SDOC-5013

Access Control Systems

NEPTUNE

Mobile User Programming Guide

SICUNET

Notices

Standards Approvals

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 when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This access control system is compliant with Level I UL 294 listed devices and must be installed in controlled locations.

Corporate Office

USA

4840 Irvine Blvd. Suite 113, Irvine, CA 92620

Tel. +1-857-346-0130 Fax. +1-714-512-6816

China

E1608 Bldg-East, Nanshan Digital Technology & Cultural Industry Park, Nanshan, Shenzhen, China 518052

Tel. +86-755-2665-6082

Korea

Samsung-Dong, 8-1 Gunsul B/D Suite 301, Gangnam-Gu, Seoul, Korea 06097

Tel. +82-70-8286-2808 Fax. +82-2-6918-4928

www.sicunet.com

Technical Support

Tel.: +1-857-346-0130

E-mail: tech@sicunet.com

Notice

It is important that this instruction manual be read and understood completely before installation or operation is attempted. It is intended that the installation of this unit will be performed only by persons trained and qualified in the installation of access control equipment. The important safeguards and instructions in this manual cannot cover all possible conditions and situations which may occur during installation and use. It must be understood that common sense and caution must be exercised by the person(s) installing, maintaining and operating the equipment.

Table of Contents

1.0 Introduction

This manual contains information regarding the mobile programming and configuration of the Neptune access control system. This system offers multi-station ability to secure doors, manage access of personnel, create and analyze reports, and monitor the system remotely from any Web browser. All monitored activity at the facility is recorded in the system memory — providing a record of all Card Holder entries and exits, input detection, and security or fire detection, if desired.

The system can be seamlessly scaled up, via software keys, to provide increased door and reader capacity, enhanced features and higher level capabilities.

1.1 General Features

The following is a feature summary of the Controller:

· Browser-based management enables system status and updates from any location, with any supported OS, using any supported browser — Chrome ver. 22 or higher; IE 9.0 or higher; Firefox ver. 13 or higher; Safari ver. 5.1.7 or higher.

· Supports access from iPhone, iPad and Android devices.

· Intuitive Wizard allows for ultra-fast setup.

· Configure the system to perform automatic functions on specific days and times. For example, schedule when a door is unlocked or when an employee can gain access to the facility.

· Create, view and print customized reports using the reporting tool.

· Create a set of instructions that the system will follow when an event occurs. For example, when a door is forced open the system can be instructed to turn on a camera and display a graphic.

· Configure the system to store custom information about each Card Holder such as phone number or employee ID.

· Define up to 30 holidays for use as special schedules. For example, schedule a door to remain locked during a holiday.

· Configure the system to send email and text message notifications.

1.2 System Information

Systems are available in a variety of models starting with one door, two reader configurations.

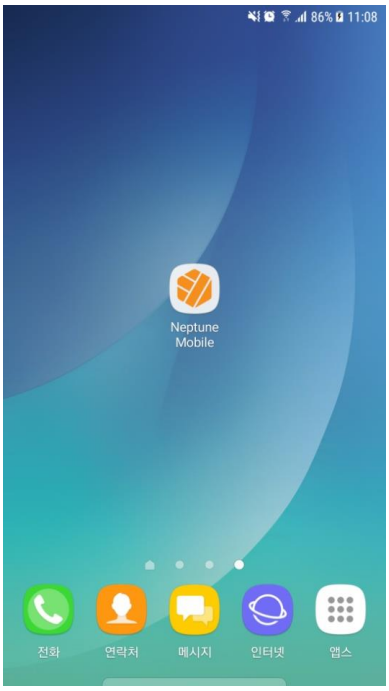
Models can be upgraded with expanded capabilities using optional software license keys. The system includes Ethernet support, an integrated web server and Power over Ethernet (PoE) support.

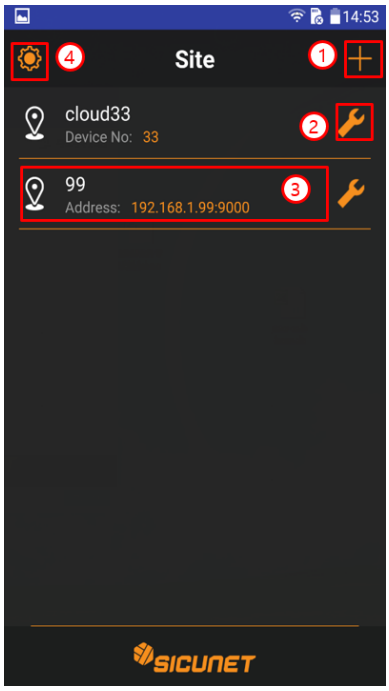
Specifications	
Processor	Quad Core Cortex, 1.5 GHz
Power	Regulated 12VDC @ 2A (24W), not supplied
Operating system	Embedded Linux
Transactions per second	> 30
Enclosure (W x H x D):	3.2 in X 3.0 in X 1.3 in (81 mm X 78 mm X 32 mm)
Temperature specification	-4°F to 120°F (-20°C to 50°C)

2.0 Software Layout

2.1 System Mobile Software

The Controller mobile software interface are simple and easy, users are available to the operator for programming and navigation. The setting provides access to all configuration options. This following illustration shows setting icon.





3.0 System Mobile Programming

3.1 Site

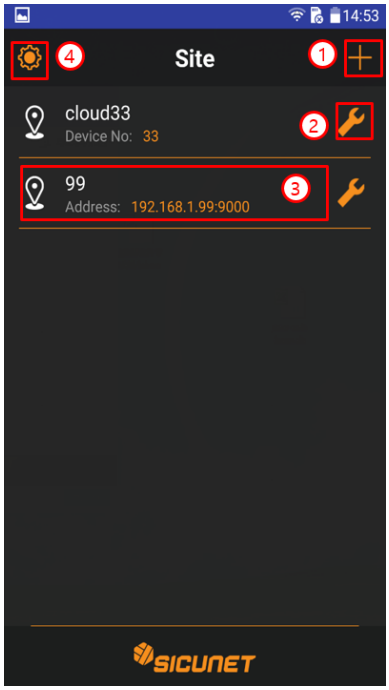
Open a mobile app on your phone and start to setup the access controller you wanted to add. The mobile presents the setup page as shown. And follow the steps below:

1. Add site information.

2. Modify site information.

3. Connect to Site.

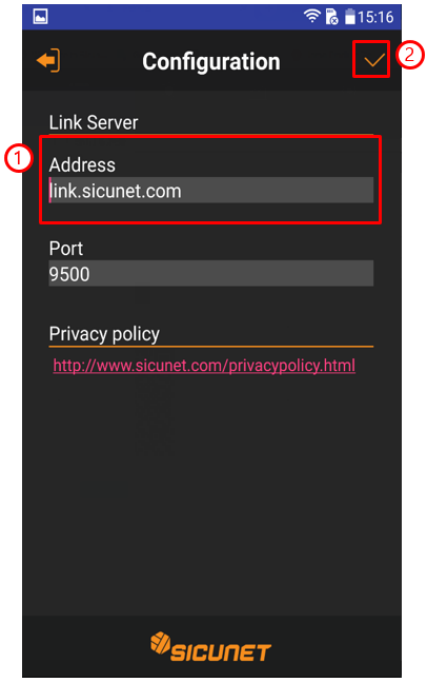
4. Configure Link Server information.



3.2 Configuration

1. Enter the address and port of the Link Server.

2. Apply the modified value.



3.3 Site > Add/Edit

1. Enter Site Name.

2. Select the method to connect to the device. There are 2 kind of connection method: Address method OR Linked method.

3. Address method VS Linked method.

1) Address method: enter the address and port

2) Linked method: input Device No. and Link Type. Link Type is AUTO, STUN, TURN, UPNP, and LAN.

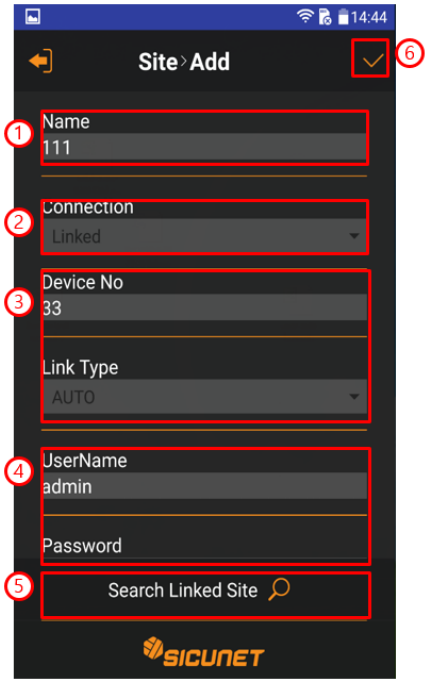
Verify that the power fault input device is functioning properly.

4. Enter your Username and Password.

1) If it is address type, it can search Local Site,

2) User can search your Linked Site if it is Linked.

Apply your changes.

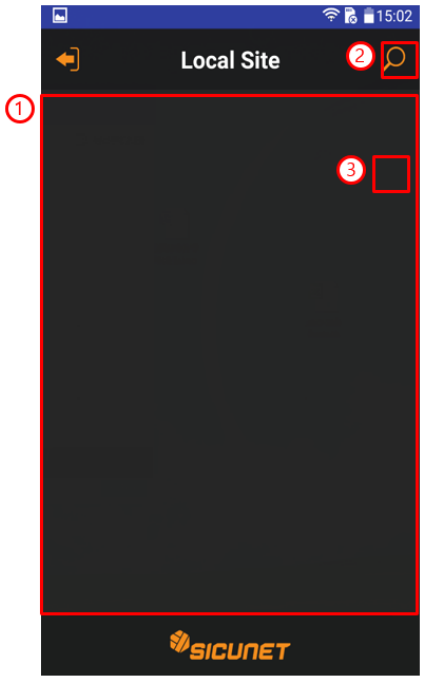


3.4 Local Site

1. Search Local Site to display site list.

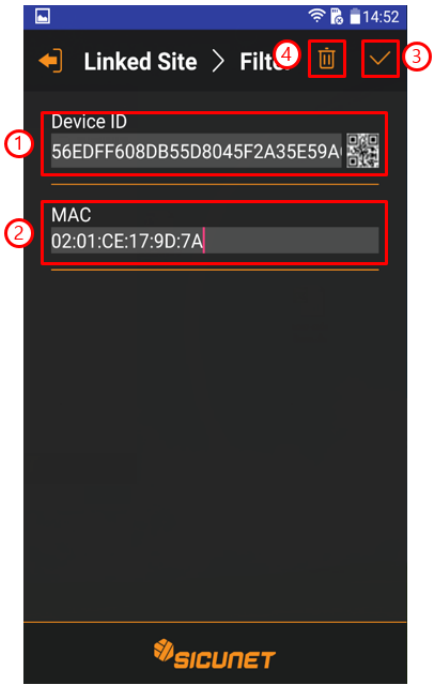
2. Search Local Site.

3. When Site is selected, the screen is closed and the address of the selected device is automatically entered on Site Edit screen.



3.5 Linked Site > Filter

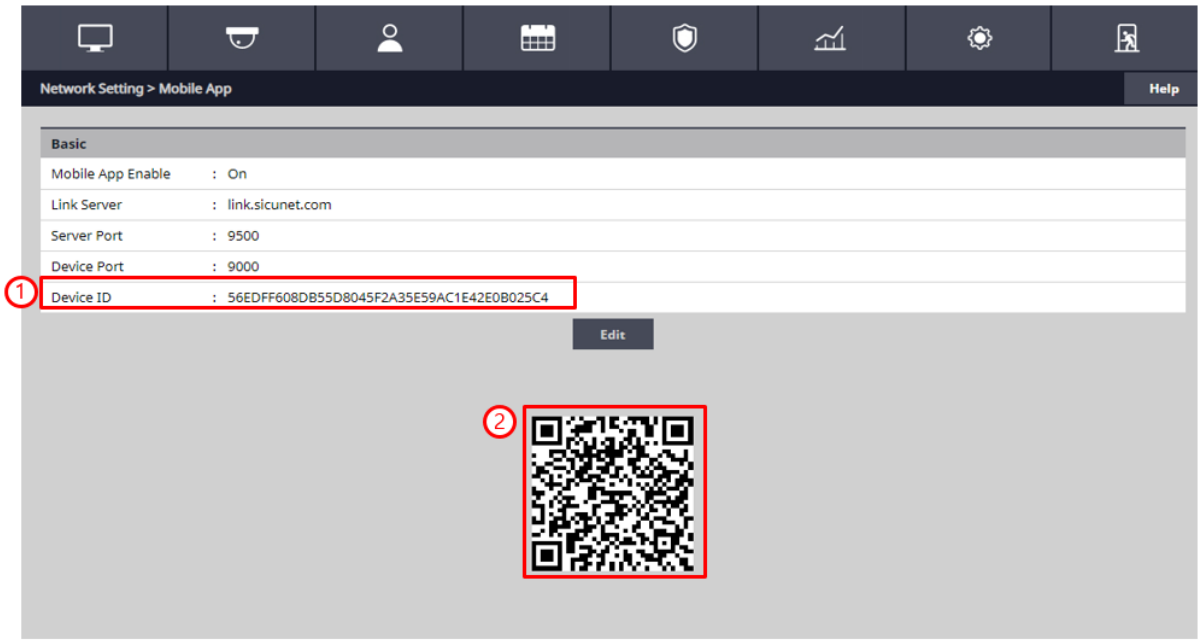
1. Enter the ID of the device to be searched. Device ID can be input easily by using QR code.
2. Enter the MAC address of the device to be searched.
3. Search Linked Site using search criteria.
4. Initialize the search filter.



3.6 Linked Site > QR Code

1. Device ID can be checked in Device's Network Setting > Mobile App.

2. Device ID can be input easily by using QR code.

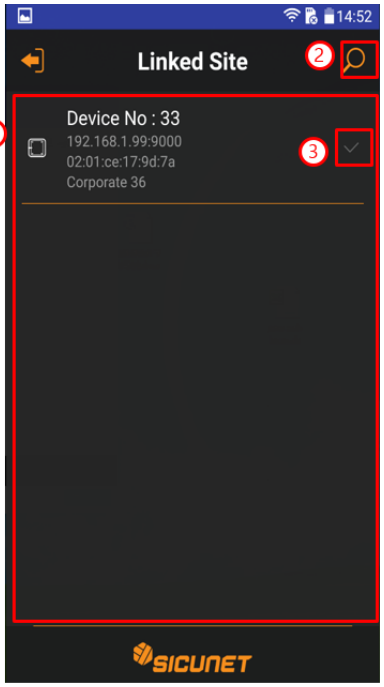


3.7 Linked Site

1. Display device list.

2. Search your Linked Site.

3. When Device is selected, the screen is closed and the No of the selected device is automatically entered on the Site Add screen.



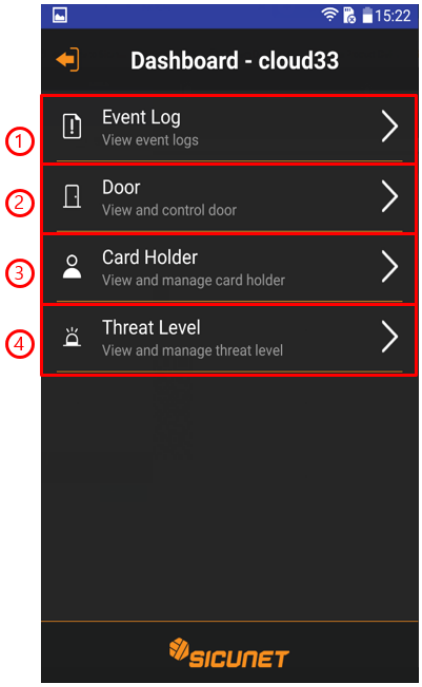
3.8 Dashboard

1. Displays Event Log information.

2. Display and control door information.

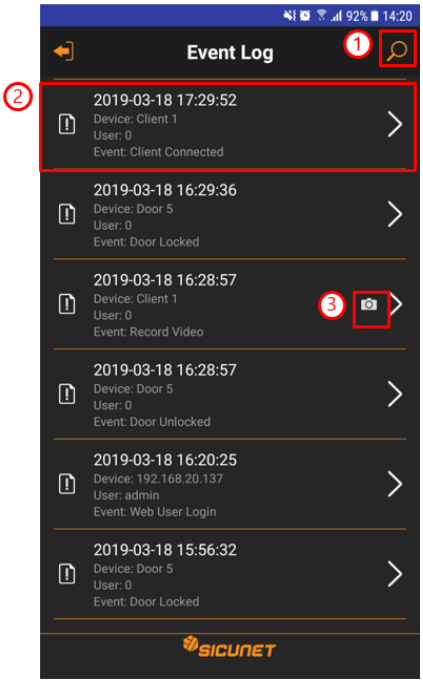
3. Display Card Holder information.

4. View and manage Threat Level information.



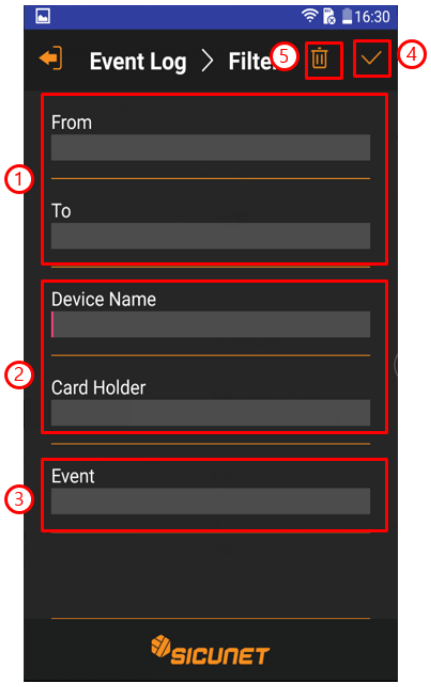
3.9 Event Log

1. Search Event Log.
2. Displays detailed information of Event Log.
3. Displays Event Video information.



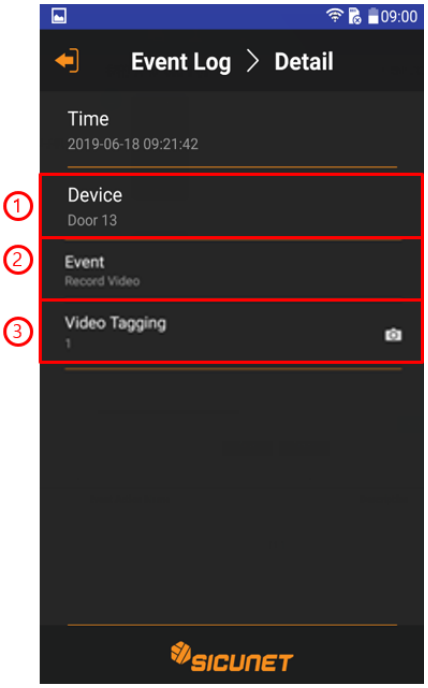
3.10 Event Log > Filter

1. Enter Event Log start and end times.
2. Enter Device Name and User Name.
3. Select Event.
4. Search Event Log using search condition.
5. Initialize the search filter.



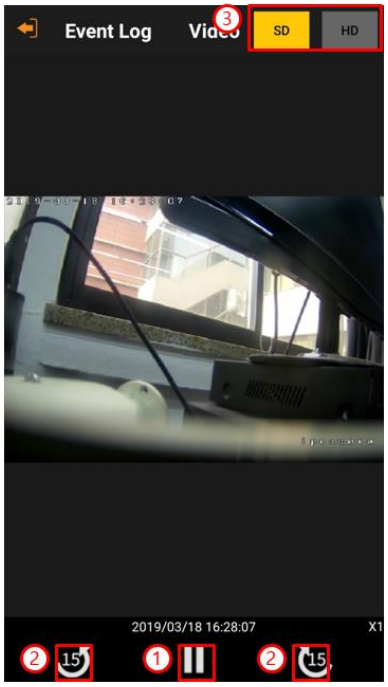
3.11 Event Log > Detail

1. Display Device and User information.
2. Event Details.
3. Display Device's Event Video information.



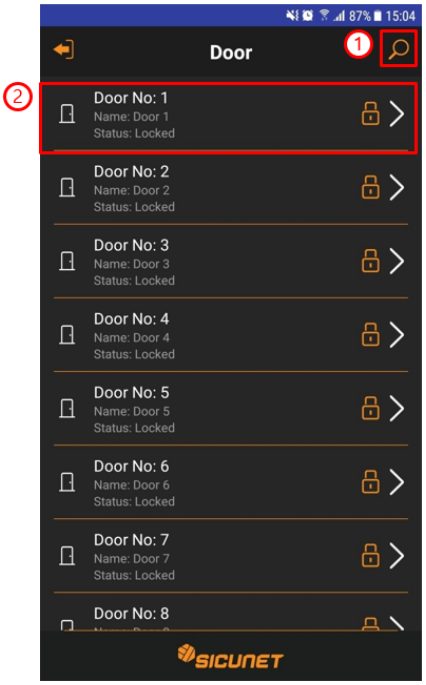
3.12 Event Log > Video

1. Play / Pause Video.
2. Move playback time 15 seconds before / back
3. Select Main / Sub Stream



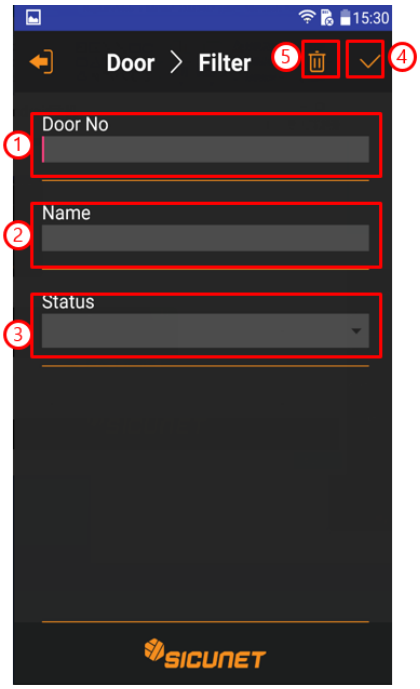
3.13 Door

1. Search door.
2. Display detailed information of door.



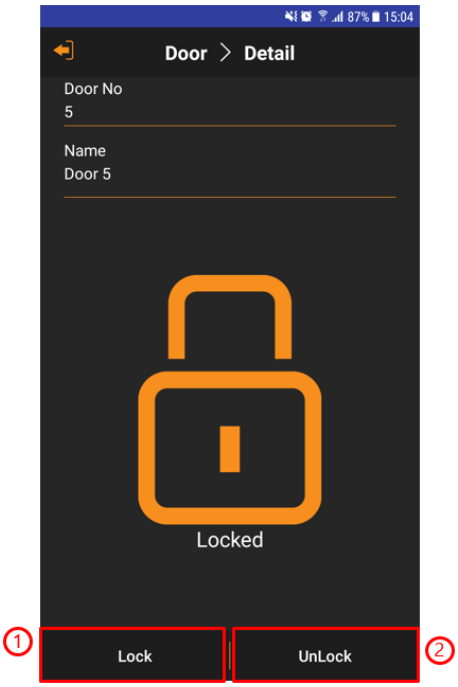
3.14 Door > Filter

1. Enter the door number.
2. Enter the name of the door.
3. Select the door status.
4. Search Door by using search condition.
5. Initialize the search filter.



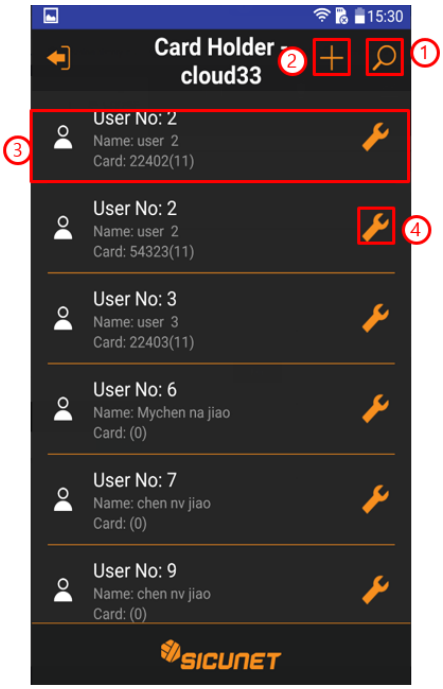
3.15 Door > Detail

1. Lock Door.
2. Unlock Door.



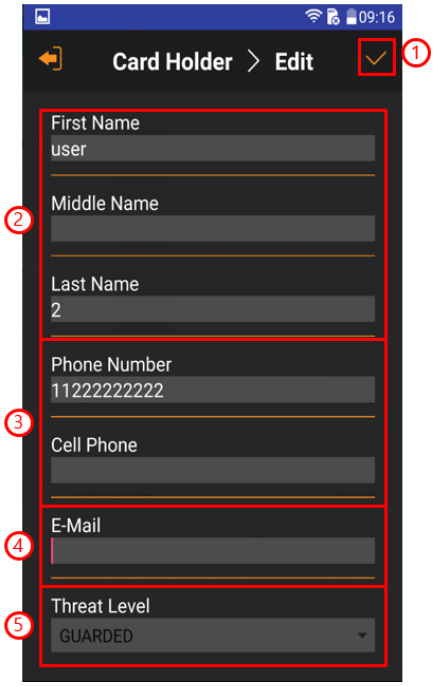
3.16 Card Holder

1. Search Card Holder information.
2. Add Card Holder information.
3. Displays detailed information of Card Holder.
4. Edit Card Holder information.



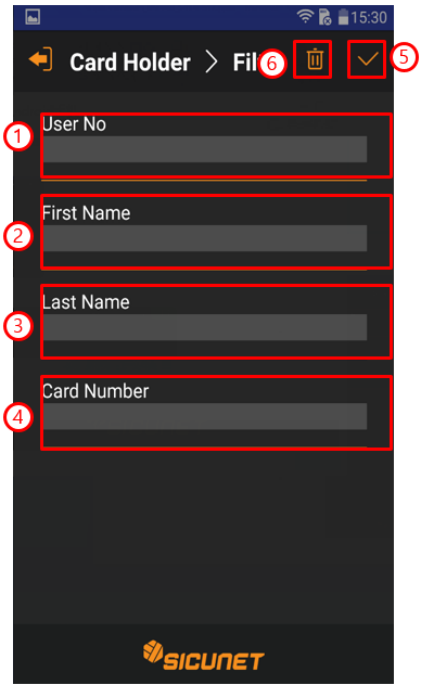
3.17 Card Holder > Add/Edit

1. Apply the modified value.
2. Input user name information.
3. Input phone number information.
4. Input E-mail information.
5. Select threat level.



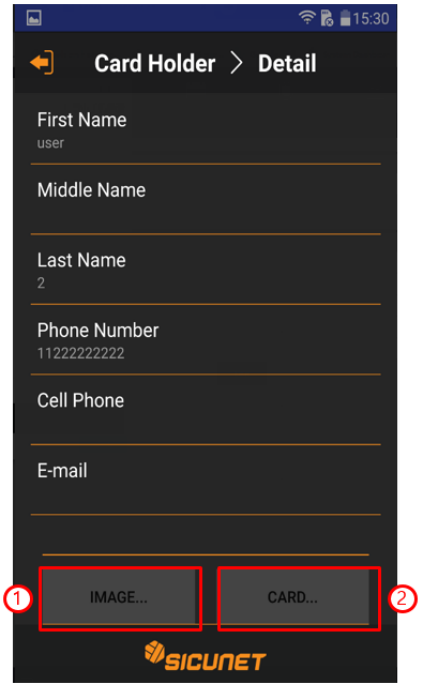
3.18 Card Holder > Filter

1. Enter the Card Holder number.
2. Enter Card Holder First Name.
3. Enter the Card Holder Last Name.
4. Search Card Holder using search criteria.
5. Initialize the search filter.



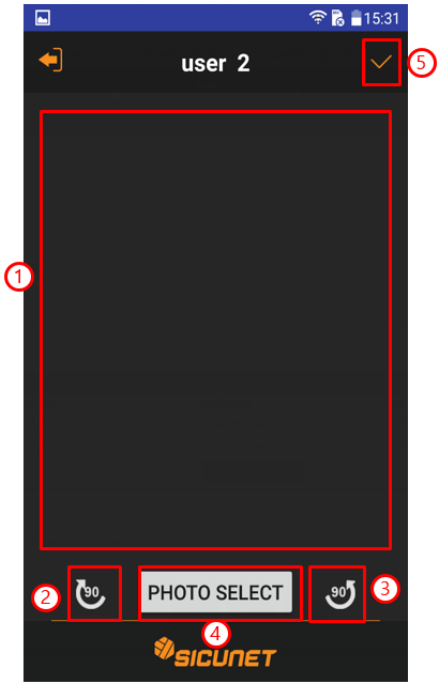
3.19 Card Holder > Detail

1. Display User Image.
2. Display Card.



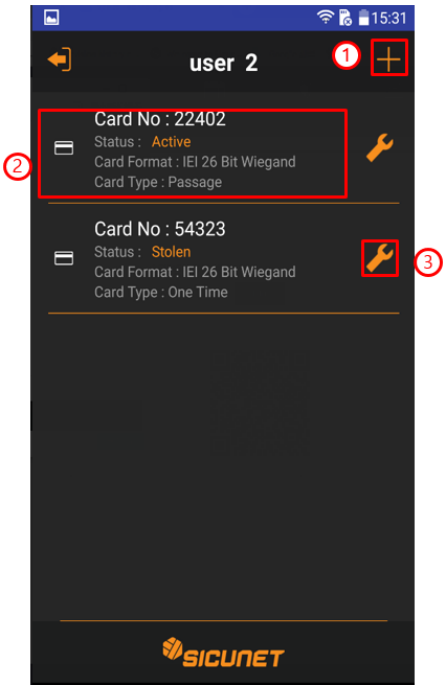
3.20 Card Holder > Image

1. Display User Image.
2. Rotate photo 90degrees to the right.
3. Rotate photo 90 degrees to the left.
4. Select photo.
5. Apply photo.



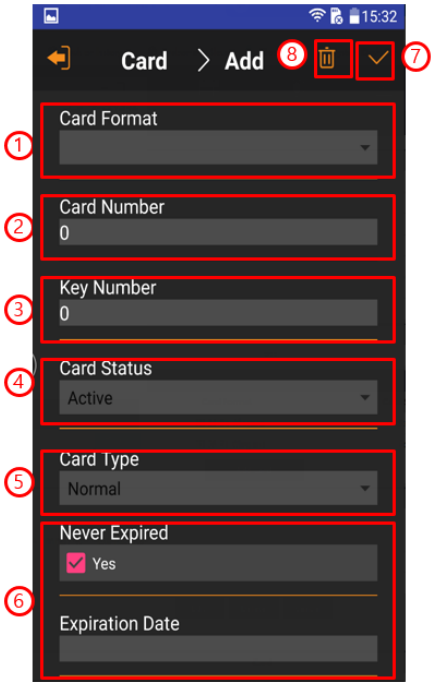
3.21 Card Holder > Card

1. Add Card.
2. Display card list.
3. Edit Card.



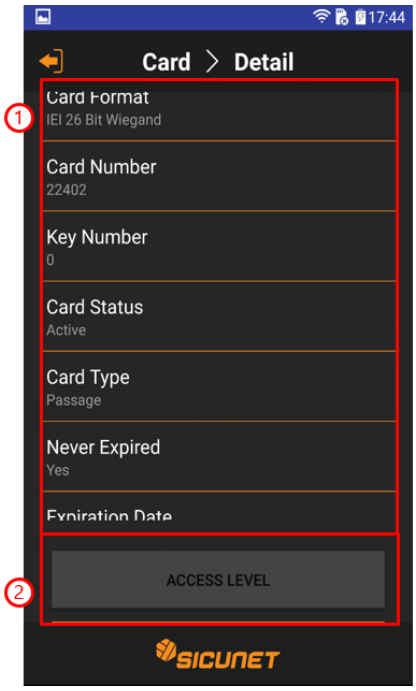
3.22 Card > Add/Edit

1. Enter the card format.
2. Enter the card number.
3. Enter key number.
4. Select card status.
5. Select card type.
6. Select never expired or set expiration date.
7. Apply card information.
8. Initialize the search filter.



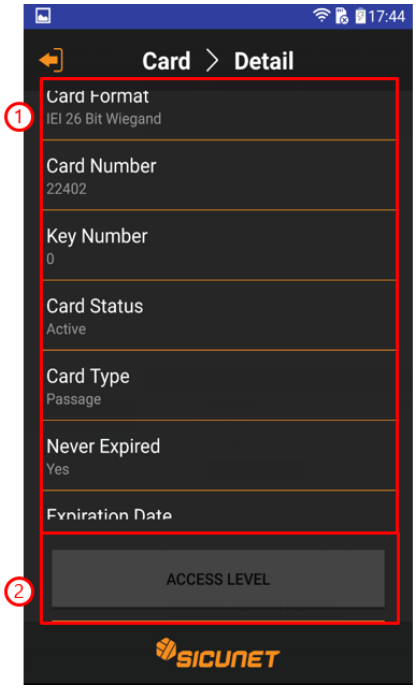
3.23 Card > Detail

1. Display card information.
2. Display and Edit Access Level.



3.24 Access Level > Edit

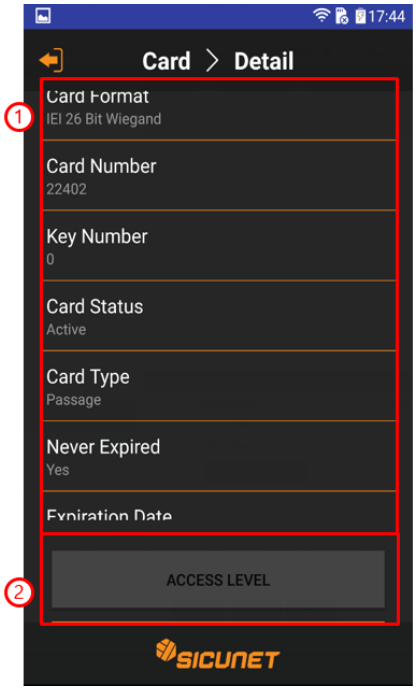
1. Display all access level.
2. Apply selected access level.



3.25 Threat Level

1. Select Threat Level.

2. Apply selected Threat Level.



4.0 Troubleshooting

For further troubleshooting assistance, please visit the following online resources:

USA

4840 Irvine Blvd. Suite 113, Irvine, CA 92620

Tel. +1-857-346-0130 Fax. +1-714-512-6816

China

E1608 Bldg-East, Nanshan Digital Technology & Cultural Industry Park, Nanshan, Shenzhen, China 518052

Tel. +86-755-2665-6082

Korea

Samsung-Dong, 8-1 Gunsul B/D Suite 301, Gangnam-Gu, Seoul, Korea 06097

Tel. +82-70-8286-2808 Fax. +82-2-6918-4928

www.sicunet.com

5.0 Test, Maintenance and Service

5.1 Testing

Monthly testing of the system is recommended.

♦ Check that all used inputs and outputs are correctly functioning with the connected devices.

♦ Check that system and log backups are occurring at scheduled times.

5.2 Maintenance

The systems require very little maintenance. It is recommended to check the following every 6 months:

♦ Installation enclosure and location is secure.

♦ Installation enclosure and location is clean and dry.

♦ All wires are securely connected to the terminals and proper strain relief is used.

5.3 Service

These systems contain Class 2 circuits. Do NOT alter or tamper with any of the components in these systems.

There are no user serviceable parts on the controllers. Contact technical service for assistance if you are experiencing operational difficulties.

5.4 Parts List

Please check installation manual according to different product.

For a replacement parts, please contact Sicunet Customer service.