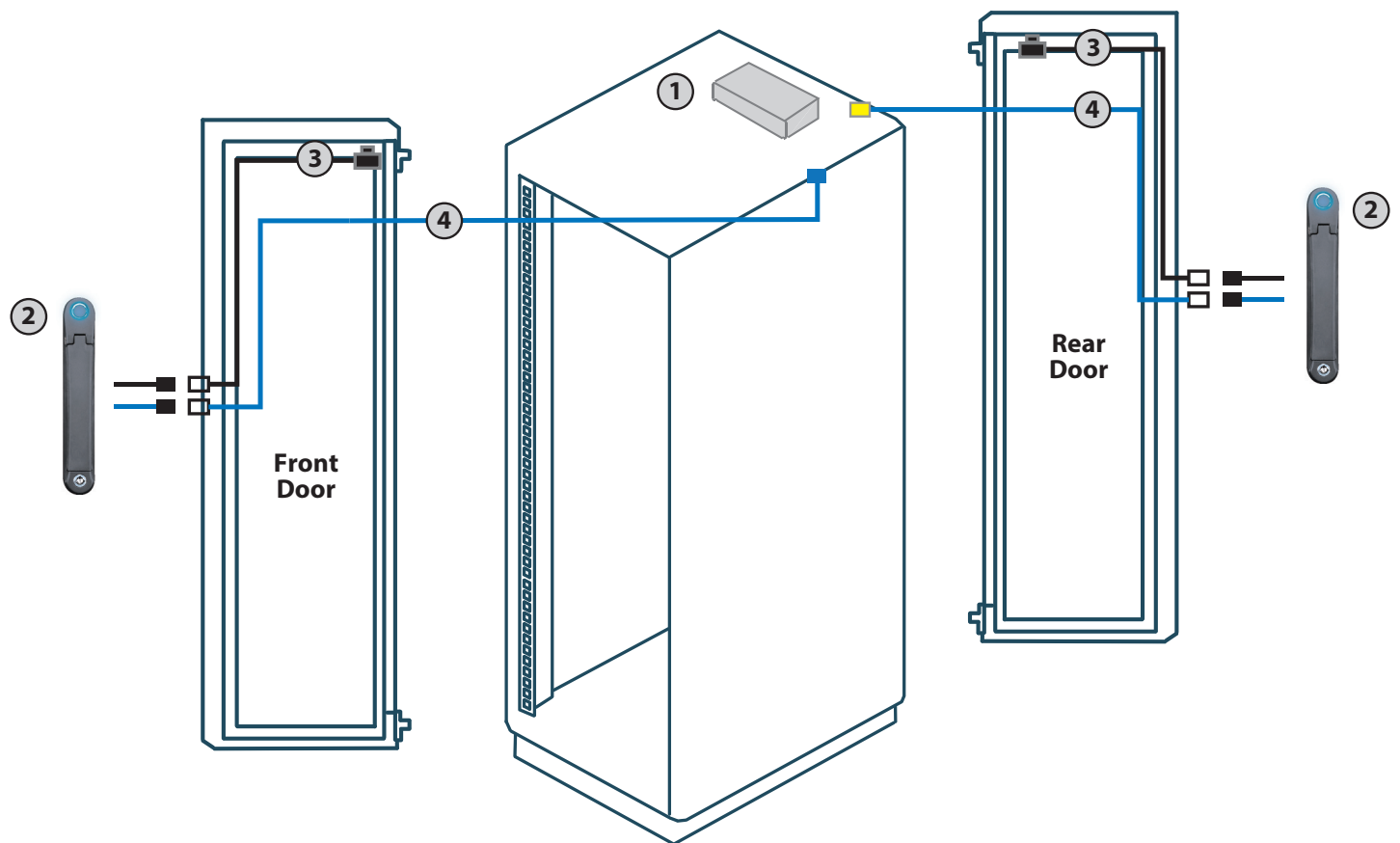
⑤

Alarm & Beacon

- **Alarm :**
Connect to 3rd party alarm system
- **Blue LED Beacon :**
Alerting user to alarm status (1m or 3m)

Product Dimension (W x D x H)	260 x 80 x 30 mm
Packing Dimension (W x D x H)	375 x 259 x 107 mm
Net / Gross Weight	2.35 kg (5.17 lbs) / 2.85 kg (6.27lbs)
Power Consumption	12VDC, 2.5A, max. 30W
Operating Temperature	0° to 55°C Degree
Storage Temperature	-5° to 60°C Degree
Relative Humidity	5~90%, non-condensing
Mounting	Side mount kit x1, rackmount kit x1
Safety Regulatory	FCC & CE certified
Environmental	RoHS2 & REACH compliant by SGS

< 1.3 > Installation Diagram



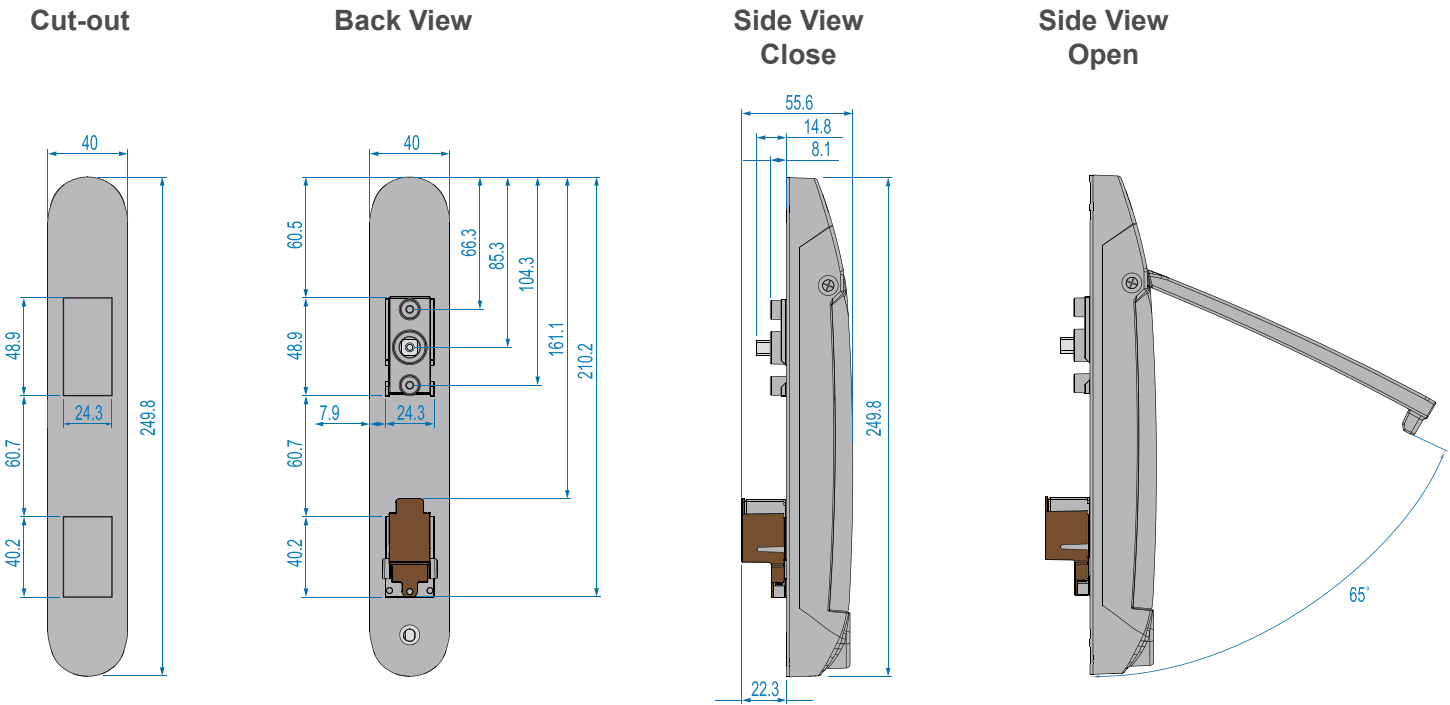
- ① InfraBox Z-3001
- ② Smartcard handle
- ③ Mechanical or IR door sensors with 6ft cable
- ④ Door cable

< 1.4 > Handle (Z-800P / Z-800M) Installation

Universal Mounting Cut-out

To achieve the highest level of interoperability offered in the rack industry, the Z-800 handle applies the universal mounting cut-out. It avoids costly and complicated door customization for the smartcard handle integration.

Unit : mm



Models of left / right side opening

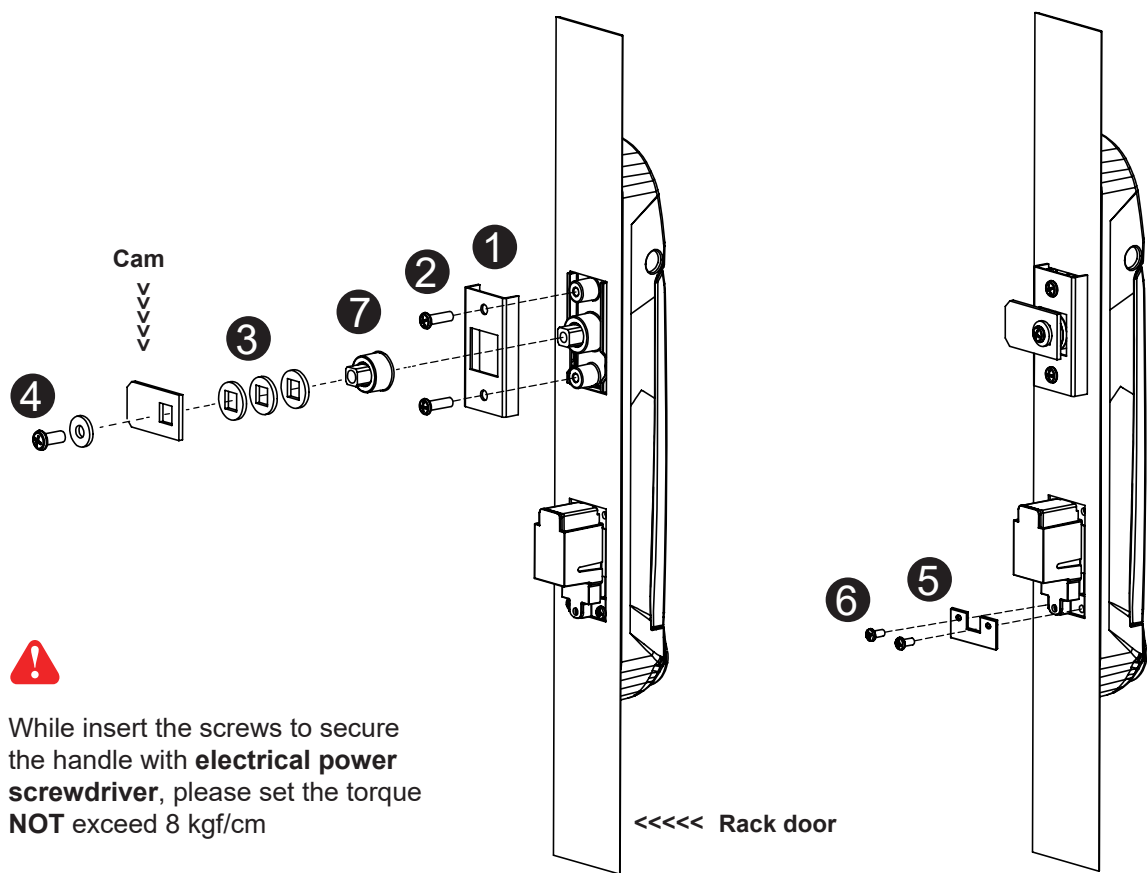
Z-800P / Z-800M support left side open. If user requires right side open, please order Z-800P-R / Z-800M-R.

Model	Left side open	Right side open
Z-800P	✓ Proximity	
Z-800M	✓ MiFARE	
Z-800P - R		✓ Proximity
Z-800M - R		✓ MiFARE

< 1.4 > Handle (Z-800P / Z-800M) Installation

Installation for

Single Point Lock



1. Mount the smartcard handle to the universal mounting position.
2. Place the ① handle mounting bracket with ② M4 x 9mm screw x 2 to secure the handle.
3. Attach the **Cam** with ③ square hole washer(s) to adjust and to fit the cam locking position.
The extension spigot ⑦ required or not for installation is subject to the rack door locking design.
Note : - If the cam cannot fit the locking position after adjustment, customization for the cam is required.
- Cam customization service upon your request, please contact your sales representative.
4. Insert the ④ M5 x 15mm screw x 1 with circle hole washer to secure the **Cam** to the handle.
5. Place the ⑤ U bracket with ⑥ M3 x 10mm screw x 2 to further secure the handle in place.

Handle mounting screw set for single point lock

		Qty.	Single Point Lock
①	Handle mounting bracket	2	✓
②	M4 x 9mm screw for ①	4	✓
③	Square hole washer	6	✓
④	Circle hole washer w/ M5 x 15mm screw	2	✓
⑤	U bracket	2	✓
⑥	M3 x 10mm screw for ⑤	4	✓
⑦	Extensions spigot	2	✓

< 1.4 > Handle (Z-800P / Z-800M) Installation

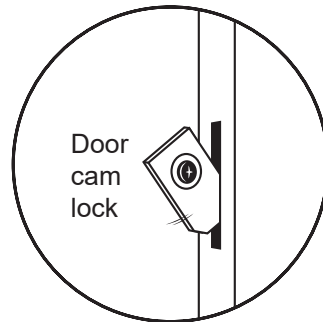


Pay attention to the following points when install the lock system.
Otherwise, it may cause handle distortion and malfunction.

1. Make sure
 - ① Cam lock can slide into the hole without stress.
 - ② The cut-out of the cam hole with enough space tolerance.

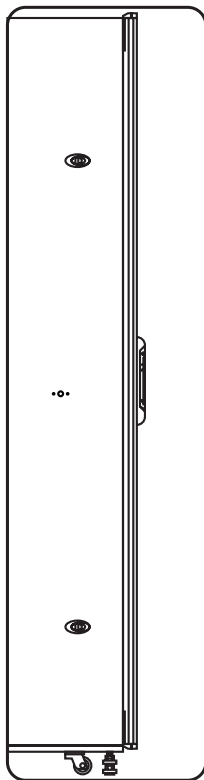


Cam lock hole
✓ enough
tolerance

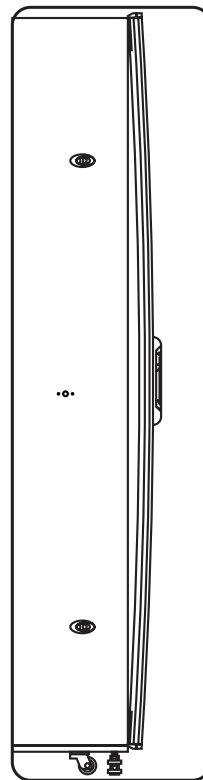


Cam lock hole
✗ limited
tolerance

2. Make sure the rack door is rigid and no bending.



✓ Rigid
door



✗ Bending
door

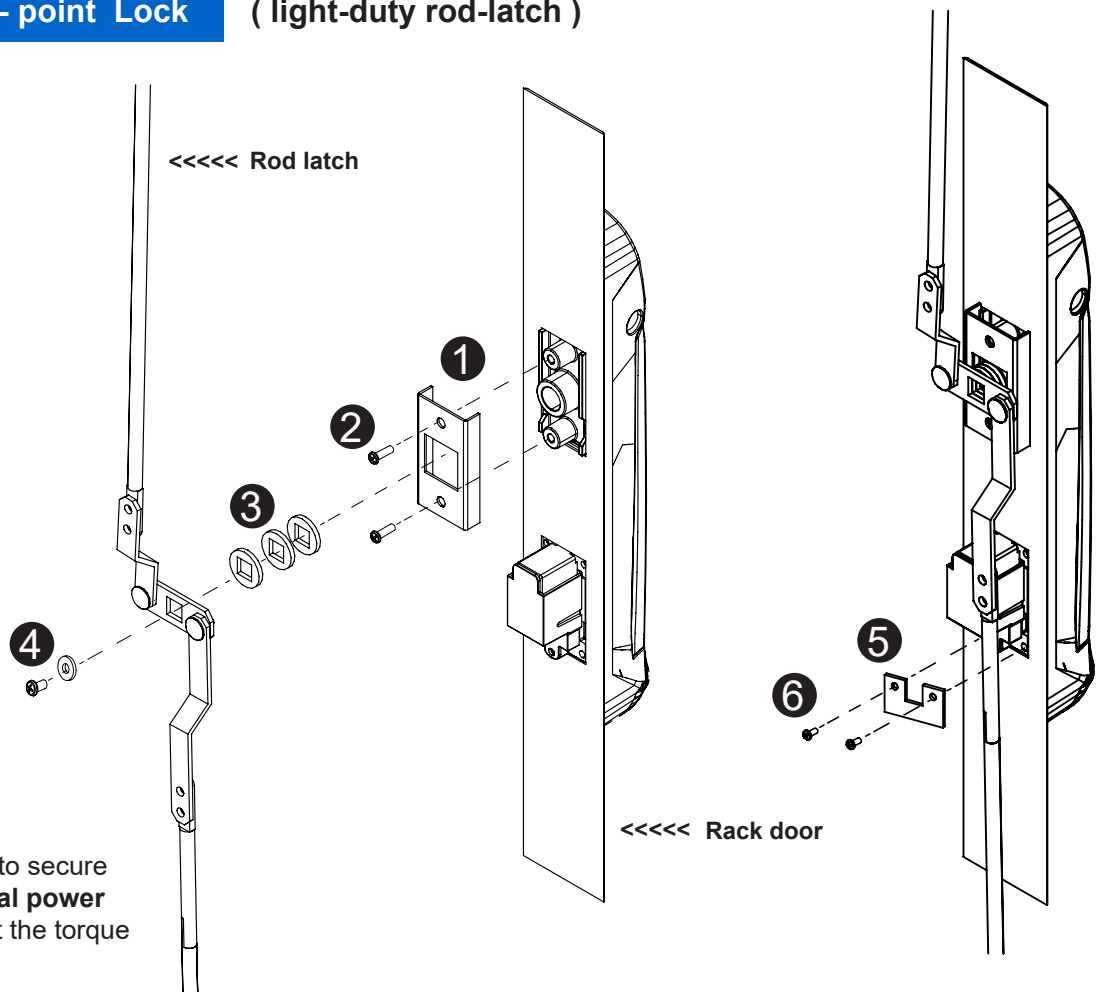
3. Don't over tighten the fixing screws.

< 1.4 > Handle (Z-800P / Z-800M) Installation

Installation for **2 - point Lock** (light-duty rod-latch)



While insert the screws to secure the handle with **electrical power screwdriver**, please set the torque **NOT** exceed 8 kgf/cm



1. Mount the smartcard handle to the universal mounting position.
2. Place the ❶ handle mounting bracket with ❷ M4 x 9mm screw x 2 to secure the handle.
3. Attach the **Rod-latch** with ❸ square hole washer(s) to adjust and to fit the door top & bottom locking position.
4. Insert the ❹ M5 x 15mm screw x 1 with circle hole washer to secure the **Rod-latch** to the handle.
5. Place the ❺ U bracket with ❻ M3 x 10mm screw x 2 to further secure the handle in place.

Handle mounting screw set for 2-point lock (light-duty)

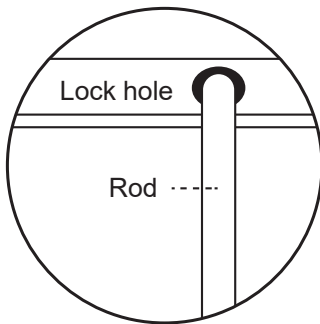
		Qty.	2-Point Lock light-duty
❶	Handle mounting bracket	2	✓
❷	M4 x 9mm screw for ❶	4	✓
❸	Square hole washer	6	✓
❹	Circle hole washer w/ M5 x 15mm screw	2	✓
❺	U bracket	2	✓
❻	M3 x 10mm screw for ❺	4	✓
❼	Extensions spigot	2	X

< 1.4 > Handle (Z-800P / Z-800M) Installation

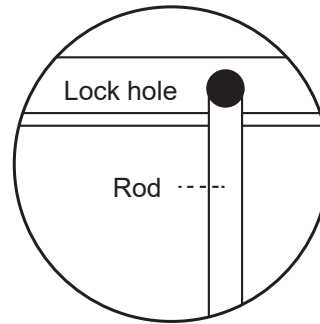


Pay attention to the following points when install the lock system.
Otherwise, it may cause handle distortion and malfunction.

1. Make sure
 - ① Two ends of latch rod can entry into the top & bottom holes without stress.
 - ② The top & bottom holes with enough space tolerance.



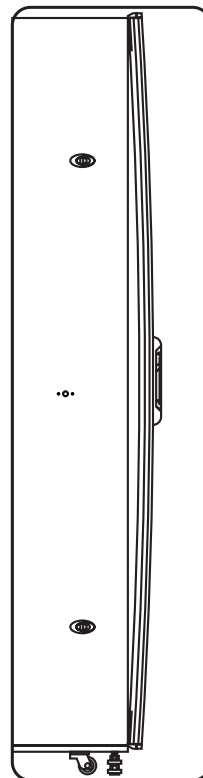
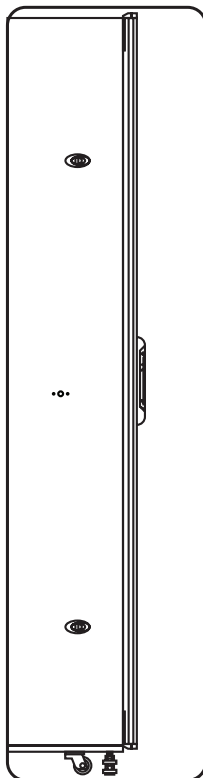
2-point lock holes
(top & bottom)



2-point lock holes
(top & bottom)



2. Make sure the rack door is rigid and no bending.



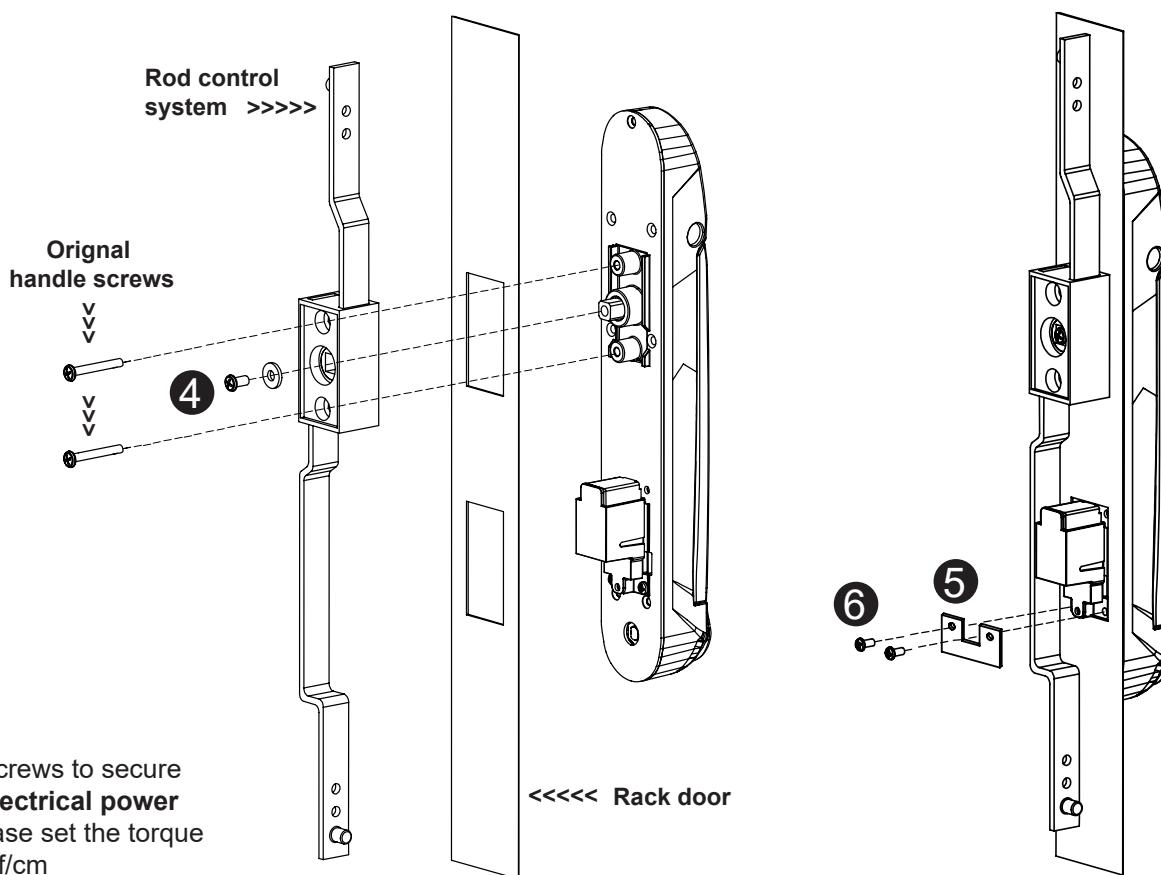
3. Don't over tighten the fixing screws.

< 1.4 > Handle (Z-800P / Z-800M) Installation

Installation for **2 - point Lock** (rod control system)



While insert the screws to secure the handle with **electrical power screwdriver**, please set the torque **NOT** exceed 8 kgf/cm



1. Mount the smartcard handle to the universal mounting position.
2. Attach the **Rod control system** to the handle and insert the **④** M5 x 15mm screw x 1 with circle hole washer to secure the position.
3. Insert **Original handle screws** x 2 through the **Rod control system** and door to the handle to fix it in place.
4. Place the **⑤** U bracket with **⑥** M3 x 10mm screw x 2 to further secure the handle in place.

Handle mounting screw set for 2-Point Lock (with rod control)

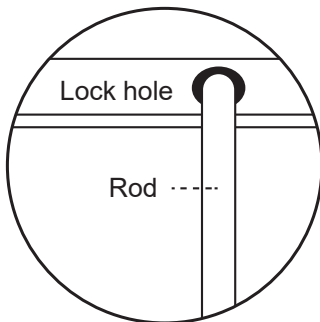
		Qty.	2-Point Lock (with rod control)
①	Handle mounting bracket	2	X
②	M4 x 9mm screw for ①	4	X
③	Square hole washer	6	X
④	Circle hole washer w/ M5 x 15mm screw	2	✓
⑤	U bracket	2	✓
⑥	M3 x 10mm screw for ⑤	4	✓
⑦	Extensions spigot	2	X

< 1.4 > Handle (Z-800P / Z-800M) Installation

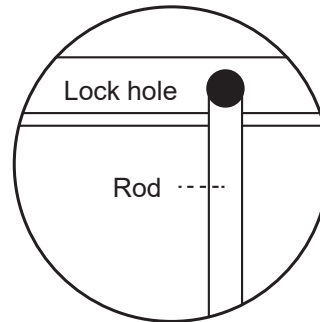


Pay attention to the following points when install the lock system.
Otherwise, it may cause handle distortion and malfunction.

1. Make sure
 - ① Two ends of latch rod can entry into the top & bottom holes without stress.
 - ② The top & bottom holes with enough space tolerance.



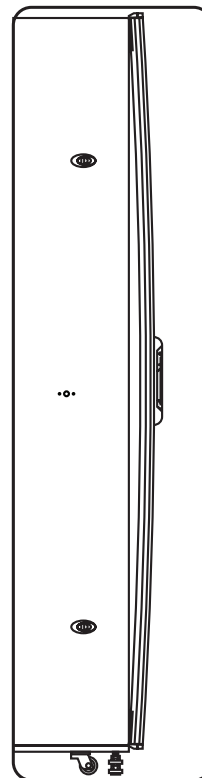
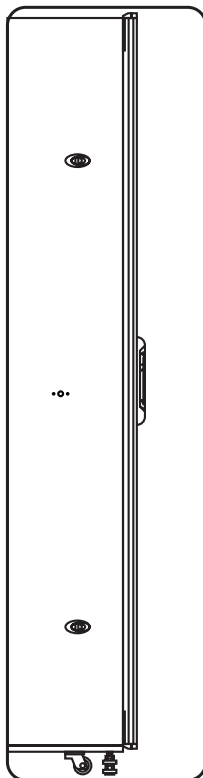
2-point lock holes
(top & bottom)



2-point lock holes
(top & bottom)



2. Make sure the rack door is rigid and no bending.



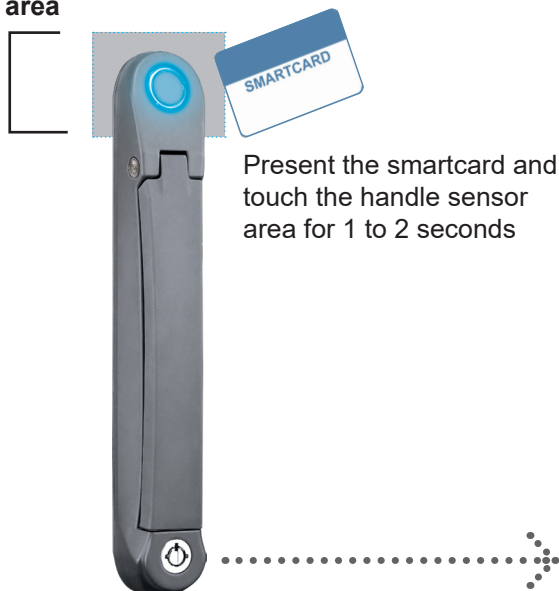
3. Don't over tighten the fixing screws.

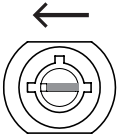
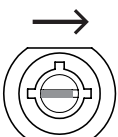
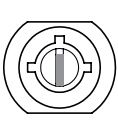
< 1.4 > Handle (Z-800P / Z-800M) Installation

Important Note for Key lock

- ⚠ • Under Smartcard mode, always keep key cylinder to 12 o'clock direction.

Sensor
area

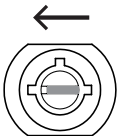
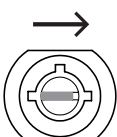


✗		Key lock mode Key cylinder to 9 o'clock direction Under key lock mode, even present the smartcard, the handle still keeps locked.
✗		Key unlock mode Key cylinder to 3 o'clock direction Under key unlock mode, the handle keeps unlocked.
✓		Smartcard mode ⚠ For smartcard operation, keep key cylinder always to 12 o'clock direction .



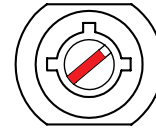
- Unless the smartcard handle is defective, lock / unlock the handle by key is NOT recommended
- Please insert & turn the key with push force



	← 	Key lock mode Key cylinder to 9 o'clock direction .
	→ 	Key unlock mode Key cylinder to 3 o'clock direction .

< 1.4 > Handle (Z-800P / Z-800M) Installation

Maintenance Key (MK-001)

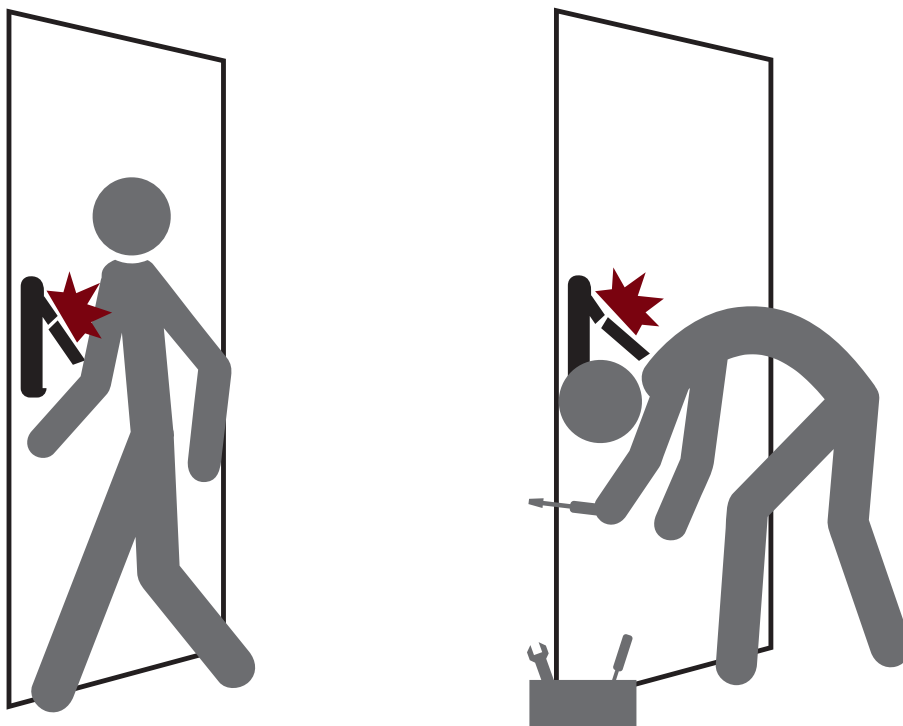


- Improper key usage may cause the cylinder stuck at abnormal direction 1 to 2 o'clock.
- Under this circumstance, the **maintenance key (MK-001)** is required to solve the problem.
- Please insert the **maintenance key** to the cylinder with push force for turning it to normal direction 9 or 12 or 3 o'clock.



Important Note for Handle

For your own safety, please return the handle to park position properly in case reckless collision.



✓ How to unlock the handle & open the door properly

Locked status in
blue or green

Unlocked status in
silver white



Within 30 seconds after smartcard detection, users should :
- lift up the handle
- open the door
- return the handle to park position properly in case reckless collision causes handle damage.
* If not open the door within 30 sec. handle will be locked automatically



Flashing

Flashing
Stop

To open the door
(within 30 seconds)

✗ Unauthorized door-open

Locked status in
blue or green

Unlocked status in
flashing red



If the door is opened improperly or by **force**, handle LED will turn to **red flashing** with audio alarm 'beep' sound.

NO Authenticated
Smartcard Detection

Door Opening
improperly or by force

✓ How to close the door properly

Unlocked status in
silver white

Locked status in
blue or green



Users should :
- lift up the handle
- close the door
- return the handle to park position properly
- the handle will **auto-lock**

To close the door

Intentionally Left Blank

< 1.5 > Door Sensor Installation

IR Sensor

IR Door Sensor, pair (S-DIR)

Features

- Magnetic base for easy setup
- No custom cutting required on doors
- Light weight & mini size (33 x 19 x 7 mm)
- 2m cord

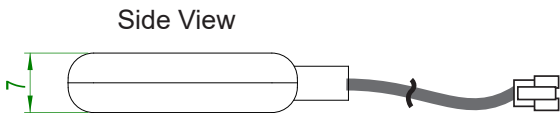
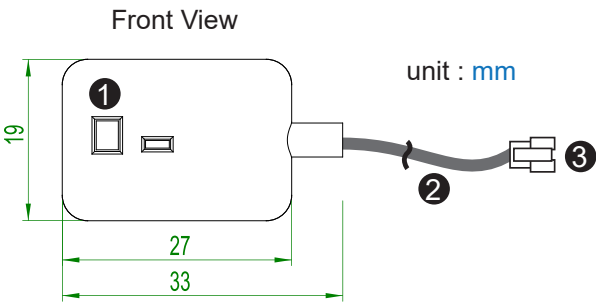


Requirement

- rack frame made of ferrous metal (iron)
- sensing distance
- door close : < 40mm
- door open : > 50mm

Package content

- IR sensor w/ 2m cable x 2
- reflective label x 2 (opposite to the IR door sensor for a better response, size: 30 x 40 mm)



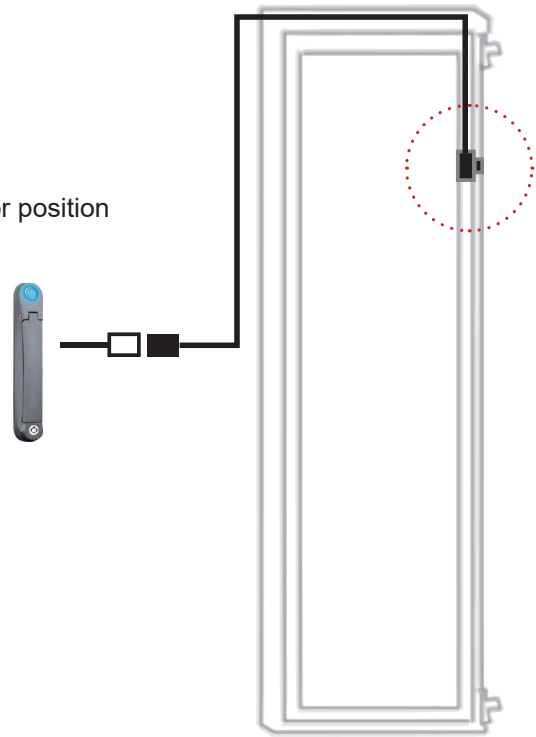
①	Sensor area
②	2m cable
③	Cable jack (connect to handle)

< 1.5 > Door Sensor Installation **IR Sensor**

Installation steps

- connect to the handle
 - guide & fix the cable with cable clips (bundle with handle package)
 - place the sensor at the top of the door, close to the hinge side
 - adjust the sensor to ensure the sensing distance between door to frame within 5mm while door in close status
 - stick the reflective label on the rack frame just opposite to the sensor position
- door close : < 40mm
door open : > 50mm

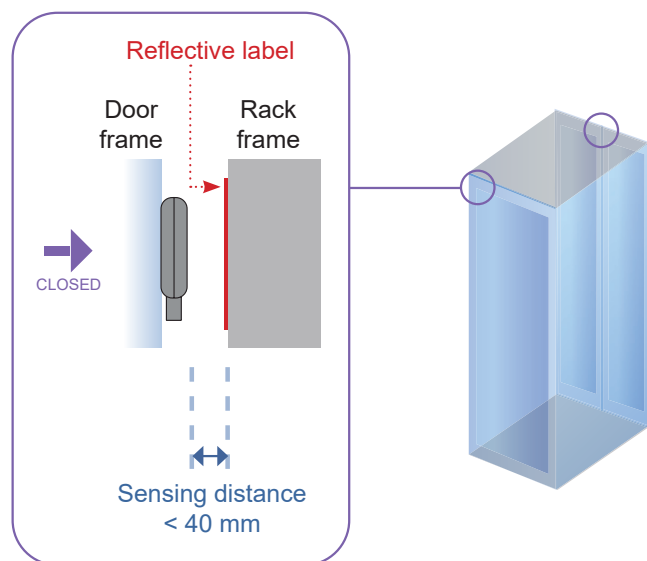
Suggested
sensor position



Sensor Operation

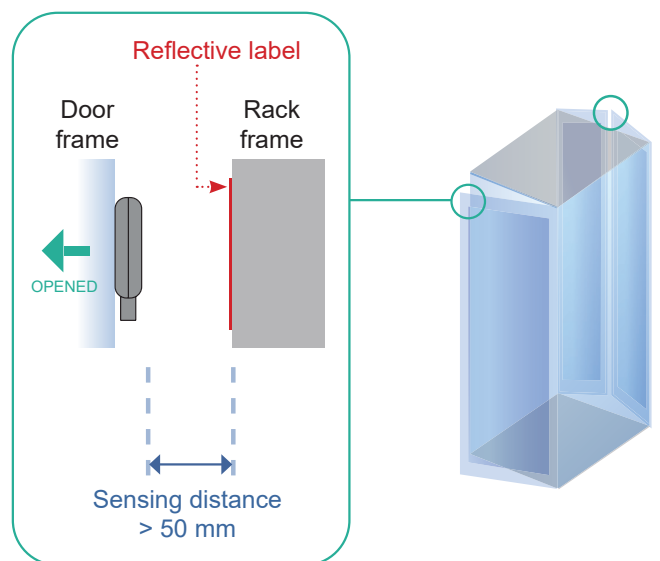
DOOR CLOSE

- close door
- IR sensor detects the rack frame
- DOOR CLOSE SIGNAL sends out



DOOR OPEN

- open door
- IR sensor lose detection with rack frame
- DOOR OPEN SIGNAL sends out



sensing distance
door close : < 40mm
door open : > 50mm

< 1.5 > Door Sensor Installation Mechanical Sensor

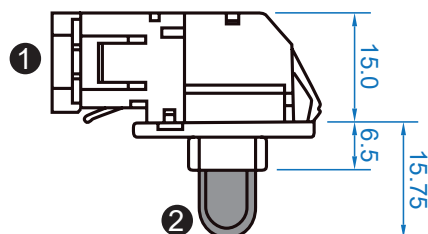
Mechanical Door Sensor, pair (S-DSW)

- Low cost / precise
- Size (36.3 x 15 x 30.75 mm)
- 2m cord

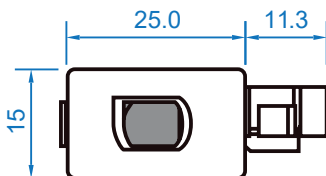
Package content

- Mechanical sensor w/ 2m cable x 2
- Mounting bracket x 2

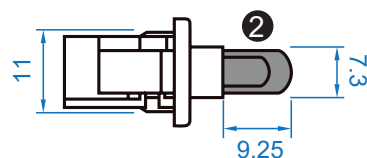
Top View



Front View



Side View

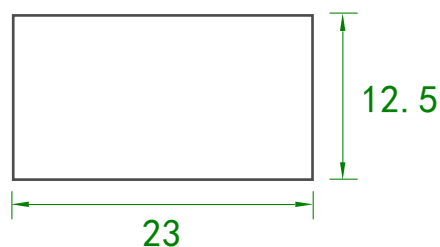


unit : mm

①	Cable connector
②	Press button (total travel distance : 9.25 mm) (min. actuation distance : 3.00 mm)

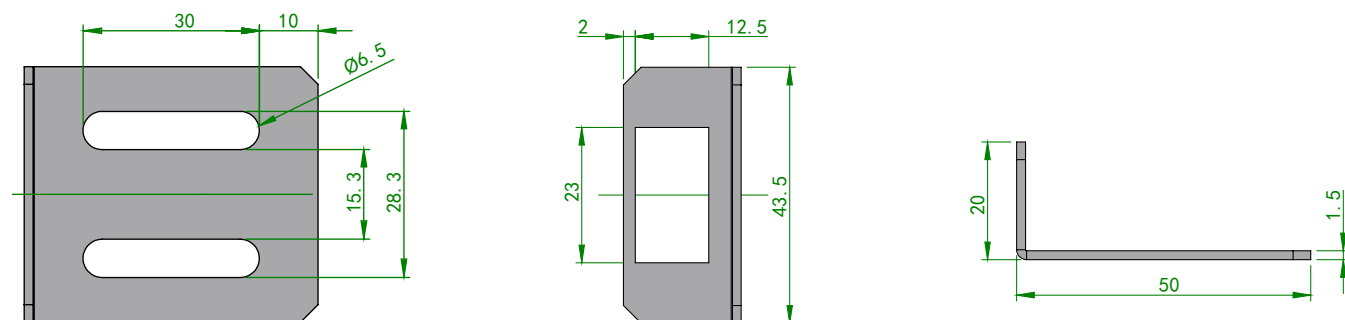
Mounting by custom cutout on door frame

- Cutout size (23 x 12.5 mm)



Mounting by bundled bracket

- Ø6.5mm hole cutting required on door frame

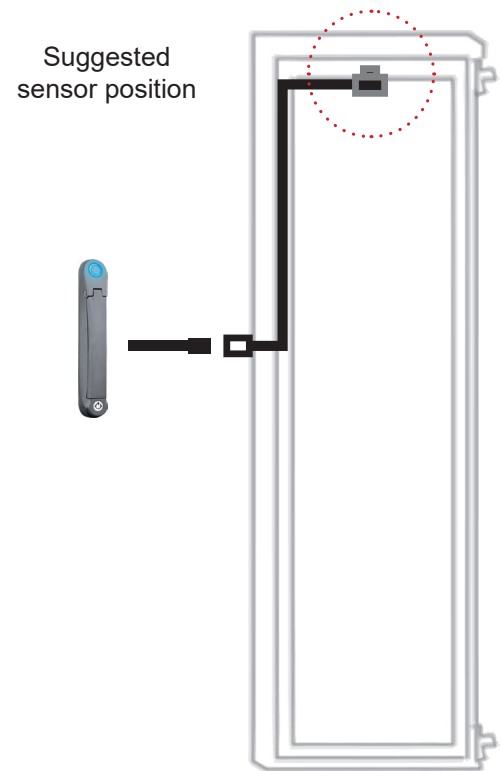


unit : mm

< 1.5 > Door Sensor Installation **Mechanical Sensor**

Installation steps

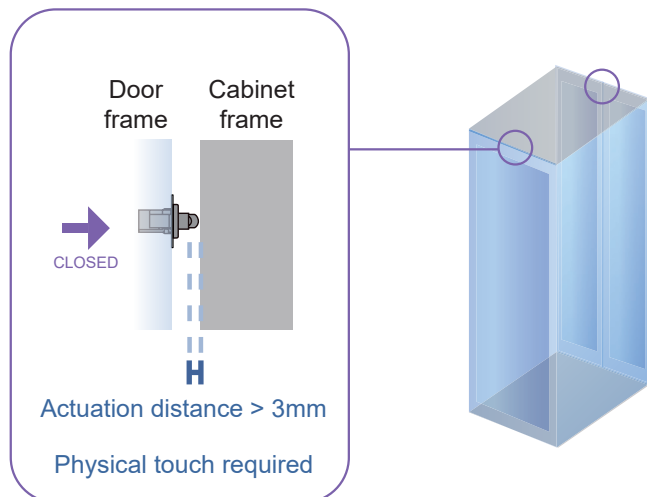
- connect to the handle
- place the sensor at the top middle of the door
- secure it with mounting screws x 2



Sensor Operation

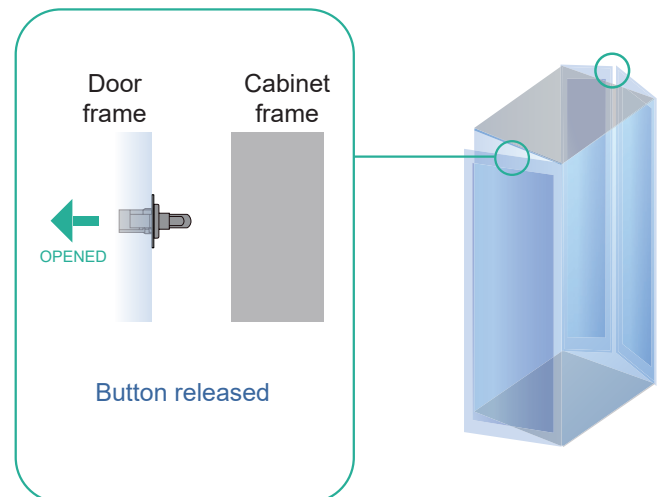
DOOR CLOSE

- close door
- Sensor button is pressed on
- DOOR CLOSE SIGNAL sends out



DOOR OPEN

- open door
- Sensor button is released
- DOOR OPEN SIGNAL sends out

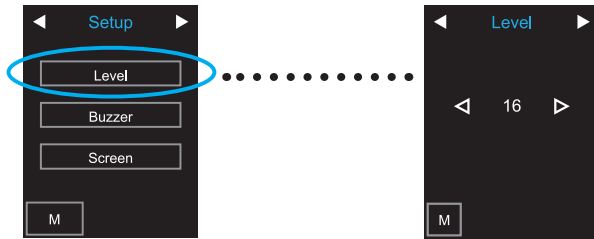


< 1.6 > Key Features

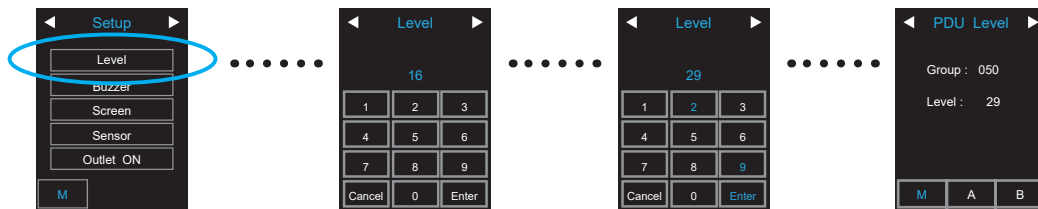
Features		
Capacity	InfraBox	1
	Concurrent user	1
System	Alarm Mail Server Setting	✓
	802.1X authentication	✓
	User authentication by Microsoft Active Directory & LDAP	✓
	SNMPv1/v2c & SNMPv3 setting	✓
Handle	Door open by remote	✓
	Last Door open & close record	✓
	Card addition to individual handle	Max. 100
PDU	Energy consumption (kWh) monitoring	✓
	Current loading (Amp.) monitoring	✓
	Outlet level measurement	✓
	Individual / multiple outlet switch ON / OFF	✓
	Current loading alarm / rising alert / low alert threshold setting	✓
	Temp-humid sensor monitoring	✓
Fan unit	CFM & Temp monitoring	✓
	Unit CFM (fan speed) setting	✓
	Auto CFM control setting	✓
	Individual fan kit on / off	✓
	Fan unit on / off	✓
Sensor	Temp-humid alarm / rising alert threshold setting	✓
	Temp-humid status monitoring	✓
	Audio & visual alarm output setting for individual sensor	✓

< 1.7 > Meter (PDU) Level Setting

With touchscreen function



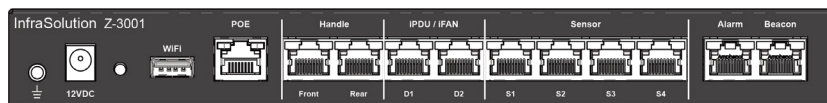
With touchscreen function



For PDU with firmware version V37 or above

< 1.8 > PDU Daisy Chain Connection

Z-3001



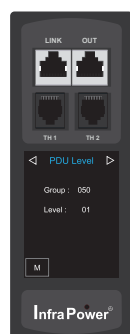
D2



Out



Link



1st level PDU

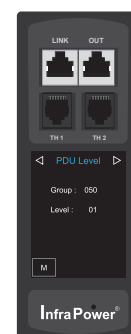
To Link port of next level PDU (max level: 4)



Out



Link



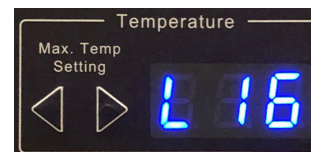
2nd level PDU

< 1.9 > Expansion Fan Units Level Setting

- Please follow the steps below to set the daisy chain level for expansion fan units
- For the cabling connection, please refer to next page.

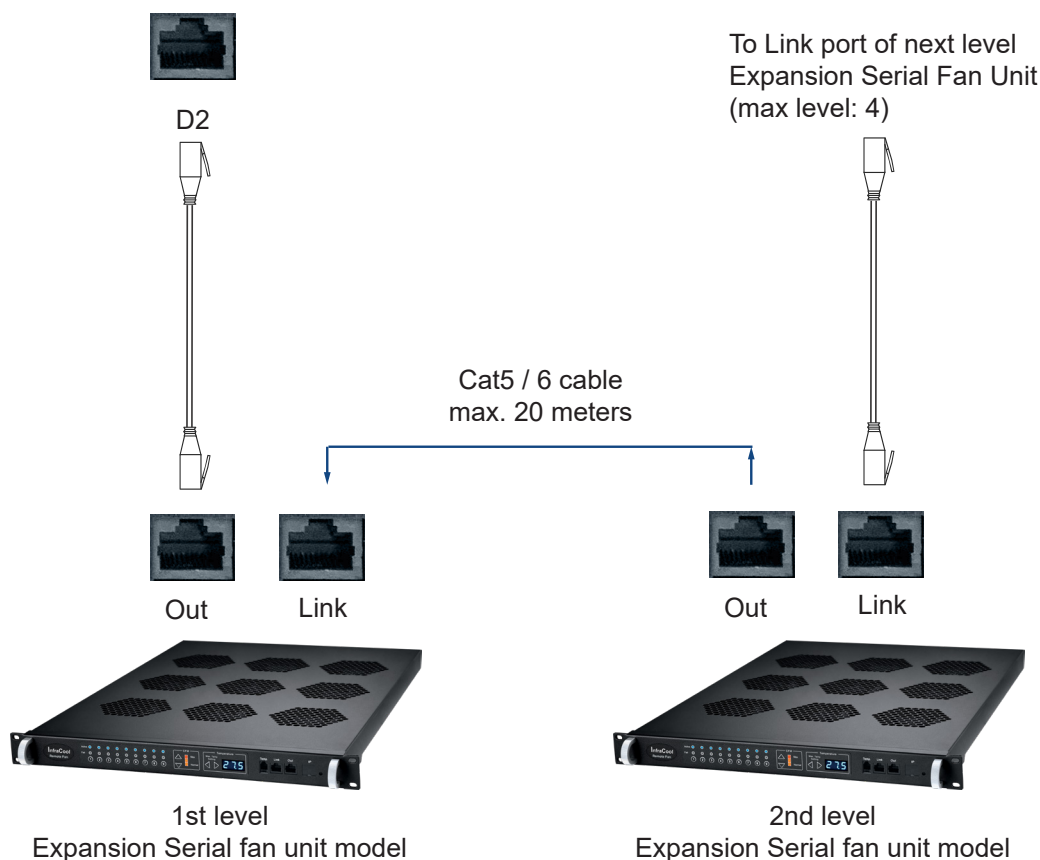
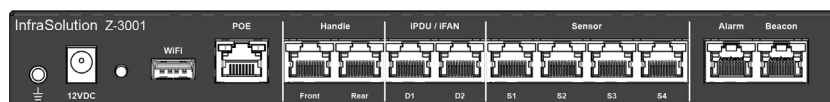
Step 1. Press and hold the “” button for 5 seconds.

Step 2. Press  or  arrow button to set the daisy chain level



< 1.10 > Fan Daisy Chain Connection

Z-3001

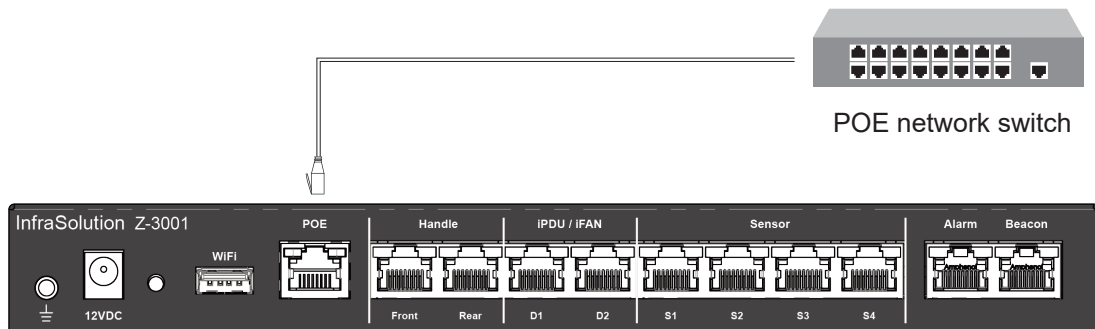


< Part 2 > Initial Installation and Configuration

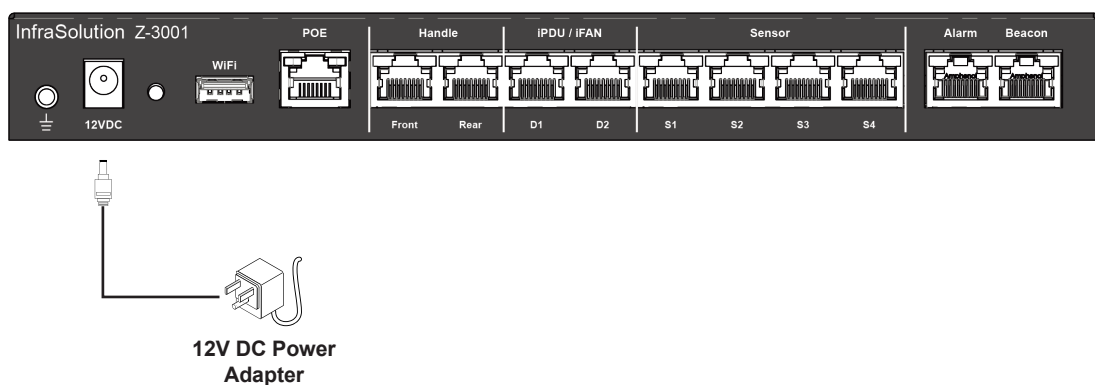
< 2.1 > Connecting the Z-3001 to a Power Source

There are 2 ways to support power to the Z-3001:

- Over POE network switch

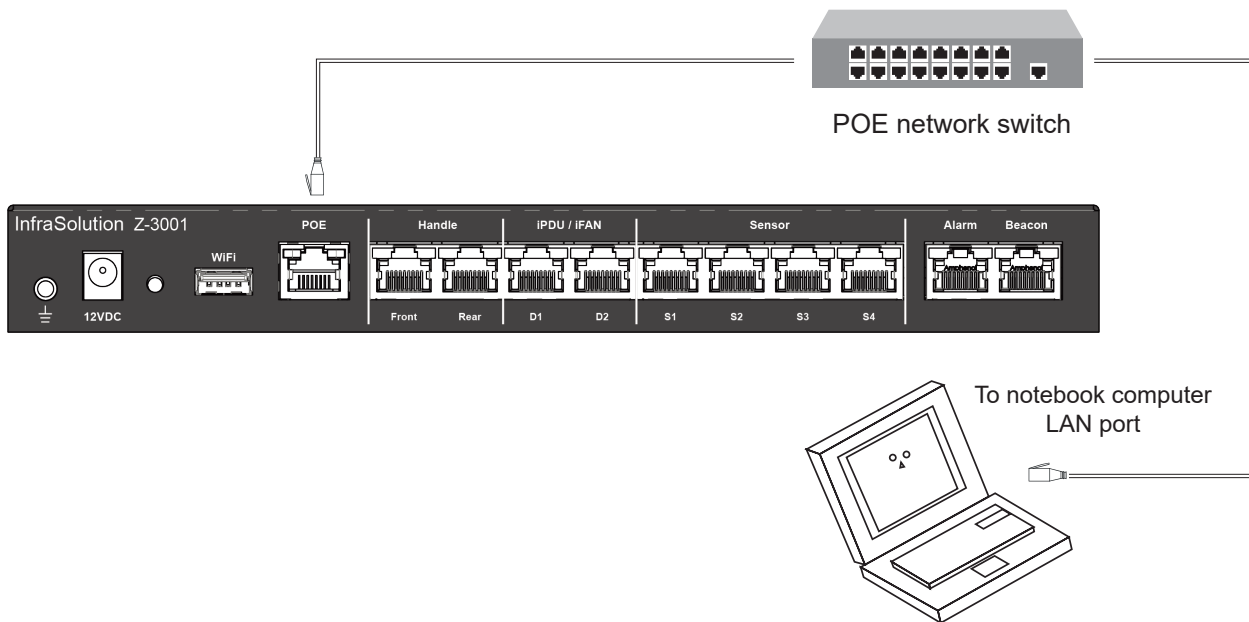


- Using a 12VDC Power adapter

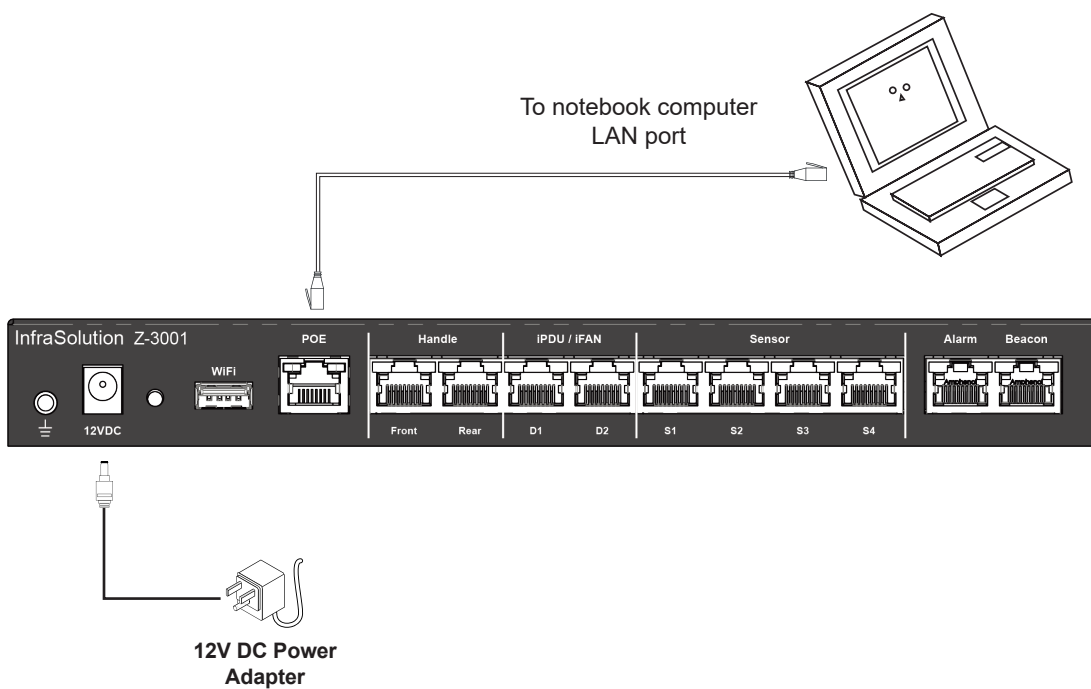


< 2.2 > Connecting the Z-3001 to a computer

- Z-3001 > POE switch > computer



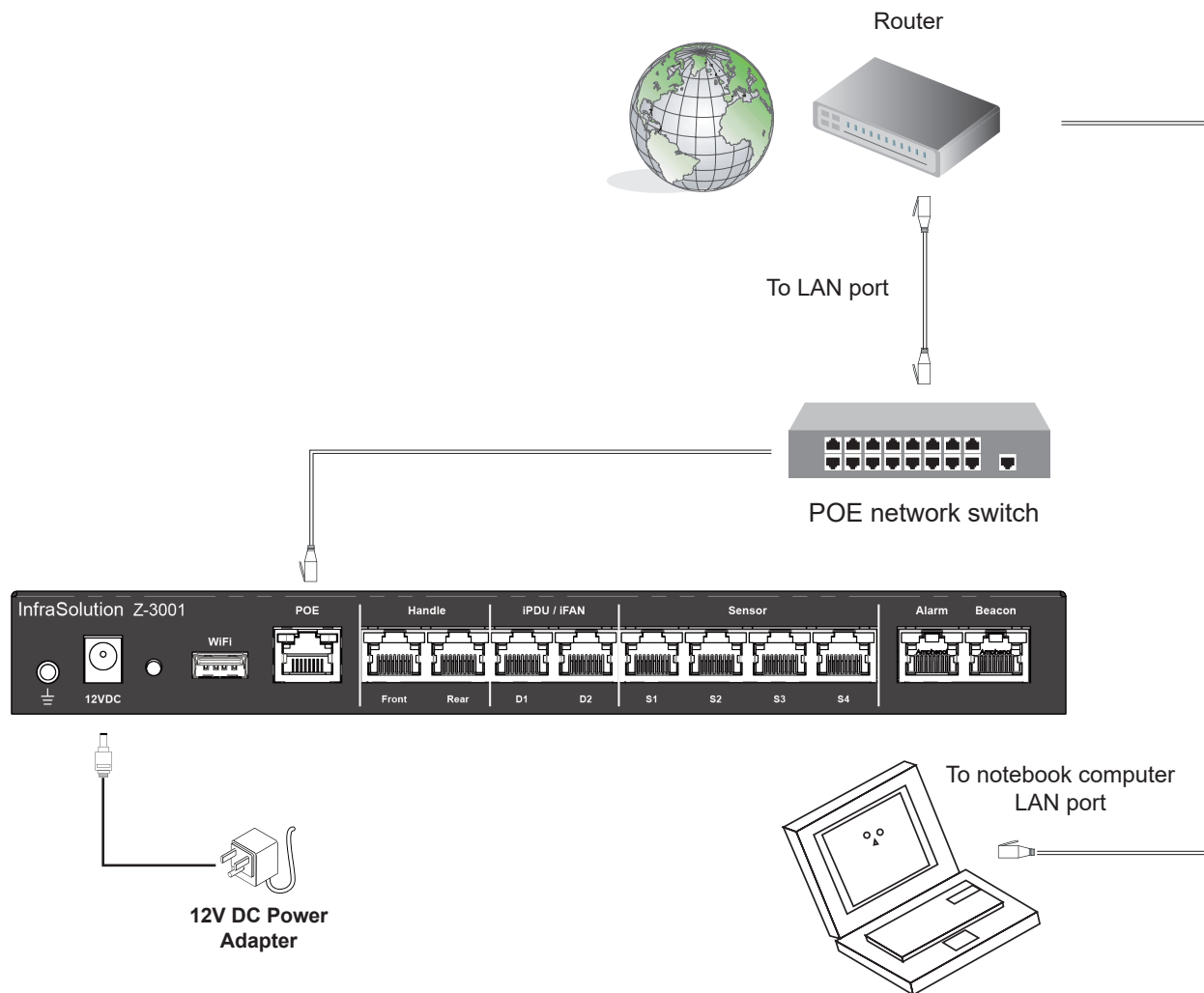
- Z-3001 > computer using 12VDC power adapter



< 2.3 > Connecting the Z-3001 to your Network

To remotely administer the Z-3001, you must connect the Z-3001 to your local area network (LAN).

- Connect a standard network patch cable to the POE port on the Z-3001
- Connect the other end of the cable to your LAN



< 2.4 > Configuring the Z-3001

You can initially configure the Z-3001 by connecting it to a computer, or to a TCP/IP network that supports DHCP.

- Configuration over a DHCP-enabled network:
 - i. Connect the Z-3001 to a DHCP-enabled IPv4 network.
 - ii. Provide the Mac address of the Z-3001 and Ask your network administrator to retrieve the DHCP-assigned IPv4 address
 - iii. Launch a web browser to configure the Z-3001. See < 3.2 > First Time Login
- Configuration using a connected computer:
 - i. Connect the Z-3001 to a computer. See < 2.2 > Connecting the Z-3001 to a computer.
 - ii. An IP address 192.168.0.1 will automatically assigned to the Z-3001.
 - iii. Configure the IP setting of the connected computer so that it is under the same network of the Z-3001.
 - iv. Use the connected computer to configure the Z-3001 via web interface.
 - v. Launch the web browser on the computer, and type 192.168.0.1 to access the Z-3001.

< Part 3 > Using the Web Interface

< 3.1 > Supported Web Browser

- Microsoft Edge
- Internet Explorer 11
- Google Chrome 128 and later
- Firefox 128 and later

< 3.2 > First Time login

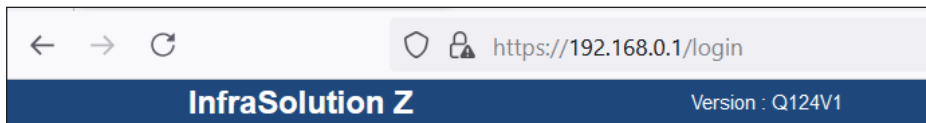
For the first time login, please use the default login name and password to login.

(Default login name and password : 00000000).

Due to the security issue, you must change the login password for the first time login.

To login to the Web interface :

- Open a browser and type the IP address of the Z-3001



- If any security alert message appears, accept it.
- The login screen displays. Input the login name and password. Then click “ Login “

Device	Z-3001
Login name	00000000
Password	00000000
Login Cancel	

- The following screen displays and you must change the login password. Otherwise, you cannot login.

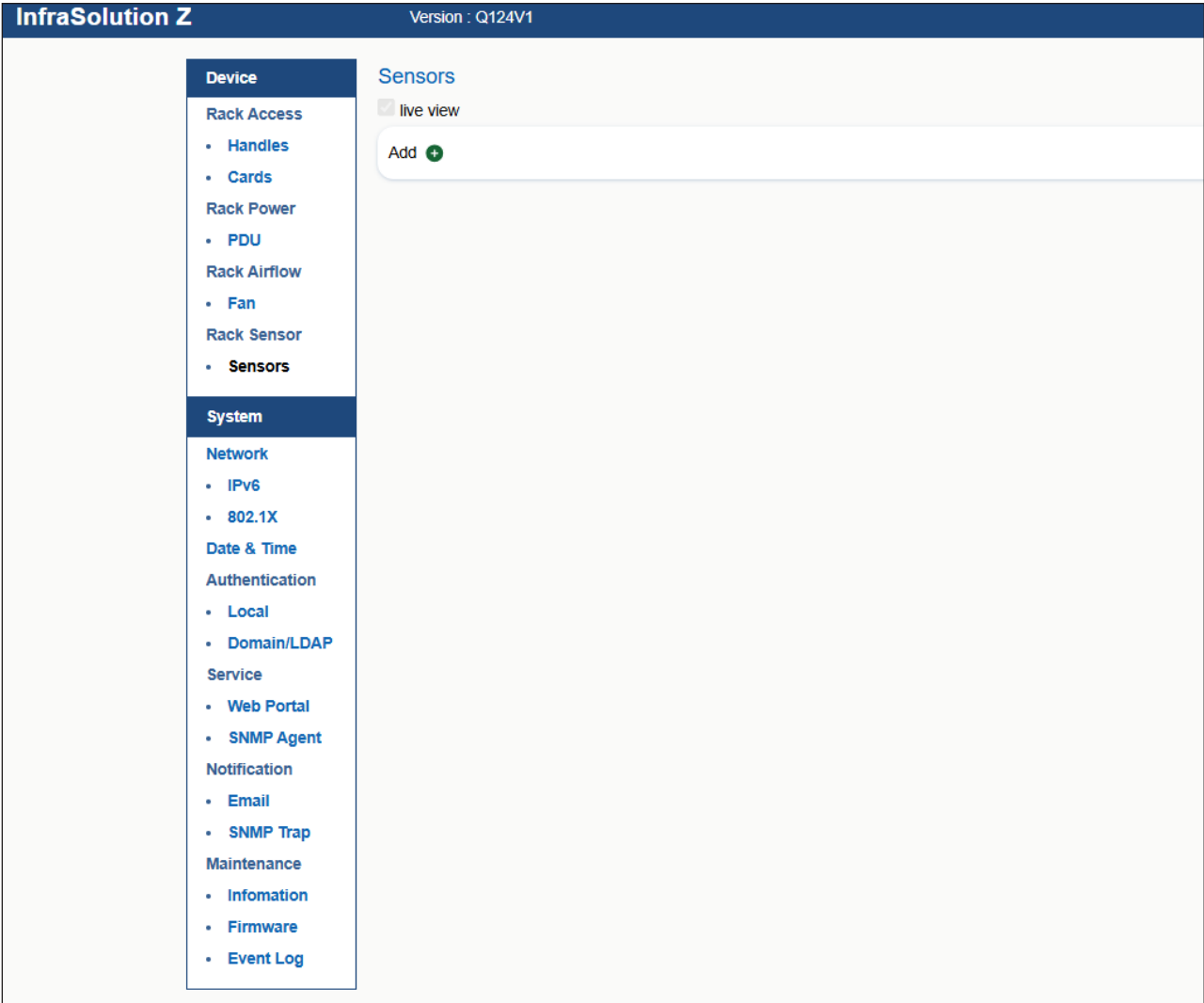
Device	Z-3001
A new password is required to replace the default password.	
New Password	
Confirm Password	
Apply Cancel	

- Input the new password and confirm the new password and click “Apply”.

Device	Z-3001
A new password is required to replace the default password.	
New Password	00000000
Confirm Password	00000000
Apply Cancel	

< 3.2 > First Time login

vi. The Z-3001 web interface similar to the following image displays.



< 3.3 > Rack Access

Under Rack Access, you can add the handle connect to the Z-3001. Once you add the handle(s), you must assign the smartcard to the handle(s) to open the door locally.

- Handle

- i. Go to Rack Access > Handles. Then click “” to add handle(s).



- ii. Tick “F” or “R” to add front / rear handle or both handles. Then click “Apply ”



- i ii. Click “ OK ” after the handle(s) are added successfully.



- iv. Then you will see the handle’s status.

Handles					
☒ live view					
Add 					
Label	Model	Name	Location	Status	
F1	X-800P	xHandle_name	xHandle_location	closed	<button>Unlock</button>
R1	X-800P	xHandle_name	xHandle_location	closed	<button>Unlock</button>

In this page, you can directly to unlock the handle remotely by clicking “ Unlock ”. If the door is not opened within 30 seconds, the handle(s) will be relocked automatically.

- v. You can move the cursor to the Label of the handle and you will see the “Remove” under the Model of the handle to remove it from the monitoring.

Handles					
☒ live view					
Add 					
Label	Model	Name	Location	Status	
F1	Z-800P Remove	xHandle_name	xHandle_location	closed	<button>Unlock</button>
R1	Z-800P	xHandle_name	xHandle_location	closed	<button>Unlock</button>

< 3.3 > Rack Access

vi. You can also click “F1” or “R1” to go to the handle detail page which provides the event log of the handles. You can also change the handle name & location.

< Handles

Port : F1

Model : Z-800P

Name : ☒ xHandle_name

Location : ☒ xHandle_location

Auto-lock timeout : 30 s

Firmware : XP8-02-230505

Status : closed

Handle

Unlocked at : 2024-09-24 10:19:01

Locked at : 2024-09-24 10:19:15

Status : Unlock

Key

Unlocked at : 2024-09-24 10:20:57

Locked at : 2024-09-24 10:21:13

Status :

Card

Last Access Card : 10804250

Last Access Time : 2024-09-24 10:19:01

Door

Opened at : 2024-09-24 10:21:05

Closed at : 2024-09-24 10:21:10

Status : closed

Recent Logs

Time	Severity	Event
2024-09-24 10:21:13	Info	Key locked.
2024-09-24 10:21:10	Warning	Key unlocked, Door closed.
2024-09-24 10:21:05	Warning	Key unlocked, Door opened.
2024-09-24 10:20:57	Warning	Key unlocked.
2024-09-24 10:19:15	Info	Handle locked.

- Cards

i. Go to Rack Access > Cards. Then click “

Cards 

ii. Input how many cards you want to add to the Z-3001 and click “OK”.

192.168.0.1 says

How many cards to be added? Max. 100 each time.

1|

OK

Cancel

iii. Input the smartcard no. and tick which handle can be unlock by this card and click “Apply”

Cards 

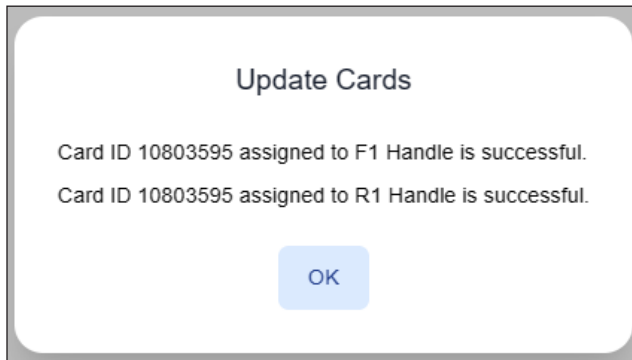
Card ID	F1 (0/100)	R1 (0/100)
1. 10803595	☐	☐

Apply

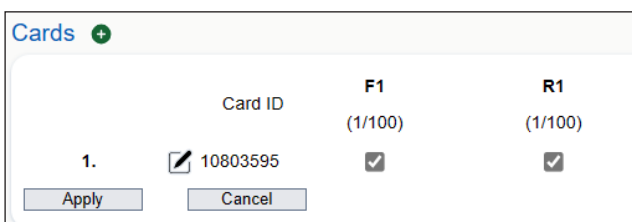
Cancel

< 3.3 > Rack Access

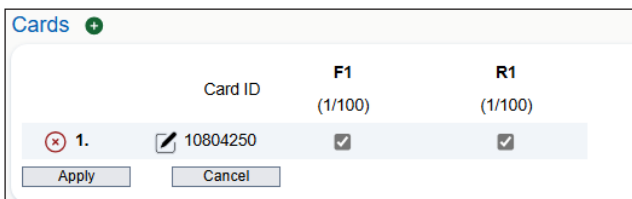
- iv. Click “OK” after the card(s) are added successfully.



- v. Now you can use the card you added to unlock the handle(s) you select. In this illustration, both front and rear handle can be unlock by the card no. 10803595.



- vi. To delete a smartcard, just move the cursor to the smartcard you want to delete. Then click “ ” and click “OK” from the pop up window to confirm.

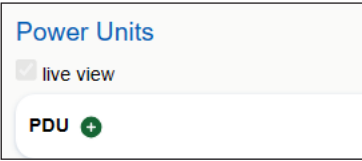


< 3.4 > Rack Power

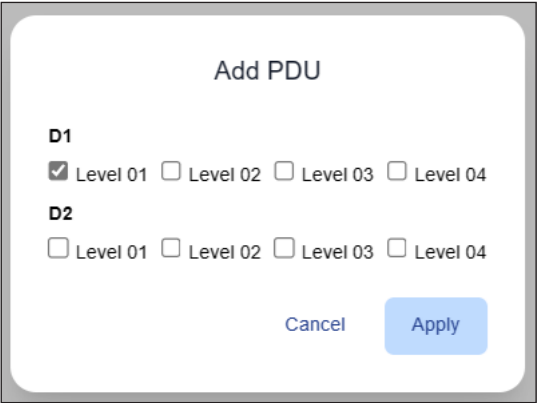
Under Rack Power, you can add the intelligent W series PDU(s) connected to the Z-3001 for monitoring and control. The max. no. of PDU in the cascade chain is 4. Ensure the PDU level in the cascade chain is unique. Please refer to P10 for PDU level setting.

- PDU

- i. Go to Rack Power > PDU, click “+” to add PDU(s) connected to the Z-3001.



- ii. Tick the level(s) of the PDU you connected to the Z-3001 & click “Apply”



- iii. Once the addition is succeeded, you can see the following similar image displays.

A screenshot of the 'Power Units' interface showing a table of PDU data. The table has columns for ID, Name, Overall status, and various power metrics. The data is as follows:

Power Units									
☒ live view									
PDU +									
D1									
01	default_pdu_name	Overall	218.9 V	0.0 A	0.00	0.00 W	0.00 VA	0.10 kWh	
		Circuit A	218.9 V	0.0 A	1.00	0.00 W	0.00 VA	0.05 kWh	
		Circuit B	218.8 V	0.0 A	1.00	0.00 W	0.00 VA	0.05 kWh	

< 3.4 > Rack Power

iv. You can click PDU level to go to the PDU details page. you can see the following similar image displays.

< Power Units

Port : D1

Level : 01

Model : V24C13-32A-WSiCR_ENI3B-1

Name : ☒ default_pdu_name

Location : ☒ default_pdu_loc

Energy Consumption : 0.00 kWh

Inlet Rated : 32A, 250V

Circuit Rated : 16A, 220V

MFG : 2@1M0000

Serial Number : 0000000000-0000-P000

Firmware : 2B-V63

Circuits

Label	Fuse Status	Voltage	Frequency	Load Amp.	Peak Amp.	Apparent Power	Active Power	Energy Consumption
Circuit A	Normal	220.0 V	50.0 Hz	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
Circuit B	Normal	220.0 V	50.0 Hz	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh

Outlets

Bulk Action : No Action

Label	Circuit	Name	Power Status	Power On Delay	Load Amp.	Peak Amp.	Apparent Power	Active Power	Energy Consumption
01	Circuit A	☒ outlet_name_01	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
02	Circuit A	☒ outlet_name_02	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
03	Circuit A	☒ outlet_name_03	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
04	Circuit A	☒ outlet_name_04	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
05	Circuit A	☒ outlet_name_05	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
06	Circuit A	☒ outlet_name_06	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
07	Circuit A	☒ outlet_name_07	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
08	Circuit A	☒ outlet_name_08	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
09	Circuit A	☒ outlet_name_09	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
10	Circuit A	☒ outlet_name_10	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
11	Circuit A	☒ outlet_name_11	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
12	Circuit A	☒ outlet_name_12	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
13	Circuit B	☒ outlet_name_13	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
14	Circuit B	☒ outlet_name_14	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
15	Circuit B	☒ outlet_name_15	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
16	Circuit B	☒ outlet_name_16	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
17	Circuit B	☒ outlet_name_17	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
18	Circuit B	☒ outlet_name_18	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
19	Circuit B	☒ outlet_name_19	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
20	Circuit B	☒ outlet_name_20	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
21	Circuit B	☒ outlet_name_21	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
22	Circuit B	☒ outlet_name_22	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
23	Circuit B	☒ outlet_name_23	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh
24	Circuit B	☒ outlet_name_24	☒ ON	☒ 1 sec	☒ 0.0 A	☒ 0.0 A	0.00 VA	0.00 W	☒ 0.00 kWh

Sensors

Add

You can :

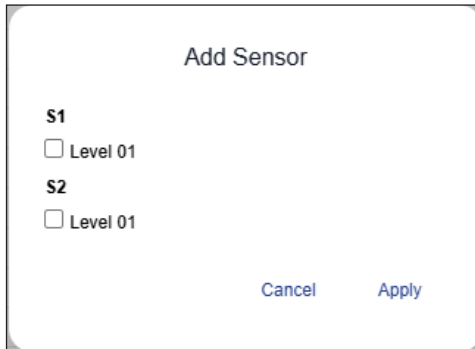
- Change the PDU name & location
- Change circuit's or bank's alarm, rising alert & low alert ampere threshold
- Reset circuit's or bank's peak ampere
- Reset circuit's or bank's energy consumption
- Switch ON or OFF outlet(s) (Switched PDU only)
- View ON / OFF status of each PDU's outlet
- View aggregated current on the PDU
- View latest loading & energy consumption of each PDU outlet (Outlet Measurement PDU only)
- View latest voltage of each PDU bank or circuit
- View the outlet power up sequence delay setting of each outlet (Switched PDU only)
- Set the outlet power up sequence delay of each outlet (Switched PDU only)
- Change the outlet name
- Enable monitoring Temp / TH / Smoke / Door sensor connected to the PDU's sensor port.

< 3.4 > Rack Power

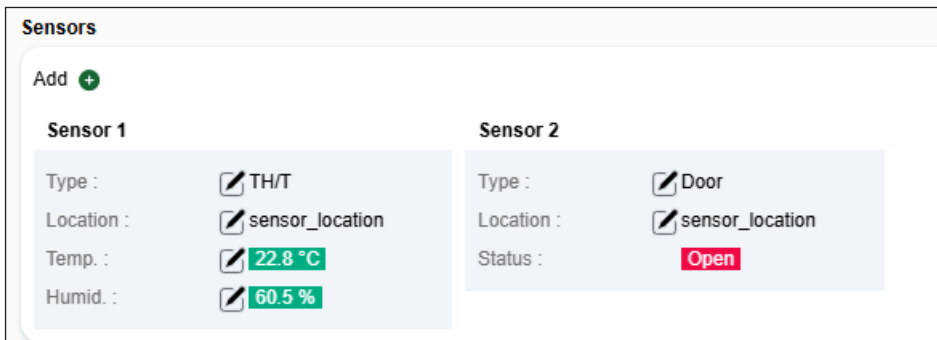
- v. To monitor the sensor(s) connected to the PDU, click “”



- vi. Tick the sensor port you have installed the sensor(s) and click “Apply”. Then click “OK” from the pop up window displays the addition of sensor is successful.



- vii. Once the addition is succeeded, you can see the following similar image displays.



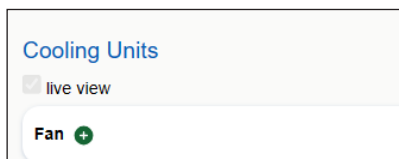
You can :

- Change the sensor type
- Change the sensor location
- View the sensor status
- View the sensor reading (Temp & TH sensor only)
- Change the Temp & Humid sensor alarm & rising alert threshold setting (Temp & TH sensor only)

< 3.5 > Rack Airflow

Under Rack Airflow, you can add the intelligent remote fan unit(s) connected to the Z-3001 for monitoring and control. The max. no. of fan unit in the cascade chain is 4. Ensure the fan unit level in the cascade chain is unique. Please refer to P13 for fan unit level setting.

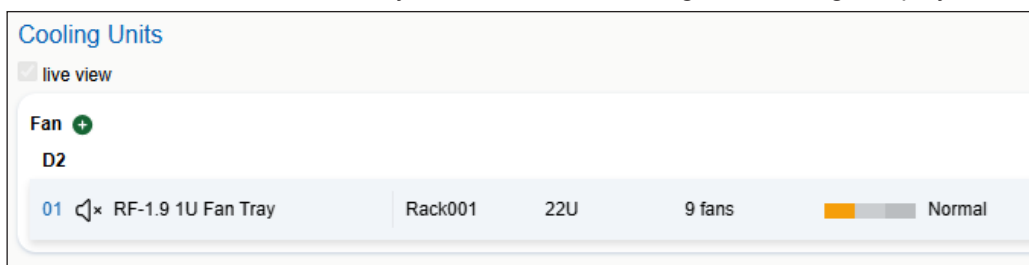
- Fan

- i. Go to Rack Airflow > Fan, click “The image shows a screenshot of the 'Cooling Units' interface. At the top, it says 'Cooling Units' in blue. Below that is a 'live view' toggle switch. Underneath, there is a 'Fan' section with a green plus icon next to it, indicating an option to add a fan unit.

- ii. Tick the level(s) of the fan unit(s) you connected to the Z-3001 & click “Apply”



- iii. Once the addition is succeeded, you can see the following similar image displays.



< 3.5 > Rack Airflow

iv. You can click Fan unit level to go to the Fan unit details page. you can see the following similar image displays.

< Cooling Units

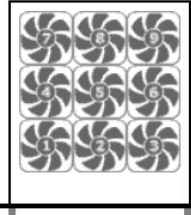
Port :
Level :
Model :
Name :
Location :
Unit CFM :
Firmware :
Serial Number :

D2
01
RF-1.9 1U Fan Tray
Rack001
22U
Normal
CFMU-F11-210421
3H9I0001

Sensor

Activation : ☒ Disabled

Fan Kit	Status	Switch
1	Off	ON
2	Off	ON
3	Off	ON
4	Off	ON
5	Off	ON
6	Off	ON
7	Off	ON
8	Off	ON
9	Off	ON



You can :

- View the fan unit model
- Change the name, location & the unit CFM setting
- Switch ON / OFF the fan unit
- View the fan unit status
- Enable monitoring Temp sensor connected to the fan unit’s sensor port.

v. To monitor the Temp sensor connected to the fan unit, click “”

Sensor

Activation : ☒ Disabled

vi. Select “Enable” & Click “Apply”.

Sensor

Activation

viii. Once the addition is succeeded, you can see the following similar image displays.

Sensor

Activation : ☒ Enabled

Location : ☒ Front_top

Auto CFM : ☒ Disabled

Temp. Reading : ☒ 25.0 °C

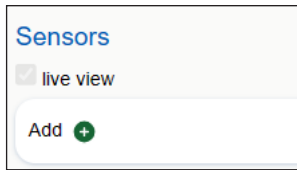
You can :

- Change the sensor location
- View the sensor status & reading
- Change the Temp sensor alarm & rising alert threshold setting.
- Enable / disable the Auto CFM control setting. When enabled, the fan unit will operate in Max. speed if the temp alarm threshold is triggered.

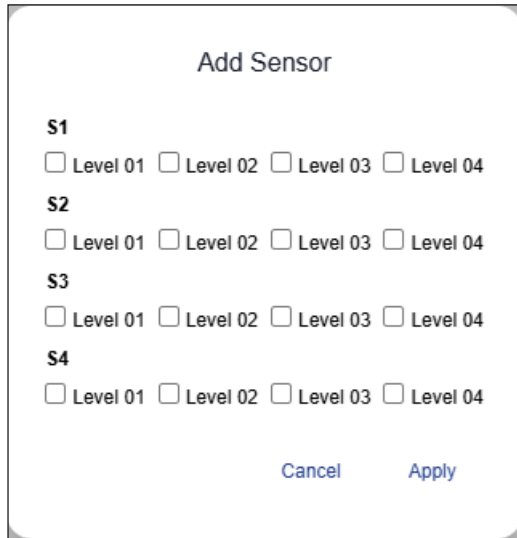
< 3.6 > Rack Sensor

Under Rack Sensor, you can add the Temp or TH sensor(s) connected to the Z-3001 for monitoring and control.

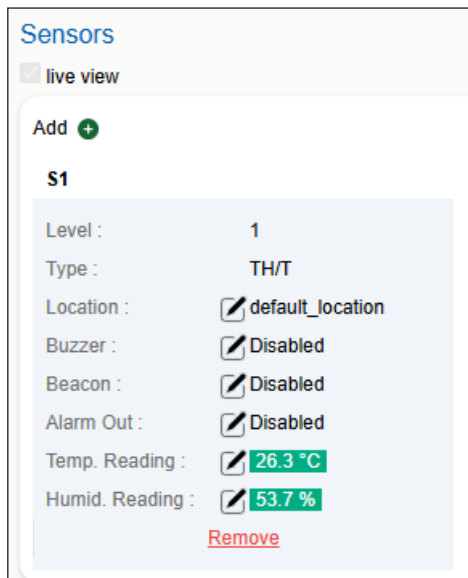
- Sensors

- i. Go to Rack Sensor > Sensors, click “A screenshot of the 'Sensors' page. At the top, it says 'Sensors' in blue. Below that is a 'live view' checkbox which is checked. At the bottom, there is an 'Add' button with a green plus icon.

- ii. Tick the level(s) of the sensor(s) you connected to the Z-3001 & click “Apply”. The sensor level is automatically detected.

A screenshot of the 'Add Sensor' dialog box. It has a title 'Add Sensor'. Below the title, there are four sections labeled S1, S2, S3, and S4. Each section has four checkboxes labeled 'Level 01', 'Level 02', 'Level 03', and 'Level 04'. At the bottom right, there are two buttons: 'Cancel' and 'Apply'.

- iii. Once the addition is succeeded, you can see the following similar image displays.



You can :

- Click “

UM-IS-Z3001-Q225V1

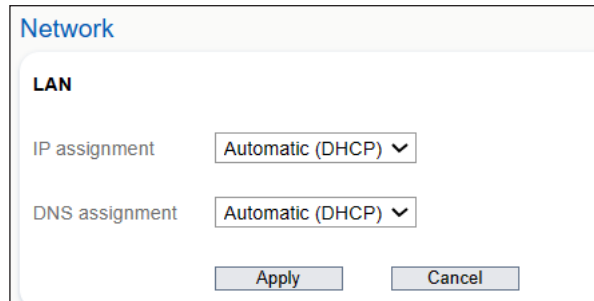
< Part 4 > System

< 4.1 > Network

Network allows you to configure the IPv4, IPv6 and 802.1x authentication setting.

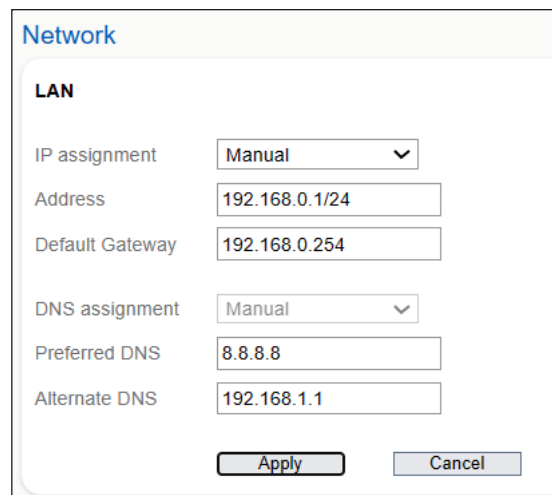
IPv4 network setting

- i. Click Network and you can see the following image displays. You can change the IPv4 setting. The default IP4 assignment and DNS assignment is DHCP.



The screenshot shows a 'Network' configuration window. Under the 'LAN' section, there are two dropdown menus: 'IP assignment' and 'DNS assignment', both set to 'Automatic (DHCP)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- ii. If your network does not support DHCP, you can change the IP assignment to "Manual". Then input the IPv4 address & subnet prefix in "Address" and the Gateway to "Default Gateway". You can input "Preferred DNS" and "Alternate DNS" or let them empty, it depends on your network requirement. Then click "Apply".

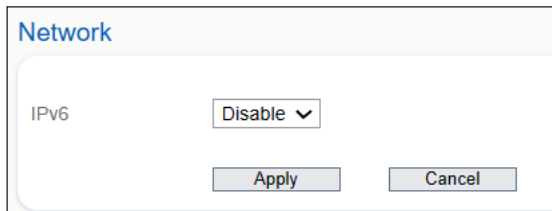


The screenshot shows the 'Network' configuration window with 'IP assignment' set to 'Manual'. The 'Address' field contains '192.168.0.1/24', 'Default Gateway' contains '192.168.0.254', and 'DNS assignment' is set to 'Manual'. Below these, 'Preferred DNS' is '8.8.8.8' and 'Alternate DNS' is '192.168.1.1'. The 'Apply' button is highlighted.

< 4.1 > Network

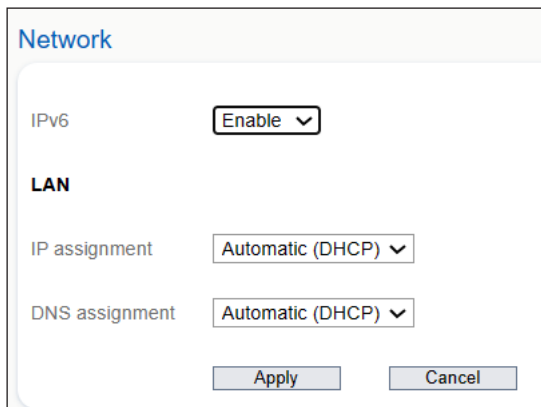
IPv6 network setting

- i. If your network supports IPv6, go to Network > IPv6 to configure your IPv6 network setting. Default IPv6 setting is “Disable”



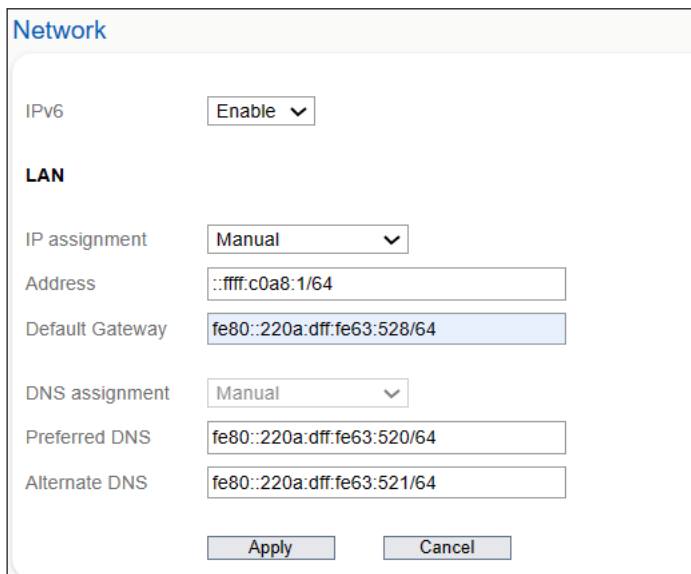
The screenshot shows a window titled "Network". Inside, there is a section for "IPv6" with a dropdown menu currently set to "Disable". Below this, there are two buttons: "Apply" and "Cancel".

- ii. Select “Enable” and you can see the following image displays. If your IPv6 network supports DHCP, click “ Apply ”.



The screenshot shows the "Network" window with "IPv6" set to "Enable". Below this, there is a section titled "LAN". Under "LAN", there are two dropdown menus: "IP assignment" set to "Automatic (DHCP)" and "DNS assignment" set to "Automatic (DHCP)". At the bottom are "Apply" and "Cancel" buttons.

- iii. If your network does not support DHCP, you can change the IP assignment to “Manual”. Then input the IPv6 address & subnet prefix in “Address” and the Gateway to “Default Gateway”. You can input “Preferred DNS” and “Alternate DNS” or let them empty, it depends on your network requirement. Then click “ Apply ”.

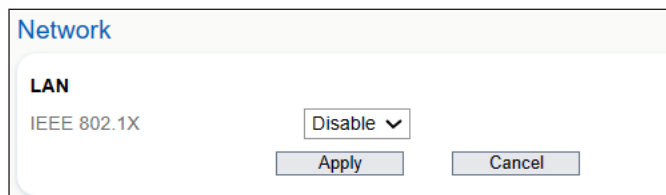


The screenshot shows the "Network" window with "IPv6" set to "Enable". Under the "LAN" section, "IP assignment" is set to "Manual". Below this, there are several text input fields: "Address" containing "::ffff:c0a8:1/64", "Default Gateway" containing "fe80::220a:dff:fe63:528/64", "DNS assignment" set to "Manual", "Preferred DNS" containing "fe80::220a:dff:fe63:520/64", and "Alternate DNS" containing "fe80::220a:dff:fe63:521/64". At the bottom are "Apply" and "Cancel" buttons.

< 4.1 > Network

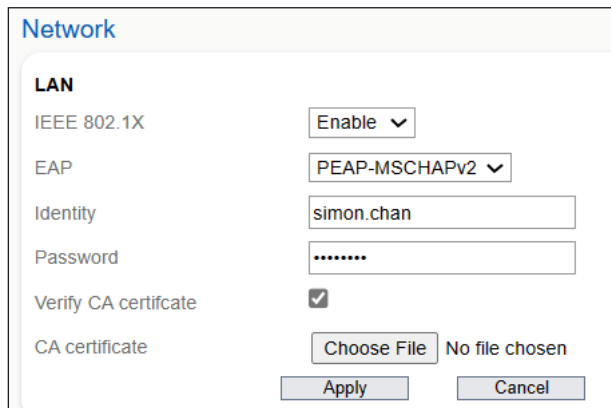
802.1x authentication

- i. Go to Network > 802.1X and you can see the following image displays.



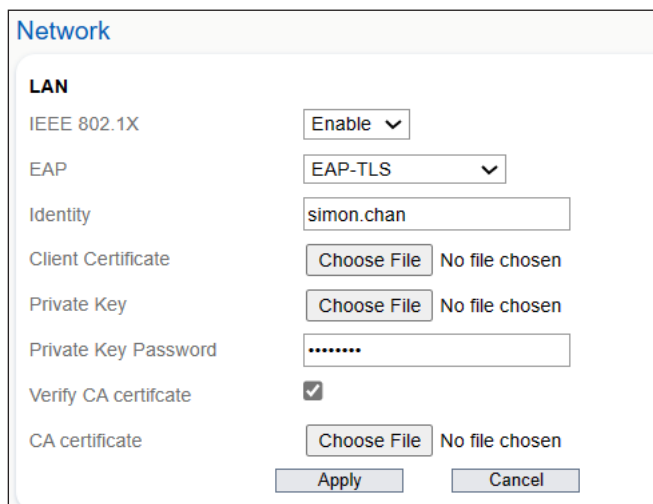
The screenshot shows a 'Network' configuration window. Under the 'LAN' section, 'IEEE 802.1X' is set to 'Disable'. There are 'Apply' and 'Cancel' buttons at the bottom.

- ii. Select "Enable" and you can select EAP authentication as "PEAP-MSCHAPv2" or "EAP-TLS". If you select "PEAP-MSCHAPv2". Input the "Identity", "Password" & CA certificate in .PEM format if you tick "Verify CA certificate". Then click "Apply".



The screenshot shows the 'Network' configuration window with 'IEEE 802.1X' set to 'Enable'. Under the 'EAP' section, 'PEAP-MSCHAPv2' is selected. The 'Identity' field contains 'simon.chan', the 'Password' field is masked with dots, and 'Verify CA certificate' is checked. The 'CA certificate' field shows a 'Choose File' button and 'No file chosen'. 'Apply' and 'Cancel' buttons are at the bottom.

- iii. If you select "EAP-TLS", input Identity, Client Certificate, Private Key, Private Key Password & CA certificate if you tick "Verify CA certificate". Then click "Apply".



The screenshot shows the 'Network' configuration window with 'IEEE 802.1X' set to 'Enable'. Under the 'EAP' section, 'EAP-TLS' is selected. The 'Identity' field contains 'simon.chan'. The 'Client Certificate', 'Private Key', and 'CA certificate' fields each show a 'Choose File' button and 'No file chosen'. The 'Private Key Password' field is masked with dots, and 'Verify CA certificate' is checked. 'Apply' and 'Cancel' buttons are at the bottom.

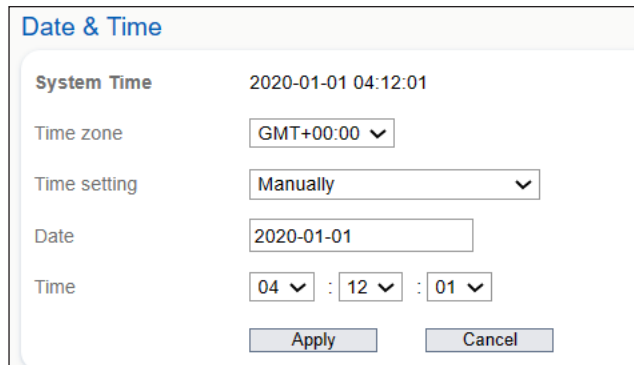
< 4.2 > Date & Time

You can set the internal clock on the Z-3001 manually or link to a Network Time Protocol (NTP) server.

To set the date & time :

- i. Go to System > Date & Time
- ii. Click the Time zone to select your time zone from the list.
- iii. Select the method for setting the date & time

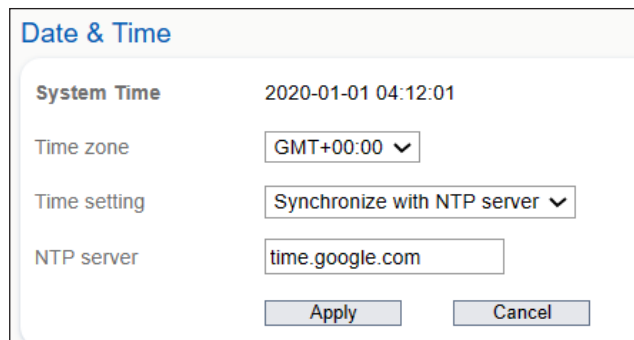
Set Date & Time Manually :



The screenshot shows the 'Date & Time' configuration interface. At the top, the 'System Time' is displayed as '2020-01-01 04:12:01'. Below this, the 'Time zone' is set to 'GMT+00:00' with a dropdown arrow. The 'Time setting' is set to 'Manually' with a dropdown arrow. The 'Date' field contains '2020-01-01'. The 'Time' field is split into three dropdowns showing '04', '12', and '01'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- Select “Manually” from the time setting field
- Input the date
- Select the time from the list
- Click “Apply ”

Using the NTP server :



The screenshot shows the 'Date & Time' configuration interface. At the top, the 'System Time' is displayed as '2020-01-01 04:12:01'. Below this, the 'Time zone' is set to 'GMT+00:00' with a dropdown arrow. The 'Time setting' is set to 'Synchronize with NTP server' with a dropdown arrow. The 'NTP server' field contains 'time.google.com'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- Select “Synchronize with NTP server” from Time setting field
- Input the NTP server to the NTP server field
- Click “Apply ”

< 4.3 > Authentication

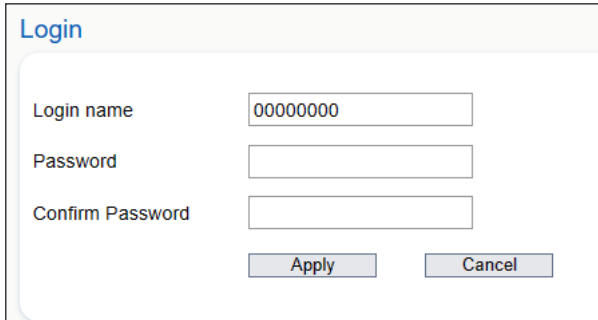
For security purposes, users attempting to login to the Z-3001 must be authenticated.

The Z-3001 supports one of the following authentication mechanisms.

- Local user on the Z-3001
- Lightweight Directory Access Protocol (LDAP)

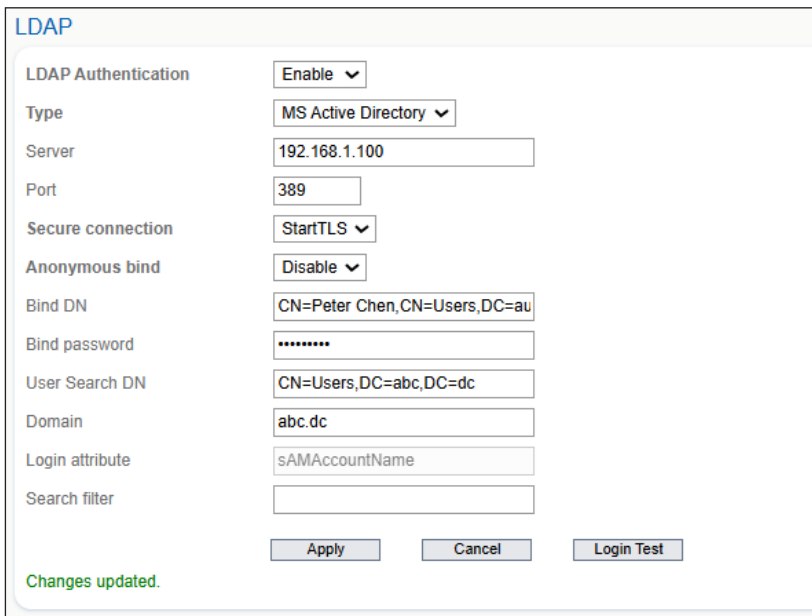
By default, the Z-3001 is configured for local authentication. If you prefer external authentication, you must provide the Z-3001 with information about the external Authentication and Authorization (AA) server.

Authentication by local user

The screenshot shows a 'Login' configuration window. It has three input fields: 'Login name' with the value '00000000', 'Password', and 'Confirm Password'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- Go to System > Authentication > Local
- Input the new login name in "Login name" field
- Input new password in " Password " field.
(You can leave the password unchanged if you just want to change the login name.)
- Input the new password in "Confirm password" field for verification
- Click " Apply "

Authentication by LDAP (MS Active Directory)

The screenshot shows an 'LDAP' configuration window. It contains several fields: 'LDAP Authentication' (dropdown set to 'Enable'), 'Type' (dropdown set to 'MS Active Directory'), 'Server' (text field with '192.168.1.100'), 'Port' (text field with '389'), 'Secure connection' (dropdown set to 'StartTLS'), 'Anonymous bind' (dropdown set to 'Disable'), 'Bind DN' (text field with 'CN=Peter Chen,CN=Users,DC=au'), 'Bind password' (password field with masked characters), 'User Search DN' (text field with 'CN=Users,DC=abc,DC=dc'), 'Domain' (text field with 'abc.dc'), 'Login attribute' (text field with 'sAMAccountName'), and 'Search filter' (empty text field). At the bottom, there are 'Apply', 'Cancel', and 'Login Test' buttons. A green message 'Changes updated.' is visible at the bottom left.

- Go to System > Authentication > Domain/LDAP
- Select "Enable" from LDAP authentication field
- Select "MS Active Directory" from the Type field.
- Input the IP address or hostname in the Server field
- Input the port no. in the port field
- Select the secure connection type (StartTLS / TLS / none) from secure connection field
- Select Enable / Disable from Anonymous bind field. Default is "Disable".
If you select Enable, you need NOT to input Bind DN & Bind Password field.
- Input the Bind DN in the Bind DN field.
- Input the Bind password in the Bind password field.
- Input user search DN in the User Search DN field.
- Input the name of the Active Directory Domain in the Domain field.
- Input the criteria for finding user objects within the directory tree in the Search filter field.
- Click " Apply "

< 4.3 > Authentication

Authentication by LDAP (OpenLDAP)

The screenshot shows a web-based configuration interface for LDAP authentication. The title is 'LDAP'. The configuration is organized into a table-like structure with labels on the left and input fields on the right. The fields are: 'LDAP Authentication' (dropdown menu set to 'Enable'), 'Type' (dropdown menu set to 'OpenLDAP'), 'Server' (text input field containing '192.168.1.16'), 'Port' (text input field containing '389'), 'Secure connection' (dropdown menu set to 'StartTLS'), 'Anonymous bind' (dropdown menu set to 'Disable'), 'Bind DN' (text input field containing 'uid=admin,cn=users,dc=rdserver,'), 'Bind password' (password input field with masked characters), 'User Search DN' (text input field containing 'cn=users,dc=rdserver,dc=austin-l'), 'Domain' (text input field containing 'example.com'), 'Login attribute' (text input field containing 'uid'), and 'Search filter' (empty text input field). At the bottom of the form are three buttons: 'Apply', 'Cancel', and 'Login Test'. Below the buttons, a green message states 'Changes updated.'

- i. Go to System > Authentication > Domain/LDAP
- ii. Select "Enable" from LDAP authentication field
- iii. Select "OpenLDAP" from the Type field.
- iv. Input the IP address or hostname in the Server field
- v. Input the port no. in the port field
- vi. Select the secure connection type (StartTLS / TLS / none) from secure connection field
- vii. Select Enable / Disable from Anonymous bind field. Default is "Disable".
If you select Enable, you need not to input Bind DN & Bind Password field.
- viii. Input the Bind DN in the Bind DN field.
- ix. Input the Bind password in the Bind password field.
- x. Input user search DN in the User Search DN field.
- xi. Input the login attribute in the Login Attribute field.
- xii. Input the criteria for finding user objects within the directory tree in the Search filter field.
- xiii. Click " Apply "

< 4.4 > Service

In Service, you can change the WEB portal setting to access the WEB interface. You can also enable or disable SNMP communication between an SNMP manager and the Z-3001.

Web Portal

The default port number of HTTP is 80 and Force HTTPS redirect is enabled. The default port number of HTTPS is 443. To change the setting :

- i. Go to Service > Web Portal
- ii. Input the new port for HTTP
- iii. Disable or enable Force HTTPS redirect
- iv. Input the new port for HTTPS

Web Portal

HTTP

Port80

Force HTTPS redirect☒

HTTPS

Port443

Upload custom key & certificate☐

Certificate Validity

Not beforeNov 29 07:31:59 2023 GMT

Not afterNov 28 07:31:59 2033 GMT

Key length2048 bit

Issued To

Common Name

Organization

Organization Unit

Default Certificate

null

null

Issued By

Common Name

Organization

Organization Unit

Default Certificate

null

null

Apply

Cancel

- v. If you check Upload custom key & certificate, you can see the following similar image displays.
- vi. Import the Key in .PEM format
- vii. Import the Certificate in .PEM format
- viii. Click “Apply”

Web Portal

HTTP

Port80

Force HTTPS redirect☒

HTTPS

Port443

Upload custom key & certificate☒

Key

Choose FileNo file chosen

Certificate

Choose FileNo file chosen

Certificate Validity

Not beforeNov 29 07:31:59 2023 GMT

Not afterNov 28 07:31:59 2033 GMT

Key length2048 bit

Issued To

Common Name

Organization

Organization Unit

Default Certificate

null

null

Issued By

Common Name

Organization

Organization Unit

Default Certificate

null

null

Apply

Cancel

SNMP Agent

- i. Go to Service > SNMP Agent

SNMP Agent

Agent

Disable

Port

161

sysName

default_name

sysLocation

default_location

sysContact

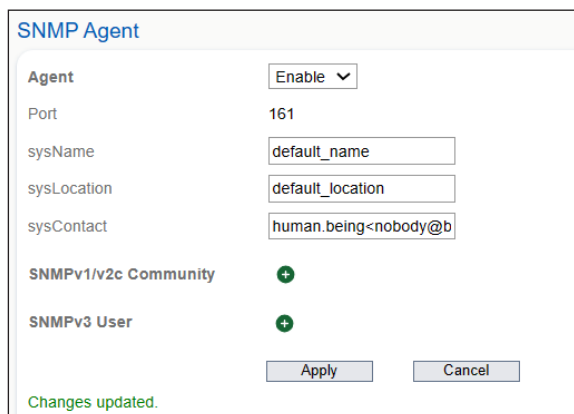
human.being<nobody@b

Apply

Cancel

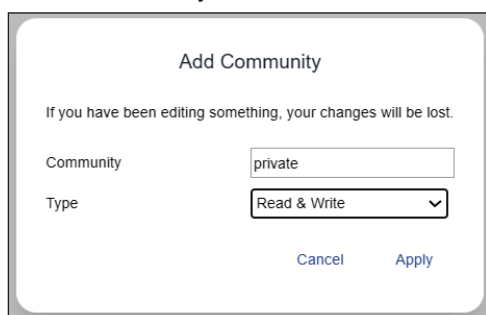
< 4.4 > Service

- ii. Enable SNMP Agent. Input sysName (default : default_name), sysLocation (default : default_location), sysContact (default : human.being<nobody@but.you>)



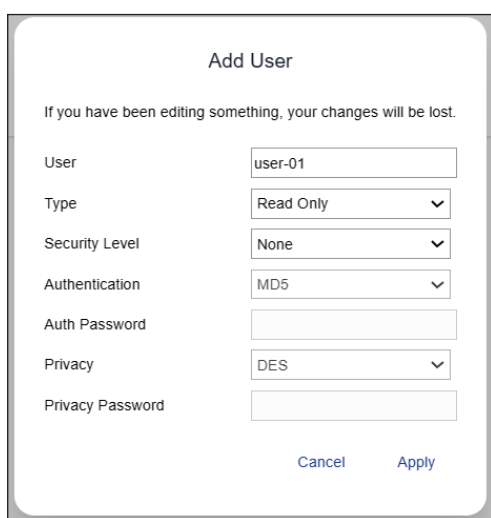
The image shows the 'SNMP Agent' configuration window. It has a title bar 'SNMP Agent'. Inside, there's a section 'Agent' with a dropdown menu set to 'Enable'. Below that, 'Port' is set to '161'. Then, 'sysName' is 'default_name', 'sysLocation' is 'default_location', and 'sysContact' is 'human.being<nobody@b'. There are two green plus icons next to 'SNMPv1/v2c Community' and 'SNMPv3 User'. At the bottom, there are 'Apply' and 'Cancel' buttons. A green message 'Changes updated.' is at the bottom left.

- iii. If you enable v1/v2c, click “” next to SNMPv1/v2c Community.
- iv. Input the value of Community.
- v. Select Read Only or Read & Write from Type field. Then click “Apply”



The image shows the 'Add Community' dialog box. It has a title bar 'Add Community'. Inside, there's a warning: 'If you have been editing something, your changes will be lost.' Below that, 'Community' is 'private' and 'Type' is 'Read & Write'. At the bottom, there are 'Cancel' and 'Apply' buttons.

- vi. If you enable SNMPv3, click “” next to SNMPv3 User.
- vii. Input the user name in User field
- viii. Select Read Only or Read & Write from Type field
- ix. Select None / Authentication / Privacy from Security Level field
- x. If you select None, then click “Apply”.



The image shows the 'Add User' dialog box. It has a title bar 'Add User'. Inside, there's a warning: 'If you have been editing something, your changes will be lost.' Below that, 'User' is 'user-01', 'Type' is 'Read Only', 'Security Level' is 'None', 'Authentication' is 'MD5', 'Auth Password' is empty, 'Privacy' is 'DES', and 'Privacy Password' is empty. At the bottom, there are 'Cancel' and 'Apply' buttons.

- xi. If you select “Authentication” from Security Level field, select MD5/SHA/SHA-224/SHA-256/SHA-384/SHA-512 from Authentication field

< 4.4 > Service

- xii. Input the password in Auth Password field (Length : 8 ~ 32 char.). Then click “Apply”

Add User

If you have been editing something, your changes will be lost.

User	user-01
Type	Read Only
Security Level	Authentication
Authentication	MD5
Auth Password	
Privacy	DES
Privacy Password	

[Cancel](#) [Apply](#)

- xiii. If you select “Privacy” from Security field,
select MD5/SHA/SHA-224/SHA-256/SHA-384/SHA-512 from Authentication field.
- xiv. Input the password in Auth Password field (Length : 8 ~ 32 char.).
- xv. Select DES/AES/AES-128/AES-192/AES-256 from Privacy field
- xvi. Input the password in Privacy Password field (Length : 8 ~ 32 char.). Then click “Apply”

Add User

If you have been editing something, your changes will be lost.

User	user-01
Type	Read Only
Security Level	Privacy
Authentication	MD5
Auth Password	
Privacy	DES
Privacy Password	

[Cancel](#) [Apply](#)

Intentionally Left Blank

< 4.5 > Notification

In Notification, you can enable the alarm email server and SNMP trap. When event or alert is triggered, the Z-3001 will send out an email and SNMP trap to a specific user(s).

Email

- i. Go to Notification > Email
- ii. Select Enable from Notification field. Default is Disable
- iii. Input the IP address or domain name of the SMTP server
- iv. Input the SMTP port. Default is 25
- v. Select Disable / Enable from Authentication field
- vi. If select Enable from Authentication field, input sender email address in Username field and password in Password field.
- vii. Select None/StartTLS from Secure Connection field
- viii. Input the sender email address in Sender email field
- ix. Input the name in the Sender name field
- x. Input the receiver's email address in the Recipient field.
If more than one recipient, please use semi-colon or comma to separate each email address.
- xi. Click "Apply".

The screenshot shows the 'Email' configuration window. It has a title bar 'Email' and a list of settings: 'Email Notification' (dropdown set to 'Enable'), 'SMTP server' (text box with 'smtp.mail.com'), 'SMTP port' (text box with '25'), 'Authentication' (dropdown set to 'Disable'), 'Username' (text box), 'Password' (text box with 'leave unchanged'), 'Secure connection' (dropdown set to 'None'), 'Sender email' (text box with 'sender@mail.com'), 'Sender name' (text box with 'sender'), and 'Recipient' (text area with 'recipient01@mail.com'). At the bottom are three buttons: 'Apply', 'Cancel', and 'Send Test'.

SNMP Trap

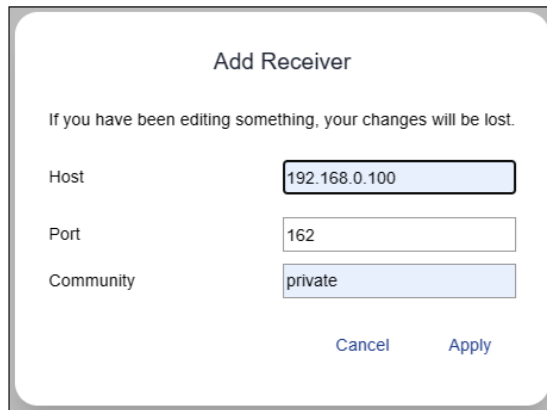
To receive event or alert notification via SNMP, please configure the SNMP trap setting.

- i. Go to Notification > SNMP Trap
- ii. Select Enable from SNMP Trap Notification field. Default is Disable.
- iii. Select Trap/Inform from Type field.
- iv. If you select Inform from Type field. Please input the time interval in seconds after which a new inform communication is resent if the first is not received in the Timeout field. Input the number of time you want to resend the inform communication if it fails in Retries field.

The screenshot shows the 'SNMP Trap' configuration window. It has a title bar 'SNMP Trap' and a list of settings: 'SNMP Trap Notification' (dropdown set to 'Enable'), 'Type' (dropdown set to 'Trap'), 'Timeout' (text box with '1'), 'Retries' (text box with '3'), and 'Receivers' (a green plus icon). At the bottom are two buttons: 'Apply' and 'Cancel'. Below the buttons, the text 'Changes updated.' is displayed in green.

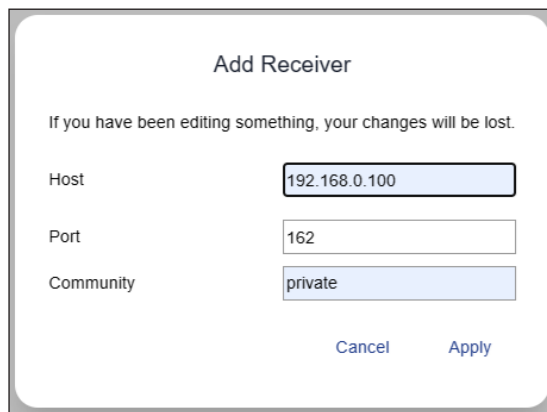
< 4.5 > Notification

- v. Click “” next to the Receivers, you can see the following similar image displays.



The image shows a dialog box titled "Add Receiver". At the top, it says "If you have been editing something, your changes will be lost." Below this, there are three input fields: "Host" with the value "192.168.0.100", "Port" with the value "162", and "Community" with the value "private". At the bottom right, there are two buttons: "Cancel" and "Apply".

- vi. Input the IP address in the Host field. This is the address to which notifications are sent by the SNMP agent.
vii. Input the port number used to access the host in the Port field.
viii. Input the value of community in Community field used to access the Z-3001
ix. Click “Apply”
x. Repeat v to ix to add more receivers.



The image shows a dialog box titled "Add Receiver". At the top, it says "If you have been editing something, your changes will be lost." Below this, there are three input fields: "Host" with the value "192.168.0.100", "Port" with the value "162", and "Community" with the value "private". At the bottom right, there are two buttons: "Cancel" and "Apply".

< 4.6 > Maintenance

In Maintenance, you can view the system information, do the firmware update and view the event log.

Information

- i. Go to Maintenance > Information, you can see the following similar image displays.

System Information

Model

Z-3001

Firmware version

1.5.3

Hardware revision

1.0

Up time

23 hours, 48 minutes

Reboot

Network Information

LAN

MAC address

20:0A:0D:67:00:0F

Connection

1000Mb/s, Full duplex, auto-negotiation on

Type

DHCP

IP address

192.168.0.1/24

Gateway

192.168.0.254

- ii. You can view the system and network information.
- iii. Click “Reboot” to reboot the Z-3001

Firmware

- To perform the firmware update of the Z-3001
- i. Download the appropriate firmware file in .img extension from the link below
 - ii. Go to Maintenance > Firmware
 - iii. Click “Choose File” to select firmware file to update

Firmware

This may take some minutes. Please do NOT power off the device while the update is in progress!

After a successful update, the device will restart automatically.

Choose File

No file chosen

Update

- iv. Once the firmware file is chosen, click “Open”

Name ^

Date modified

Type

Size

Z3001-1.5.4

12/8/2024 3:19 pm

Disc Image File

11,877 KB

All files

Upload from mobile

Open

Cancel

< 4.5 > Maintenance

- v. Click “Update” to start the firmware update process.
Once the firmware update completes, the WEBUI goes back to the login page.

This may take some minutes. Please do NOT power off the device while the update is in progress!

After a successful update, the device will restart automatically.

Choose File

Z3001-1.5.4.img

Update

Event Log

Event log shows the Date, time, severity level and details of the events or alerts from the Z-3001.

Logs

Date	Time (UTC+08:00)	Severity	Message
2024-10-09	21:37:28	Info	S1 Sensor 01 connected.
2024-10-09	21:37:28	Info	S1 Sensor 01 addition is successful.
2024-10-09	21:37:09	Info	S2 Sensor 01 removal is successful.
2024-10-09	21:37:05	Info	S1 Sensor 01 removal is successful.
2024-10-09	21:36:51	Critical	S1 Out of range.
2024-10-09	21:36:03	Critical	SNMP inform 192.168.1.174:162 is failed.
2024-10-09	21:36:03	Critical	SNMP inform 192.168.1.174:162 is failed.

The company reserves the right to modify product specifications without prior notice and assumes no responsibility for any error which may appear in this publication.

All brand names, logo and registered trademarks are properties of their respective owners.

Copyright 2025 Austin Hughes Electronics Ltd. All rights reserved.

UM-IS-Z3001-Q225V1

www.austin-hughes.com