User Manual

ST10-MEK Metal Reader

Applicable Model: ST10-MEK
Date: December 2025
Version 1.0

Trademark

DEFENDAS is a registered trademark of LT Security Inc. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the LT Security Inc. equipment. The copyright in all the documents, drawings, etc. in relation to the Defendas supplied equipment vests in and is the property of LT Security Inc. The contents hereof should not be used or shared by the receiver with any third party without express written permission of LT Security Inc.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact LT Security Inc. before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/ equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

Defendas offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. Defendas does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

Defendas does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

Defendas in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if Defendas has been advised of the possibility of such

damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. Defendas periodically changes the information herein which will be incorporated into new additions/amendments to the manual. Defendas reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/ equipment. The said additions or amendments are meant for improvement/better operations of the machine/unit/equipment, and such amendments shall not give any right to claim any compensation or damages under any circumstances.

Defendas shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

If there is any issue related to the product, please contact us.

LT Security Inc.

Address: 17333 Freedom Way, City of Industry, CA 91748

Phone: 626-435-2838

For business related queries, please write to us at: Contact.LosAngeles@ltsecurityinc.com

To know more about our global branches, visit ltsecurityinc.com

About the Manual

This manual introduces the operations of **ST10-MEK Metal Reader**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Table of Contents

1 Introduction

1.1 Overview

The ST10-MEK metal reader is one of the most compact multi-frequency RFID readers available, supporting more than 100 RFID card types, QR code recognition, and both NFC and Bluetooth Low Energy credentials. Bluetooth support for Defendas ID/Defendas Connect.

1.2 Parts Included

Make sure your box contains everything listed. If any pieces are missing, contact your dealer. Please save the original box and packing materials if you ever need to ship your device.

- Metal Reader - ST10-MEK (1pc)
- Quick Start Guide (1pc) and Mounting Template (1pc)
- Mounting Plate (1pc)
- Screwdriver (1pc)
- Grub screw/Countersunk KA3.6 x 1.57 inchs (40mm) self - tapping screws (4pcs) and Anchors (4pcs) - for mounting directly to a wall (no junction box)
- Torx screw TM3 x 0.24 inches (6mm) (1pc) - for fixing the reader to the mounting plate

1.3 Recommended Parts (not supplied)

- Cable

  5-10 conductor (Wiegand)

  4 conductor Twisted Pair Over-All Shield and UL approved, Belden 3107A or equivalent (OSDP)
- Certified LPS DC power supply
- Metal or plastic junction box
- Drill with various bits for mounting hardware
- Mounting hardware

1.4 Appearance

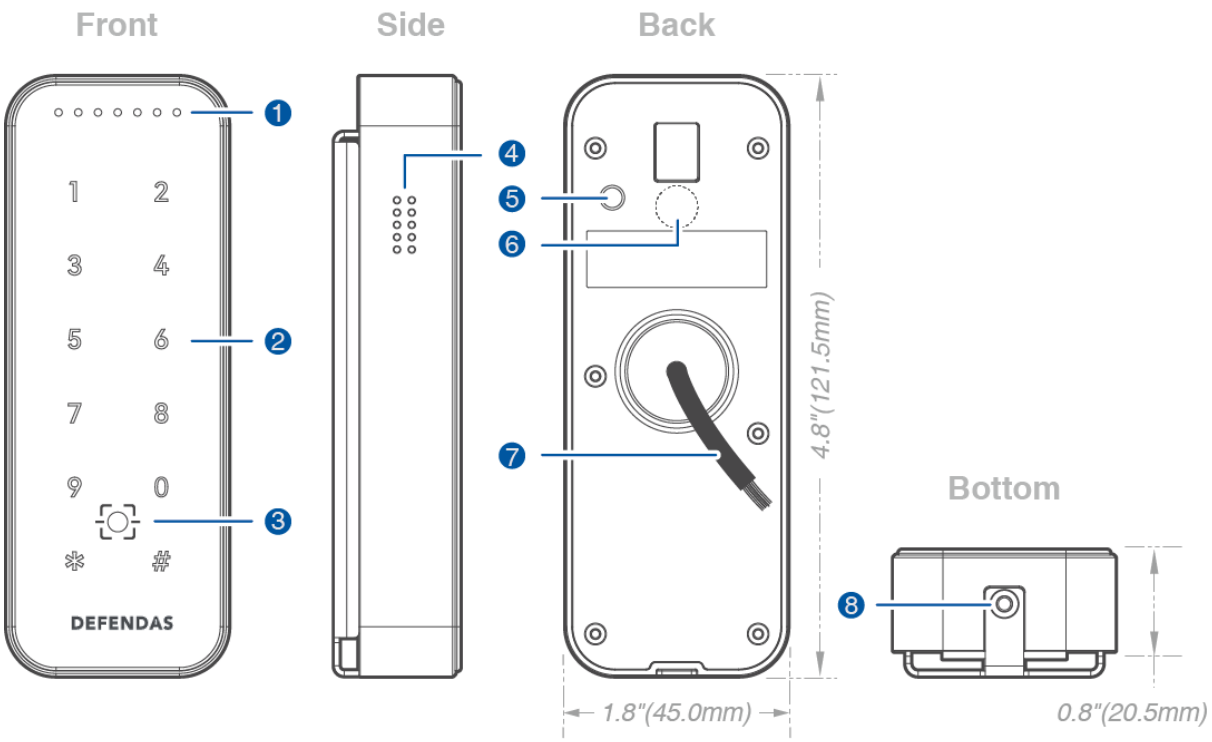


Figure 1-1 ST10-MEK Metal Reader Series Appearance

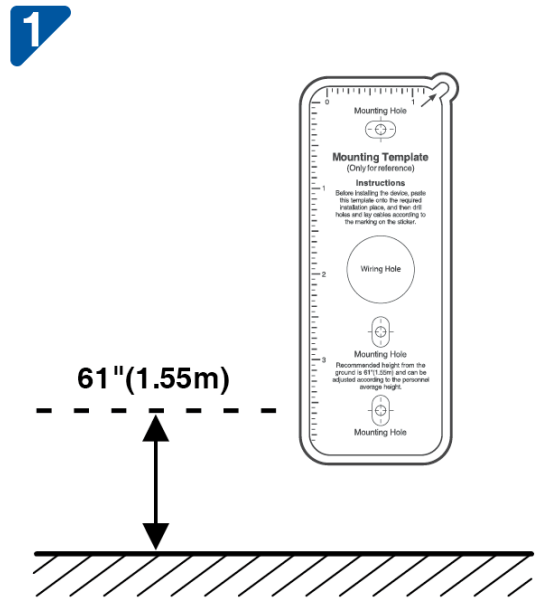
NO.	Descriptions
1	LED Indicator
2	Touch Keypad
3	QR Code Scanner & Card Reading Area
4	Speaker
5	Beeper
6	Tamper Switch
7	Cable
8	Mounting Hole

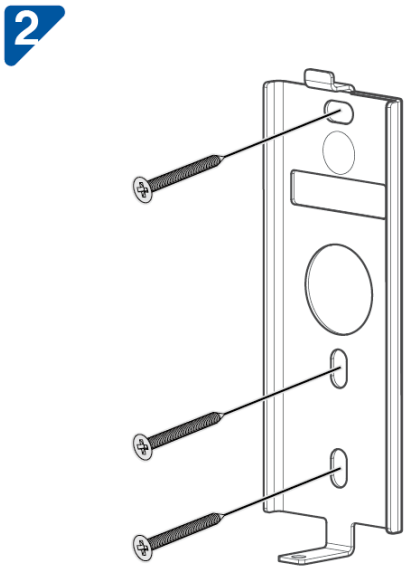
2 Installation

Make sure that the device is installed as per the installation instructions. Otherwise, you will bear any consequence resulting from your actions.

Installation on the wall

1. Attach the mounting template sticker to the wall 61 inches (1.55m) from the ground (adjustable) and drill holes according to the mounting paper.
2. Secure the mounting plate on the wall with the wall mounting screws.
3. After passing the wires through the wiring hole and connecting them, attach the device to the mounting plate from top to bottom.
4. Fasten the device to the mounting plate with a security screw.





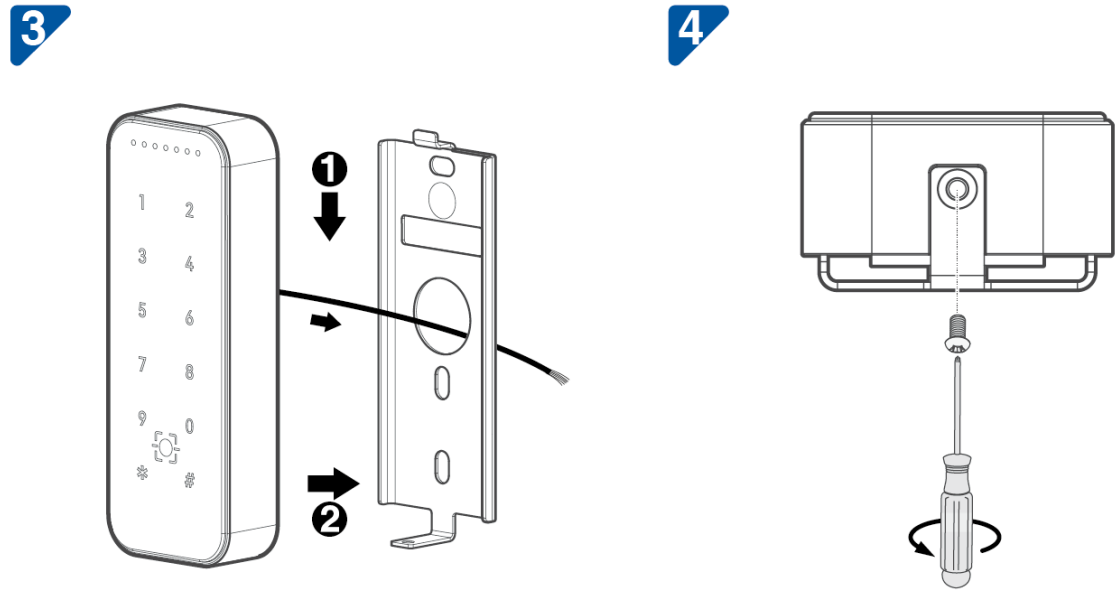


Figure2-1 ST10-MEK Metal Reader Installation

Remarks:

1. *ST10-MEK Metal Reader shares the same casing, and the installation and wiring methods are the same.*

2. *The pictures in the manual are for reference only, and the actual product purchased by the customer shall prevail.*

3 Terminal and Wiring Description

3.1 Terminal Description

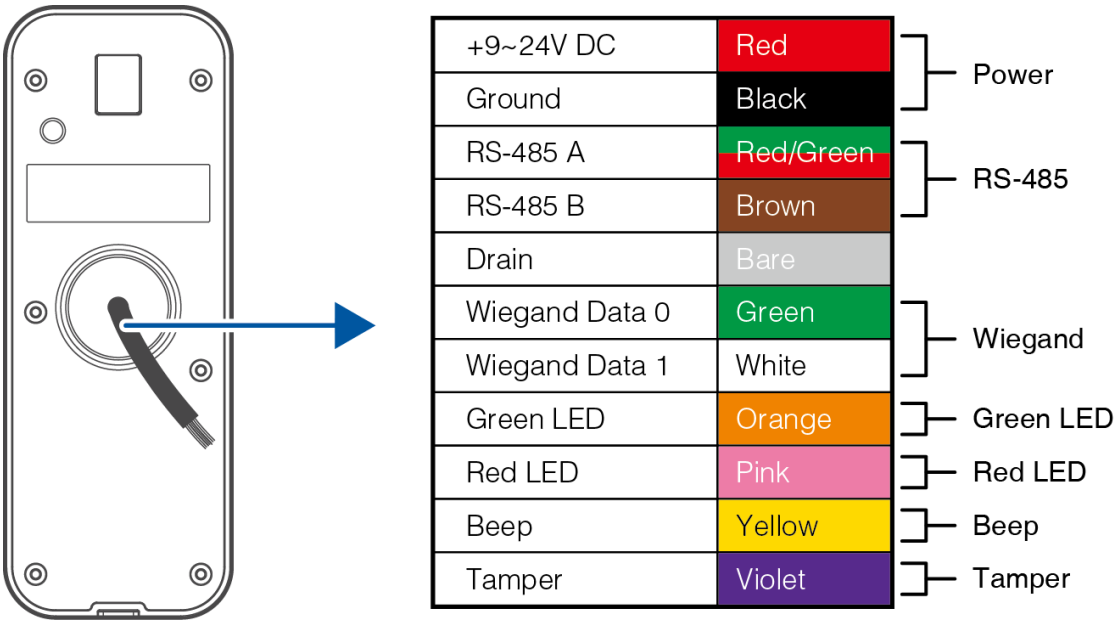


Figure 3-1 Terminal Description

Name	Terminal	Descriptions
Power	+9~24V DC	+9~24V DC Input
	Ground	
RS-485	RS-485 A RS-485 B	RS-485 Communication Interface
Drain	Drain	Drain
Wiegand Out	Wiegand Data 0	Wiegand Output 0
	Wiegand Data 1	Wiegand Output 1
Green LED	Green LED	Green LED Input
Red LED	Red LED	Red LED Input
Beep	Beep	Beep Input
Tamper	Tamper	Tamper

3.2 Wiring Description

3.2.1 Power Wiring

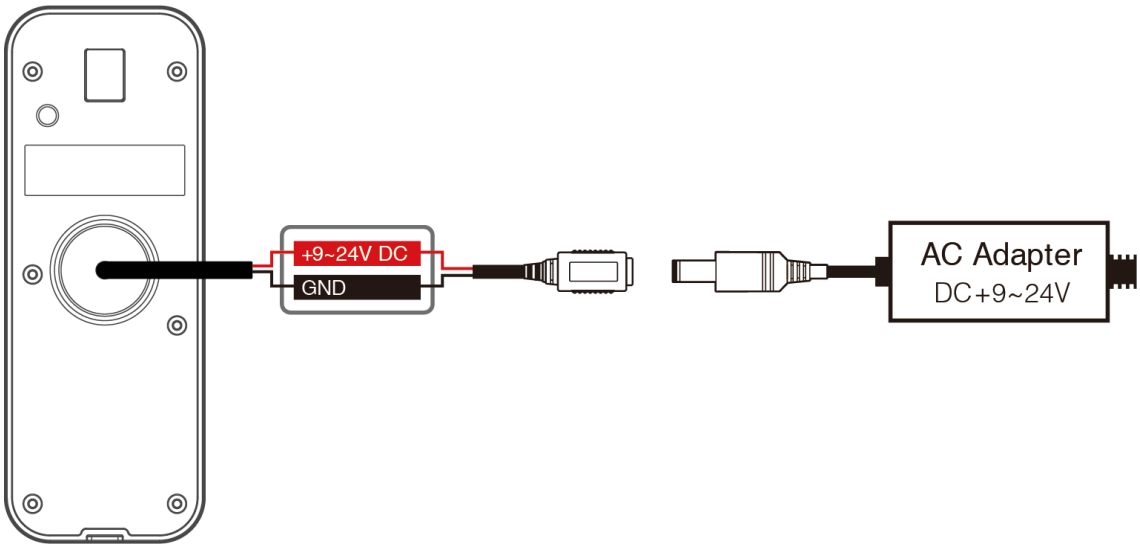


Figure 3-2 Power Wiring

Notes:

1. *Users need to configure their own suitable power adapter according to the product power specifications.*
2. *To share power with other devices, use an AC adapter with higher current ratings.*

3.2.2 Wiring to controller via RS-485 (OSDP)

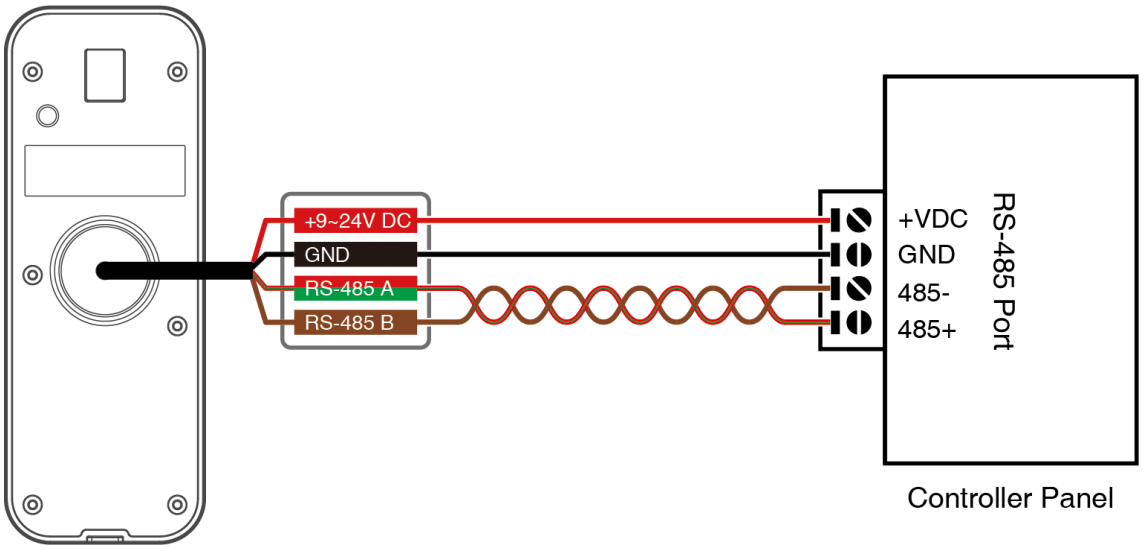


Figure 3-3 Wiring to controller via RS-485 (OSDP)

3.2.3 Wiring to controller via Wiegand

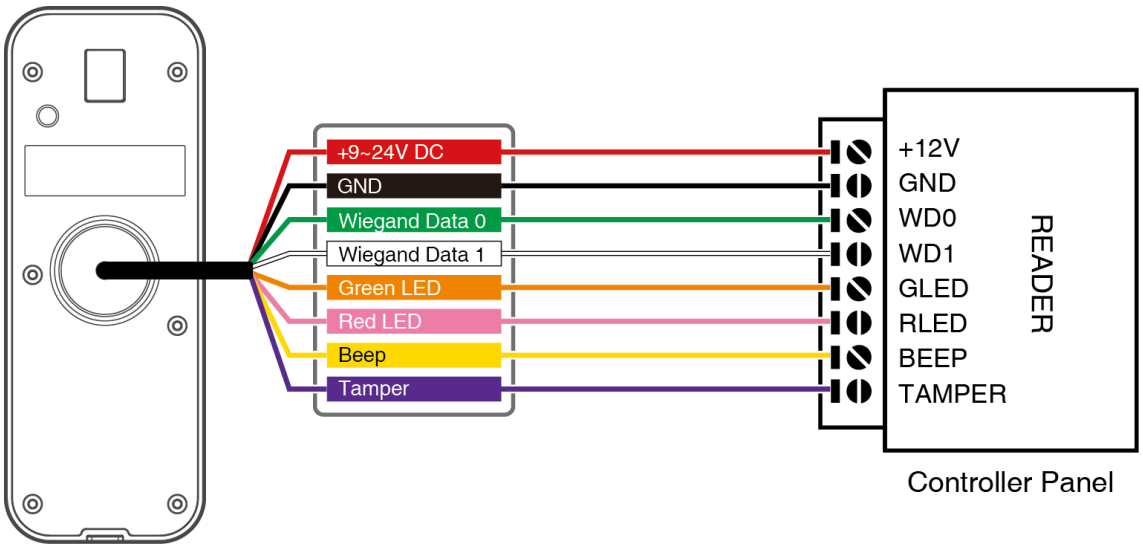


Figure 3-4 Wiring to controller via Wiegand

4 Connecting to DEFENDAS Connect and DEFENDAS ID

The ST10-MEK Metal reader supports connection to DEFENDAS CONNECT App, DEFENDAS ID App via Bluetooth.

- Through the DEFENDAS CONNECT App, administrators can manage the ST10-MEK Metal readers more conveniently. Such as can easily adjust some configuration settings (e.g. audio/video settings, BLE read range settings), upgrade firmware, check connected card reader status.
- And the end users can activate their mobile credentials by entering a specific activation code on the DEFENAS ID App. The user can then use this mobile credential to swipe the card in Card Mode or Remote Mode on the ST10-MEK Metal Series reader. It is extremely convenient for users to travel.

4.1 Connect to the DEFENDAS CONNECT App

4.1.1 Download and Install the APP

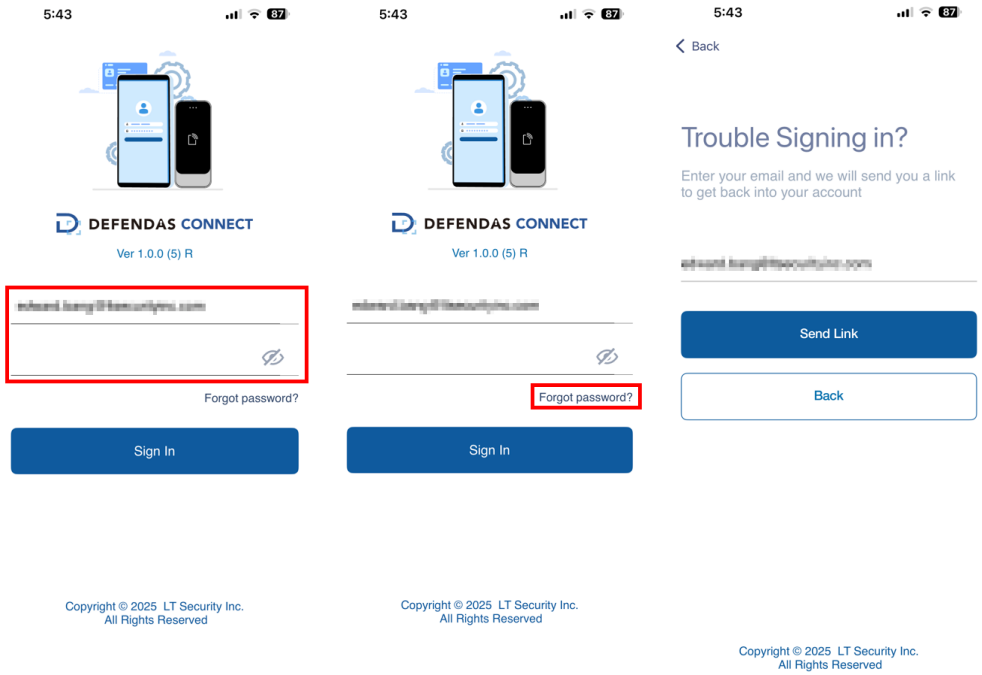
1. Ensure your mobile device is connected to the internet via a mobile or Wi-Fi network.
2. On your mobile device open the Google Play (Android) or Apple (iOS) store.
3. Search for DEFENDAS CONNECT APP.
4. Download and install the app on your mobile device.

4.1.2 Log Into The App

After the account activation process is complete, you can log in to the DEFENDAS CONNECT App with your account and password.

1. Enter the account and the password. Click **Sign In** to log into the app. The password is set when the account is activated.

2. If you have forgotten your login password, tap **Forgot Password?**. Enter your email address and tap **Send Link**. Your password will be reset through the ACMS mailbox.



4.1.3 Bind Device

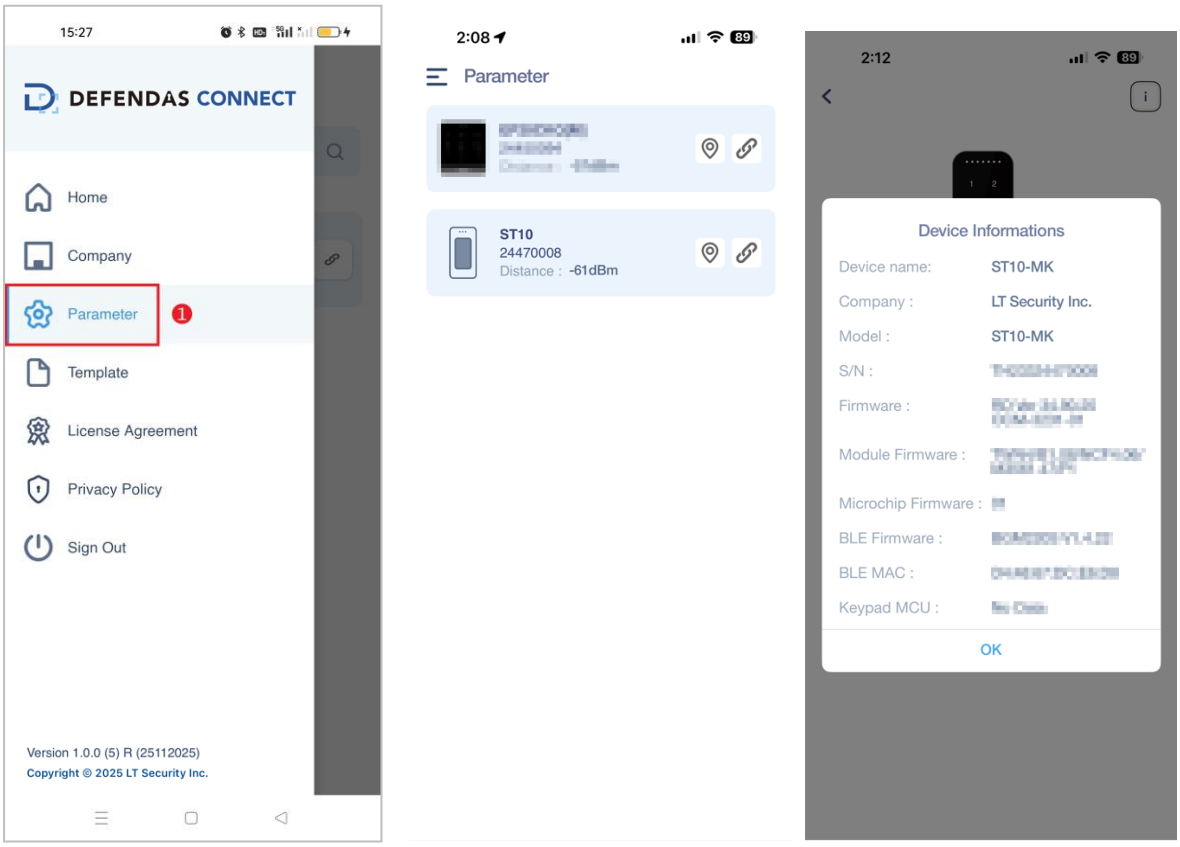
1. Click ☰ > **Parameter** to enter the parameter setting screen.

2. Turn on the Bluetooth function of the mobile device and click 🔍 to search for the device. All searched devices will be displayed in the list.

3. Click 📍 to confirm your device.

4. Click 🔗 to enter the device parameter setting screen. Here you can set the relevant parameters of the device.

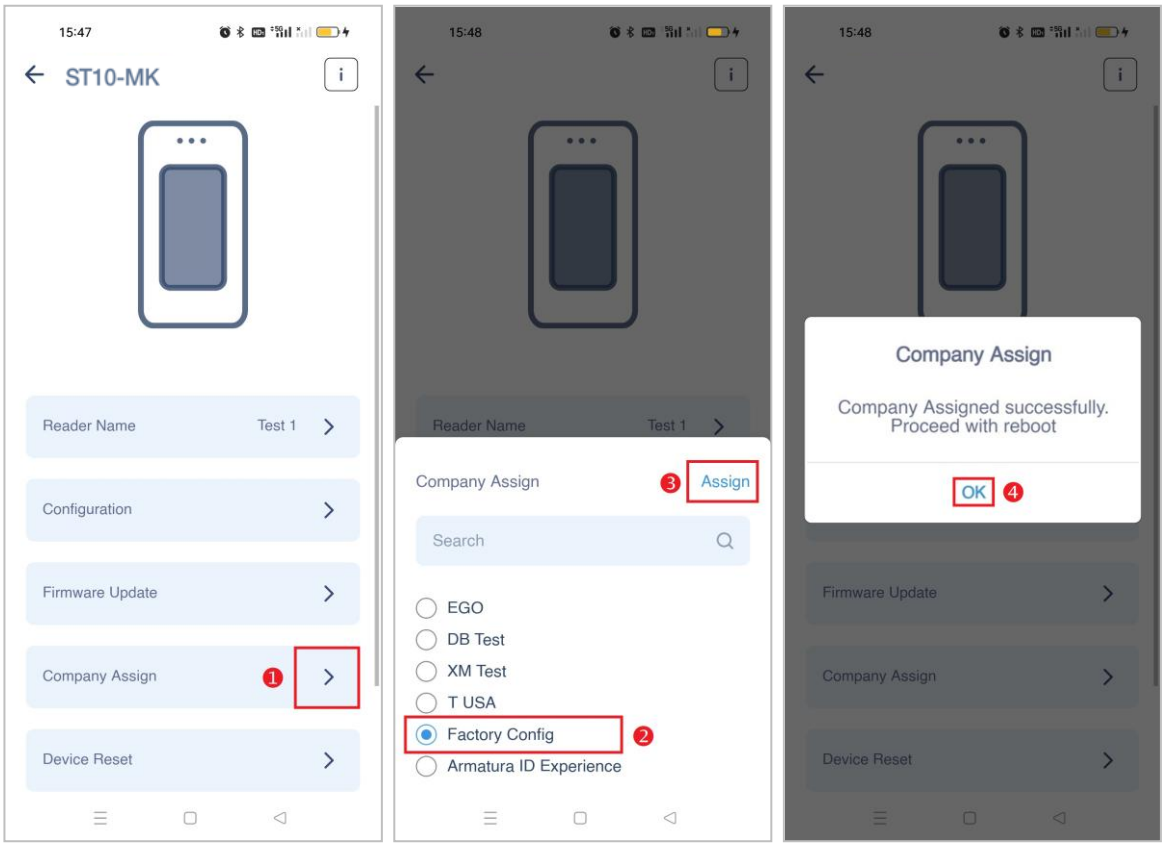
5. Click ⓘ to view reader information, including device name, company, S/N, firmware, module firmware, microchip firmware, BLE firmware and BLE MAC. As shown in the following figure.



4.1.4 Company Assign

This function is used to assign the device to the company. The Bluetooth function of the mobile device needs to be turned on before operation.

1. Click > of the **Company Assign** item to open the setting interface. And the Assignment window will pop up. Select the company and click **Assign** to assign the device to the selected company.
2. Click **OK** when prompted that the assignment is successful.
3. After completing the above steps, please wait for the device to reboot. **Note:** After each configuration of the reader parameters, the reader will reboot.



After the device configuration is complete, employees of the company can use the mobile credentials to operate on the Defendas ID APP.

4.2 Connect to the DEFENDAS ID App

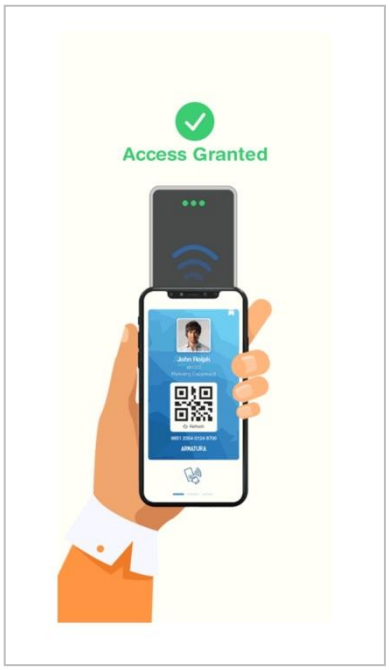
DEFENDAS ID allows end users to use their mobile devices (smartphones) to securely and conveniently enter the workplace by extending access control capabilities to smart devices.

When the end user approaches the ST10-MEK Metal reader within a set distance, the following interaction modes of access are available through their mobile device：

- **Card Mode:** When using this mode, the end user's mobile device is brought very close to, or touching the reader (a similar user experience to using a physical credential).
- **Remote Mode:** This mode allows end users to use mobile devices to perform remote control within the set range.

Note:

1. *The effective distance of Card Mode is 0 to 20 inches (0 to 50 centimeters). The effective distance of Remote Mode is 0 to 394 inches (0 to 1000 centimeters).*



Card Mode

Remote Mode

4.2.1 Download the DEFENDAS ID APP

1. Search for the DEFENDAS ID APP in the Apple App Store (for iOS devices), Google Play Store (for Android devices) or scan the QR code below to download the App on your mobile phone.

DEFENDAS ID

Download on the App Store

GET IT ON Google Play

4.2.2 Activate the Credentials

After completing the installation of the APP, you first need to activate the credentials. There are three ways to activate the credentials: click the activation link to activate automatically, enter the activation code to activate, and scan the QR code to activate. The specific

operation steps are as follows.

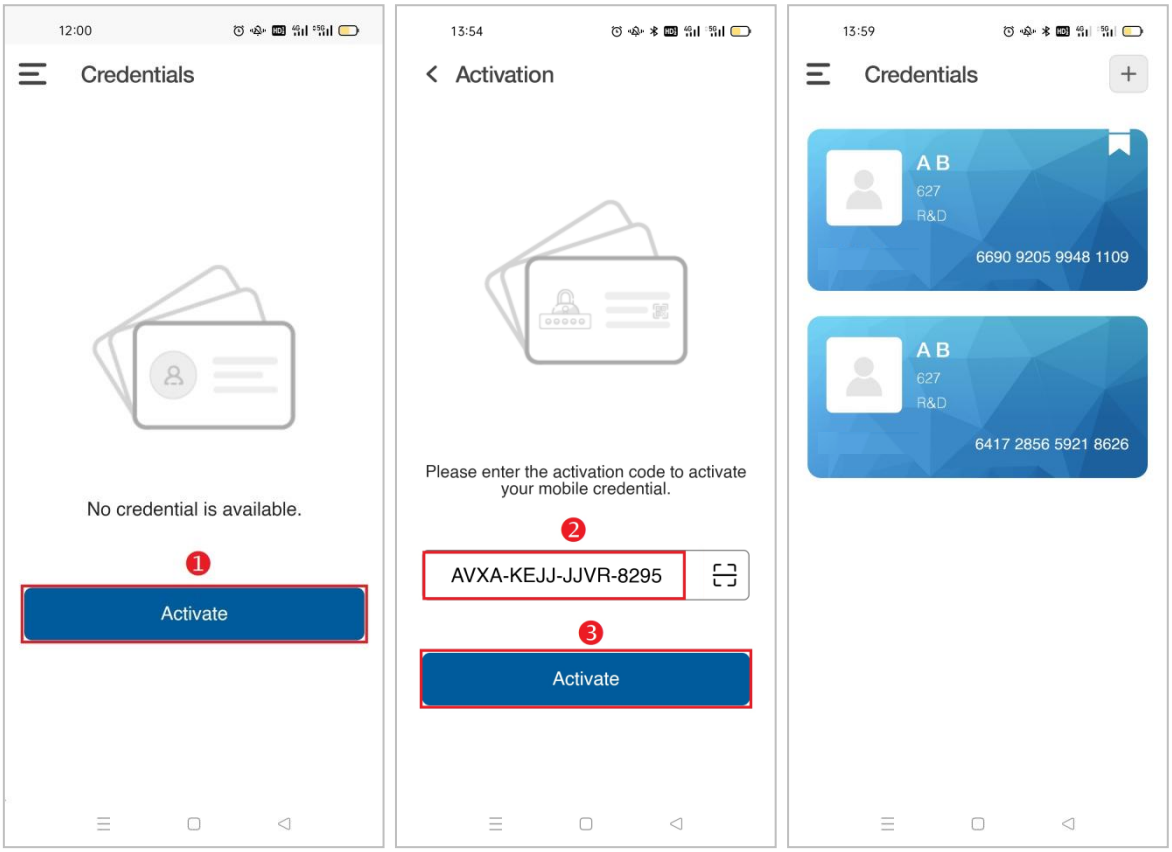
First, please open the activation code email sent by Defendas Credential Management System. It is sent by the site administrator of your company via DCMS.

- **Click the Activation Link to Activate**

Click the link on mobile to activate credentials automatically. Follow the prompts.

- **Enter the Activation Code to Activate**

1. Open the DEFENDAS ID APP and enter the Credentials interface. Click **Activate**.
2. Manually enter the activation code from the email in the input field.
3. Click **Activate** on the Activation interface.
4. A mobile credential will be displayed after successful activation.

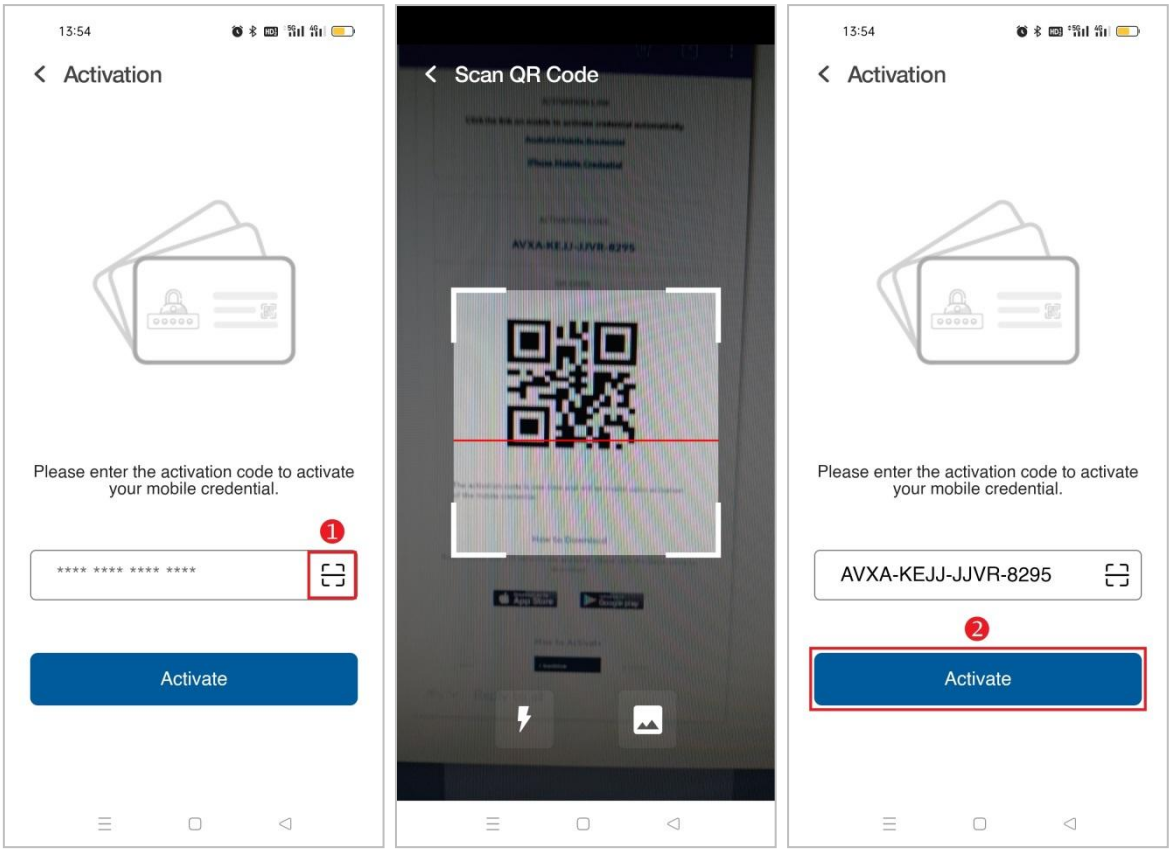


- **Scan the QR Code to Activate**

1. Open the DEFENDAS ID APP and enter the Credentials interface. Click **Activate**.
2. Click ⛶ to scan the QR code on the email. And the system will automatically enter the activation code.
3. Then click **Activate** to activate the credential.
4. A mobile credential will be displayed after successful activation.

Notes:

1. *Please turn on the Bluetooth function of your mobile phone before scanning.*
2. *In order to allow access for users' devices, the site administrators need to assign devices under their company beforehand.*

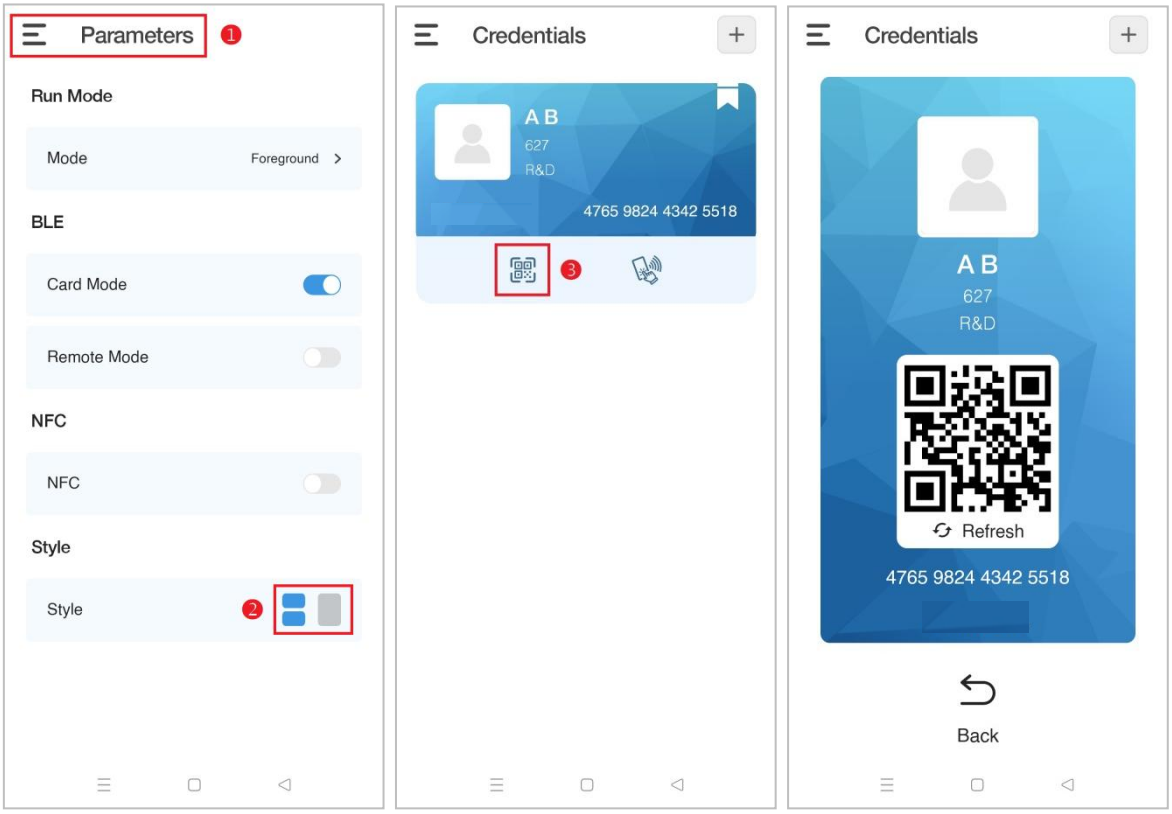


4.2.3 Use of Mobile Credentials

The end users can swipe their cards through **QR code**, **NFC** and **Bluetooth**.

- **Swipe the card through QR code**

1. Click **Parameters** > **Style** on the main menu to modify the display style.
2. Under the card style, you need to click to call up the dynamic QR code. In the tiled style, the dynamic QR code can be seen directly on the card.
3. You just need to swipe the QR code on your mobile phone on the ST10-MEK Metal Series reader to open the door.
4. Click to return to the previous interface.

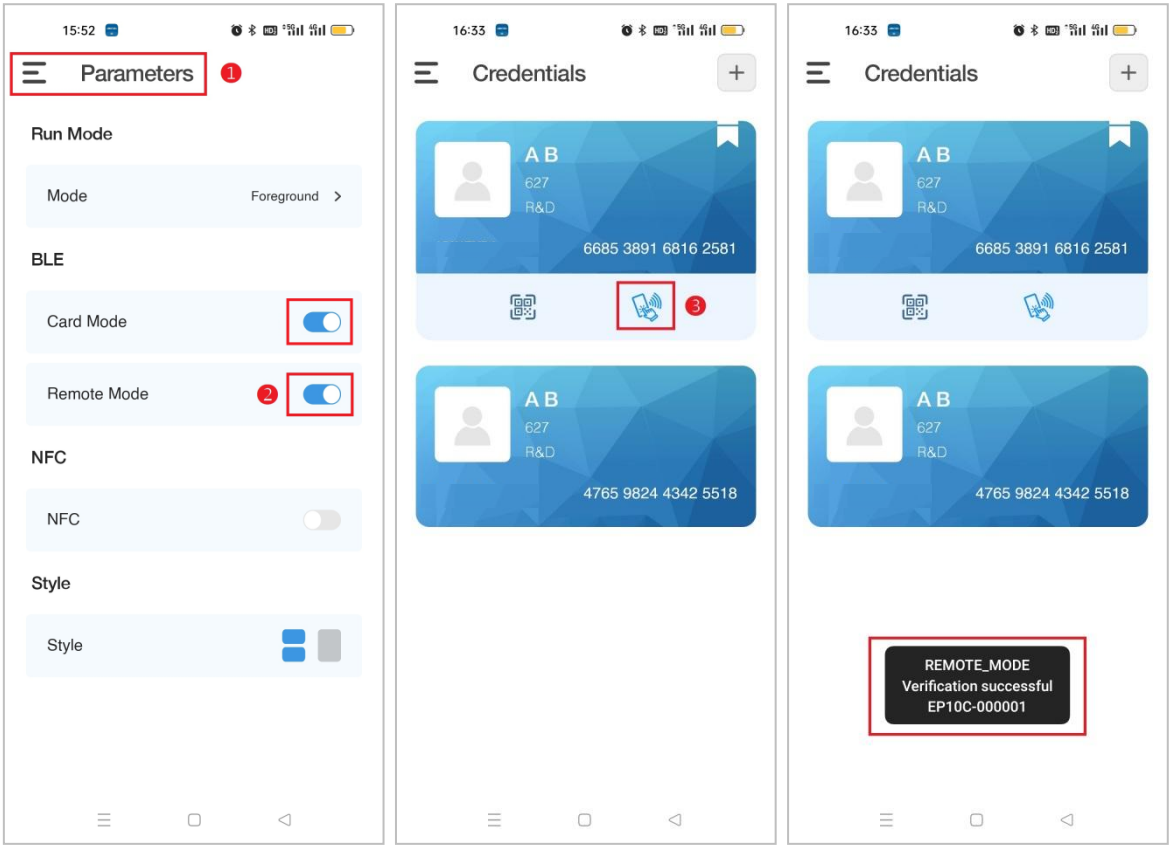


- **Swipe the card through Bluetooth**

Card mode functions require the end user to hold the mobile device close to the card reader to swipe the card. Remote mode functions like a remote control. With the remote mode, you don't need to swipe the card on the reader, just get close to the reader within the effective range.

1. Turn on the Bluetooth functions on your mobile phone.
2. Click **Parameters** on the **Main Menu** screen to enter the parameter setting interface.
3. Click of the **Card Mode** or **Remote Mode** to enable the function.
4. Then you can swipe the card with the mobile phone close to the reader or click of the card to swipe the card remotely within the set range.

5. At the same time, the reader beeps twice and the LED turns green. And the mobile device screen prompts that the verification is successful.



Note:

1. *For other specific operations, please refer to DEFENDAS CONNECT User Manual and DEFENDAS ID User Manual.*

5 Appendix

5.1 Privacy Policy

Notice:

To help you better use the products and services of Defendas, hereinafter referred to as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help with the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.
2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.
3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**
4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**
5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you know the potential security risk. In such a case, you shall take responsibility for storing the data. You should know that some data cannot be downloaded for sake of data security.
6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://ltsecurityinc.com/ to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. You are welcome to visit our official website at any time to learn our latest privacy policy.

5.2 Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.