DEFENDAS

# User Manual

DEFENDAS CONNECT App

## Copyright © 2026 LT Security Inc. All rights reserved.

## 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 DEFENDAS equipment. The copyright in all the documents, drawings, etc. in relation to the LT Security Inc. 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.

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

LT Security Inc. 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.

LT Security Inc. 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 LT Security Inc. has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. LT Security Inc. periodically changes the information herein which will be incorporated into new additions/amendments to the manual. LT Security Inc. 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.

LT Security Inc. 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.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on https://ltsecurityinc.com

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

## LT Security Inc.

Address: 17333 Freedom Way, City of Industry CA 91748

For business related queries, please write to us at: info@LTSecurityinc.com.

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

## About the Manual

This manual introduces the operations of **DEFENDAS CONNECT App**.

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 Purpose

This document provides an overview of the DEFENDAS Reader Management Solution. Procedure for registering customers and assigning installers with the Defendas Credential Management System (“DCMS”) and providing information to customers and integrators:

- Download and install the DEFENDAS CONNECT mobile app.
- Register and authenticate the DEFENDAS CONNECT app on a mobile device.
- Enroll Integrators and issue Mobile Credentials in the DCMS portal.
- Change configurations for supported ST10 Series Readers.
- Update firmware for supported ST10 Series Readers.
- The supported ST10 Series Readers are connected to the controller through RS485 or Wiegand.

## 1.2 Intended Audience

This document is intended for personnel performing the following roles:

- **Integrator:** the Systems Integrator performs the following tasks:
    - Carrying out compatibility checks for the reader and DEFENDAS CONNECT App.
    - Self-registration within the DEFENDAS CONNECT App.
    - Assigning readers to their company.
    - Performing reader configuration changes and firmware upgrades.
    - Reader configuration update testing.

# 1.3 DEFENDAS Reader Management Solution Overview

The DEFENDAS Reader Management solution streamlines management of BLE capable readers in the field.

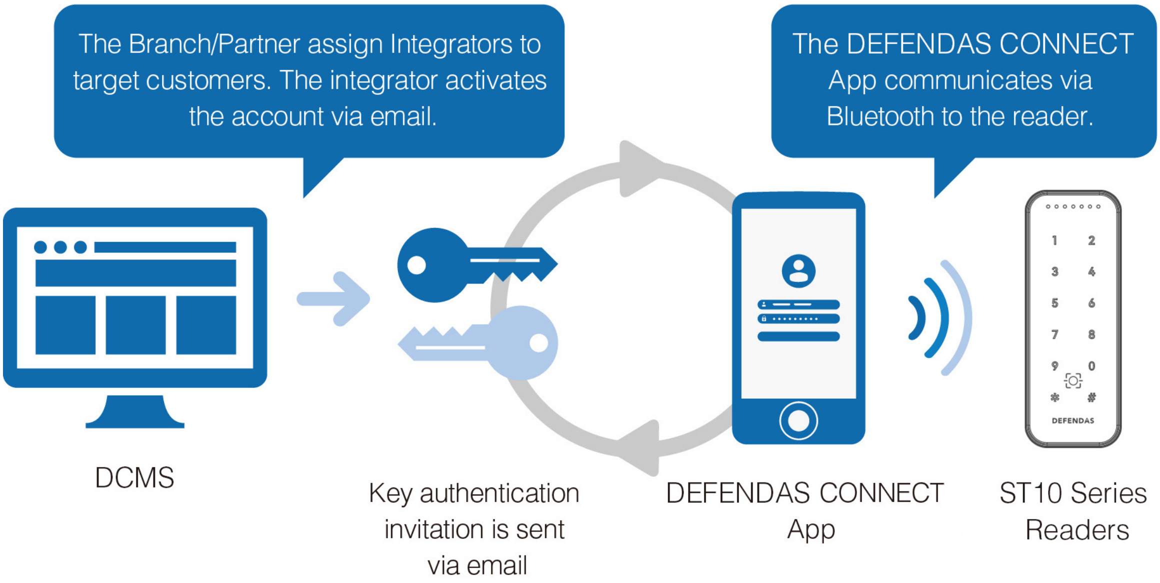
Integrators can easily adjust certain configuration settings such as audio/visual settings, BLE read range settings, upgrade firmware, check reader status & more.

The main components of the DEFENDAS Reader Management solution are:

**DEFENDAS CONNECT Application:** Mobile app which connects via Bluetooth, to a reader for configuration changes, firmware upgrades and reader status.

**Defendas Credential Management System:** DCMS facilitates integrators to use the DEFENDAS CONNECT app with ST10 Series Readers. The DCMS can be used by customers & integrators to manage & issue credentials.

**Controller:** The supported ST10 Series Readers are connected to the controller through RS-485 or Wiegand.


The Branch/Partner assign Integrators to target customers. The integrator activates the account via email.
The DEFENDAS CONNECT App communicates via Bluetooth to the reader.
DCMS
Key authentication invitation is sent via email
DEFENDAS CONNECT App
ST10 Series Readers
DEFENDAS

# 2 DEFENDAS CONNECT APP

This section provides the required steps and procedures to be performed by the integrator in order to install, register, and activate the DEFENDAS CONNECT App on a mobile device. The section also provides information on the functionality of DEFENDAS CONNECT App.

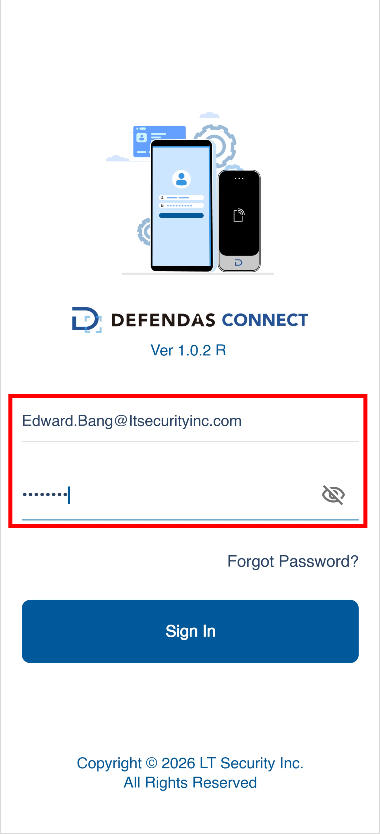
## 2.1 Download and Install the App

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**.
4. Download and install the app on your mobile device.

## 2.2 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.

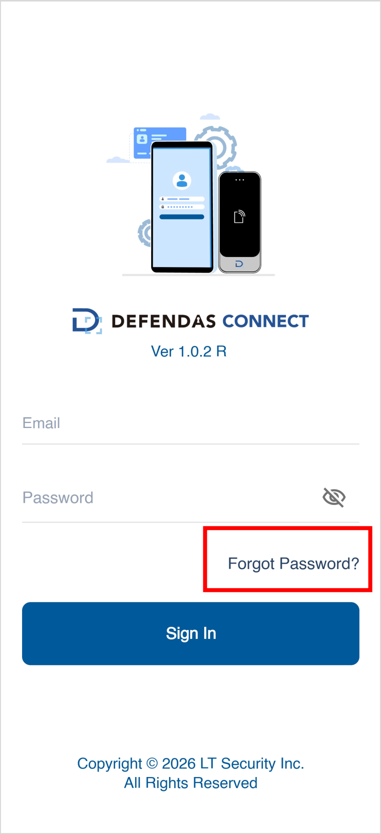
1. Enter the account and the password. Click **Sign In** to log into the app. The password is set when the account was activated.
2. If you have forgotten your login password, tap **Forgot Password?**. Enter your email address and tap **Send Link**. Your password will be reset through the DCMS mailbox.



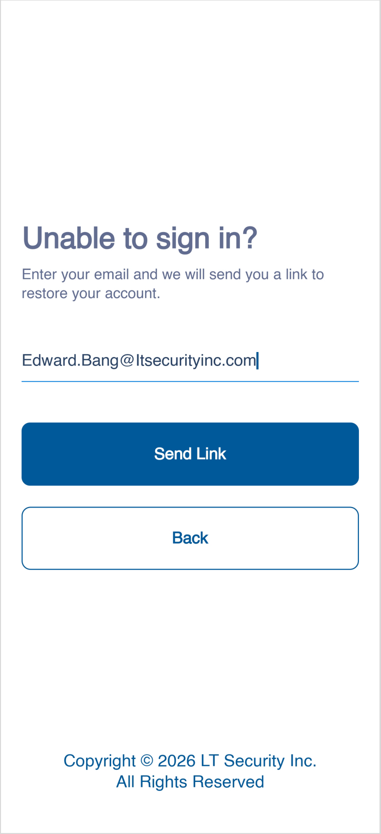
Edward.Bang@ltsecurityinc.com

••••••••

Copyright © 2026 LT Security Inc.
All Rights Reserved



Copyright © 2026 LT Security Inc.
All Rights Reserved


Unable to sign in?

Enter your email and we will send you a link to restore your account.

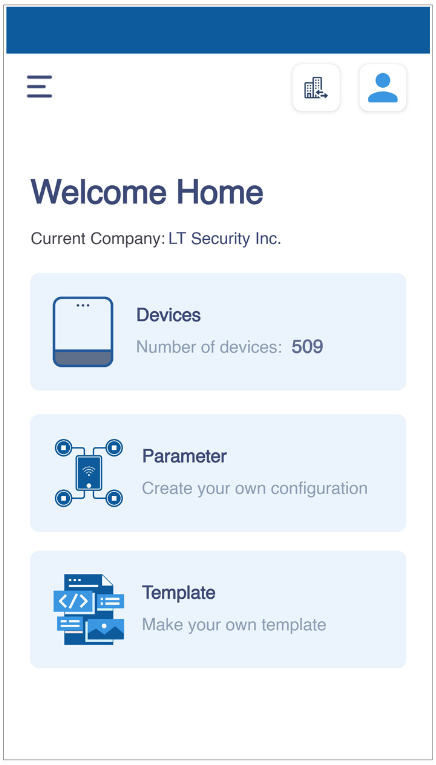
Edward.Bang@ltsecurityinc.com

Copyright © 2026 LT Security Inc.
All Rights Reserved

**Remark:** Please refer to the ***DCMS User Manual*** for instructions on how to obtain an account and password.

## 2.3 Home Screen Layout

After successfully logging in, select the company and you will enter the home screen.



Welcome Home

Current Company: LT Security Inc.

**Main Menu button** Click to view the main menu.

**Switch Company** Click to select a company.

**My Profile** Click to view or update the name and phone number.

**Devices** A list of readers can be found here.

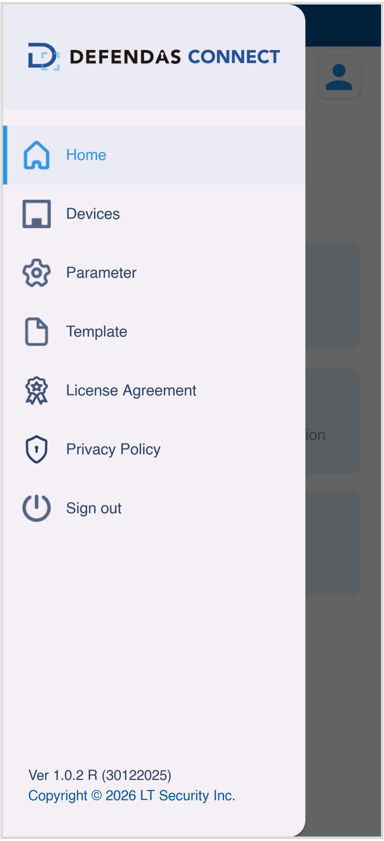
**Parameter** Configure the parameters of the reader here.

**Template** Templates can be created here and synchronized to the selected reader.

## 2.4 App Menu Items

The following provides a description of the menu options available in the app.

1. Open the **DEFENDAS CONNECT App** on your mobile device.
2. Click ☰ to access the menu options.



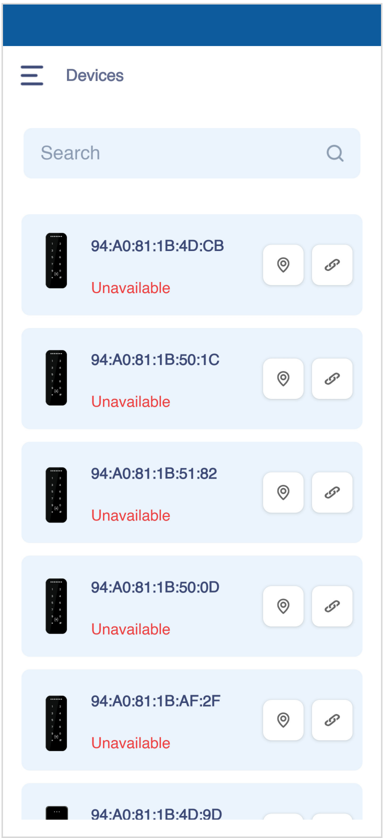
**Function Description**:

| **Menu** | **Descriptions** |
|---|---|
| **Home** | Displays the Home screen. |
| **Devices** | Displays the list of the readers assigned to the company. |
| **Parameter** | Search and set parameters of the reader. |
| **Template** | When a template is created it can be applied to multiple readers that require the same configuration. |
| **License Agreement** | To display the end user's license agreement. See the 4 Appendix for details. |
| **Privacy Policy** | To display the content of the privacy policy. See the 4 Appendix for details. |
| **Sign Out** | Log out of the current account. |

## 2.4.1 Device Settings

This function is convenient for viewing the list of the readers under each company. Here you can set the parameters of the readers that have been assigned to this company.

### 2.4.1.1 View the Device List



Devices

Search

94:A0:81:1B:4D:CB
Unavailable

94:A0:81:1B:50:1C
Unavailable

94:A0:81:1B:51:82
Unavailable

94:A0:81:1B:50:0D
Unavailable

94:A0:81:1B:AF:2F
Unavailable

94:A0:81:1B:4D:9D

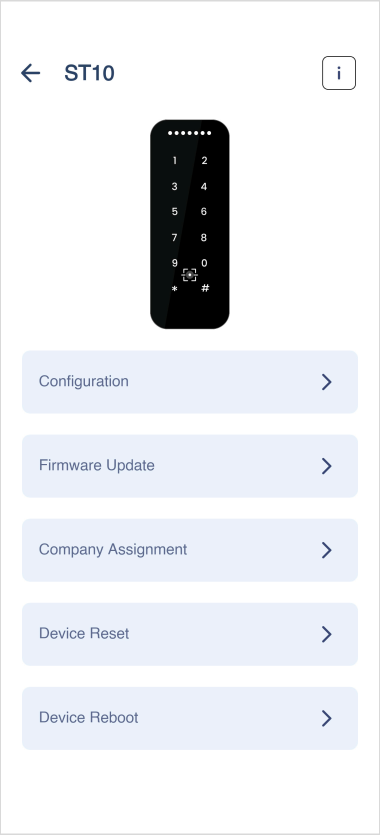
1. Click ☰ > **Devices** to enter the device list screen. It will display a list of readers assigned to this company.

2. In the reader list, you can view the information of the reader, such as the reader name, operating status and distance, etc.

## 2.4.2 Parameter Settings

This function is mainly used by the integrator to search for the reader, set the relevant parameters of the reader, and assign the reader to the company.

After you select the reader and enter the reader parameter setting interface, you can view the reader information, configure parameters, update the firmware and reboot the reader.



**Function Description**:

| Menu | Descriptions |
|---|---|
| **Configuration** | Configure the reader parameters, including device alias, communication, function, UID output, mobile credentials, 125kHz, 13.56MHz, visual & audio, keypad and QR. |
| **Firmware Update** | Displays the current firmware information, click **Offine Update** to upgrade the firmware. |
| **Company Assign** | Assign the current reader to the company and click **Assign** to complete. |
| **Device Reset** | Click **Device Reset** to reset the reader to the default factory settings. Click **OK** to confirm. |
| **Device Reboot** | Click **Device Reboot** to reboot the reader. Click **OK** to confirm. |

### 2.4.2.1 View the Reader Information

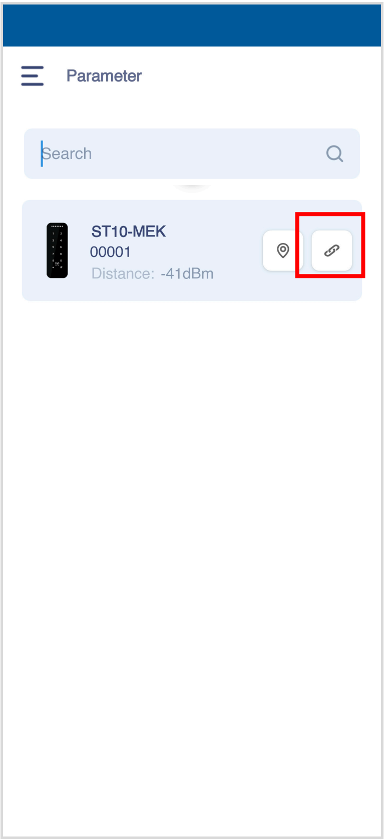
1. Click ☰ > **Parameter** to enter the parameter setting screen.

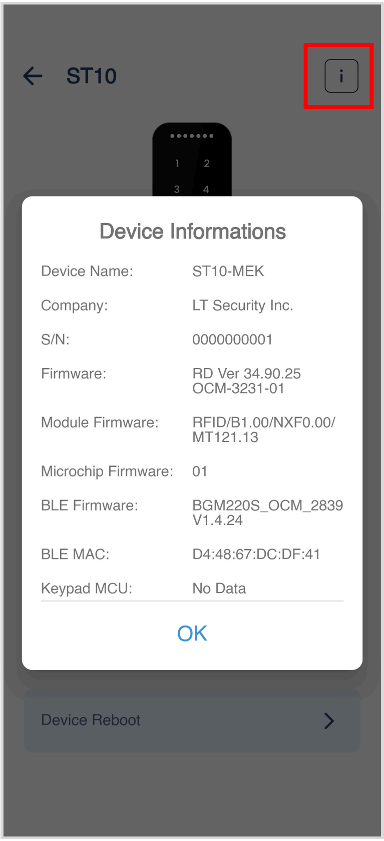
2. Turn on the Bluetooth function of the mobile device, it will search for the reader automatically. All searched readers will be displayed in the list.

3. Click 📍 to confirm your reader.

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

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.





Device Informations

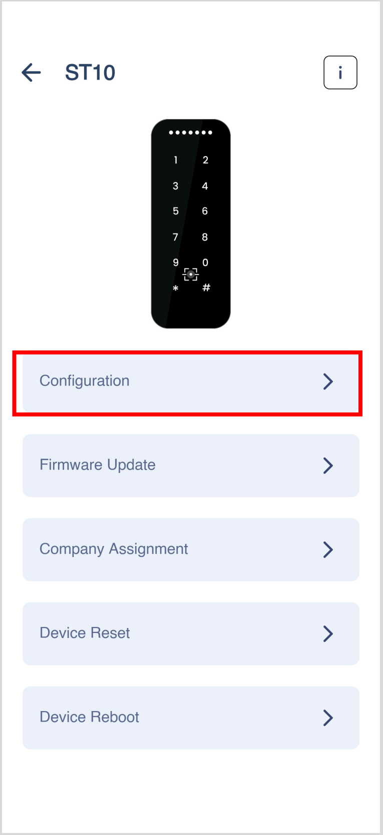
| | |
|---|---|
| Device Name: | ST10-MEK |
| Company: | LT Security Inc. |
| S/N: | 0000000001 |
| Firmware: | RD Ver 34.90.25 OCM-3231-01 |
| Module Firmware: | RFID/B1.00/NXF0.00/ MT121.13 |
| Microchip Firmware: | 01 |
| BLE Firmware: | BGM220S_OCM_2839 V1.4.24 |
| BLE MAC: | D4:48:67:DC:DF:41 |
| Keypad MCU: | No Data |

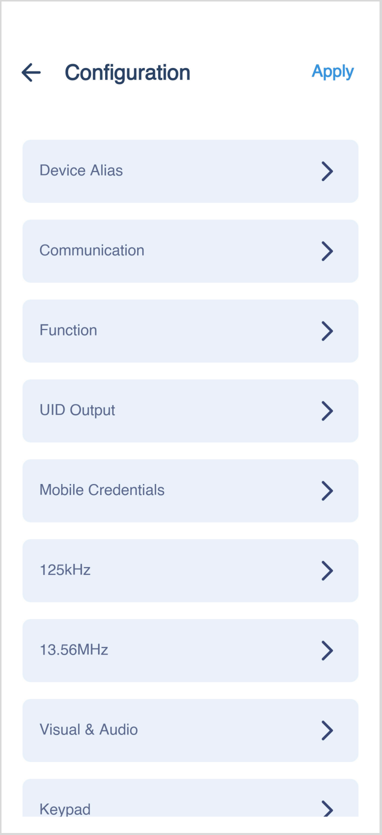
OK

### 2.4.2.2 Configure the Reader Parameters

Search your reader on the **Parameter** screen and select it, then click 🔗 to enter the reader parameter setting interface. Then you can operate the following steps.

**Configuration the reader parameters**





1. Click **Configuration** item to open the configuration setting interface.
2. To configure the reader parameters. The details are shown in the table below.

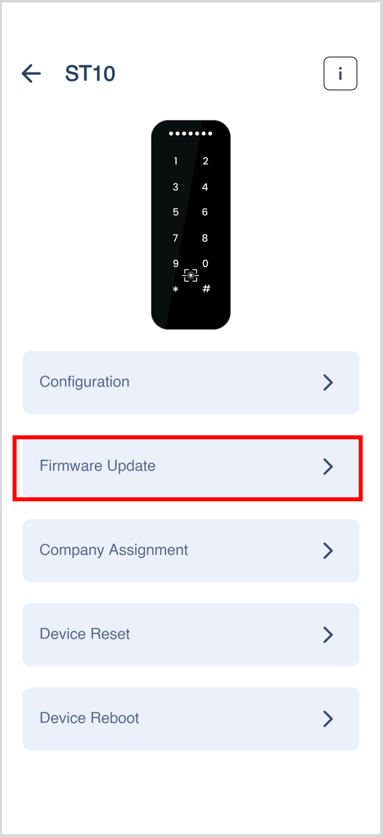
**Function Description**:

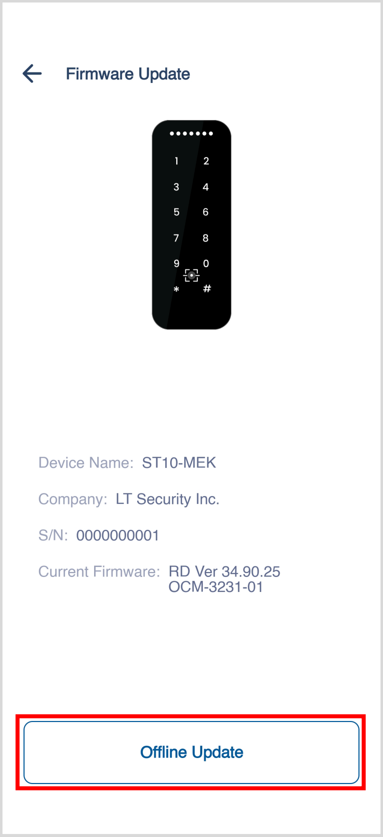
| Menu | Descriptions |
|---|---|
| **Device Alias** | Set the device alias of the reader. |
| **Communication** | Set the communication type of the reader, there are two options: OSDP (via RS-485) and Wiegand. |

| | |
|---|---|
| **Function** | - **Tamper Alarm:** Enable/disable the tamper alarm function.<br>- **Card Detect Timeout:** The amount of time taken to detect card verification. Valid value: 5 to 10 seconds. |
| **UID Output** | To set the format of UID output, Wiegand and RAW are optional. |
| | When selecting Wiegand format, the following parameters need to be set:<br>- **Wiegand:** Select the corresponding output bit digits of the Wiegand format, valid value: 1 to 66 bits.<br>- **MSB/LSB:** Set the significant bit. MSB: Most Significant Bit. LSB: Least significant bit.<br>When selecting RAW format, the following parameters need to be set:<br>- **Length:** Valid bytes are 1 to 8.<br>- **MSB/LSB:** Set the significant bit. MSB: Most Significant Bit. LSB: Least significant bit. |
| **Mobile Credentials** | Enable/Disable the Card Mode and Remote Mode.<br>- **Card Mode:** The adjustment range is 0 to 40 inches.<br>- **Remote Mode:** The adjustment range is 0 to 394 inches. |
| **125kHz** | Set the relevant parameters of the 125kHz RFID card.<br>**Note:** In the 125 kHz band, ST10 Series Readers support only RFID cards that are in the native EM4100/4102 format, or that can emulate these formats. |
| **13.56MHz** | Set the relevant parameters of the 13.56MHz RFID card. |
| **Visual & Audio** | Customize the LED display effect and volume of the reader.<br>**Indicator & Buzzer:** Includes settings for the following parameters. |

| | |
|---|---|
| | ▪ **Boot Up Successfully:** Set the Times and Color of the LED display after a successful boot. The Times can be set to none, 1 time, 2 times, or 3 times, and 7 colors are available.<br>▪ **Wiegand Idle:** Set the idle time and color of the reader in the Wiegand mode. The time can be set to none and ∞ , and 7 colors are available.<br>▪ **Controller Not Connected:** The time and color of the LED display when the reader is not connected to the controller. The time can be set to none and ∞ , and 7 colors are available.<br>▪ **Card detection:** The time and color of the LED display when the card is detected. The time can be set to none,1s, 2s and 3s, and 7 colors are available.<br>▪ **Tamper Alarm:** The time can be set to none, 1s, 2s, 3s, 4s and ∞ , and 7 colors are available.<br>▪ **Card Swipe Timeout:** When swiping the card time operation to set the time, the time and color of the LED display. The time can be set to none, 1s, 2s, 3s, 4s and ∞ , and 7 colors are available.<br>**Volume:** Adjust the volume of the reader; valid values are: 0, 30, 60, and 100. |
| **Keypad** | Set keypad mode, with DORADO, Password (4Bit) and Wiegand 26 Output optional. Applies only to readers equipped with a keyboard. The product actually purchased by the user shall prevail.<br>**Note:** The feature is only available for Wiegand Communication. |
| **QR** | Set the QR mode as RAW, Defendas ID or Formatted Static. Applies only to readers equipped with QR code reader. |

## Firmware Update





Device Name: ST10-MEK

Company: LT Security Inc.

S/N: 0000000001

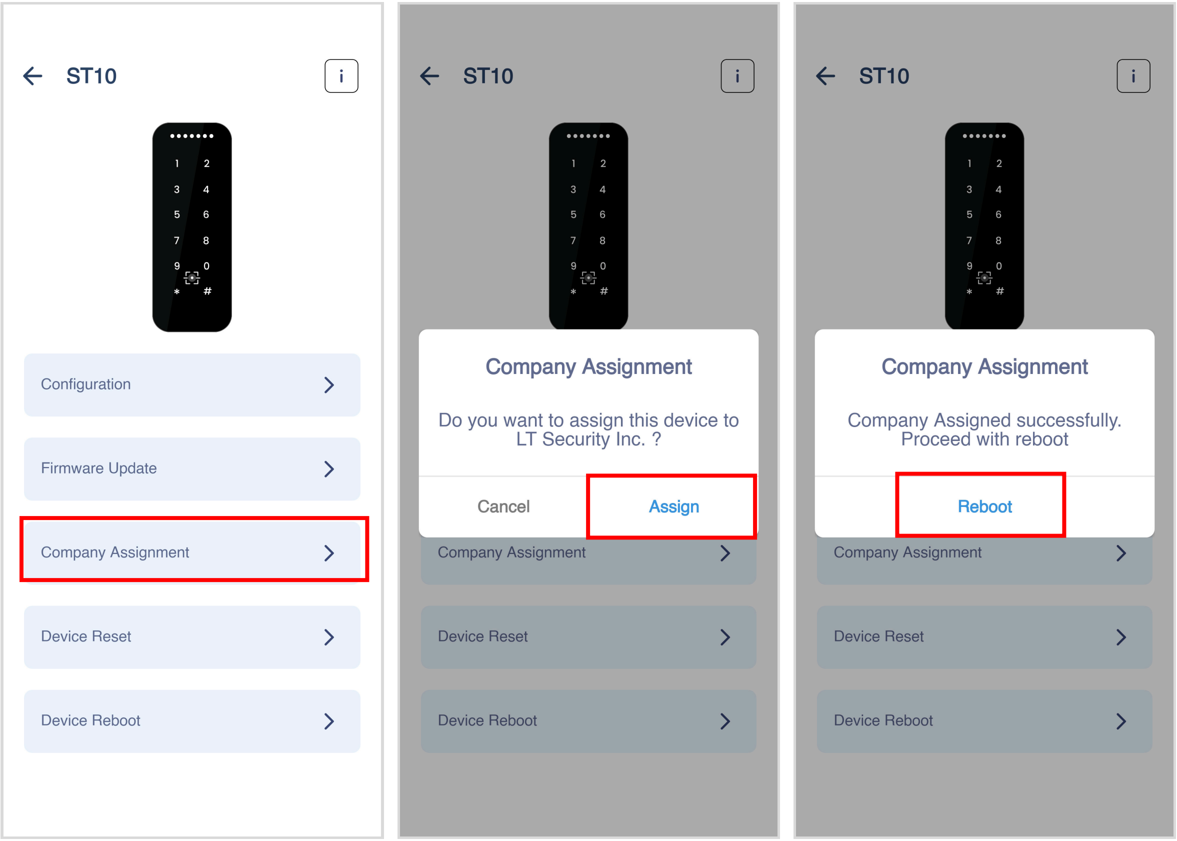
Current Firmware: RD Ver 34.90.25
OCM-3231-01

1. Click **Firmware Update** item to open the update setting interface. Here you can view the current firmware information.

2. Click **Offline Update** to upgrade the firmware.

## Company Assignment

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



Company Assignment

Do you want to assign this device to LT Security Inc. ?

Company Assignment

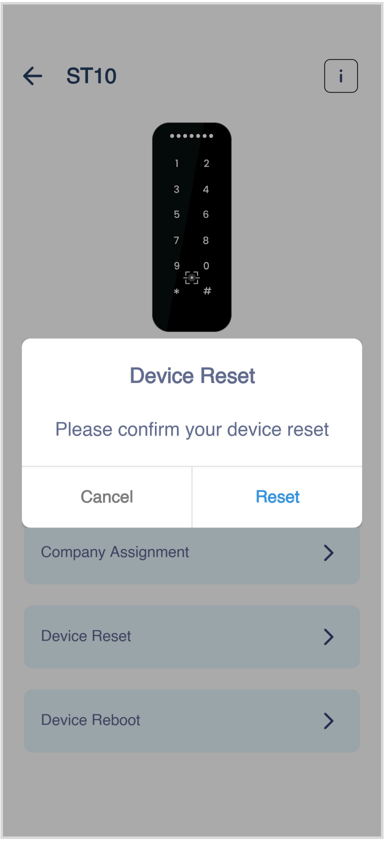
Company Assigned successfully. Proceed with reboot

1. Click **Company Assignment** item to open the setting interface. Click **Assign** to assign the reader to the company.

2. Click **Reboot** when prompted that the assignment is successful.

3. After completing the above steps, please wait for the reader to reboot. **Note:** After each configuration of the reader parameters, the reader will reboot.

## Device Reset



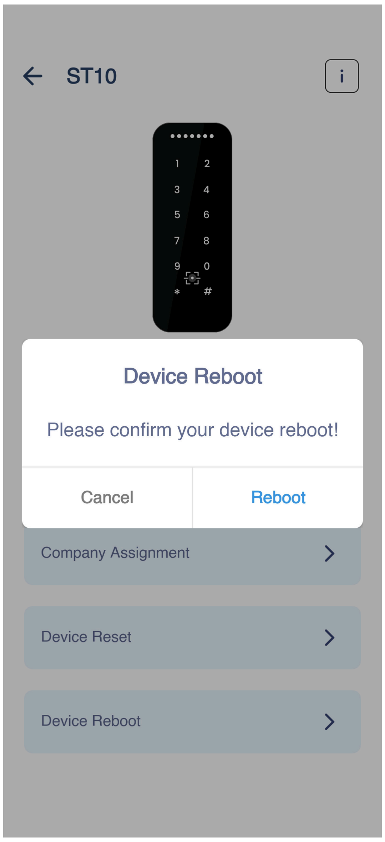
ST10

Device Reset

Please confirm your device reset

Click **Device Reset** to reset the reader to the default factory settings. Click **Reset** to confirm.

## Device Reboot



Device Reboot

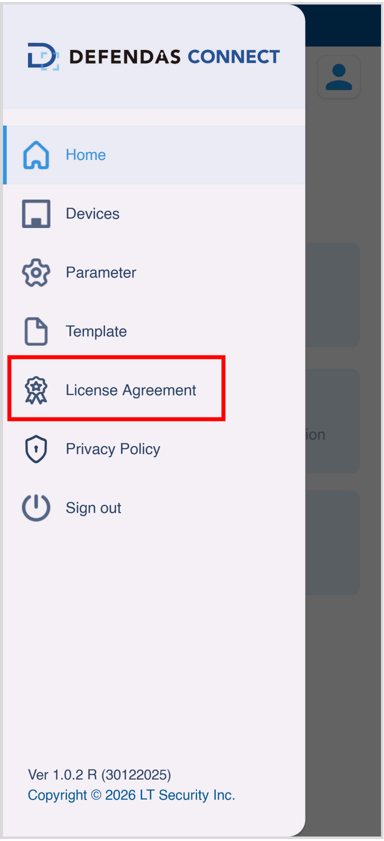
Please confirm your device reboot!

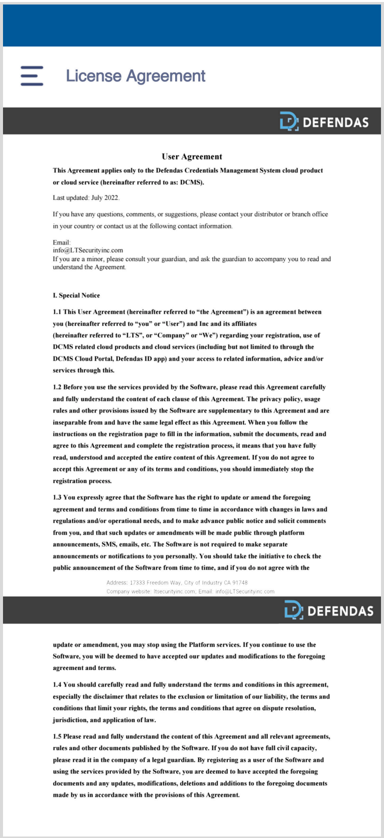
Cancel Reboot

Click **Device Reboot** to reboot the reader. Click **Reboot** to confirm.

## 2.4.3 License Agreement

Click ☰ > **License Agreement** to view the end user's license agreement.





User Agreement

**This Agreement applies only to the Defendas Credentials Management System cloud product or cloud service (hereinafter referred to as: DCMS).**

Last updated: July 2022.

If you have any questions, comments, or suggestions, please contact your distributor or branch office in your country or contact us at the following contact information.

Email:
info@LTSecurityinc.com
If you are a minor, please consult your guardian, and ask the guardian to accompany you to read and understand the Agreement.

**I. Special Notice**

**1.1 This User Agreement (hereinafter referred to "the Agreement") is an agreement between you (hereinafter referred to "you" or "User") and Inc and its affiliates (hereinafter referred to "LTS", or "Company" or "We") regarding your registration, use of DCMS related cloud products and cloud services (including but not limited to through the DCMS Cloud Portal, Defendas ID app) and your access to related information, advice and/or services through this.**

**1.2 Before you use the services provided by the Software, please read this Agreement carefully and fully understand the content of each clause of this Agreement. The privacy policy, usage rules and other provisions issued by the Software are supplementary to this Agreement and are inseparable from and have the same legal effect as this Agreement. When you follow the instructions on the registration page to fill in the information, submit the documents, read and agree to this Agreement and complete the registration process, it means that you have fully read, understood and accepted the entire content of this Agreement. If you do not agree to accept this Agreement or any of its terms and conditions, you should immediately stop the registration process.**

**1.3 You expressly agree that the Software has the right to update or amend the foregoing agreement and terms and conditions from time to time in accordance with changes in laws and regulations and/or operational needs, and to make advance public notice and solicit comments from you, and that such updates or amendments will be made public through platform announcements, SMS, emails, etc. The Software is not required to make separate announcements or notifications to you personally. You should take the initiative to check the public announcement of the Software from time to time, and if you do not agree with the update or amendment, you may stop using the Platform services. If you continue to use the Software, you will be deemed to have accepted our updates and modifications to the foregoing agreement and terms.**

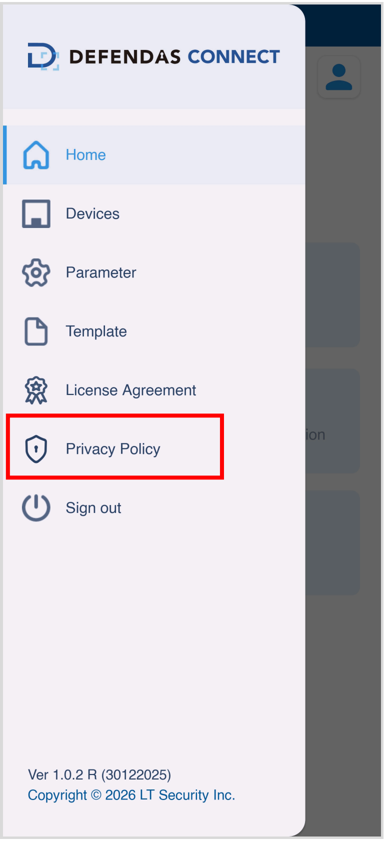
Address: 17333 Freedom Way, City of Industry CA 91748
Company website: ltsecurityinc.com; Email: info@LTSecurityinc.com

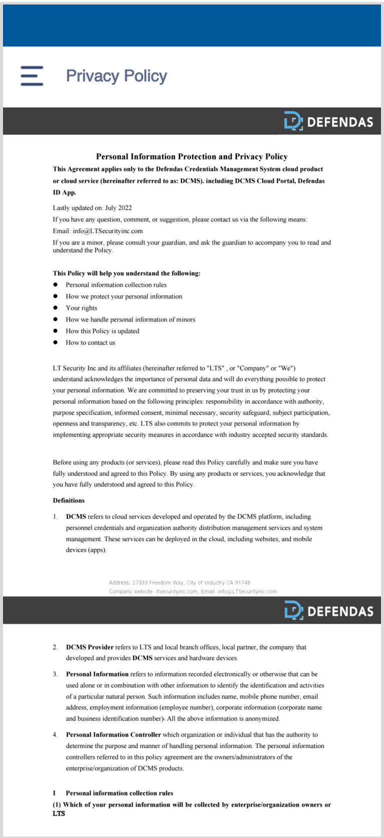
**1.4 You should carefully read and fully understand the terms and conditions in this agreement, especially the disclaimer that relates to the exclusion or limitation of our liability, the terms and conditions that limit your rights, the terms and conditions that agree on dispute resolution, jurisdiction, and application of law.**

**1.5 Please read and fully understand the content of this Agreement and all relevant agreements, rules and other documents published by the Software. If you do not have full civil capacity, please read it in the company of a legal guardian. By registering as a user of the Software and using the services provided by the Software, you are deemed to have accepted the foregoing documents and any updates, modifications, deletions and additions to the foregoing documents made by us in accordance with the provisions of this Agreement.**

## 2.4.4 Privacy Policy

Click ☰ > **Privacy Policy** to view the contents of the privacy policy.





**Personal Information Protection and Privacy Policy**

**This Agreement applies only to the Defendas Credentials Management System cloud product or cloud service (hereinafter referred to as: DCMS). including DCMS Cloud Portal, Defendas ID App.**

Lastly updated on: July 2022

If you have any question, comment, or suggestion, please contact us via the following means:

Email: info@LTSecurityinc.com

If you are a minor, please consult your guardian, and ask the guardian to accompany you to read and understand the Policy.

**This Policy will help you understand the following:**

- Personal information collection rules
- How we protect your personal information
- Your rights
- How we handle personal information of minors
- How this Policy is updated
- How to contact us

LT Security Inc and its affiliates (hereinafter referred to "LTS" , or "Company" or "We") understand acknowledges the importance of personal data and will do everything possible to protect your personal information. We are committed to preserving your trust in us by protecting your personal information based on the following principles: responsibility in accordance with authority, purpose specification, informed consent, minimal necessary, security safeguard, subject participation, openness and transparency, etc. LTS also commits to protect your personal information by implementing appropriate security measures in accordance with industry accepted security standards.

Before using any products (or services), please read this Policy carefully and make sure you have fully understood and agreed to this Policy. By using any products or services, you acknowledge that you have fully understood and agreed to this Policy.

**Definitions**

1. **DCMS** refers to cloud services developed and operated by the DCMS platform, including personnel credentials and organization authority distribution management services and system management. These services can be deployed in the cloud, including websites, and mobile devices (apps).

Address: 17333 Freedom Way, City of Industry CA 91748
Company website: ltsecurityinc.com; Email: info@LTSecurityinc.com

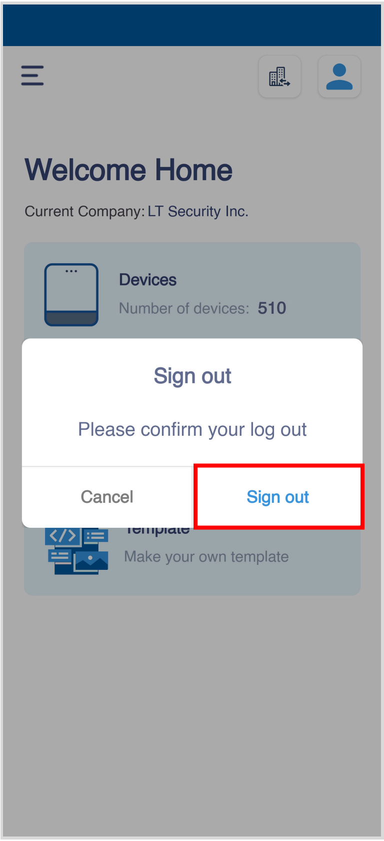
2. **DCMS Provider** refers to LTS and local branch offices, local partner, the company that developed and provides **DCMS** services and hardware devices.
3. **Personal Information** refers to information recorded electronically or otherwise that can be used alone or in combination with other information to identify the identification and activities of a particular natural person. Such information includes name, mobile phone number, email address, employment information (employee number), corporate information (corporate name and business identification number). All the above information is anonymized.
4. **Personal Information Controller** which organization or individual that has the authority to determine the purpose and manner of handling personal information. The personal information controllers referred to in this policy agreement are the owners/administrators of the enterprise/organization of DCMS products.

**I Personal information collection rules**

**(1) Which of your personal information will be collected by enterprise/organization owners or LTS**

## 2.4.5 Sign Out

Click ☰ > **Sign Out** to sign out of the current account.



Welcome Home

Current Company: LT Security Inc.

Devices
Number of devices: 510

Sign out

Please confirm your log out

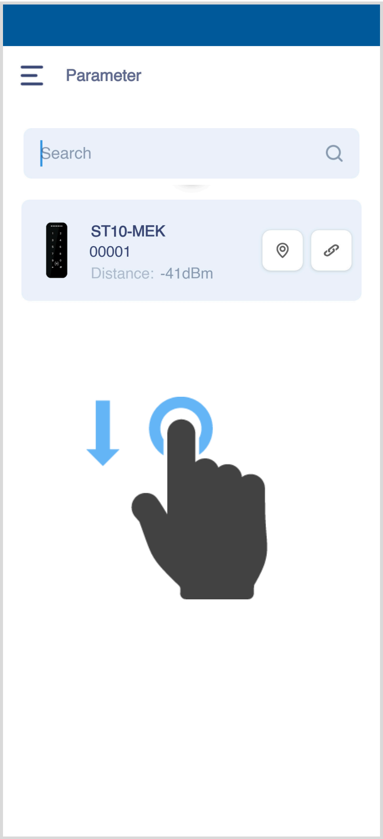
# 3 Basic App Functionality

This section provides steps and procedures for basic application functionality.

## 3.1 Search the Reader

Please turn on the Bluetooth function of the mobile device before operating.

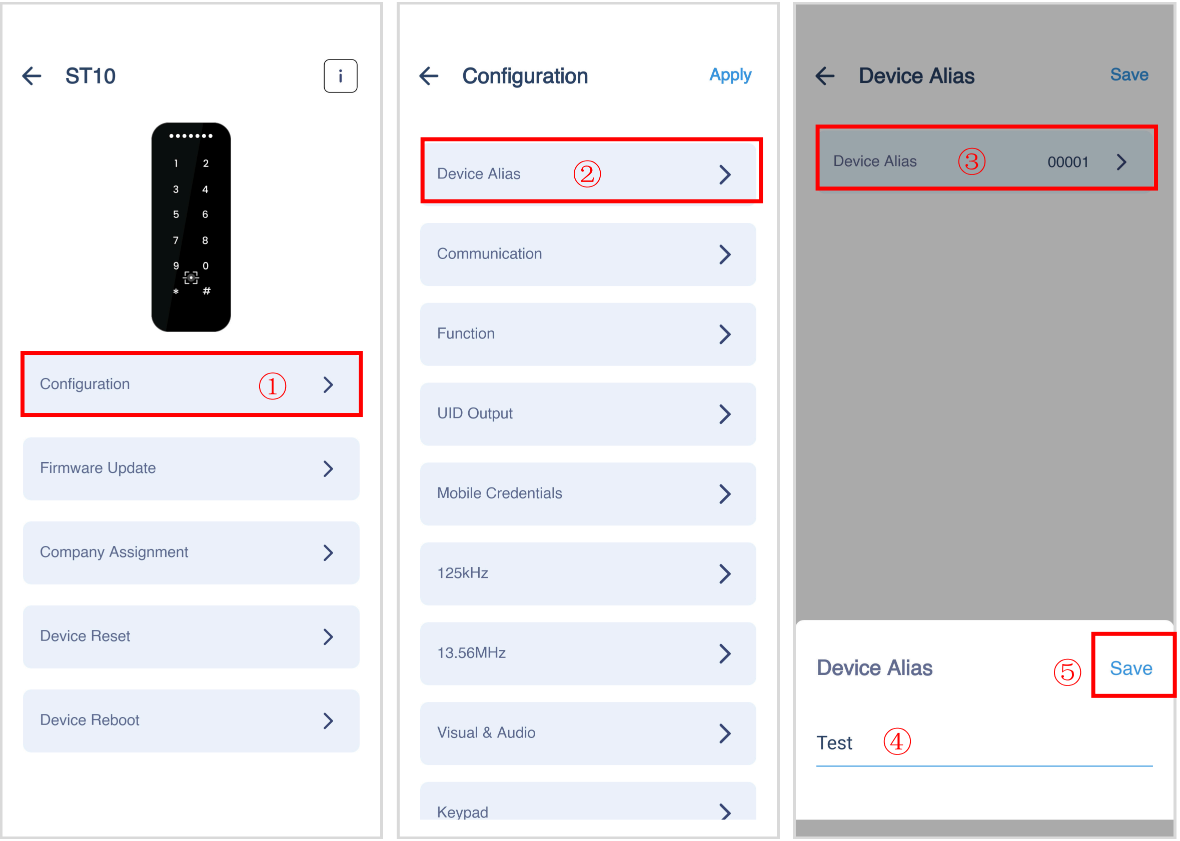
1. Click ☰ > **Parameter** to enter the **Parameter** setting screen.
2. If the readers are not displayed, swipe down to refresh the screen. All found readers will be displayed in the list.
3. Or enter the reader name and click 🔍 to search for a specific reader.



## 3.2 Change the Reader Name

The integrator can customize the reader name. This custom reader name is visible from within any other integrators DEFENDAS CONNECT App.

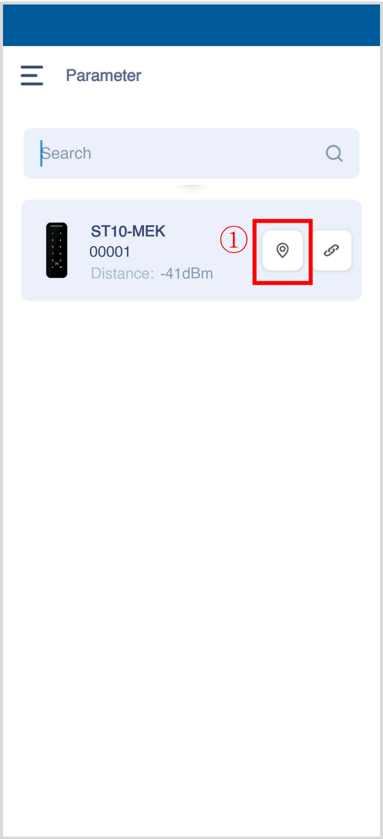
1. On the **Parameter** screen, click 🔗 to enter the reader parameter setting screen.
2. Click **Configuration** > **Device Alias** > **Device Alias** to open the setting window.
3. Enter the reader name. And then click **Save** to save the settings and exit to the previous menu.

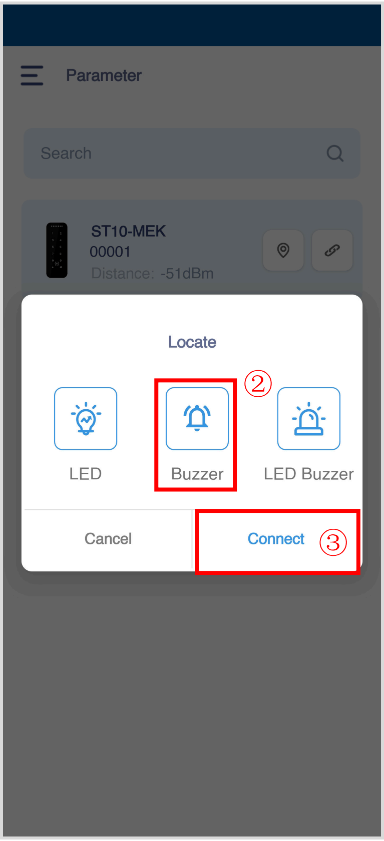


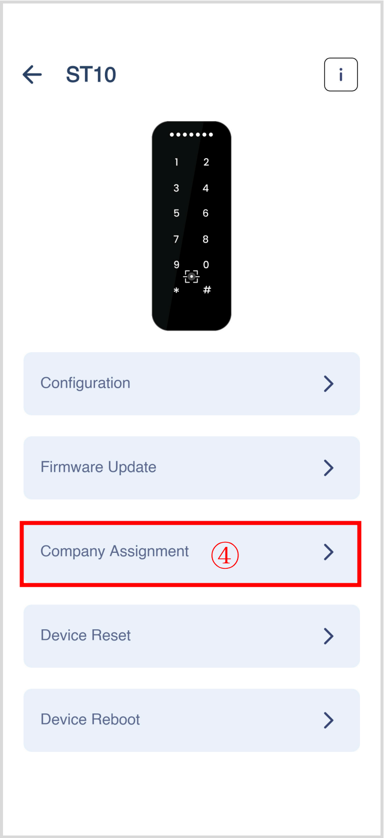
## 3.3 Assign the Reader to the Company

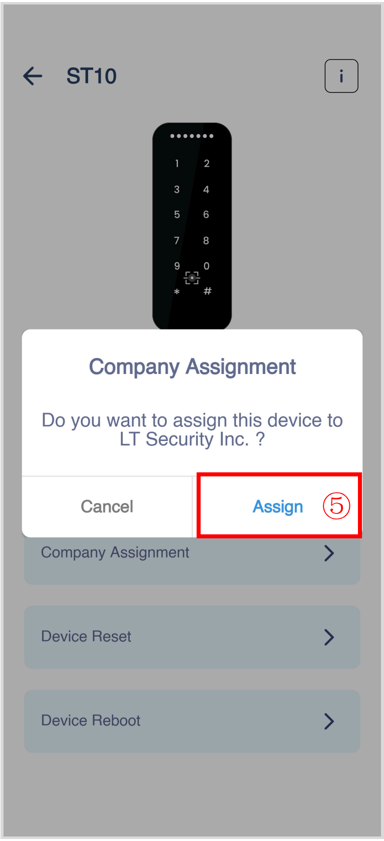
Please turn on the Bluetooth function of the mobile device before operating.

1. Click ☰ > **Parameter** to enter the **Parameter** setting screen.
2. Place your mobile device close to the reader, then find the closest reader in the list and click 📍 in the pop-up window. Click 🔔 in the pop-up window, and confirm your current reader according to the reader prompt.
3. Click **Connect** or 🔗 to enter the reader parameter setting screen.
4. Click **Company Assignment** and the Assignment window will pop up. Click **Assign** to assign the reader to the company.
5. Click **Reboot** when prompted that the assignment is successful.
6. After completing the above steps, please wait for the reader to reboot. **Note:** After each configuration of the reader parameters, the reader will reboot.





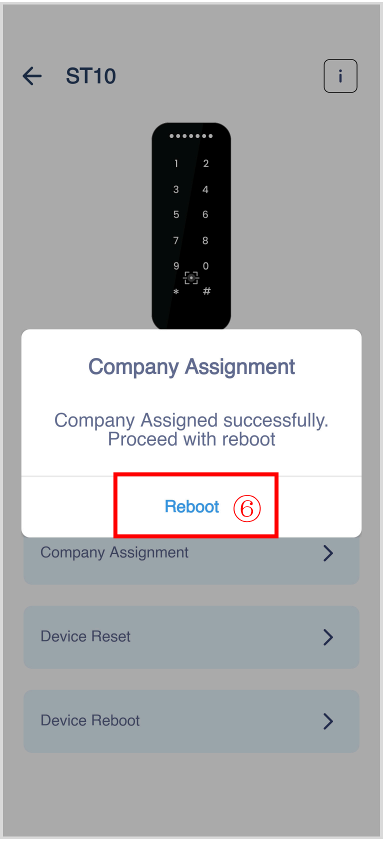




ST10

Company Assignment

Do you want to assign this device to LT Security Inc. ?



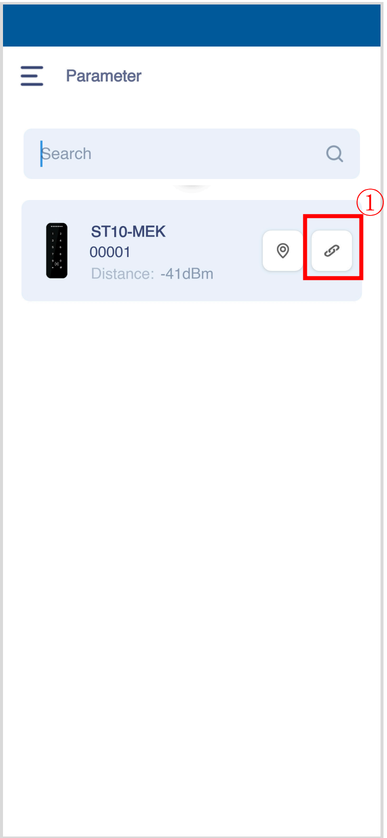
ST10

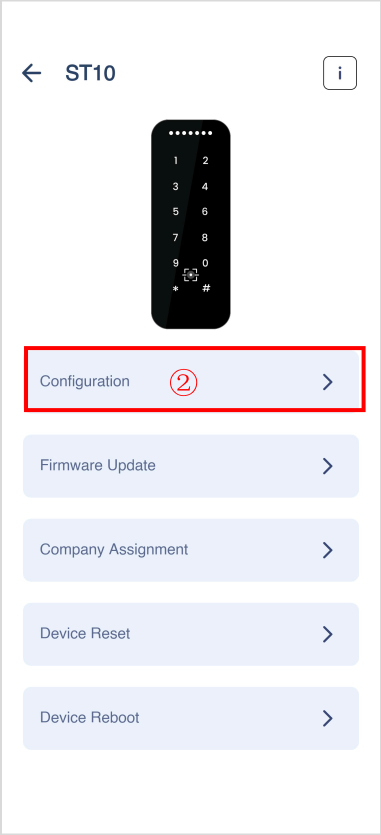
Company Assignment

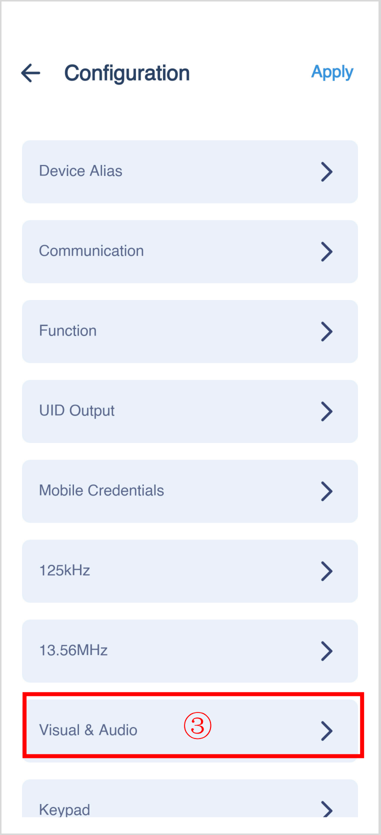
Company Assigned successfully. Proceed with reboot

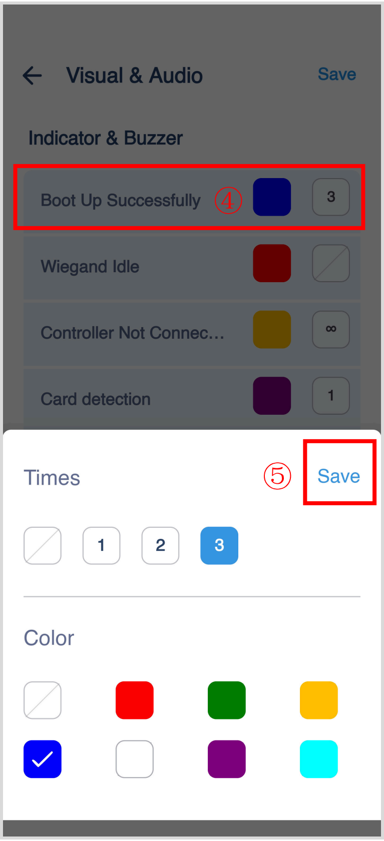
## 3.4 Audio & Visual Settings

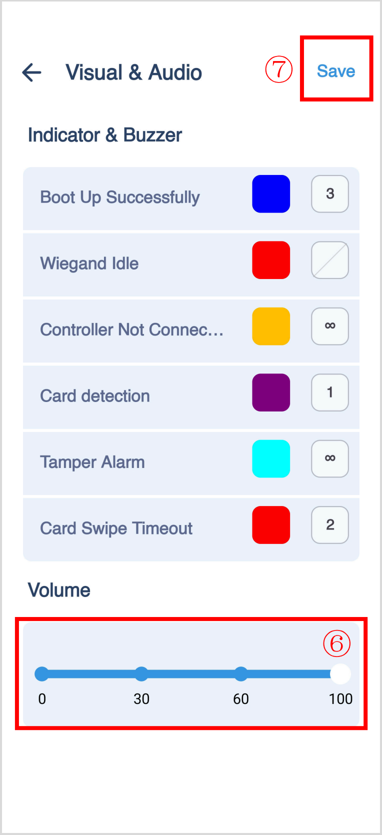
1. On the **Parameter** screen, click 🔗 to enter the reader parameter setting screen.
2. Click **Configuration** > **Visual & Audio** to enter the setting screen.
3. Select the option to be set in the Indicator & Buzzer list. Select the times and a color and click **Save**. There are a total of 7 colors to choose from, and each option is best set to a different color for easy identification.
4. Adjust the reader's volume in the volume bar; valid values are: 0, 30, 60, and 100.
5. Click **Save** to save the settings and exit to the previous menu.











Indicator & Buzzer

| | | |
|---|---|---|
| Boot Up Successfully | 🟦 | 3 |
| Wiegand Idle | 🟥 | |
| Controller Not Connec… | 🟨 | ∞ |
| Card detection | 🟪 | 1 |
| Tamper Alarm | 🟦 | ∞ |
| Card Swipe Timeout | 🟥 | 2 |

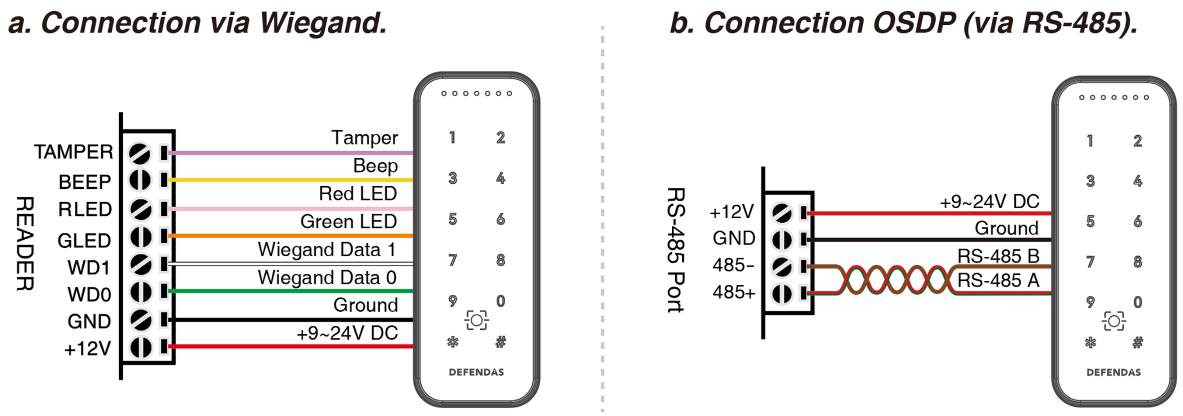
Volume

0 30 60 100

## 3.5 Communication Settings

The supported ST10 Series Readers are connected to the controller through OSDP (via RS-485) or Wiegand.

1. Before setting the parameters, make sure that the reader is connected to the controller according to the OSDP (via RS-485) or Wiegand wiring in Figure 1.



*a. Connection via Wiegand.*

*b. Connection OSDP (via RS-485).*

**Figure 1** Controller and reader OSDP (via RS-485) and Wiegand wiring diagram

2. In the reader parameter setting interface, click **Configuration** > **Communication** to enter the setting screen.

3. Click **Communication Type** to enter the setting screen. You can choose the appropriate communication type to carry out OSDP (via RS-485) or Wiegand connection with the controller according to your needs.

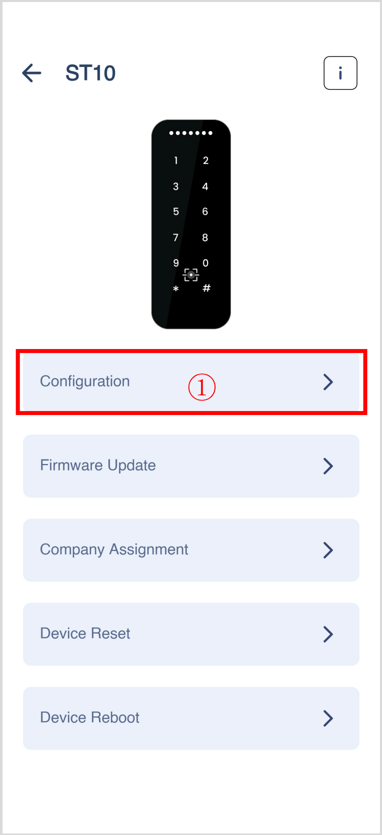
4. Click **Save** to save the settings and exit to the previous menu.

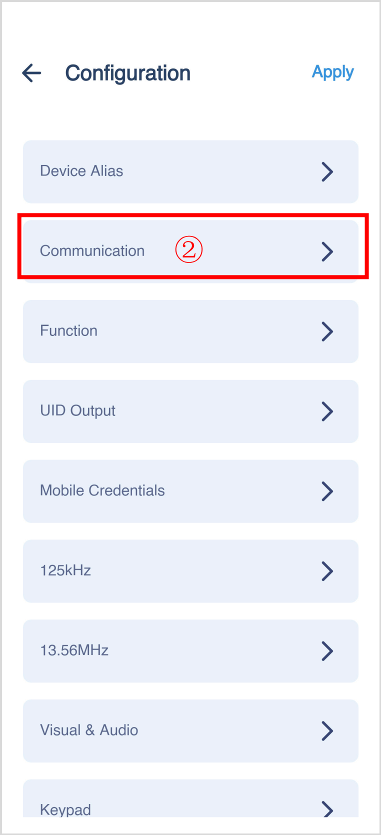
***Remark:***

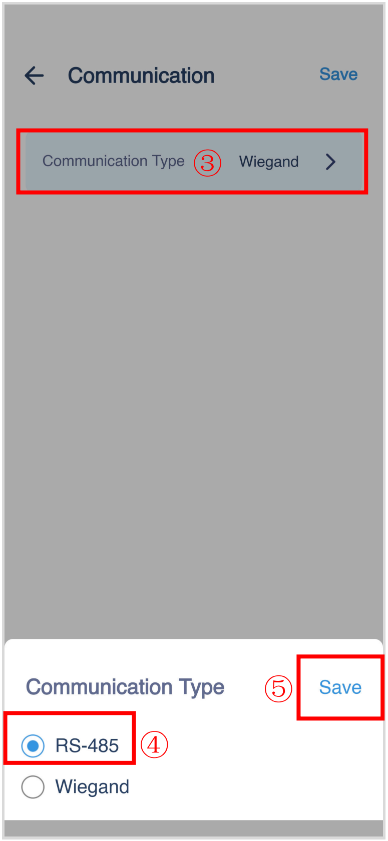
***When communicating with the device through the OSDP (via RS-485) serial port, please consider the baud rate and addressing points below:***

- *The baud rate at which the data is communicated with reader, there are 6 options of baud rate: 115200(default), 57600, 38400, 19200, 9600 and 4800.*
- *The higher the baud rate, the faster the communication speed, but also the less reliable.*
- *Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate would be more reliable.*

- *You need to set the RS-485 address, the default is 1.*





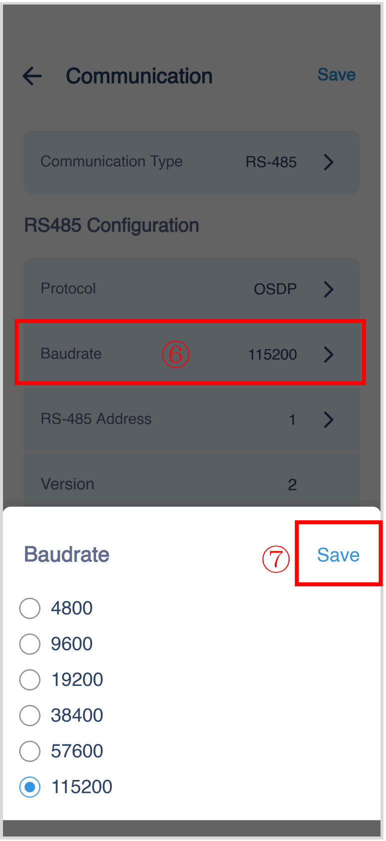


Communication Type: Wiegand

Communication Type

● RS-485

○ Wiegand



Communication Type: RS-485

Protocol: OSDP

Baudrate: 115200

RS-485 Address: 1

Version: 2

Baudrate

○ 4800

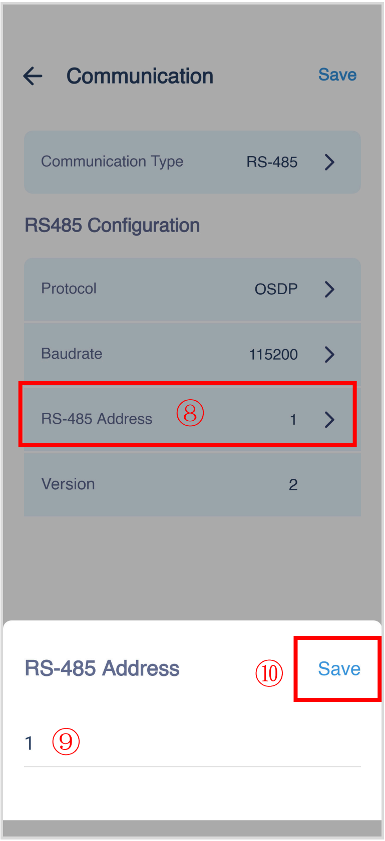
○ 9600

○ 19200

○ 38400

○ 57600

● 115200



Communication Type: RS-485

Protocol: OSDP

Baudrate: 115200

RS-485 Address: 1

Version: 2

RS-485 Address

1

# 4 Appendix

## User Agreement

**This Agreement applies only to the Defendas Credentials Management System cloud product or cloud service (hereinafter referred to as: DCMS).**

Last updated: November 2025

If you have any questions, comments, or suggestions, please contact your distributor or branch office in your country or contact us at the following contact information.

Email: info@LTSecurityinc.com

If you are a minor, please consult your guardian, and ask the guardian to accompany you to read and understand the Agreement.

### I. Special Notice

**1.1 This User Agreement (hereinafter referred to “the Agreement”) is an agreement between you (hereinafter referred to “you” or “User”) and Inc and its affiliates (hereinafter referred to “LTS”, or “Company” or “We”) regarding your registration, use of DCMS related cloud products and cloud services (including but not limited to through the DCMS Cloud Portal, Defendas ID app) and your access to related information, advice and/or services through this.**

**1.2 Before you use the services provided by the Software, please read this Agreement carefully and fully understand the content of each clause of this Agreement. The privacy policy, usage rules and other provisions issued by the Software are supplementary to this Agreement and are inseparable from and have the same legal effect as this Agreement. When you follow the instructions on the registration page to fill in the information, submit the documents, read and agree to this Agreement and complete the registration process, it means that you have fully read, understood and accepted the entire content of this Agreement. If you do not agree to accept this Agreement or any of its terms and conditions, you should immediately stop the registration process.**

**1.3 You expressly agree that the Software has the right to update or amend the foregoing agreement and terms and conditions from time to time in accordance with changes in laws and regulations and/or operational needs, and to make advance public notice and solicit comments from you, and that such updates or amendments will be made public through platform announcements, SMS, emails, etc. The Software is not required to make separate announcements or notifications to you**

**personally. You should take the initiative to check the public announcement of the Software from time to time, and if you do not agree with the update or amendment, you may stop using the Platform services. If you continue to use the Software, you will be deemed to have accepted our updates and modifications to the foregoing agreement and terms.**

**1.4 You should carefully read and fully understand the terms and conditions in this agreement, especially the disclaimer that relates to the exclusion or limitation of our liability, the terms and conditions that limit your rights, the terms and conditions that agree on dispute resolution, jurisdiction, and application of law.**

**1.5 Please read and fully understand the content of this Agreement and all relevant agreements, rules and other documents published by the Software. If you do not have full civil capacity, please read it in the company of a legal guardian. By registering as a user of the Software and using the services provided by the Software, you are deemed to have accepted the foregoing documents and any updates, modifications, deletions and additions to the foregoing documents made by us in accordance with the provisions of this Agreement.**

### II. Service Content

2.1 The software provides you with related services, including but not limited to

Personnel and organization management: personnel credentials and organization authority distribution management services

2.2 You agree and acknowledge that the Company shall only provide the services explicitly agreed in this Agreement, except for the equipment related to the relevant software services (such as personal computers, cell phones, other devices related to access to the Internet or mobile networks) and the related fees charged by third parties (such as telephone and Internet access fees paid for access to the Internet and cell phone fees paid for the use of mobile networks), which shall be borne by you.

### III. Declaration of Intellectual Property Rights

3.1 The Company is the owner of the intellectual property rights of the Software. All copyrights, trademarks, patents, trade secrets and other intellectual property rights of the Software, as well as all information content related to the Software (including but not limited to text, pictures, audio, video, graphics, interface design, layout frames, relevant data or electronic documents, etc.) are protected by the laws and regulations of the state of Georgia and the corresponding international treaties. The Company shall enjoy the above-mentioned intellectual property rights, except for the rights that the relevant right holders shall enjoy in accordance with the provisions of the law.

3.2 Without the written consent of the Company or the relevant right holder, the User shall not implement, utilize or transfer the above intellectual property rights for any commercial or non-commercial purposes by itself or license any third party.

## IV. Change, Interruption, or Termination of Services

4.1 The user understands that the Company needs to overhaul or maintain the Software or related equipment on a regular or irregular basis, and that the ability to connect to the Internet is limited by the stability of the global network, the state of technology, the location of the user and the network used, power supply, government control, computer viruses, hacker attacks and other existing uncertainties, and that the Company shall not be liable for any interruption of service caused by such circumstances, and shall provide prior notice except in special circumstances.

**4.2 The Company has the right to interrupt or terminate the provision of all or part of the software and services under this Agreement to you at any time without any liability to you or any third party if any of the following circumstances occurs.**

**1) The personal information provided by you is untrue.**

**2) You violate the rules of use set forth in this Agreement.**

**3) You do not pay the corresponding service fee to the Company as required when using the software fee service.**

**4) Your behavior violates laws and regulations or government regulations.**

**4.3 The user's registered account or use of the Software and services shall not engage in behavior or manner that violates laws, regulations or national policy requirements, or infringes on the legitimate rights and interests of any third party, and if any of the above circumstances exist, the user shall bear the corresponding legal responsibility, and the Company shall have the right to prohibit the user from continuing to use the account or stop the user from continuing to use the Software, or provide the relevant information to the government, court or prosecuting authority in accordance with the relevant laws or government orders, and the user shall bear the liability for any loss caused to the Company as a result.**

**4.4 If you decide to stop using for the payment application, you may voluntarily submit a request to our partners & us to terminate the service, but we will not refund a portion of the fees for the service that you have enjoyed from the time you started the service until the moment which you submit the termination.**

**4.5 If, as a person in the enterprise/organization, you no longer use the paid services provided in our software products, please make your own request to the owner/administrator of the enterprise/organization.**

## V. Use Rules

**5.1 After the user's registration is completed, a user account is automatically generated, which is under the control of the software user and gains the right to use the account. Once the account is used, any form of transfer, including but not limited to gift, loan, rent, transfer or sale, is prohibited. The user assumes responsibility for the safekeeping of the account and password and is solely responsible for all activities under his account, sub-accounts created by his account and password (whether or not done by or with the authorization of the user), and the user is**

**responsible for the safekeeping of the registered account information and the actions under the password, and the user is legally responsible for the registered account and the actions under the password. Users agree not to use other members' accounts and passwords under any circumstances.**

**5.2 Users shall not transfer or lend their accounts and passwords to others for use. If the user finds that his or her account has been used illegally by others, he or she should immediately notify our company. The user shall be responsible for all losses that occur due to hacking or the user's negligence in keeping the account and password illegally used by others, and the Company shall not be responsible for any losses. If this causes damage to the Company, the user agrees to compensate the Company for the damage.**

5.3 The user has the right to change and delete personal data, registration information and transmission content in the Software, but it should be noted that deletion of the relevant information will also delete any text and images you have stored in the system, and the user shall bear the risk.

5.4 Users shall comply with the terms and conditions of this Agreement and use the Local Services correctly and appropriately. If the User violates any of the terms and conditions of this Agreement, the Software shall have the right to terminate the provision of services to the account of the defaulting User in accordance with the Agreement. At the same time, the Software reserves the right to withdraw the account and user name of the Software at any time.

5.5 Users shall provide true, accurate, legal, valid and complete information as guided by the registration page if necessary when registering for an account. For individual users, including and not limited to the use of their real name, cell phone number, cell phone SMS, ID card or other supportable documents and other personal information for real name verification; for legal person users, including and not limited to the enterprise unified social credit code / business registration number, the legal representative of the enterprise ID card number, enterprise CA certification and other information for real name verification.

5.6 Users shall not register with false information or other illegal and undesirable information. The ownership of the user's account belongs to the Software. After the user completes the application registration procedure, he/she only obtains the right to use the account, and the right to use belongs to the applicant registrant only. At the same time, the applicant registrant shall not gift, transfer or otherwise license the account to others.

5.7 Users are obliged to ensure the security of their accounts and passwords. If the user discovers that the account has been used without authorization or any other security problems, such as being informed by others of their registration data, or the account is used illegally due to hacking or the user's negligence in storage, the user shall bear the loss, including but not limited to the loss of the service data of the Software, the information data carried in the account, etc. The Software and the owner of the Software shall not bear any the software and the software owner shall not be held responsible. If the user loses or forgets the password and resets the password by cell phone number, password fingerprint, password face, etc., the Software is only responsible for verifying whether the verification information is consistent with the information related to the account, and is not responsible for the impersonation verification and the loss caused by it.

5.8 Users may incur data traffic costs in the process of using the Software, and users are required to find out the relevant tariff information from the operators and bear the related costs.

5.9 Users fully understand and agree that the Software is only a platform for users to share, transmit and obtain information, and users must be responsible for all actions under their registered accounts, including any content transmitted by you and any results arising therefrom. Users shall exercise their own judgment regarding the content in the Software and bear all risks arising from the use of the content, including risks arising from the correctness, completeness, usefulness or reliance on the content. The Software shall not be liable for any loss or damage arising from the User's actions.

5.10 Any content transmitted by the user in or through the Software does not reflect the views and policies of the Software and the Software assumes no responsibility for them.

5.11 The user fully understands and agrees that the Software is a product based on the user's identity service, and the user must assume full responsibility for the authenticity, legality, and validity of the information registered in the Software. Users shall not impersonate others, shall not use the name of others to disseminate any information, shall not maliciously register and use the registered account to cause other users to misidentify, otherwise the Software has the right to immediately stop providing services, and the user alone shall bear all legal responsibilities arising therefrom.

5.12 The user must be solely responsible for the authenticity, legality, harmlessness and validity of the information transmitted in the Software, and any legal responsibility related to the information disseminated by the user shall be borne by the user and has nothing to do with the Software.

5.13 The services provided by the Software may include advertisements, and the User agrees to display advertisements provided by the Software and third-party suppliers and partners in the course of use.

5.14 Users must follow the following principles in the process of using the Software.

1) comply with all agreements, regulations and procedures relating to the Software and the Services.

2) not to use the software for any illegal purpose.

3) not to use the Software in any form to infringe upon the commercial interests of the Company, including and not limited to publishing commercial advertisements that are not permitted by the Company.

4) shall not use the Software for any act that may adversely affect the normal operation of the Internet or mobile network.

5) shall not use the Software to upload, display or transmit any false, harassing, libelous, abusive, threatening, vulgar and obscene or any other illegal information data.

6) shall not infringe on the patent rights, copyright trademark rights, reputation rights or any other legitimate rights and interests of any other third party.

7) shall not use the Software and the Services for any conduct detrimental to the Company.

5.15 Any content produced, copied, published or disseminated by users in the course of using the Software and Services, including but not limited to account avatars, names, user descriptions and other registration information, or text, voice, images, etc. sent, replied to, accompanying graphics and related link pages, as well as other content generated by the use of the account or the Software and Services, shall not infringe the legitimate rights and interests of other users or third parties, including but not limited to

1) Spreading rumors, disturbing social order and destabilizing society

2) Spreading obscenity, pornography, gambling, violence, terrorism or abetting crime

3) Insulting or slandering others and infringing on their legitimate rights and interests

4) Inciting illegal assemblies, associations, marches, demonstrations, and gatherings to disrupt social order

5) Activities in the name of illegal civil organizations

6) Containing other contents prohibited by laws and administrative regulations

7) Publishing, transmitting, disseminating, storing content that infringes on the legal rights of others such as reputation, portrait rights, intellectual property rights, trade secrets, etc.

8) Involving the privacy, personal information or information of others

9) Publishing, transmitting, disseminating harassment, advertising information, excessive marketing information and spam or containing any sexual or sexually explicit information

10) Other information that violates laws, regulations, policies and public order and morality, social morality or interferes with the normal operation of the Software and violates the legitimate rights and interests of other users or third parties.

5.16 Except as permitted by law or with the written permission of the Software, users shall not engage in the following acts in the course of using the Software.

1) Deleting the information on the Software and its copies regarding copyright.

2) Reverse engineer, reverse assemble, reverse compile, or otherwise attempt to discover the source code of the Software.

3) Illegal use, rental, lending, copying, modification, linking, reproduction, compilation, publication, publication, establishment of mirror sites, etc. of the content of which the owner of the Software owns the intellectual property rights.

4) Copying, modifying, adding, deleting, linking, running or creating any derivative works of the Software or the data released into the memory of any terminal during the operation of the Software, the interaction data between the client and the server during the operation of the Software, and the system data necessary for the operation of the Software, including but not limited to using plug-ins, plug-ins or third-party tools/services not authorized by the Software to access the Software and related systems.

5) Adding, deleting, changing the functions or operating effects of the Software by modifying or falsifying the instructions or data in the operation of the Software, or operating or disseminating the Software or methods used for such purposes to the public, whether or not such acts are for commercial purposes.

6) Interfering with the Software, its components, modules and data by itself or authorizing

others or third party software.

5.17 Any statements, notices, warnings, etc. made by the Company by various means (including but not limited to web announcements emails, SMS alerts, etc.) for the use of certain specific software/services are considered part of this Agreement, and the user is deemed to be aware of and agree to the contents of such statements, notices, warnings if he/she uses the software/services.

5.18 The Company shall have the right to review and supervise the use of the Software Services (including but not limited to free or paid services) by the User in accordance with the terms of the Privacy Policy of the Software (including but not limited to the review of the content stored by the User in the Company), and if the User violates any of the above provisions when using the Software Services, the Company shall have the right to require the User to correct or directly take all necessary measures (including but not The Company reserves the right to require the user to correct or directly take all necessary measures (including but not limited to changing or deleting the user's posted content, suspending or terminating the user's right to use the software and services) to mitigate the impact of the user's misconduct. Due to the user's own behavior to be responsible to third parties, the user shall bear their own responsibility, and the Company has nothing to do.

5.19 Software Updates.

Although the company is not obligated to provide you with update services, it may still provide you with software updates. Replacement or supplemental software updates provided by the Company are governed by this Agreement, unless such updates are accompanied by a separate user service agreement, in which case they will be governed by the latter. If you decide not to download the updates provided by us, you understand and acknowledge that you may be placing the Software at serious security risk and may render the Software unavailable or unstable. Some Software features may be version limited and therefore updating to the latest version may enhance your user experience.

5.20 If a user uses a service function that involves a service provided by a third party of the Software, in addition to complying with this Agreement, the user shall also comply with the user agreement and rules of the third party. The correctness, accuracy, security, effectiveness and any possible risk of uncertainty of the services provided by third parties are not related to the Software and all parties to the Software. The Software and the Owners of the Software shall not be liable for any disputes or damages arising from the services provided by third parties. Any dispute arising from third party software or technology used by the Software shall be resolved by the third party and the Software and the Software Owners shall not be liable for any dispute.

## VI. License and Permissions

6.1 Subject to your compliance with this Agreement, we grant you a limited, non-exclusive, non-transferable license to download and install one copy of the Application onto a single mobile device owned or controlled by you and to run such copy of the Application solely for your own personal use.

6.2 You may not.

1. License, sublicense, sell, resell, transfer, assign, distribute, distribute, or otherwise

commercially exploit or make available the Services or Application to any third party in any manner.

2. Modify the Services or Applications or create derivative works therefrom.

3. Create Internet "links" to the Services, or "design" or "mirror" any Application on any other server or wireless or Internet-based device.

4. Reverse engineering or accessing an application to design or build a competitive product or service, designing or building a product using ideas or graphics similar to those of a service or application, or copying any idea, feature, function or graphic of a service or application.

5. Launch automated programs or scripts that send multiple server requests per second or programs that overburden or impede the work and/or performance of the service or application.

6.3 In addition, you may not.

1. Send spam or other forms of repetitive or unwanted mail that violate applicable law.

2. Send or store infringing, obscene, threatening, defamatory or otherwise illegal or infringing material, including material that endangers children or offends the privacy rights of third parties.

3. Sending or storing information containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs.

4. Obstruct or disrupt the integrity or performance of the website, applications, services or data contained therein.

5. Attempting to gain unauthorized access to the website, application, service or its associated systems or networks.

6.4 To the maximum extent permitted by law, we will have the right to investigate and prosecute any such violations. We may participate in and assist law enforcement authorities in prosecuting users who violate this Agreement. We reserve the right to remove or disable access to any Content at any time without notice if we believe that such Content violates this Agreement or otherwise jeopardizes the Site, the Software and/or the Services or Application Stalk order therein.

## VII. Privacy Protection

7.1 Protection of user privacy is a basic policy of the Company, and the Company guarantees that it will not disclose or provide to third parties not affiliated with the Company the registration data of individual users and the non-public content stored in the Software by users when using the Software and the Services, except for the following cases.

1. With the prior express authorization of the user.

2. In accordance with the requirements of relevant laws and regulations.

3. In accordance with the requirements of the relevant governmental authorities.

4. In order to safeguard the interests of the public

5. For the purpose of maintaining the legitimate rights and interests of the Company.

7.2 The privacy policy published by the Software is a valid part of this Agreement, and you agree that the Company may update the privacy policy from time to time and accept the updated privacy policy.

## VIII. Disclaimer

**8.1 The Company shall not be liable for any problems arising from the use of the Software due to abuse, misuse or unauthorized modification. The user expressly agrees that the risk of using the Company's software and services will be borne entirely by the user; all consequences arising from the user's use of the Company's software and services will also be borne by the user, and the Company shall not be liable to the user in any way.**

**8.2 The Company makes no warranty of any kind with respect to the Software and Services, including, but not limited to, the timeliness, security, and accuracy of the Software and Services, and the Company shall not be liable for direct, indirect, incidental, special, and consequential damages and risks arising from the use of or inability to use the Software and Services under any circumstances.**

**8.3 Installation of the Software may affect the availability of third party software, applications or services. The Company does not guarantee that the functions or services contained in the Software will meet your requirements, that the Software and its services will be completely error/bug-free or that they will provide continuous and durable service. In addition, the Company does not warrant that the Software will be compatible with any third party software or services.**

**8.4 The User understands that the Company cannot guarantee that the products or services it provides will be free of defects, but the Company is committed to continuously improving the quality and level of service. Therefore, the user agrees that even if there are defects in the services provided by the Company, such defects are unavoidable at the time of the technical level of the industry and will not be considered as a breach of contract by the Company. The user agrees to cooperate with the Company to solve the above-mentioned defects.**

**8.5 Our software is designed for non-profit organizations, private business organizations and individuals. We do not provide services to any illegal organizations or terrorists.**

## IX. Compensation

**9.1 By accepting this Agreement and using each application and/or service in the Software, you agree that you shall indemnify and hold harmless the Company from and against any and all claims, costs, damages, losses, liabilities and expenses (including legal fees and court costs) arising out of or related to the following matters**

**1. Your violation or breach of any provision of this Agreement or any applicable law or regulation (whether or not referred to herein).**

**2. You have violated any rights of any third party.**

**9.2 To the extent permitted by applicable law, we shall not be liable under any circumstances (regardless of cause) for: 1. any indirect, intentional, punitive, incidental, exemplary, special or consequential damages; 2. loss of business or opportunity; 3. loss of revenue; 4. loss of profits; 5. loss of goodwill; 6. loss of content; or 7. loss of data.**

## X. Modification of the Agreement

**The Company has the right to modify any of the terms of this Agreement at any time. Once the content of this Agreement changes, the Company will publish the modified content of the Agreement on the DCMS webpage and mobile app, and request users to re-view and agree to the modified content.**

## XI. Force Majeure

**The user agrees that the lessor is obligated by law to provide basic security, but cannot be held responsible for damages caused to the user due to failure of information network infrastructure, information network equipment maintenance connection, failure of computer, communication or other systems, power failure, strike, riot, fire, natural disaster, explosion, war, governmental action, order of judicial and administrative authorities, conflicts between employees and administrators in the management of the enterprise or due to third parties.**

## XII. Service of Notice

12.1 All notices from the Company to the User under this Agreement may be made by means of web announcements, e-mail, cell phone text messages or conventional mail transmission; such notices shall be deemed to have been delivered to the recipient on the date of delivery.

12.2 Notices from users to the Company shall be delivered through the Company's officially published mailing address, fax number, e-mail address and other contact information. Such notices shall be served on the date of actual receipt by the Company.

## XIII. Legal Jurisdiction

**The verification, interpretation, modification, performance, and dispute resolution of this Agreement is governed by the laws of the state of California, without regard to conflict of law provisions. You accept that this Agreement will be considered to have been signed in California. In the event of any dispute concerning the content or performance of this Agreement, both parties shall endeavor to resolve the dispute**

**through amicable negotiation. If the dispute cannot be resolve through amicable negotiation, either party may submit the dispute to the people's court with jurisdiction over the location this Agreement was signed for litigation.**

# Personal Information Protection and Privacy Policy

**This Agreement applies only to the Defendas Credentials Management System cloud product or cloud service (hereinafter referred to as: DCMS), including DCMS Cloud Portal, Defendas ID App.**

Lastly updated on: November 2025

If you have any question, comment, or suggestion, please contact us via the following means: Email: info@LTSecurityinc.com

If you are a minor, please consult your guardian, and ask the guardian to accompany you to read and understand the Policy.

**This Policy will help you understand the following:**

- Personal information collection rules
- How we protect your personal information
- Your rights
- How we handle personal information of minors
- How this Policy is updated
- How to contact us

LT Security Inc and its affiliates (hereinafter referred to "LTS" , or "Company" or "We") understand acknowledges the importance of personal data and will do everything possible to protect your personal information. We are committed to preserving your trust in us by protecting your personal information based on the following principles: responsibility in accordance with authority, purpose specification, informed consent, minimal necessary, security safeguard, subject participation, openness and transparency, etc. LTS also commits to protect your personal information by implementing appropriate security measures in accordance with industry accepted security standards.

Before using any products (or services), please read this Policy carefully and make sure you have fully understood and agreed to this Policy. By using any products or services, you acknowledge that you have fully understood and agreed to this Policy.

**Definitions**

1. **DCMS** refers to cloud services developed and operated by the DCMS platform, including personnel credentials and organization authority distribution management services and system management. These services can be deployed in the cloud, including websites, and mobile devices (apps).
2. **DCMS Provider** refers to LTS and local branch offices, local partner, the company that

developed and provides **DCMS** services and hardware devices.

3. **Personal Information** refers to information recorded electronically or otherwise that can be used alone or in combination with other information to identify the identification and activities of a particular natural person. Such information includes name, mobile phone number, email address, employment information (employee number), corporate information (corporate name and business identification number). All the above information is anonymized.

4. **Personal Information Controller** which organization or individual that has the authority to determine the purpose and manner of handling personal information. The personal information controllers referred to in this policy agreement are the owners/administrators of the enterprise/organization of DCMS products.

## I Personal information collection rules

### (1) Which of your personal information will be collected by enterprise/organization owners or LTS

We will collect and use your personal information for the following purposes:

1. To Help You Activate DCMS accounts.

The company's administrator/HR/data protection officer will assist in transferring your personal information (including employee ID, name, email, phone number, department, and position) to the background of DCMS, which will be used to produce electronic vouchers for you, but only employees The job number, name, and email address are required. They are used by DCMS to send you an activation code email and identification in the system. Others are optional.

2. Providing You with DCMS Services.

1) Information to Provide by You

In using our services, you may provide feedback to help us better understand your experience and needs, so as to better improve our surveys.

2) Information We Collect During Your Use of the Service

To provide you with services, pages, and search results that better meet your needs; understand product suitability; and identify any issues with your account, we will collect information about the products and/or services you use, along with how you use them. This information includes:

**DCMS Cloud Portal:** When you use products or services provided by our website or client end, we will automatically collect detailed use information of our services and save them as relevant web logs. For example, your search and query content, IP address, browser type, language used, date and time of visit, and the records of webpages visited. Organization information, personnel information. For example: Organization Name, Employee Name, Employee Email, Employee Credentials.

**Defendas ID App:** When you use Defendas ID App for the first time, in order to prevent your credentials from being maliciously activated or impersonated, Defendas ID App will transmit your mobile phone information to DCMS for registration of mobile phone identity.

In order to provide better technical support, Defendas ID App will collect technical information about the mobile device and application, as well as usage information. After you submit a support request to the technical support team and obtain your permission, these data will be sent to the technical support team and the R&D team. Data sharing, including but not limited to app submission to DCMS.

This information includes:

Technical Information about the Device and Application

Device manufacturer and model

Hardware capabilities, such as Bluetooth and NFC support

Operating system version

Identifier and version information for the app

Device phone serial number

Device MAC

APP Bluetooth connection record

**Separate log information cannot be used to identify particular natural person.**

If we combine such non-personal information with other information to identify a specific natural person, or use this information in combination with personal information, such non-personal information will be treated as personal information during the combined use. We will anonymize and de-identify such personal information unless we obtain your authorization or are otherwise required by laws and regulations.

When you contact us, we may save your communication or call records, content, or contact information to better help you solve the problem, contact you in the future, or to help us solve related problems.

3. Security

To prevent, detect, and investigate fraud, infringement, breach of security, unlawfulness, or violations of agreements, policies, or rules with us and/or our partners, we may collect or integrate your user information, service usage information, device information, log information, and information that we and/or our partners have obtained your authorization to share or that is shared under the law.

If we cease to operate DCMS Cloud services, we will promptly cease the continued collection of information about you and your employees and will delete or anonymize your personal information in our possession.

### (2) How we use your personal information

Your information is collected to provide you with services, and to improve the quality of those services. To this end, we will use your information for the following purposes:

1. To provide you with DCMS cloud product or cloud services, and to maintain, improve, and optimize these services and your user experience.
2. To prevent, discover, and investigate fraud, infringement, acts endangering security, violations of laws and our agreements, policies, or rules, and to protect you, other users, or the public, along with us and our legitimate rights and interests, we may use or integrate your user information, service use information, device information, log information and information that was obtained by us, our partners, or shared under the law to comprehensively determine risks of your account and transactions, verify identities, detect and prevent security incidents, and take the necessary recording, auditing, analyzing, and disposing measures according to relevant laws.
3. We may process your information or combine it with information from other services for the purpose of providing you with a more personalized service, such as to recommend content that may be of interest to you, including but not limited to sending you information about DCMS cloud services, presenting you with personalized third-party promotions through the system, or sharing information with DCMS partners with your consent so that they may send you information about their products and services.
4. If you do not provide this information, it will not affect your use basic function of the products and services.

### (3) How we use Cookies

1. Cookies

Cookies and similar technologies are widely used in the Internet. To ensure the smooth operation of our website, we will store a small data file named Cookie in your computer or mobile device. A Cookie typically contains identifiers, site names, and some numbers and characters. With the Cookie, our website can store your preference and other data. We will not use Cookies for any other purpose than that specified in this Policy. You may manage the Cookie according to your own preference or delete it. You may choose to delete all Cookies saved in your computer, and most of the web browsers have a feature to block the Cookies. But if you do this, you will need to change the user settings each time you visit our website.

### (4) How we share, transfer, and disclose your personal information

**1. Share**

Without your explicit consent prior, we will not share your personal information with any other company, organization and individual.

We may share your personal information with an external institution if required by laws and regulations or government authorities.

**2. Transfer**

We will not transfer your personal information to any other third-party company, organization or individual, except under the following circumstances:

a) Transfer with your explicit consent: with your explicit consent, we will transfer your personal information to other parties;

b) If any merger, acquisition or bankruptcy process involves transfer of your personal information, we will request the new company or organization in possession of your personal information to continue to be bound by the personal information protection policy, or we will request the new company or organization to seek your permission again.

**3. Public disclosure**

We will only disclose your personal information in the following circumstances:

a) With your explicit consent;

b) Permitted by Applicable Law: we may disclose your personal information in cases where such disclosure is required by laws, legal proceedings, litigation, or government authorities, including in cases:

- **Related to personal information controller’s performance of obligations prescribed by laws and regulations;**
- **Directly related to national security or national defense security;**
- **Directly related to public safety, public health or vital public interests;**
- **Directly related to crime investigation, prosecution, trial and judgment execution;**
- **Where such disclosure is necessary for protecting the vital legitimate interests such as life and property of the subject of personal information or any other individual while it is difficult to obtain the consent therefrom;**
- **Where the personal information involved is disclosed to the public by the subject itself;**
- **Where such disclosure is necessary for signing and performing the contract concerned according to the requirements of the subject of personal information;**
- **Where the personal information is collected from legally and publicly disclosed information, such as legal news reports and publicized government information;**
- **Where such disclosure is necessary for maintaining safe and stable operation of the products/services provided, such as identification or disposal of failures of products/services;**
- **Where the personal information controller is a news agency and such disclosure is necessary for legal news reporting;**
- **Where the personal information controller is an academic research institute, and such disclosure is necessary for statistics or academic research in the public interest, and the personal information contained in the results of academic research or description provided externally is de-identified.**

**Please note that according to law, sharing, transferring, or disclosing personal**

**information does not include the scenario in which personal information is de-identified in such a way that the recipient of such information cannot restore the information or re-identify the subject of personal information before it is shared, transferred, or disclosed. As a result, we may store or process such information without notifying you or obtaining your consent.**

**II How we protect your personal information**

(1) We take the security of personal data seriously. We use appropriate physical, managerial and technical safeguards to protect your personal data from unauthorized access, disclosure, use, modification, damage or loss. For example, we use encryption technology to ensure the confidentiality of data; we use protection mechanisms to prevent malicious attacks on data; we deploy access control mechanisms to ensure that only authorized personnel have access to personal data; and we conduct security and privacy training courses to enhance employee awareness of the importance of protecting personal data. We will do our best to protect your personal data, but please note that no security measure can be foolproof.

(2) We will retain your personal data for as long as necessary to achieve the purposes described in this policy, unless we are required or permitted by law to extend the retention period or are permitted by law to do so. Because the period of data storage may vary based on different scenarios and products and services, the criteria we use to determine the retention period include: the period of time required to retain personal data to fulfill the business purpose, including providing products and services, maintaining corresponding transaction and business records, controlling and improving the performance and quality of products and services, ensuring the security of systems, products and services, responding to possible user inquiries or complaints, problem location, etc.; whether the user agrees to a longer retention period; whether there are special requirements for data retention by law, contract, etc. We will retain your registration information for as long as your account is necessary to provide the service to you. You can also choose to cancel your account, after you cancel your account, we will stop providing products and services based on that account and delete your corresponding personal data without special legal requirements.

(3) After the unfortunate occurrence of a personal information security incident, we will inform you in accordance with the requirements of laws and regulations (no later than within 30 natural days): the basic situation of the security incident and the possible impact, the disposal measures we have taken or will take, the suggestions you can independently prevent and reduce the risk, the remedial measures for you, etc. We will inform you by email, letter, telephone, push notification, etc. When it is difficult to inform the subject of personal information one by one, we will take a reasonable and effective way to publish the announcement. At the same time, we will also report the disposition of personal information security incidents in accordance with the requirements of regulatory authorities.

(4) The Internet environment is not 100% secure, and although we have these security measures in place, please note that there are no "perfect security measures" on the Internet, and we will do our best to ensure the security of your information.

(5) To ensure a smooth browsing experience, you may receive content or web links from third parties external to us and our partners ("Third Parties"). We have no control over such third parties. You may choose whether to access links, content, products and services provided by third parties. We have no control over the privacy and data protection policies of third parties, and such third parties are not bound by this Policy. Before submitting personal information to a third party, please refer to that third party's privacy policy.

### III Your rights

In accordance with of the state of Georgia laws, regulations, standards, and established practices of other countries and jurisdictions, we will protect your rights to:

**(1) Access your personal information**

You have the right to access your personal information, unless otherwise provided by laws and regulations. You may access your personal information by contacting: **Your enterprise/organization administrator**

For other personal information generated during your use of our products or services, if you want to exercise your right to access your personal data, please send an email to **your enterprise/organization administrator**

**(2) Correct your personal information**

Upon noticing any of your personal information we processed is wrong, you have the right to request us to make corrections. You may submit the request via means listed in Item "(1) Access your personal information".

**(3) Delete your personal information**

In the following cases, you may request your enterprise/organization to delete your personal information:

1. The enterprise/organization process your personal information in violation of laws and regulations;
2. The enterprise/organization collect or use your personal information without your consent;
3. The enterprise/organization process personal information in violation of the agreement with you;
4. You can no longer use our products or services, or you want to canceled your account;

We do not make any changes to enterprise/organization information and are only in charge of secure storage and secure deletion. When your enterprise/organization deletes your information, the system will automatically and permanently delete your personal information.

In circumstances prescribed by applicable laws, you have the right to revoke your consent to your enterprise/organization processing of your personal data at any time.

However, the cancellation will have no bearing on the legality and effectiveness of your personal data that your enterprise/organization previously processed with your consent, or other appropriate legitimacy.

When you have legal incident or disputes with enterprises/organizations, you can contact us to provide the relevant legal proof. The appropriate application and description of the incident must be provided beforehand, and we will review and determine whether to provide the relevant information and request documents with legal basis, such as your national public and security department's inquiry requirements.

**(4) Respond to your request**

To safeguard security, you may need to provide a request in writing or otherwise prove your identity. We may ask you to provide proof of your identity before processing your request.

We may not respond to your request in the following circumstances:

1. The request is related to personal information controller’s performance of obligations prescribed by laws and regulations;
2. The request is directly related to national security or national defense security;
3. The request is directly related to public safety, public health or vital public interests;
4. The request is directly related to crime investigation, prosecution, trial and judgment execution;
5. The personal information controller has sufficient evidence that the subject of personal information is subjectively malicious or abusing his/her rights;
6. Not responding to the request is for protecting the vital legitimate interests such as life and property of the subject of personal information or any other individual, while it is difficult to obtain the consent therefrom;
7. Responding to request of the subject of personal information will bring serious damage to the legitimate rights and interests of the subject or any other individual or organization;
8. The request involves trade secrets.

## IV How we handle personal information of minors

DCMS is designed to be used by companies, whose managers should comply with local anti-law regulations that prohibit the employment 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.

## V How this Policy is updated

Our personal information protection and privacy policy is subject to change from time to time. We will update this document and request your agreement for new feature additions if they are related to privacy.

Without your explicit consent, we will not cut your rights you are entitled to under this Policy. We will post any change to this Policy on our website.

For major changes, we will also provide a more prominent notification (for some services, we will send notice via email, stating the particulars of changes to this Policy).

Major changes referred to in this Policy include, but are not limited to:

1. Major changes of our service model, such as change of purpose, type or way of use of personal information;
2. Major changes in ownership structure or organizational structure, such as changes caused by business adjustment, bankruptcy, merger and acquisition;
3. Change of the party with which we share personal information or to which we transfer or disclose personal information;
4. Major changes in your rights of participating in the handling of personal information or the way you exercise such rights;
5. Changes of the department responsible for personal information security, or of the contact information or of the channel for filing a complaint;

We will also archive the previous versions of this Policy for your reference.

DEFENDAS

LT Security Inc.　https://ltsecurityinc.com　E-mail:info@LTSecurityinc.com