

User Manual

ARMATURA ID App

Copyright © 2022 ARMATURA LLC. All rights reserved.

Without the prior written consent of ARMATURA LLC, no portion of this manual can be copied or forwarded in any way or form. All parts of this manual belong to ARMATURA LLC and its subsidiaries (hereinafter the "Company" or "Armatura").

Trademark

ARMATURA is a registered trademark of ARMATURA LLC. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

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

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 Armatura 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.

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

Armatura 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.

Armatura 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 Armatura has been advised of the possibility of such damages.

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

Armatura 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 <http://www.armatura.us>.

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

Armatura LLC. Co., Ltd.

Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005 USA

Phone: +1-650-4556863

For business related queries, please write to us at: sales@armatura.us.

To know more about our global branches, visit www.armatura.us.

About the Manual

This manual introduces the operations of **ARMATURA ID App**.

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

Table of Contents

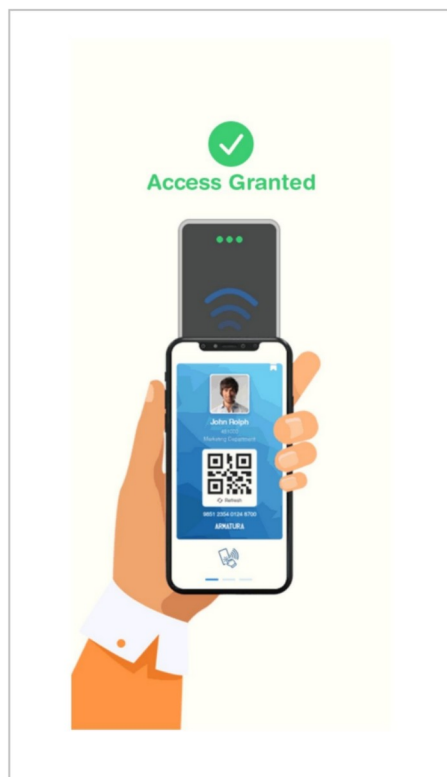
1 Overview	1
2 Connecting to App	2
2.1 Download the ARMATURA ID App	2
2.2 Installation of the ARMATURA ID App	2
2.2.1 Installing the App on an Android Device	2
2.2.2 Installing the App on an iOS Device	3
2.3 Activate the Credentials	4
2.3.1 Click the Activation Link to Activate	5
2.3.2 Enter the Activation Code to Activate	5
2.3.3 Scan the QR Code to Activate	6
3 Operation Instructions of the App	7
3.1 Important Information	7
3.2 Main Menu	8
3.3 Credentials	9
3.3.1 View the Mobile Credentials	9
3.3.2 Add and Activate the Mobile Credentials	10
3.3.3 Delete the Mobile Credentials	11
3.3.4 Use of the Mobile Credentials	12
3.4 License Agreement	14
3.5 Privacy Policy	14
3.6 Parameters Settings	15
3.7 Quick Guide	16
3.8 Other Shortcuts Settings	17
3.8.1 Set as widget	17
3.8.2 Show notifications	18
4 Cautions When Using	20
5 Appendix	21
Enduser License Agreement (EULA)	21
Personal Information Protection and Privacy Policy	27

1 Overview

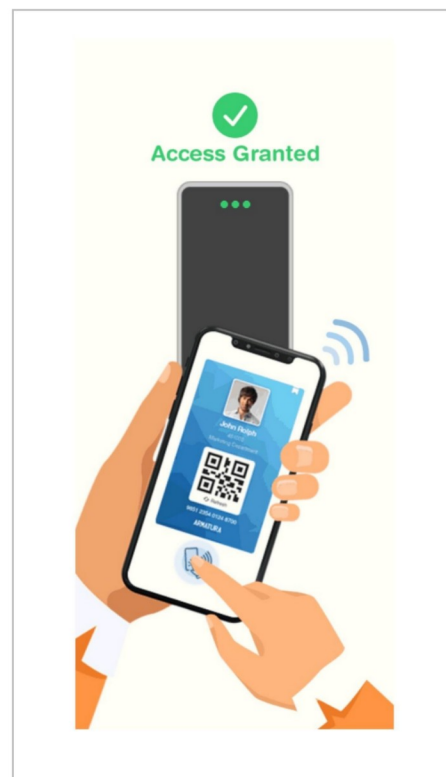
ARMATURA ID allows end users to use their mobile devices (smartphones) to securely and conveniently enter the workplace by extending access control capabilities to smart devices.

When the user approaches the reader, the following interaction modes can be performed through their mobile device to access:

- **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.



Card Mode



Remote Mode

Note:

- *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).*
-

2 *Connecting to App*

2.1 Download the ARMATURA ID App

Ensure the mobile device is connected to the internet (either via mobile data network or Wi-Fi) during device registration and Mobile ID delivery. Both Android and iOS versions are available, please download the APP according to the following instructions.

1. Search for the ARMATURA 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.

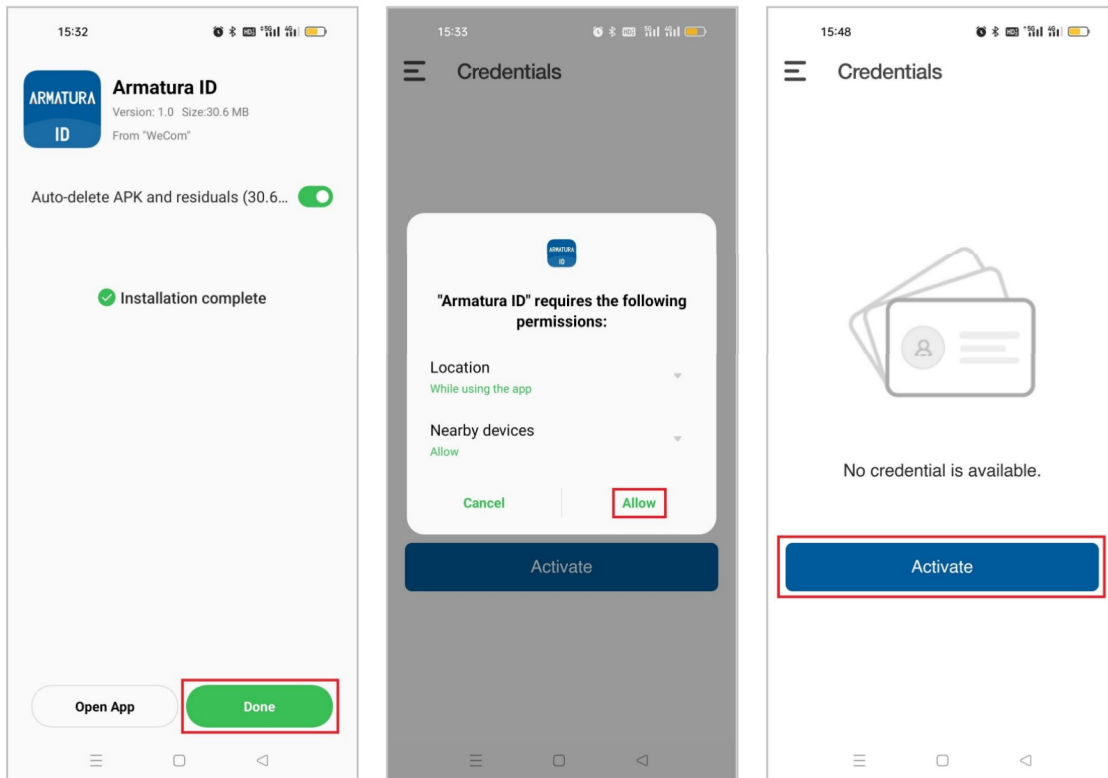


2. You can also download the App by clicking on the store icons in the activation code email sent by the server mailbox Armatura Credential Management System.

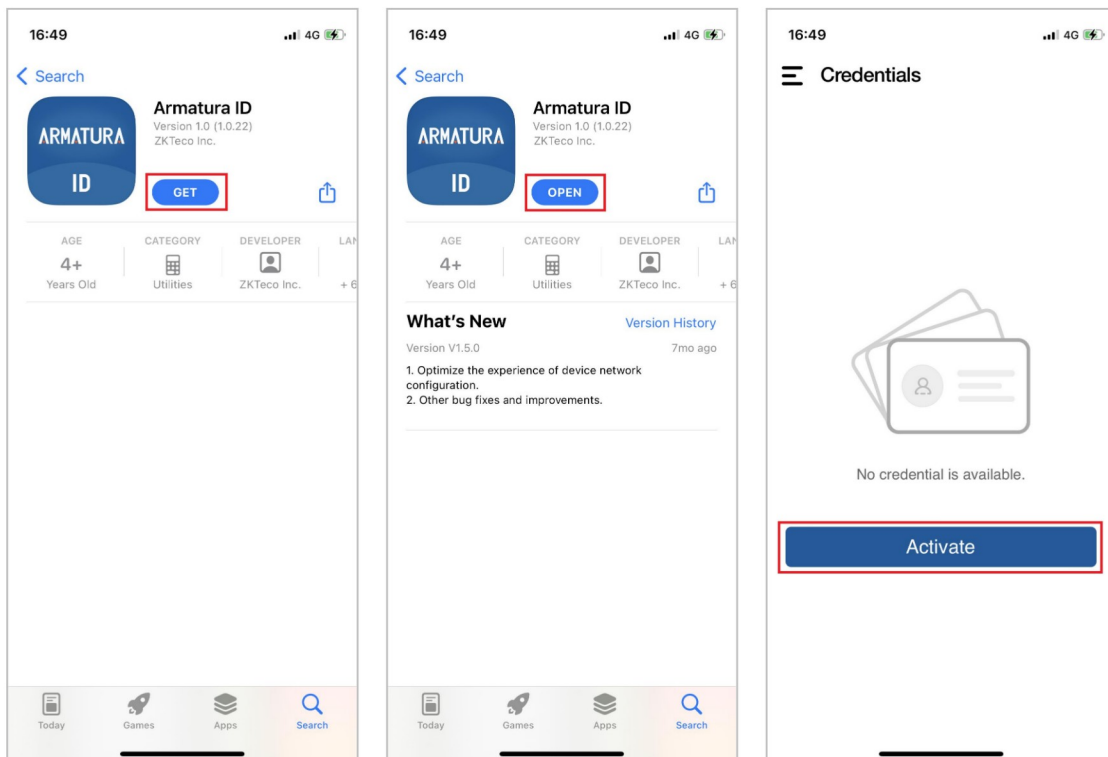
2.2 Installation of the ARMATURA ID App

2.2.1 Installing the App on an Android Device

1. After the download is complete, follow the prompts to install the App. The interface is shown in the figure below.
2. At present, the language of the App is synchronized with the system language of the mobile phone, that is, it can be changed by modifying the mobile phone language.



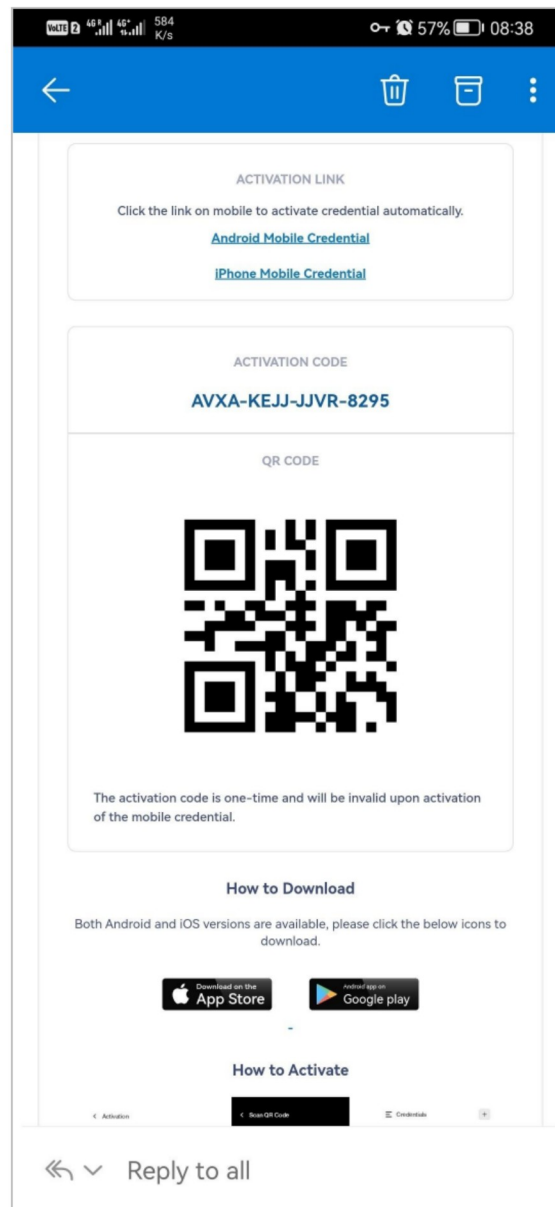
2.2.2 Installing the App on an iOS Device



2.3 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 Armatura Credential Management System. It is sent by the site administrator of your company via ACMS.



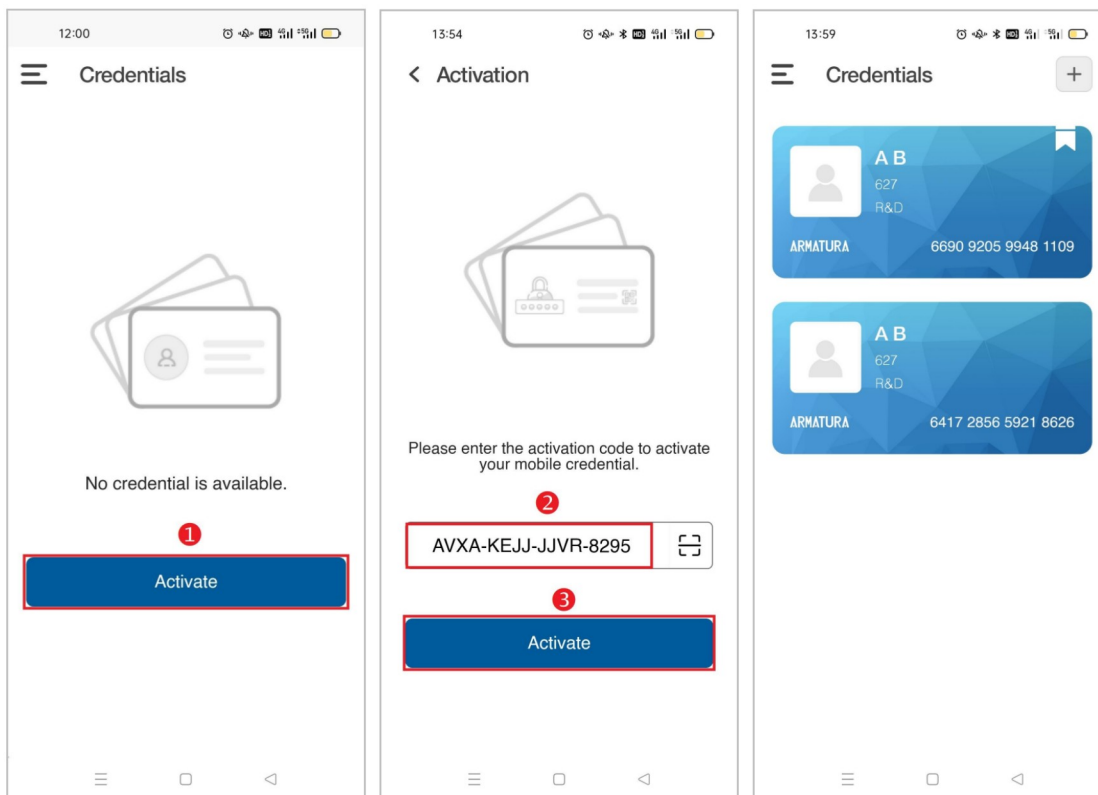
2.3.1 Click the Activation Link to Activate

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



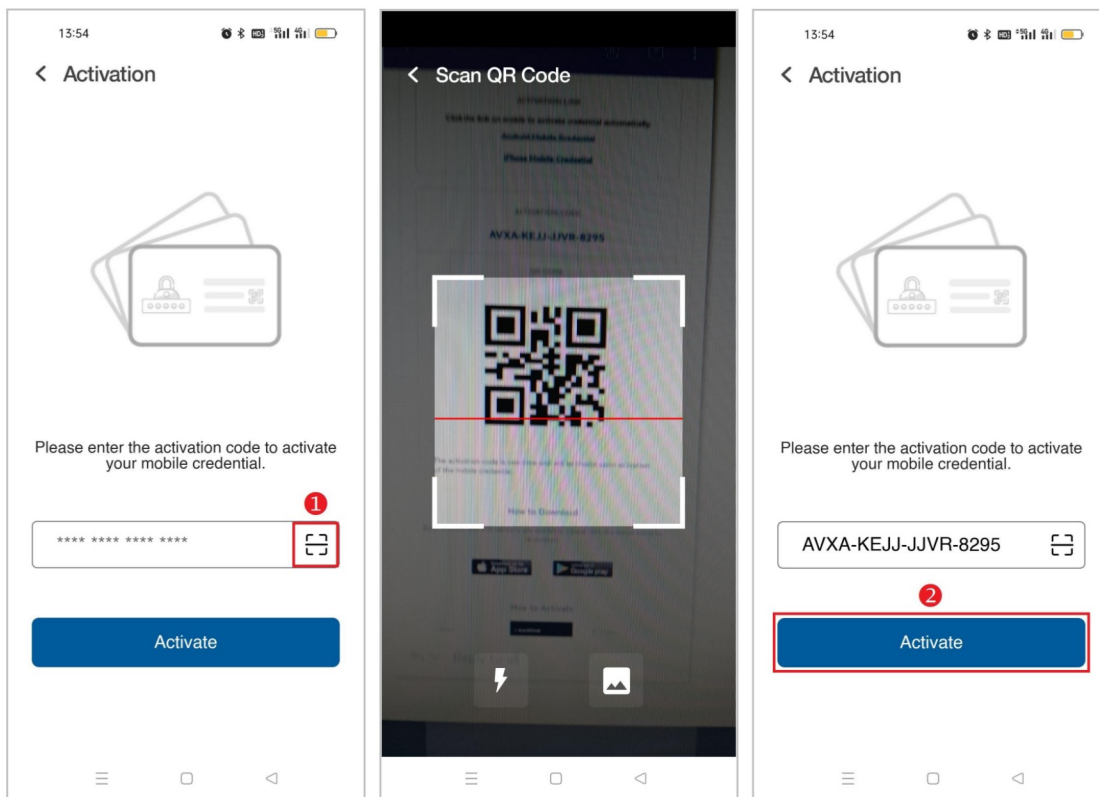
2.3.2 Enter the Activation Code to Activate

1. Open the ARMATURA 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.



2.3.3 Scan the QR Code to Activate

1. Open the ARMATURA 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.



Note:

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

3 *Operation Instructions of the App*

3.1 Important Information

- ARMATURA ID lets you use the Bluetooth® Low Energy technology in your Android device to gain access to secure areas on your site and interact with your building systems. Requires an authorized access credential. Background operation also needs to enable the Location and related permissions.
- Push Notifications allow you to receive instant updates about important events.
- **Usage tips:**

Battery Optimisation: Some phones will shut down the ARMATURA ID App for Battery Optimisation. If you wish to use background access, we recommend disabling optimisation for the ARMATURA ID App. Battery Optimisation is found under your mobile phone Settings.

- **BLE:** Bluetooth® Low Energy (BLE) while less reliable and slower than NFC, it has range advantages. NFC's range is centimeters, BLE can be configured to up to 328ft (100m) (the Explorer Series Outdoor Multi-tech Smart readers configuration).

***Note:** When using the scan function to activate the certificate, the Bluetooth function of the mobile phone requires to be turned on, and the relevant permissions of the camera should be used.*

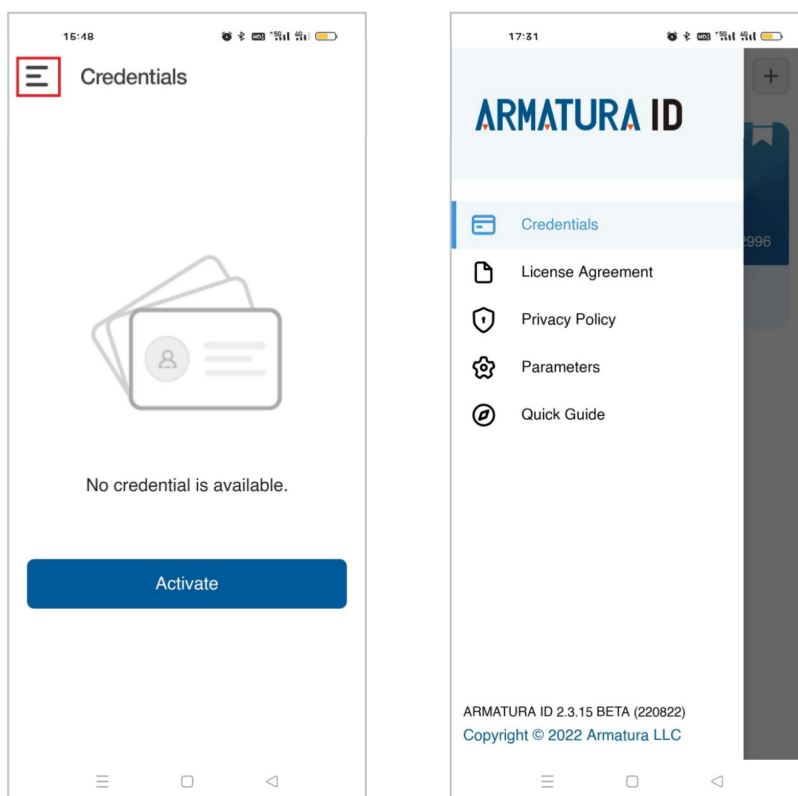
- **NFC:** Near Field Communication (NFC) uses a lot less battery and is generally faster and more reliable than Bluetooth, however it is still affected by Battery Optimisation. If you do use NFC, we recommend changing Bluetooth Background Access to 'No Background Bluetooth'.

***Note:** Only some Explorer Series Outdoor Multi-tech Smart readers support NFC function, and the actual product purchased shall prevail. The NFC function of mobile phones must be only available on mobile phones with NFC chips. If you want to use the NFC function, the above two conditions must be supported.*

- **Note:** Bluetooth® Low Energy uses Location to discover the Explorer Series readers. You can switch off Bluetooth and Location and use NFC for Access, however NFC will need to be enabled on the Explorer Series readers.
- Bluetooth® Background scanning can be disabled on the settings screen.

3.2 Main Menu

Open the ARMATURA ID App and click  to access the menu options, as shown in the figure below.



Function Description:

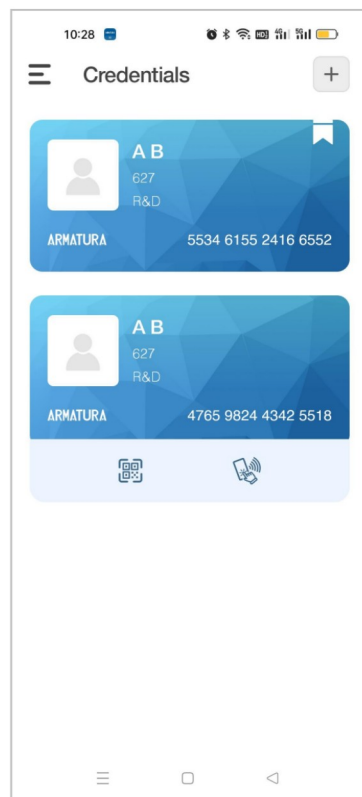
Menu	Descriptions
Credentials	Displays all cards that the user has activated. Here the user can select the desired card or activate a new one.
License Agreement	To display the end user's license agreement. See the 5 Appendix for details.
Privacy Policy	To display the content of the privacy policy. See the 5 Appendix for details.
Parameters	To set the relevant parameters of Run Mode, BLE, NFC and Style of mobile credential display.
Quick Guide	To display how the card mode and remote mode operate.

3.3 Credentials

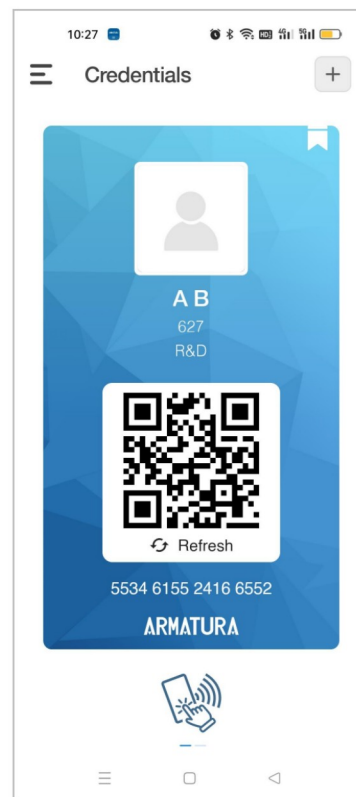
This feature enables end users to view, add and activate their mobile credentials and how to use them.

3.3.1 View the Mobile Credentials

Click **Credentials** on the **Main Menu** screen to enter the credentials list interface. All activated cards are listed here. There are two display styles, as shown below.



Card Style



Tiled Style

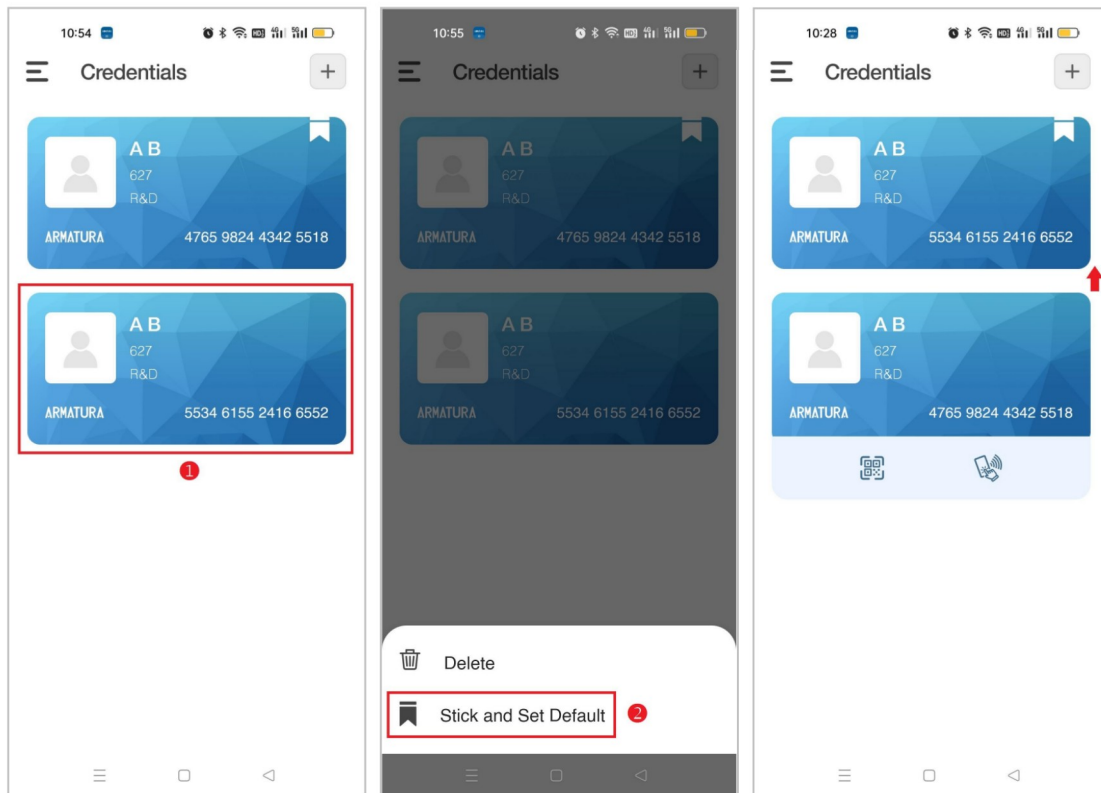
Note:

- Touch the card in the card style, and the function bar will pop up, as shown above.
 - The tiled style interface displays only one card, and you can switch cards by swiping left and right.
 - Click **Parameters - Style** on the main menu to modify the display style.
-

Stick and Set Default

When the end user has a lot of cards, the following methods can be used to put the commonly used card at the top, so that it can be found more quickly.

Under Card Style, select and long-press a card, and select **Stick and Set Default** from the pop-up menu to pin the card to the top, as shown below.



In the Tiled Style, the operation method is the same, and will not be repeated here.

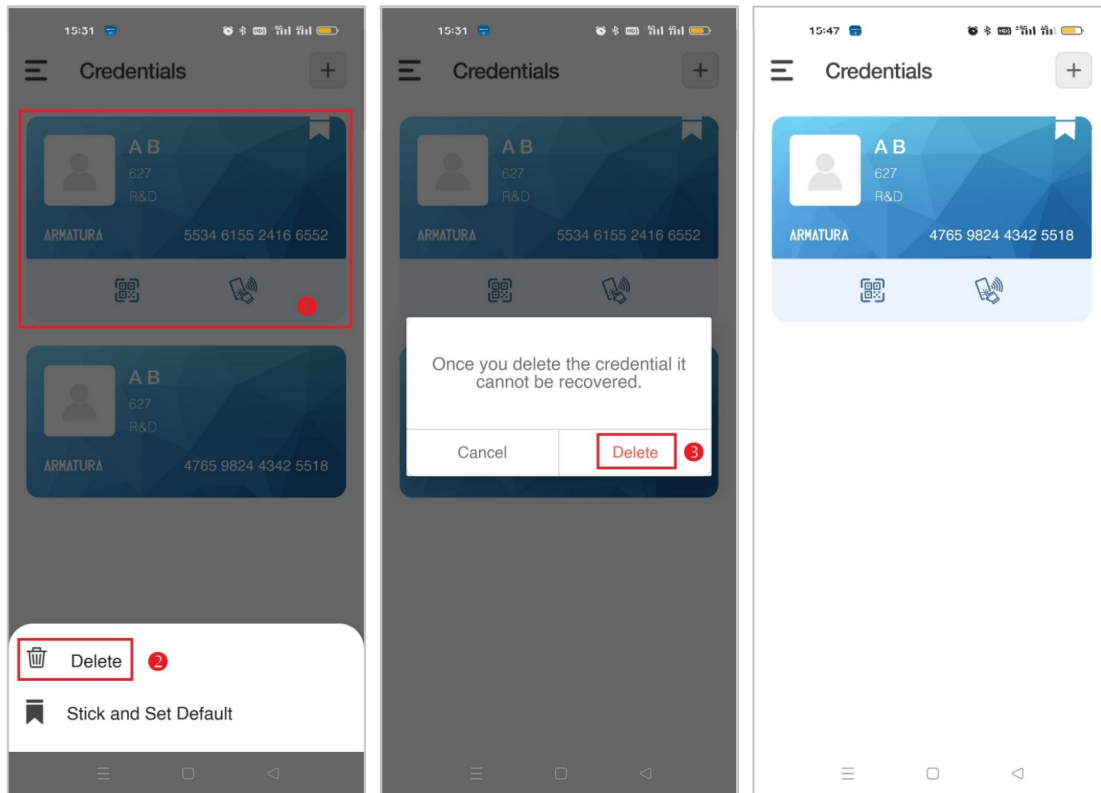
3.3.2 Add and Activate the Mobile Credentials

If the end user needs to add multiple cards, the following can be done.

Click **Credentials** in the **Main Menu** to enter the Credentials interface. Click  in the upper right corner to add a new mobile credential, refer to [2.3 Activate the Credentials](#) for the specific operation method.

3.3.3 Delete the Mobile Credentials

The end users can delete all activated cards. **However, once the card is deleted, it cannot be recovered, so please operate with caution.**



- 1) Select and long press the card you want to delete, and then select **Delete** from the pop-up options.
- 2) Click **Delete** in the pop-up confirmation window to confirm and delete the card.

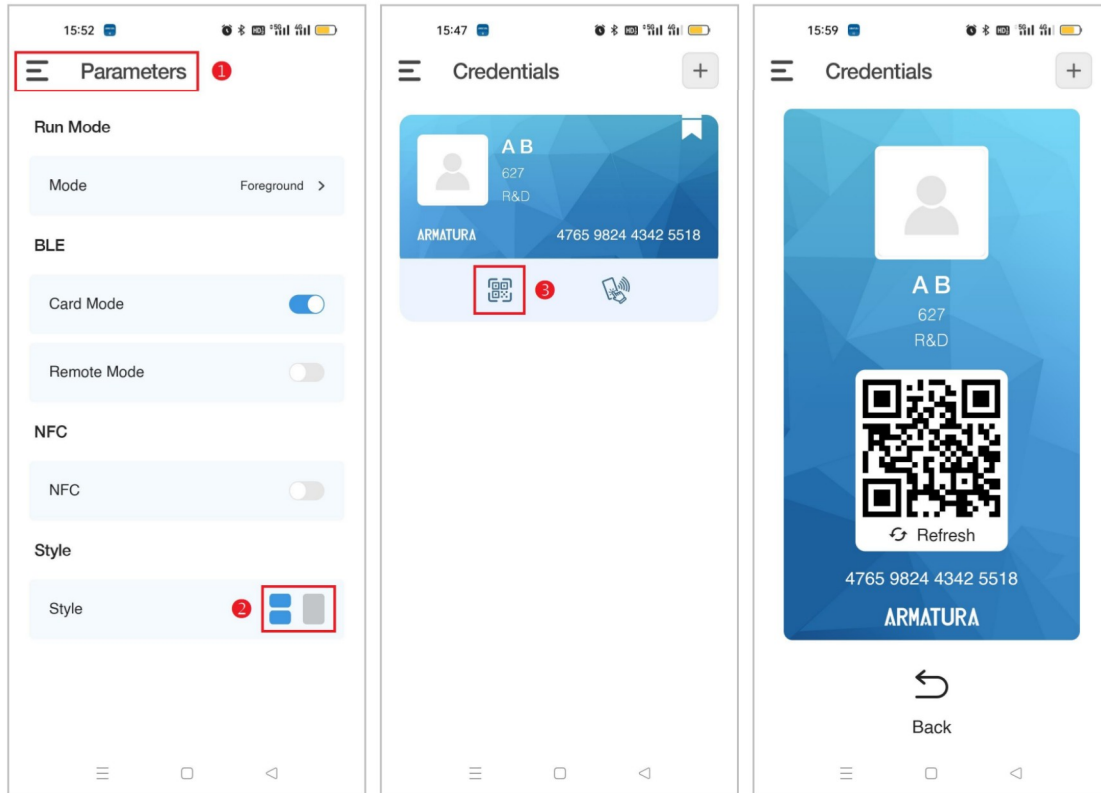
Note:

- Be very careful when deleting, once the credential is deleted, it cannot be recovered.
 - If you delete the card by mistake, you can only contact the administrator to re-issue the card, which is likely to be a new card.
-

3.3.4 Use of the Mobile Credentials

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

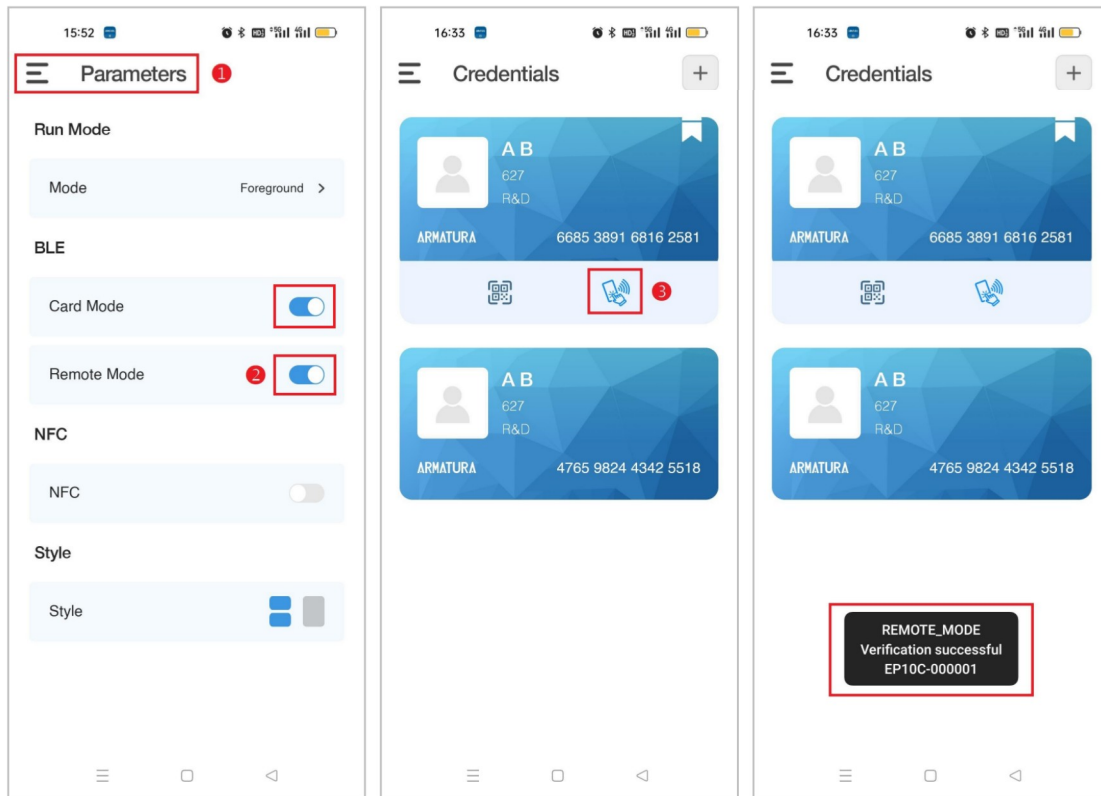
1. Swipe the card through QR code



- 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 reader to open the door.
- 4) Click  to return to the previous interface.

2. Swipe the card through Bluetooth

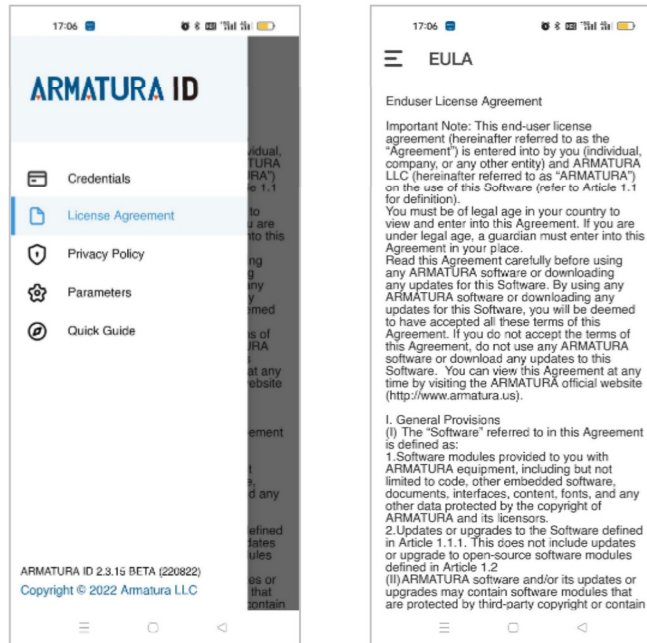
Card mode functions requires the end user to hold the mobile device close to the card reader to swipe the card. Remote mode functions like a remote control. With the remote mode, you don't need to swipe the card on the reader, just get close to the reader within the effective range.



- 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.

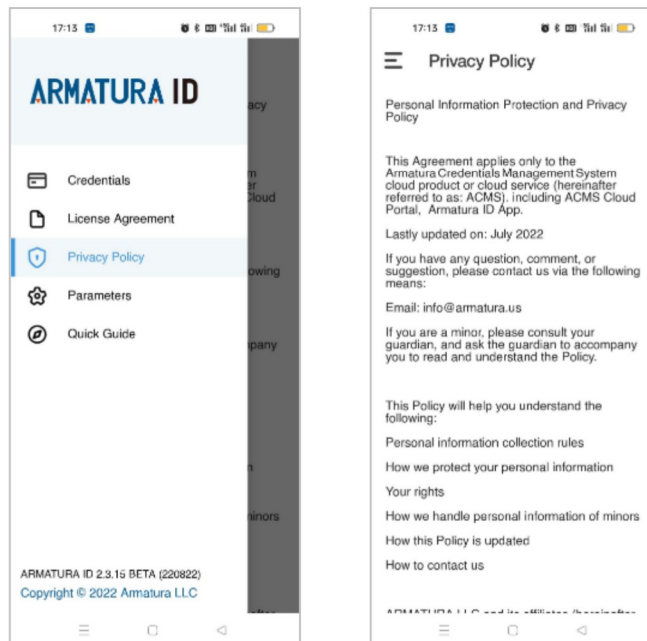
3.4 License Agreement

Click **License Agreement** on the **Main Menu** screen to view the end user's license agreement.



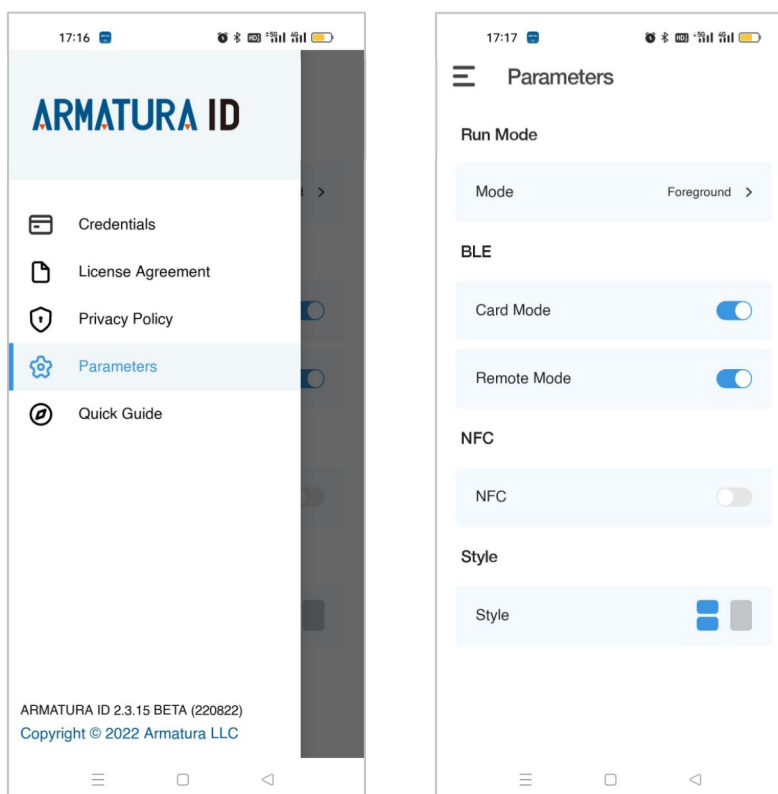
3.5 Privacy Policy

Click **Privacy Policy** on the **Main Menu** screen to view the contents of the privacy policy.



3.6 Parameters Settings

This feature enables end users to set the relevant parameters of run mode, BLE, NFC and style of mobile credential display.



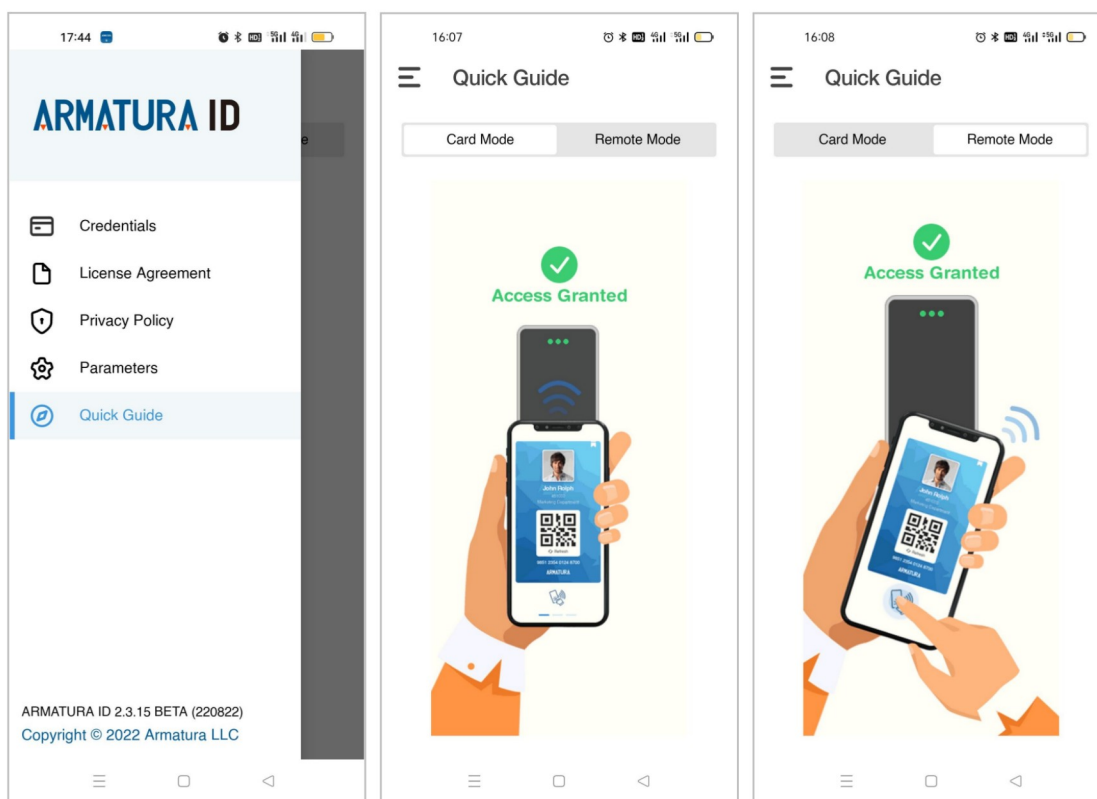
Function Description:

Menu	Descriptions
Run Mode	Used to set the run mode of the App. Including Foreground Mode and Background Mode. Foreground: Credential service only runs while the app is open. Background: Credential service continues to run when app is in the background.
BLE	Card Mode: Enable/disable the feature, similar to the user experience with physical credentials. The end user's mobile device is required to be very close to the reader. <i>The effective distance is 0 to 20 inches (0 to 50 centimeters).</i> Remote Mode: Enable/disable the feature, allows end users to use mobile devices to perform remote control within the set range. <i>The effective distance is 0 to 394 inches (0 to 1000 centimeters).</i>

NFC	Enable/disable the feature, swipe card through NFC communication. Only some Explorer Series Outdoor Multi-tech Smart readers support NFC function, and the actual product purchased shall prevail. The NFC function of mobile phones must be only available on mobile phones with NFC chips. If you want to use the NFC function, the above two conditions must be supported.
Style	Display styles for mobile credentials, including Card Style and Tiled Style.

3.7 Quick Guide

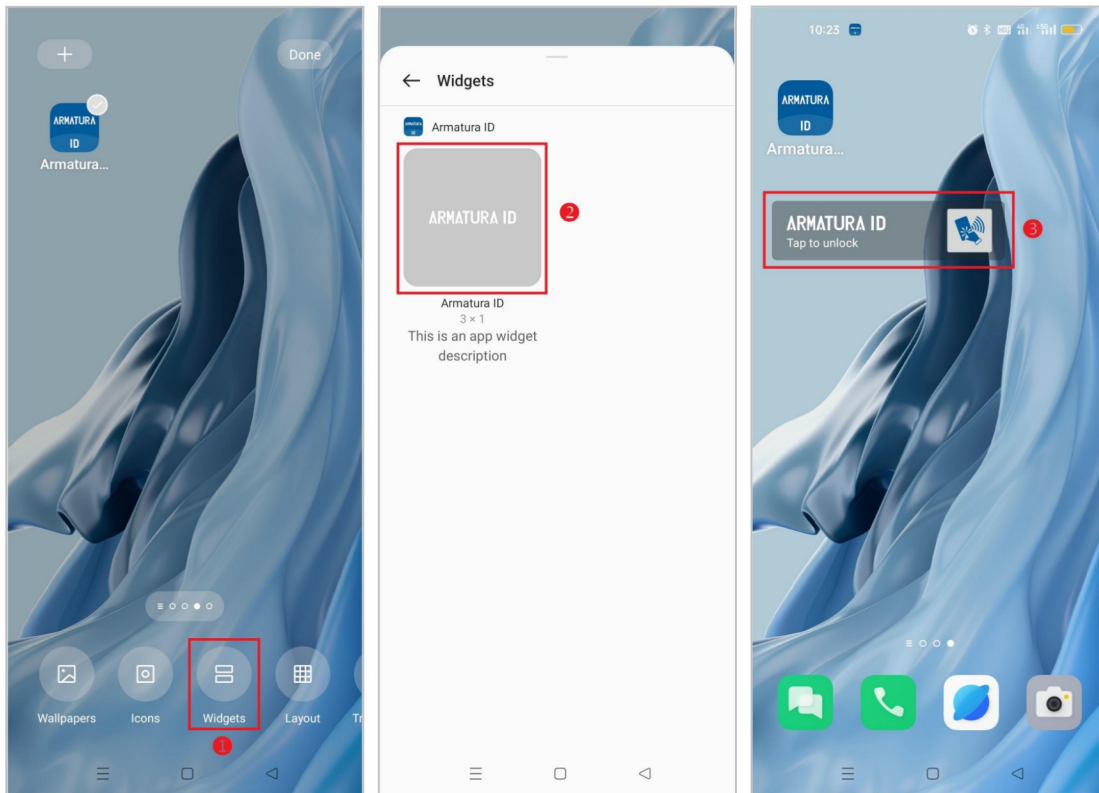
A quick guide video tutorial on how to use card mode and remote mode.



3.8 Other Shortcuts Settings

3.8.1 Set as widget

The ARMATURA ID App can be set as a widget on the mobile phone desktop, which is equivalent to a small remote control, making it more convenient for you to operate.

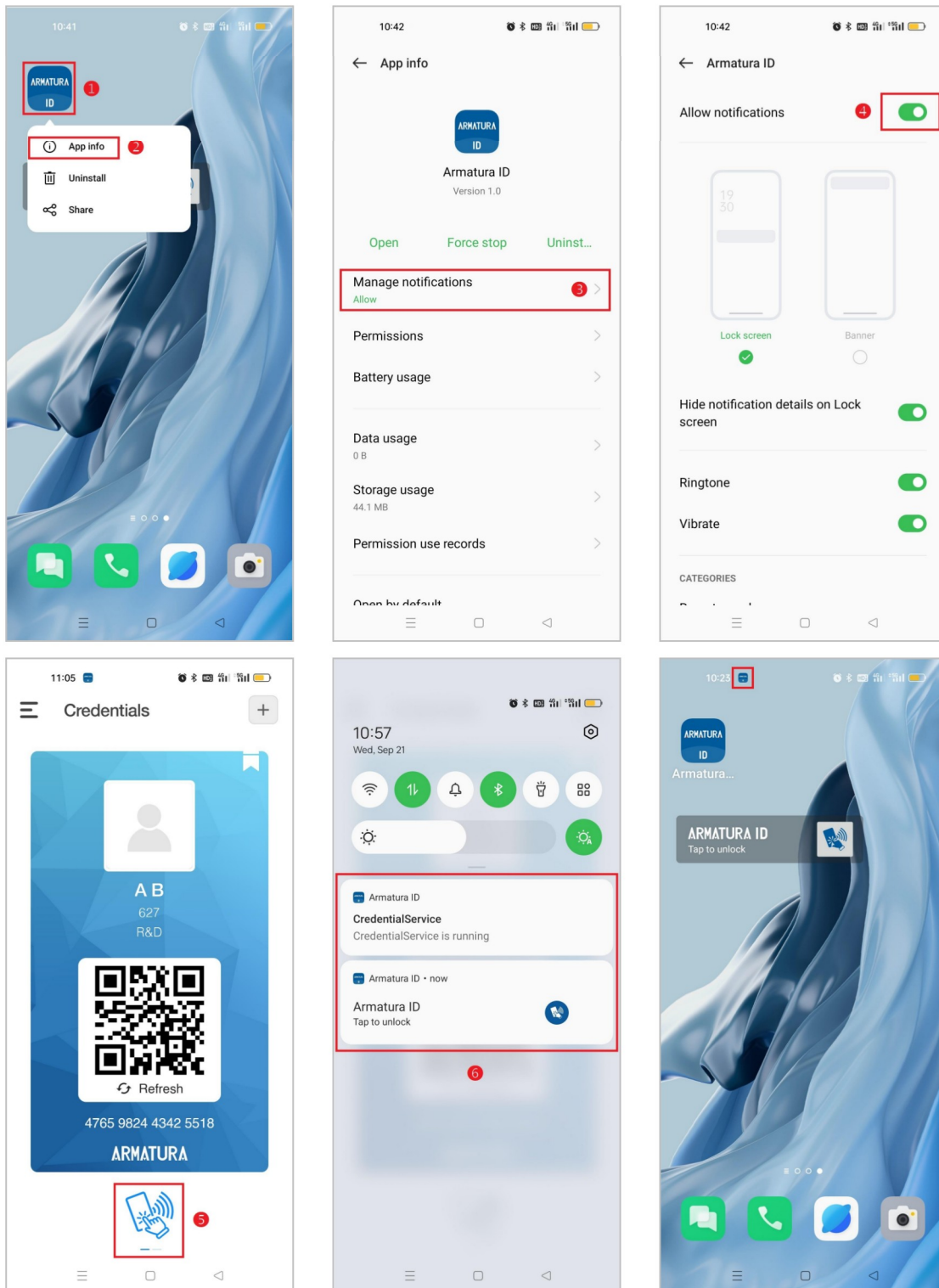


- 1) Call up the **Widgets** operation icon on the home screen of the mobile phone, as shown in the figure above.
- 2) Click  to enter the widgets setting interface. Find the ARMATURA ID icon and click it, then click **Done** to confirm setting it as a widget.
- 3) After completion, the ARMATURA ID's widget will be displayed on the home screen, as shown in the figure above.
- 4) You can click the widget to achieve quick unlock.

Note: The operations here are for reference only, and the specific details are based on the user's mobile phone.

3.8.2 Show notifications

Users can enable notifications and view *ARMATURA ID*'s instant notification information.



- 1) *Long press the ARMATURA ID icon on the home screen.*
- 2) *Select **App info** in the pop-up menu.*
- 3) *Select **Manage Notifications** on the App info setting interface to enable **Allow notifications**.*
- 4) *After the setting is completed, when you open the App to operate, the notification bar will display the ARMATURA ID icon, drag it down to view the instant notification, as shown in the figure above.*

4 *Cautions When Using*

When you want to delete a mobile credential, please note that once deleted, it cannot be recovered. You will need to contact the administrator to reissue, possibly a new card. Please proceed with caution.

Mobile credentials cannot be transferred to a new or different mobile device. If you change your mobile phone, please contact your administrator to report the lost card and resend the card on the ACMS.

Note: This enhances the security of the mobile credentials.

Mobile credentials are preserved if the ARMATURA ID App or the device Operating System is upgraded.

If your mobile device is lost or stolen, this should be treated as a lost or stolen access credential. Notify your security administrator immediately.

5 Appendix

Enduser License Agreement (EULA)

Important Note:

This end-user license agreement (hereinafter referred to as the “Agreement”) is entered into by you (individual, company, or any other entity) and ARMATURA LLC (hereinafter referred to as “ARMATURA”) on the use of this Software (refer to Article 1.1 for definition).

You must be of legal age in your country to view and enter into this Agreement. If you are under legal age, a guardian must enter into this Agreement in your place.

Read this Agreement carefully before using any ARMATURA software or downloading any updates for this Software. By using any ARMATURA software or downloading any updates for this Software, you will be deemed to have accepted all these terms of this Agreement. If you do not accept the terms of this Agreement, do not use any ARMATURA software or download any updates to this Software. You can view this Agreement at any time by visiting the ARMATURA official website (<http://www.armatura.us>).

I General Provisions

1. The “Software” referred to in this Agreement is defined as:
 - 1) Software modules provided to you with ARMATURA equipment, including but not limited to code, other embedded software, documents, interfaces, content, fonts, and any other data protected by the copyright of ARMATURA and its licensors.
 - 2) Updates or upgrades to the Software defined in Article 1.1.1. This does not include updates or upgrade to open-source software modules defined in Article 1.2
2. ARMATURA software and/or its updates or upgrades may contain software modules that are protected by third-party copyright or contain open-source licenses (hereinafter referred to as “open-source software modules”). These open-source software modules are indicated by the Software’s license information, which displays the license applicable to each module. When using these open-source software modules, you will be subject to the terms and conditions of their individual licenses. This Agreement does not affect any of your rights and obligations under such licenses. If there is any conflict between the licensing provisions outlined in this Agreement with an open-source software module license, the open-source license will prevail.
3. Unless otherwise specified, the defined Software is bound to the terms of this Agreement, regardless of whether it is stored in read-only memory, any other media, any other form, or in an online location authorized by ARMATURA.

II End-User License

Subject to the terms and conditions of this Agreement, you have the right to use this Software in a limited, non-exclusive manner (as defined in Article 1.1). This Software may not be sold, transferred, or used for any other commercial purpose.

III Specific Use Restrictions

1. Without the express consent of ARMATURA, you may not use its technology or intellectual property to develop software or design, develop, manufacture, sell, or grant licenses for third-party software/accessories associated with ARMATURA software.
2. You may not distribute or provide this Software to third-parties over a network available to multiple devices or clients at the same time.
3. Without the written consent of ARMATURA, you may not sell, rent, lease, lend, sublicense, or distribute this Software in full or part to any third-party. However, you may permanently transfer the license to this Software in full, along with the associated ARMATURA equipment, provided that:
 - 1) The transfer must include the ARMATURA equipment and all associated ARMATURA software.
 - 2) You may not store any backups of any ARMATURA software, in full or in part.
 - 3) The party receiving the ARMATURA equipment and software has read and accepted all the terms and conditions of this Agreement.
4. Unless expressly permitted, you shall not and shall not allow any other party to copy, reverse engineer, decompile, disassemble, or create derivatives of the Software. You shall not and shall not allow any other party to export the source code from, decode, or modify this Software; any service provided by this Software; or any part thereof.
5. You agree not to use this Software and its related updates to engage in the following actions:
 - 1) Copy or use any part of this Software outside the scope of this Agreement.
 - 2) Provision of this Software to any third-party in full or in part (including but not limited to the applications, services, code, and source code contained within this service) without the written consent of ARMATURA.
 - 3) Use of this Software in a deceptive manner or for deceptive purposes.
 - 4) Deletion of any copyright notices or prompts contained within this Software.
 - 5) Attempts to destroy, bypass, modify, invalidate, or evade any digital copyright management system related to this Software and/or its integral components.
 - 6) Any other improper or illegal behavior.
6. Before saving or copying this Software, you must first obtain authorization from the relevant copyright holder in your country or region. The copy functionality provided by this

ARMATURA Software is limited to copying files without copyrights, files for which you have a copyright, or files for which you have obtained authorization or legal permissions to copy. You understand that the ownership and intellectual property rights of any files displayed, stored, or accessed through this Software belong to their respective copyright holders. These files may be subject to copyright laws, other intellectual property laws and treaties, or third-party terms of use. Unless otherwise specified, this Agreement does not grant you any rights to, nor the continued use of such files.

7. You agree to comply with all applicable laws and regulations of the country/region in which this Software is stored or being used (including but not limited to the laws of the country/region in which you reside, or download/use this Software from).

IV All Rights Reserved

ARMATURA and its licensors reserve all rights and entitlements to this Software, including any other rights not expressly granted to you in this Agreement.

V Privacy Policy

The ARMATURA Privacy Policy (hereinafter referred to as the "Privacy Policy") provides information related to the data collected by ARMATURA, and how it utilizes such data. During your use of this Software, ARMATURA will collect data in accordance with the provisions of this Agreement and its Privacy Policy.

VI Use of Data

1. You agree that ARMATURA and its affiliates/licensors may collect data from your Software to improve its provision of services and products to you. By default, we do not actively collect data from your software, and we may only collect personal data upon your instructions and in compliance with data protection laws. In order to facilitate ARMATURA's provision of software updates, upgrades, product support, and other product services, you agree that ARMATURA and its affiliates/licensors may collect system and application data from your Software. This includes your software name, system and application version, region and language settings, software version, software identification data, network service provider, and IP address. All data is anonymized before collection and processing.
2. During your use of this Software, collected data may be processed or transmitted to ARMATURA offices, affiliates, or licensors outside your country/region of residence. As such, your data may be transferred to or accessed from jurisdictions outside the country/region in which you are using ARMATURA products or services. These jurisdictions may have differing data protection laws, and may not offer the same protections. ARMATURA warrants that your data will be protected at an adequate level in accordance with all applicable laws and regulations.
3. ARMATURA will only retain your data within the period of time necessary for the purposes outlined in this Agreement and Privacy Policy, unless longer retention is permitted or required by law. ARMATURA warrants that it will take all appropriate technical and organizational

measures to prevent unauthorized access or disclosure of data. You understand, however, that no measures can guarantee absolute security.

VII Software Updates

ARMATURA may provide you with software updates, though you understand it is under no obligation to do so. Unless accompanied by a separate end-user license agreement, any updates provided by ARMATURA for this Software shall be subject to this Agreement. By deciding not to download updates provided by ARMATURA, you understand and accept that you may be subjecting yourself to serious security risks, and that the Software may become unstable or unusable. Some software functionality may only be available in certain versions. It is recommended to keep the Software up-to-date to ensure the best possible user experience.

VIII Termination and Continued Validity

1. This Agreement shall take effect from the day you install this Software. You may terminate this Agreement at any time by permanently deleting, destroying, or returning this Software, including all backup copies and related materials provided by ARMATURA. All corresponding costs shall be borne by you. If you fail to comply with any its terms or conditions outlined in this Agreement, ARMATURA or its licensors have the right to terminate this Agreement at any time and without prior notice. After this Agreement is terminated, you must immediately cease using this Software and delete all related software and materials that have been copied to and/or installed on your ARMATURA equipment or computer.
2. Articles 6, 9, 10, 11, 12, 14, and 15 shall continue to be effective even after the termination of this Agreement.

IX Disclaimer

1. You accept that this Software is provided to you “as is” without any express or implied warranty, and to the maximum extent permitted by applicable laws, ARMATURA and its licensors/affiliates or copyright holders do not provide any express or implied warrants or guarantees. This includes but is not limited to guarantees regarding merchantability, quality, suitability, accuracy, confidentiality, and non-infringement of third-party rights. Neither ARMATURA nor any other party guarantees that the functionality of this Software is suitable to your requirements, nor that its operation will be uninterrupted or without error. By opting to use this Software to obtain a specific result, all responsibilities and risks associated with its install and use shall be borne by you.
2. Installing this Software may affect the availability of third-party software, applications, or services. ARMATURA does not guarantee that the functions or services contained within this Software will meet your requirements, nor does it guarantee that the Software and its services will be without error, lack bugs, or provide continuous and lasting services. Furthermore, ARMATURA does not guarantee that this Software will be compatible with any third-party software or service.

3. You understand that ARMATURA's software and services are not suitable for certain applications, including but not limited to operation of nuclear energy facilities, aircraft navigation and communication systems, air traffic control systems, and life support or weapon systems. Errors or time delays in ARMATURA software in these situations may lead to personal injury, death, or serious physical and environmental damage.

X Limitation of liability

1. ARMATURA does not assume any responsibility for problems that may result from the misuse or unauthorized modification of the Software.
2. To the extent not expressly prohibited by applicable laws, ARMATURA and its employees, licensors, and affiliates are not liable for the compensation of any profit loss, sales loss, data loss, cost of purchasing alternative goods or services, property damage, personal injury, business interruption, business information loss; or any special direct, indirect, incidental, economic, punitive, or ancillary damages regardless of theory of liability (contract, tort, negligence, or other), even if they were aware of the possibility of such damages. Certain jurisdictions do not allow the limitation of liability for personal injury, incidental, or consequential damages. As such, these limitations may not apply to you.
3. The total damages for which ARMATURA may be liable to you shall not exceed the price you paid for the purchase of its equipment/software (excluding cases of personal injury or death due to negligence by ARMATURA, subject to applicable laws and regulations).
4. The laws of certain countries/regions do not allow Agreements to exclude or limit certain warrants, guarantees, or liabilities. If these laws apply to you, some or all of the limitations outlined in this Article may not apply to you. No provision outlined in this Agreement affects your legal rights as a consumer, and these rights cannot be modified or waived through your acceptance of this Agreement.

XI Technical Support

ARMATURA has no obligation to provide you with any technical support services for this Software outside of those required by law. No verbal and written information or advice given by a ARMATURA authorized representative shall constitute a warranty. Should ARMATURA software or services prove defective, you assume the entire cost of all necessary repairs or corrections.

XII Export Control

Unless otherwise authorized by applicable laws and relevant regulations in ARMATURA's resident jurisdiction, you may not use, export, or re-export ARMATURA software.

XIII Contact Method

If you have any questions, comments, or suggestions, you may contact ARMATURA at (470) 816-1970 by phone or info@armatura.us by email.

XIV Dispute Resolution and Applicable Law

The verification, interpretation, modification, performance, and dispute resolution of this Agreement is governed by the laws of the state of Georgia, without regard to conflict of law provisions. You accept that this Agreement will be considered to have been signed in Atlanta, GA. 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 resolved 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.

XV Entire Agreement

This Agreement constitutes the entire agreement between you and ARMATURA in regards to the use of this Software, and will replace any previous agreement between you and ARMATURA in regards to the aforementioned. You may be subject to other applicable terms and conditions during use or purchase of open-source software, third-party content, or other services from ARMATURA.

Personal Information Protection and Privacy Policy

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

Lastly updated on: July 2022

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

Email: info@armatura.us

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

ARMATURA LLC and its affiliates (hereinafter referred to "Armatura", 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. Armatura 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. **ACMS** refers to cloud services developed and operated by the ACMS 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. **ACMS Provider** refers to Armatura and local branch offices, local partner, the company that developed and provides **ACMS** 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 ACMS products.

I Personal information collection rules

1. Which of your personal information will be collected by enterprise/organization owners or Armatura

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

1) To Help You Activate ACMS 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 ACMS, 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 ACMS to send you an activation code email and identification in the system. Others are optional.

2) Providing You with ACMS Services.

a. 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.

b. 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:

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

In order to provide better technical support, Armatura 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 ACMS.

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 ACMS 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 ACMS 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 ACMS cloud services, presenting you with personalized third-party promotions through the system, or sharing information with ACMS 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

ACMS 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.



ARMATURA LLC www.armatura.us E-mail: sales@armatura.us
Copyright © 2022 ARMATURA LLC. All rights reserved.