



# F-Pass Reader (CDR10018) User Manual

# Contents

<b>Before Use .....</b>	<b>2</b>	<b>7. Setting Network .....</b>	<b>16</b>
1. Cautions for Safety.....	3	<b>8. Using USB .....</b>	<b>17</b>
2. F-Pass Reader (CDR10018).....	5	<b>9. Viewing .....</b>	<b>18</b>
2.1. Device Exterior Guide.....	5		
2.2. Button data.....	5		
 <b>User Manual (CDR10018).....</b>	<b>6</b>	 <b>Other Information .....</b>	<b>19</b>
1. Things to Know Before Enrolling Users ....	7	1. Check Before Arming!.....	20
1.1. Authentication Methods by User .....	7	2. Contact S1 for the Following Cases! .....	20
1.2. Process to Enroll Users .....	7	3. Troubleshooting for Emergency Situations?.....	21
2. Going to Menu.....	7	4. Risky Situations! .....	21
3. Enrolling Users.....	8	5. Convenient and Safe Voice Mailing System (VMS) .....	22
3.1. Enrolling Face Auth. Users .....	8	5.1. Security Check .....	22
4. Viewing Users.....	9	5.2. Auto Alarm Service .....	22
4.1. Viewing Users by Card Auth. ....	9	6. Other Information.....	23
4.2. Viewing Users by Face Auth. ....	10	6.1. General Cautions and Instructions.....	23
4.3. Viewing Users by Customer Number ...	10	6.2. Standard Specifications.....	23
5. Viewing User Groups.....	11		
6. Setting User Environment .....	12		
6.1. Setting Face Auth. ....	12		
6.2. Setting Display .....	13		
6.3. Setting Sound .....	14		
6.4. Device Restart .....	15		

## Basic Terms Used by S1

- Arm : To turn on a security system.
- Disarm : To turn off a security system.
- Restricted Time : Time between entry and disarming. Please discuss with S1 staff for restricted time before the initial contract.

# Before Use



# 1. Cautions for Safety

## **Warning** Failure to follow these instructions may lead to death or serious injuries.



Do not modify or reinstall the product on your own.

- It may cause breakdown, electric shock or fire.
- Please contact S1 (+82-2-1588-3112) to modify or reinstall the product.
- Additional expenses will be charged for the product relocation.



Do not disassemble, repair or alter the product on your own.

- It may cause breakdown, electric shock or fire.
- Please contact S1 (+82-2-1588-3112) for repair services.



Do not keep the product close to inflammables.

- The product may melt down resulting in electric shock or fire.

## **Caution** Failure to follow these instructions may lead to serious injuries or property damages.



Do not impact or shake the product.

- It may cause permanent breakdown.



Do not keep the product close to magnets.

- It may cause breakdown or malfunction.



Do not install the product in places with dust or high humidity.

- It may cause electric shock or breakdown.



Do not clean the product with benzene, thinner or alcohol.

- It may cause breakdown, malfunction or fire.



Do not use fingerprints for purposes other than access control, arming or disarming.

- It may damage the product causing breakdown or malfunction.



Do not use sharp objects such as needles and pencils to press buttons.

- It may cause breakdown.



Do not let children touch the product.

- It may cause safety accidents for children or breakdown.



Do not spray pesticides or combustible materials over the product.

- It may cause breakdown or fire.



Clean the product gently to remove dust on it. Specify whether clean with wet towel, dry tissue, etc.

- Be careful not to damage buttons when cleaning it. It may cause degraded functionality or malfunction.



Do not keep the product close to sharp things such as knife.

- It may damage the surface of the product.

**⚠ Caution** Failure to follow these instructions may lead to serious injuries or property damages.



Do not scribble or keep cards and wireless devices scratch dirty.

— It may damage the surface of the product.



Please contact S1 (+82-2-1588-3112) first when you experience breakdowns or other problems related to the product.



Be careful not to lose cards and wireless devices and contact S1 (+82-2-1588-3112) if immediately you lost your card.



Do not keep cards within children's reach and near devices such as Televisions, refrigerators, magnets or heaters, etc.



Be careful not to get hurt by sharp edges of the card while using them.



Do not bend cards, punch holes or cut them.

## FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### FCC Compliance Statrment

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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:

- Reorient 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.
- Consult the dealer or an experienced radio/TV technician for help.

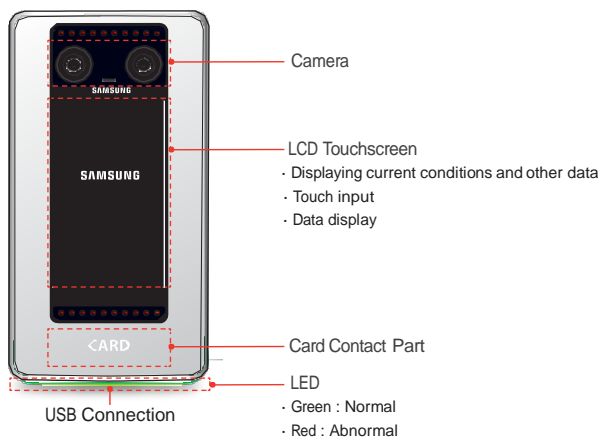
### Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

# 2. F-Pass Reader (CDR10018)

The device enforces arm or disarm, or open the door by using user data such as face recognition, BLE or card.

## 2.1. Device Exterior Guide



## 2.2. Button data

Arm	<ul style="list-style-type: none"><li>● Place your card close to the contact part or allow the device to recognize your face through camera, and then touch [Arm] button.</li><li>● Once the system activates the arm display will appear.</li></ul>
Disarm	<ul style="list-style-type: none"><li>● Place your card close to the contact part or let the device recognize your face through the camera, and then touch [Disarm] button.</li><li>● When the system deactivates arm, the disarm display will appear.</li></ul>

# User Manual (CDR10018)



# 1. Things to Know Before Enrolling Users

CDR10018 can enroll up to 200,000 users.

## 1.1. Authentication Methods by User

Authentication Method	Notes
Card Auth.	This is for users who don't want to register their faces. Register your card for authentication.
Face Auth.	Register your face and NID for Usually we say facial recognition.
Face Auth. or Card Auth.	You can register both, your face and your cards, and then select either one at your discretion for authentication.
Face Auth. + Card Auth.	When a high level of security is required, you can register your face and your card and simultaneously use both for authentication.
Face Auth. + NID	Register your face and NID and use both for authentication.

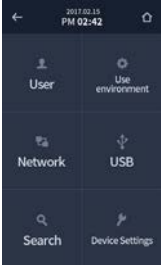
## 1.2. Process to Enroll Users

Authentication Method	Notes
Face Auth.	Register card ► Register face

※ The device supports Face Auth. only for enrolling users.

# 2. Going to Menu

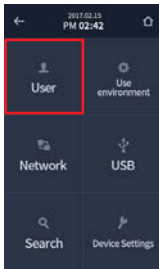
You need to go to menu first to use various functions of the system.  
Menu functions are available to admins and S1 technicians only.



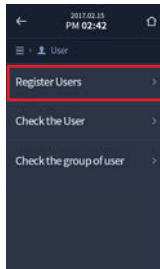
1. Input admin's face or card on the idle screen for authentication and then touch the left area.
2. Once the authentication is completed, you will see the above menu.

## 3. Enrolling Users

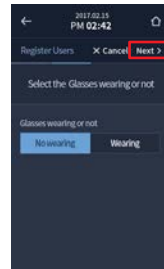
### 3.1. Enrolling Face Auth. Users



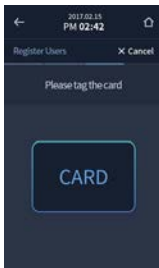
1. See "2. Going to Menu" for admin authentication, and then touch [User] menu to go to user menu.



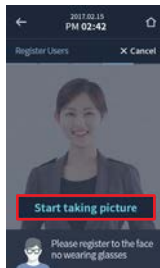
2. Select [Register Users] in user menu to go to enroll users menu.



3. Selecting users with or without glasses and then touch [Next] button to proceed.



4. Once you see the above screen, tag cards to be registered on the device to complete the process.



5. Those without glasses touch [Take Photo] button to proceed and those with glasses should take them off before taking photo.



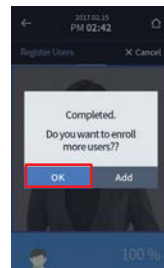
6. Let the camera view your face and then move your face up and down slowly until the status bar reaches 100% (those without glasses go to 9.)



7. Those with glasses wear them and then touch [Take Photo] button.



8. Once again, let the camera view your face and then move your face up and down slowly until the status bar reaches 100%.



9. Once completed, if you want to enroll more users, touch [Add] and then go back to "3. Selecting User Level and Qualification" Otherwise, select [OK] to complete.

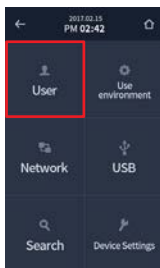
# 4. Viewing Users

You can view, edit and delete already enrolled users.  
Only admins and s1 personnel can edit and delete users.

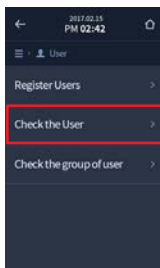
※ Authentication methods available for viewing users

View Method	Authentication data Available for Viewing
Card Auth.	All Users
Face Auth.	Users enrolled with Face Auth. and Face or Card Auth.
NID	All Users

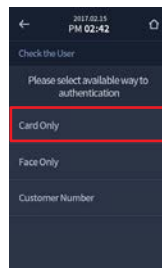
## 4.1. Viewing Users by Card Auth.



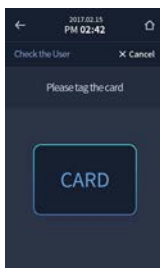
1. See "2. Going to Menu" for admin authentication, and then touch [User] menu to go to user menu.



2. Select [Check the User] in user menu to view users.

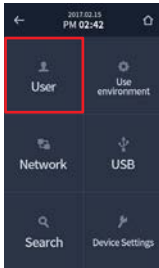


3. Select [Card Only] to proceed.

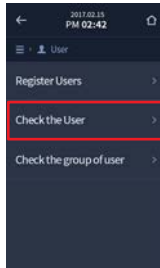


4. Tag the card you want to view and confirm the result.

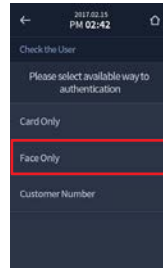
## 4.2. Viewing Users by Face Auth.



1. See "2. Going to Menu" for admin authentication, and then touch [User] menu to go to user menu.



2. Select [Check the User] in user menu to view users.

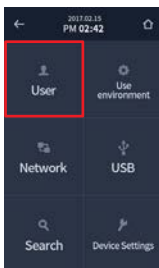


3. Select [Face Only] to proceed.

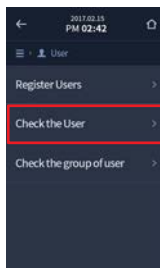


4. Authenticate the face you want to view and confirm the result.

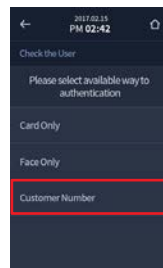
## 4.3. Viewing Users by Customer Number



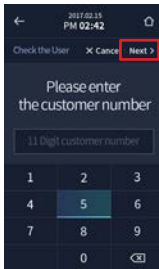
1. See "2. Going to Menu" for admin authentication, and then touch [User] menu to go to user menu.



2. Select [Check the User] in user menu to view users.

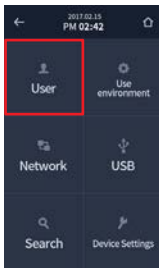


3. Select [Customer Number] to proceed.

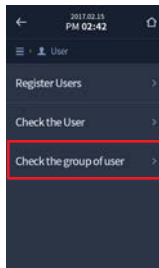


4. Enter the Customer Number you want to view and confirm the result.

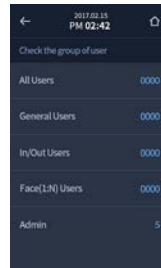
## 5. Viewing User Groups



1. See "2. Going to Menu" for admin authentication, and then touch [User] menu to go to user menu.



2. Select [Check the group of user] in user menu to view user groups.



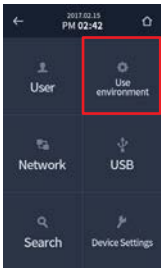
3. You want to view and confirm the result.

# 6. Setting User Environment

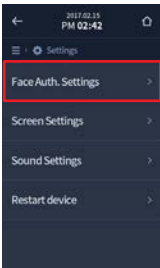
You can arrange various settings such as Face Auth., Voice or Device Restart required for you to use CDR10018 reader.

## 6.1. Setting Face Auth.

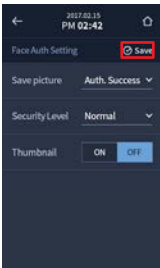
Item	Notes
Save Images	For face authentication, 4 options for images can be selected (1) When authentication succeeded (2) When authentication failed (3) Always (4) Do not save A total of 300,000 image can be saved
Security Level	3 levels of normal, safe and most safe are available. Higher levels mean higher security.
View Thumbnails	You can choose to show thumbnails on the screen for authentication.



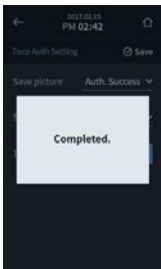
1. See "2. Going to Menu" for admin authentication and then touch [User Environment] to go to user environment menu.



2. Touch [Face Auth. Settings] to proceed.



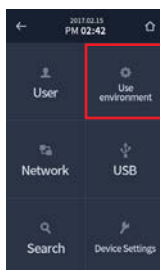
3. Select the settings you want in each item and then touch [Save] button.



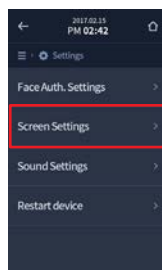
4. Confirm the above completion message.

# 6.2. Setting Display

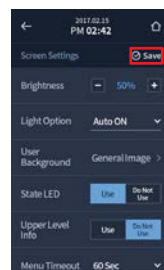
Item	Notes
Brightness	You can adjust screen brightness between 10% and 100%. Higher numbers mean brighter screen.
Light Option	You can change auto light on according to the user security settings. As it is closely related to external security, please contact S1 (+82-2-1588-3112) for settings.
Status LED Settings	You can configure the LED at the lower part of the reader and choose to use it or not.
Upper Level Info	You can configure the screen to show the current time on top.
Menu Time Out	You can configure time to keep the menu on without button input. You can set to 10 sec., 20 sec., 30 sec., or Do Not Use.
Date	You can configure the current date.
Time	You can configure the current time.



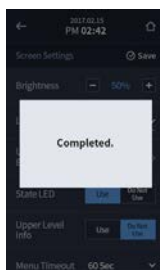
1. See "2. Going to Menu" for admin authentication and then touch [User Environment] to go to user environment menu.



2. Touch [Screen Settings] to proceed.



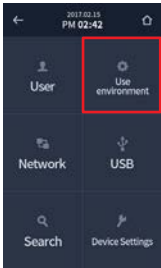
3. Select the settings you want for each item and then touch [Save] button.



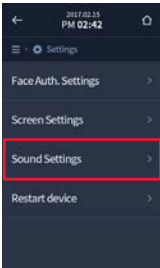
4. Confirm the above completion message.

### 6.3. Setting Sound

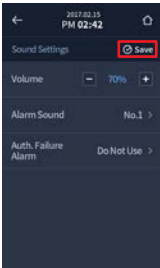
Item	Notes
Volume	You can adjust the volume between 0% and 100%. Higher volume means bigger sound.
Alarm Sound	You can select the alarm sound among 3 different options.
Auth. Failure Alarm	You can select the alarm sound among 4 different options including Do Not Use.



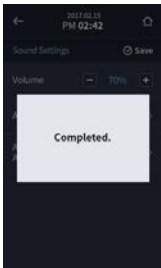
1. See "2. Going to Menu" for admin authentication and then touch [User Environment] to go to user environment menu.



2. Touch [Sound Settings] to proceed.



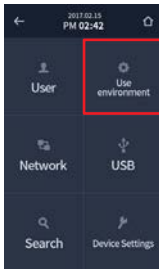
3. Select the settings you want in each item and then touch [Save] button.



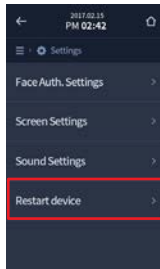
4. Confirm the above completion message.



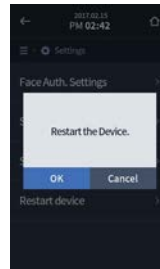
## 6.4. Device Restart



1. See "2. Going to Menu" for admin authentication and then touch [User Environment] to go to user environment menu.



2. Touch [Restart device] to proceed.

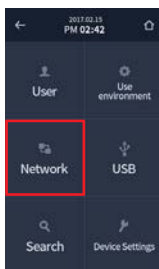


3. Once you see the popup, touch [OK / Cancel] depending on your choice on whether to restart the device.

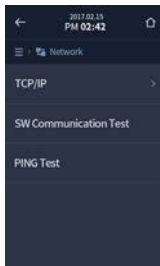
# 7. Setting Network

Network setting and communication testing items to connect Cles Manager.

Item	Notes
TCP/IP Settings	Setting product IP to connect Cles Manager.
SW Communication Testing	Testing communication status of Cles Manager.
PING Testing	Testing the communication status between the applicable IP and the product.



1. See "2. Going to Menu" for admin authentication and then touch [Network] to go to network menu.



2. Touch the network setting you want to configure.

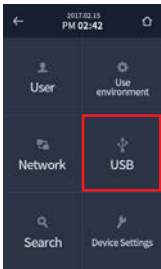
## Caution

- If you need to configure the network settings again, please contact S1 (+82-2-1588-3112).

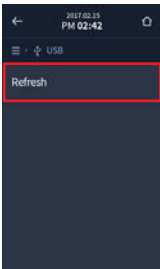
# 8. Using USB

You can export log data from the device to USB, and upgrade firmware.

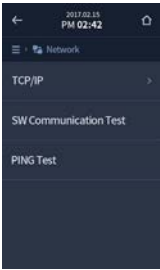
Item	Notes
Export Log Data	Saving log data of the device onto USB.
Firmware Upgrade	Applying firmware file of USB to the device for upgrade.
Refresh	Update data.



1. See "2. Going to Menu" for admin authentication and then touch [USB] to go to USB menu.



2. Insert USB into the lower part of the device and then touch [Refresh] to read the USB data.

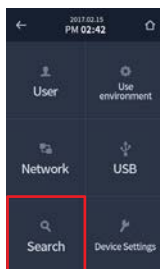


3. Touch the functions that you want.

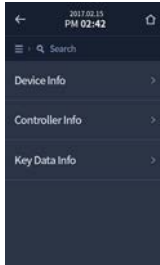
# 9. Viewing

You can view device info, authentication methods registered in the device.

Item	Notes
Device Info	Showing the version info, of the device.
Upper Level Device Info	Showing the information of the upper level device connected.
Key Data Info	Showing the card key and mobile key info.



1. See "2. Going to Menu" for admin authentication and then touch [Search] to go to view menu.



2. Touch the info that you want to view.

# Other Information

# 1. Check Before Arming!

Before arming, please check the following to prevent unexpected accidents and other risks.



Can you see any movement inside?

- Check whether people still occupy the premises.
- Any movement inside may prevent activation of arming or lead to unnecessary visits for S1 staff.



Is the safe detector installed in front of the safe door? (Where the safe detector is installed)

- Check whether the safe door is closed and then place the detector at the door.



Can you see gas leakage light, cigarette or heaters turned on?

- Check for light cigarette, heaters and places with inflammables in advance.
- Check whether there is any gas or water leakage.
- Turn off heaters and coolers 20 minutes before going out.



Did you lock all windows and access doors?

- It would be dangerous if you do not lock windows and access doors. They might be opened by winds or other reasons to prevent activation of arming or lead to unnecessary visits for S1 staff.



Is the detector in place?

- If the detector is not in place, please contact S1 (+82-2-1588-3112).



Is there any object that blocks the detector? (Where the heat ray detector is installed)

- Remove any objects that block the detector.

## 2. Contact S1 for the Following Cases!



If your card damaged?



You have changed your emergency call network!



If you lose your card?



When you change your interior decorations?



If you going to leave the premises for long due to business trips or vacations?



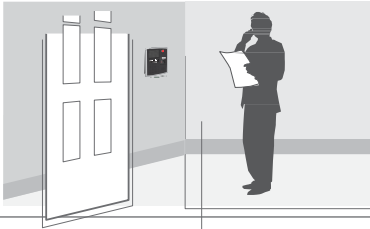
If there is loss of electricity for any reason?



If you had a new internet line installed?

### 3. Troubleshooting for Emergency Situations?

In event of fire or theft, please remain calm and follow the following instructions.



The screen displays messages for abnormal situations and the alarm activates!

- In such cases, you hear a sudden alarm sound of "Beep! Beep! Beep!"
- Check the locations with abnormal or risky situations on the screen and then contact S1 (+82-2-1588-3112) to investigate the situations.
- Investigate the locations with abnormal situations and then touch [Disarming] to restore the system.



A thief breaks in!

- Press the emergency button. S1 emergency staff will visit your premises and the situation is also communicated to the police station.
- Once you press the emergency button, only S1 staff can restore the system.
- The above instructions are applicable for customers who selected emergency alarm services only.

### 4. Risky Situations!



It is dangerous to go out without enforcing arming!

- Any accident will not be detected and no abnormal signal will be sent to S1. Thus, we will not be able to help in such cases.



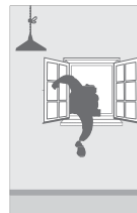
Access was allowed or the system is disarmed during the agreed arming hours!

- S1 recognizes this situation as unauthorized access and therefore our staff will visit the premises to check your identity. So please be careful to avoid any inconvenience. Plan your access with advance consultation with us.



I have mistakenly armed/disarmed!

- We cannot confirm the cause of accidents under such situations of wrong arming and such mistakes may lead to unnecessary visits for our staff.



I did not pass through the final access door!

- Be careful that arming should be activated again as such activity is recognized as unauthorized access.

#### Caution

- You need to arm/disarm by yourself.
- Our visits may be delayed if we received excessive number of requests during busy hours.

# 5. Convenient and Safe Voice Mailing System (VMS)

VMS (Voice Mailing System) is a service that allows you to monitor the system via phone and it automatically informs you when arming has not activated as per pre-defined time limits.

## 5.1. Security Check

Please contact +82-2-1588-3122 to check your security conditions.

1. "Hello, this is S1. Please press 1 for security check services and 2 to talk with our customer service representative."  
Please press 1.
2. Press your card number followed by asterisk(\*) button.
3. "Security check services."  
Please press 1 for security check and 2 to extend the time.
4. You will hear below voice messages below and you will be directed to the control center for any abnormal situations.
5. If you do not know the phone number of the customer service or want to talk directly to our representative please press 9.
6. You will be directed to our representative.

If your arming is activated under normal conditions	Your arming for 000 is in normal conditions. The System have been armed at 00:00 in Month 00. Our current staff responsible for your security is 000.
If you disarm the system under normal conditions	Your arming for 000 is now disarmed. The System has been disarmed at 00:00 in Month 00. Our current staff responsible for your security is 000.
If there is an abnormal situation	Your arming for 000 detected an abnormal situation. Please wait for a second. You will be directed to our representative.
If you entered a wrong card number	When you enter a wrong number once or twice: "You entered a wrong number." message will appear heard. When you enter a wrong number more than 3 times: "Sorry for the inconvenience. Please check your card number and contact us again."

## 5.2. Auto Alarm Service

The service automatically informs you when arming is not activated as per pre-defined time limit. You need to activate arming in accordance with the ARS voice guide.

1. "Hello, this is S1 SECOM situation room. Your arming was not activated so far. Please press 1 if you can activate arming within 30 minutes or press 2 if you want to extend the time. If you made a wrong call, please press 0.  
Press a button for your situation.

If you press 0	"Sorry for the wrong call."
If you press 1	"Please activate your arming within 30 minutes. Thank you."
If you press 2	"Please enter the first 6 digits of your customer enrollment number and then press an asterisk(*) button."



## 6. Other Information

### 6.1. General Cautions and Instructions

It is not allowed to copy or reproduce this guide without prior written consent of S1.  
Product specification may change without notice for improved quality or change in functionality.  
Please contact S1 with the following information for any questions related details about the product.

- Contact : +82-2-1588-3112
- Website : [www.s1.co.kr](http://www.s1.co.kr)

### 6.2. Standard Specifications

- Outlines

- 1)Form : Used in indoor installation
- 2)Size : (W)100 × (H)190 × (D)37 [mm]
- 3)Weight : about 220g

- Electrical Specifications

- 1)Input Voltage : DC 12V
- 2)Current consumption : Less than 1300mA @ DC 12V

- RF Specifications

This proximity cardreader shall produce an energizing RF field which couples to the card to transfer power and which shall be modulated for communication and follows ISO14443 Type-A,B standard.

- 1)Operating frequency : 13.56MHz
- 2)Channel : 1 ch
- 3)Modulation type : ASK

- 2.4 GHz RF Specifications

- 1)Bluetooth v4.0 specification
- 2)Operating frequency : 2402MHz ~ 2480MHz
- 3)Channel : 40 ch
- 4)Modulation type : GFSK
- 5)-92.5dBm receive sensitivity

- Use Environment

- 1)Use temperature : -20℃ ~ +50℃
- 2)Use humidity : 30% ~ 90% (relative humidity)
- 3)Installation requirements
  - Convenient place for manipulating machine.
  - Install on none-metal
  - Place which has not direct ray.
  - Place which is not affected by heat.
  - Place which has not vibration.
  - Install at the place that reading distance should be kept more than 3 cm..

## Do you have any questions about us?

Contact **+82-2-1588-3112**

S1 offers 24/7 customer service to promptly respond to your questions or complaints. We offer detailed counseling services for your questions or complaints in a fast manner. It is not allowed to reproduce this guide without written consent of S1.

Product specification may change without prior notice for improved quality or change in functionality. Please contact S1 for any questions on product details.

You can also visit S1 website ([www.s1.co.kr](http://www.s1.co.kr)) for detailed user manual.

S1 Website ([www.s1.co.kr](http://www.s1.co.kr)) – Customer Support - Archive