HID® Amico™ Biometric Readers

VL35LF and VL70LF

User Guide

PLT-07752, Rev. A.2
November 2025

Copyright

Trademarks

Contacts

For technical support, please visit: **https://support.hidglobal.com**.

What's new

Date	Description	Revision
November 2025	Minor updates.	A.2

A complete list of revisions is available in **Revision history**.

Section 01

Introduction

1.1 Document purpose

This document provides procedures for administrators to set up HID® Amico™ VL35LF and VL70LF, and for operators to carry out tasks associated with enrollment and credential/biometric data management.

1.2 Intended audience

This document is for users with the following roles:

- **HID Amico administrator:** set up and configure the HID Amico reader
- **HID Amico operators:** install and configure network detected HID Amico readers, enroll people in the system, and add credentials and biometric data

1.3 Interaction with the reader

Use the touchscreen to configure all settings of the HID Amico VL35LF and VL70LF readers by accessing the administration menu. Alternatively, connect the reader to a network, or directly to a PC via an Ethernet cable, and configure the device through the web interface.

1.3.1 To access the on-screen administration menu

Tap **Menu** on the touchscreen. The reader does not require any authentication to access the menu before administrators are enrolled.

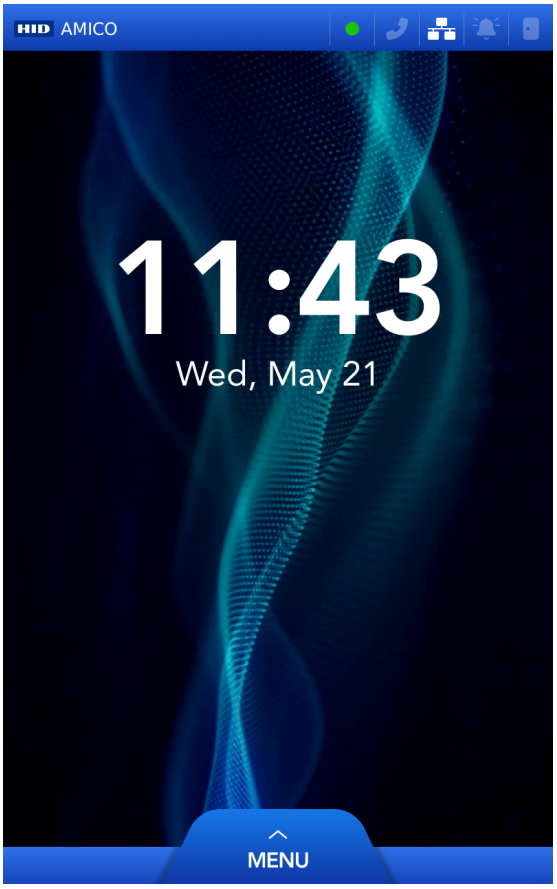
> **Note:** It is recommended to enroll an administrator before using the reader in a production environment.

1.3.2 To access the web interface

1. Use a web browser to navigate to the default **http://192.168.0.129** (or the custom address if you have changed it, or you are using a dynamically assigned IP address (DHCP)). The login screen is displayed.
2. Log in using the credentials set during the HID Amico reader set up.

1.4 Idle screen

The reader displays the current date and time when idle and uses that information to record identification attempts in the access log, which displays the results of the identification attempt (unidentified, authorized, or unauthorized). The **1.4.1 Status bar** is shown at the top of the screen, and the **1.5 Main menu** button is shown at the bottom of the screen.



Note: The idle screen can be customized to add time and attendance buttons or a logo.

1.4.1 Status bar

The status bar displays status, operation, and use of the reader.

Icon	Description
Operation status	Flashing under normal operation. A solid icon indicates a problem.
Intercom (VL70LF only)	Indicates an active intercom call.
Network	Indicates the reader is connected to the network.
Alarm	Indicates when an alarm has been triggered.
Door	Indicates that the door is open. **Note:** If there is no door sensor installed, this icon indicates that the relay is open.

1.4.2 Standard command buttons

The following buttons may be displayed on all screens.

Button	Function
Back	Return to the previous screen.
Exit	Return to the idle screen.
OK	Save any changes made and return to the previous screen.
Add	Add users, departments, or schedules.
More	Tap for extra menu items.
Remove	Remove users, biometrics, cards, or panic fingers.
Save	Save any changes made.

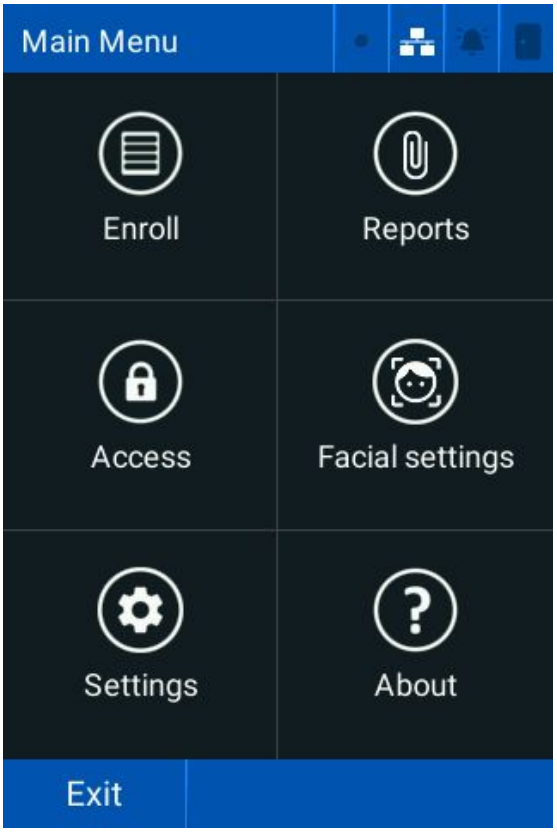
1.5 Main menu

Tap **Menu** on the idle screen to access the **Main Menu**.

- Enroll users, departments, and schedules - see **2.3 Enrollment**
- View reports - see **3.1 Reports**
- Access settings - see **4.1 Access**
- Facial settings - see **5.1 Facial settings**
- Settings - see **7.3 Alarms**
- About - see **7.16 About**

> **Note:** The main menu is only available to non-administrator users when there are no administrators enrolled in the reader.

Log in using your biometrics, card, or password. The main menu is displayed when an administrator logs in.



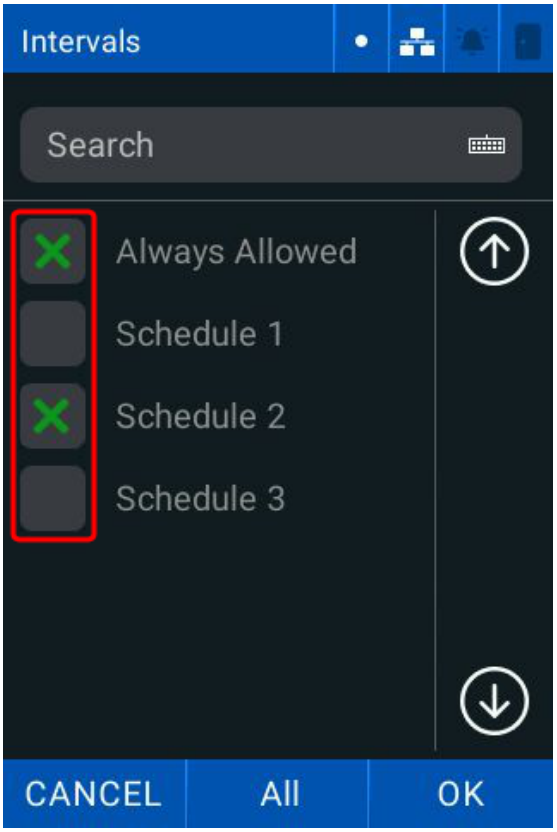
> **Note:** If you do not have an administrator account, an **Administrator Identify yourself** message is displayed.

1.6 Text editing screen

Edit the text field when the keypad (⌨) is displayed.

1.7 Options box

Tap the checkboxes to select multiple options in a list.



Section 02

Enroll and manage users

2.1 User enrollment

The enrollment process includes:

- Enrollment of a unique identification code (ID)
- Enrollment of identification factors (for example, biometric templates, card, or password)
- Assign users with additional data such as names, departments, schedules, or administrator privileges (optional)

Users are associated with the **Standard** department by default. You can associate the user with another department or schedule.

Note: A user must be associated with a department or schedule to access any areas controlled by a reader.

2.1.1 User attributes

Each user can have the following attributes:

Attribute	Description
ID	A unique numerical value (15 digits maximum).
Name (optional)	A user name helps facilitate identification for reports and user lists. This field is blank by default.
Departments	Associates a group of users with common schedules simultaneously.
Photo	Photo assigned to a user's biometric template during enrollment. Note: Storing user photos may not be supported if the database capacity has been extended.
Proximity card	Proximity card(s) assigned to a user.
Password	A numeric password to identify a user. Note: A password is a non-unique number and can be used by multiple users with different IDs.
PIN	A unique numeric password to authenticate a user.
Privilege level	Administrator, or normal user.
Schedules	Allows user access for a defined time period(s).
Registration number (optional)	A number for recording purposes only. Note: Registration is not a method of user identification within HID Amico. You can use it to keep your own external record of users.
Opening timeout	A per-user defined duration that the door is opened (relay activated). It overrides the Time of opening (ms) parameter.

Note: Manage users through both the HID Amico reader touchscreen and the web interface.

2.2 User verification

The HID Amico reader has four forms of identification:

- **Facial biometrics**: detects the users face
- **Proximity card**: detects the users card
- **Password**: validates the users ID and password
- **QR Code**: scans a QR Code (in numeric or alphanumeric format)

Registered HID Amico users have two privilege levels:

- **Ordinary user**: normal user of the system that can only identify themselves
- **Administrator**: full access to the reader

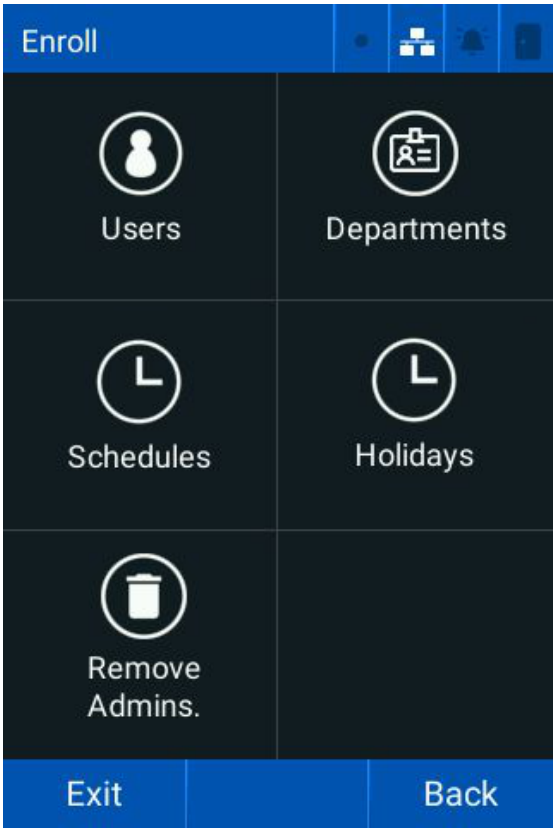
No users are enrolled on the reader by default, and access to the main menu is available to all users.

> **Note:** It is recommended to enroll an administrator before starting reader operation.

2.3 Enrollment

The enrollment screen allows you to add, remove, and edit user data.

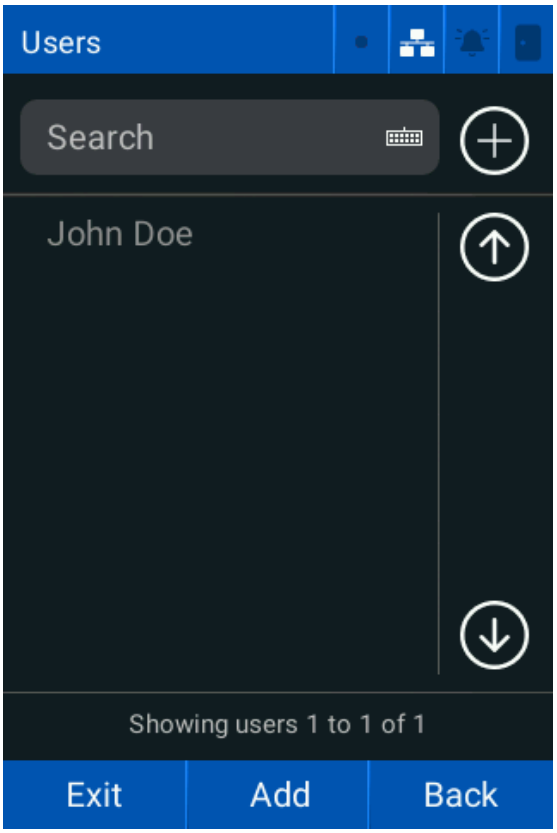
Tap **Menu** > **Enroll**.



2.4 Users

The **Users** menu allows you to:

- Search for users
- Enroll new users
- Edit or remove existing users



2.4.1 Search for a user

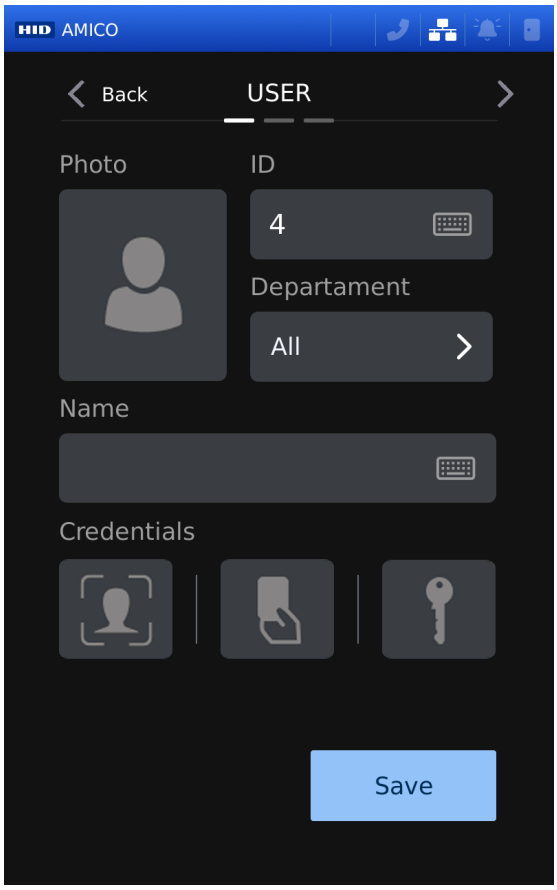
1. Tap **Menu** > **Enroll** > **Users**.
2. Tap **Search** and enter the **user name** or **user ID**.
3. Tap **Confirm**.

Note: HID Amico associates each user with a single person for access where the reader is installed.

Important: While possible, it is not recommended to associate more than one person with a single user (sharing the ID and access password, or registering multiple cards held by different people). This harms the consistency of the data recorded in the access and alarm reports.

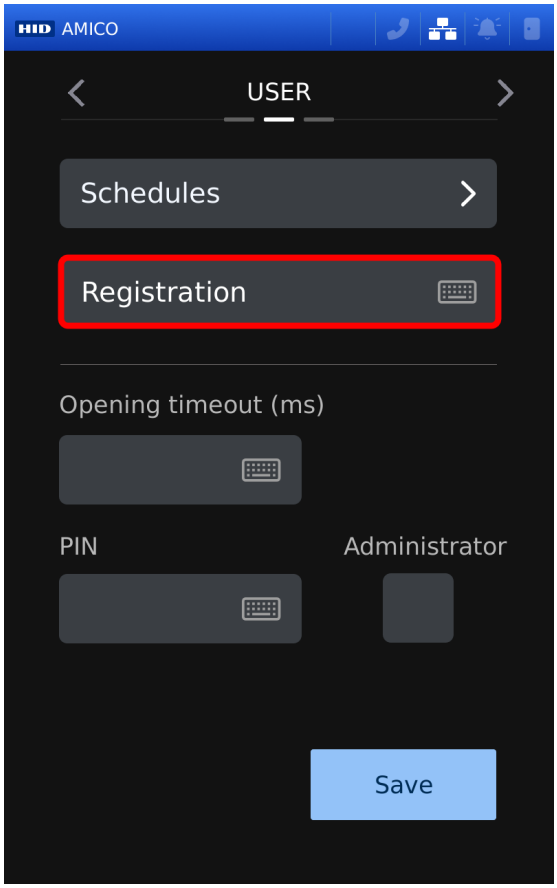
2.4.2 Register new users

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap **Add**.
3. Enter the required **ID** and **Name**.



4. Tap **Department** and tap the required departments you want to associate the user with.
5. Tap the **Photo** icon and follow the on screen-prompts to assign a photo. See **B.1 Face capture - best practices** for more information.
6. Tap the **Password** icon and enter the required password. Tap **Next** to continue.

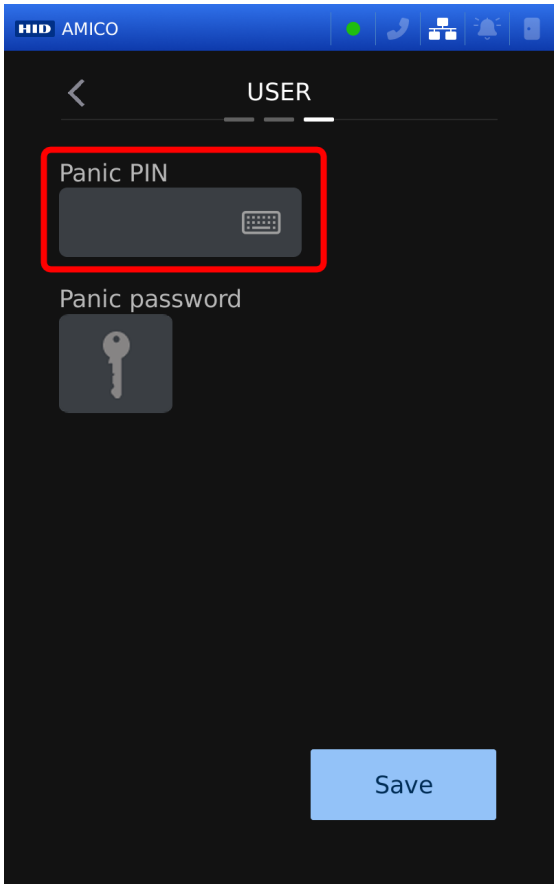
7. Tap the **Registration** keyboard and enter a unique user registration number.



8. Tap the **Opening timeout (ms)** keyboard and enter the required time a user has to open the door after a user identification.
9. Tap the **Pin** keyboard and enter the required security key.
10. Tap the **Administrator** checkbox to make the user an administrator. Tap **Next** to continue.

> **Note:** The user is automatically linked to the schedules of their associated departments.

11. Tap the **Panic PIN** keyboard and enter the required pin.



12. Tap the **Panic password** icon and enter the required password.

> **Note:** See **7.3.2 Internal alarms (VL70LF only)** for more information on enabling the Panic PIN and Panic password.

13. Tap **Save**.

2.4.3 Credential enrollment

The **Advanced Options** screen allows you to:

- Assign a facial biometric to a user
- Assign a card to a user

2.4.4 Enroll facial biometrics

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap the  button. The **Facial Registration** screen is displayed.
3. Position your face an appropriate distance from the reader and wait for the identification process.

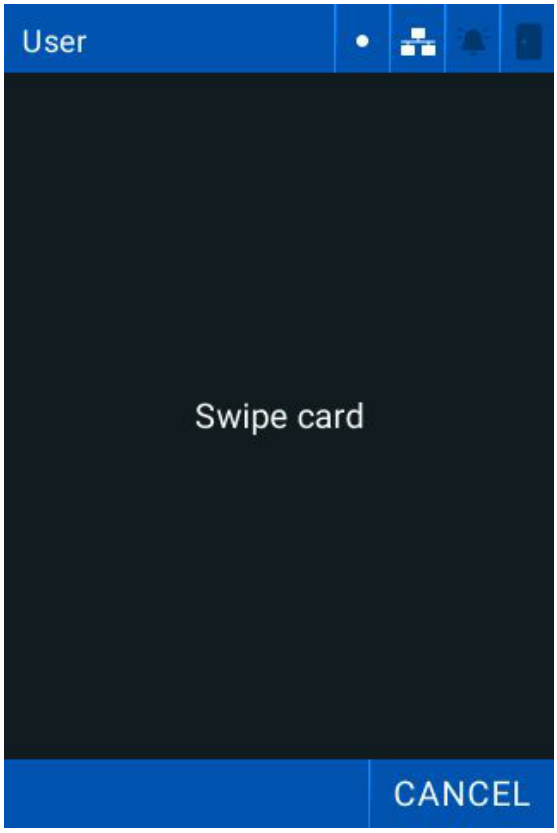
   Note:
   - If your face is too close or poorly framed, a message prompts you to reposition your face.
   - The registered face must be unique for each user. If a face is already registered with a different user, an error message is displayed and the registration is not carried out.
4. Position yourself correctly and tap **Take Photo**. Follow the on-screen prompts to register the image.

   Note:
   - Tap **Back** to cancel the registration.
   - If the reader is in **Template on Card** mode, you will be required to save the template to a Seos® card.

Note: The facial registration process can also be initiated via the web interface.

2.4.5 Enroll a card

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap  **Enroll Card**.
3. Hold the card up to the reader.



4. If successful, a **Card number successfully registered!** message is displayed.

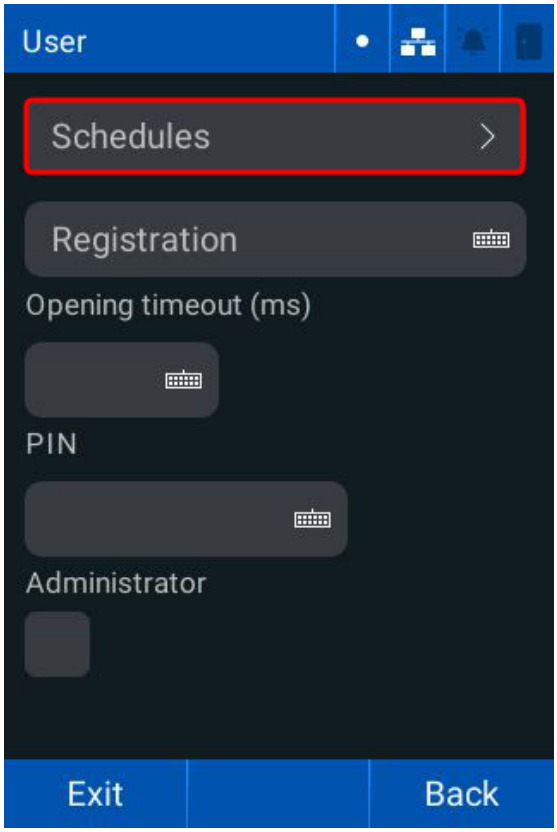
> **Note:**
> - If the card is already registered, a **Card already registered** message is displayed.
> - If the card cannot be read the operation will time out and return to the previous screen.

5. Tap **OK**.

2.4.6 Schedules

This allows you to link a user to one or more schedules:

1. Tap **Menu** > **Enroll** > **Users** > **More**.
2. Tap **Schedules** and tap the required schedules.



3. Tap **Back**.
4. Tap **OK**.

2.4.7 Edit a user

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap the required user.
3. Tap the required data field and make the required changes.

> **Note:** Tap **Remove** and select the required user attributes you want to delete.

4. Tap **OK**.

2.4.8 Delete a user

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap the required user.
3. Tap **Remove** and select **User** from the data list.

   > **Important: You cannot recover any user data after they are deleted. Access logs are available, but only the ID number is visible.**

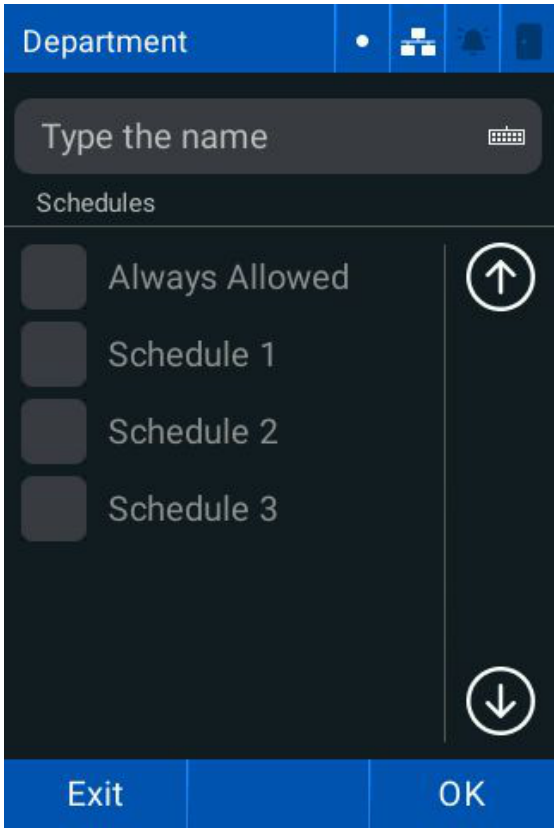
4. Tap **OK**.
5. Tap **OK** to remove the selected data.

2.5 Departments

The **Departments** screen allows you to associate users with multiple departments and inherit all the schedules of the departments with which they are associated. Departments associate groups of users with common schedules.

2.5.1 Create a department

1. Tap **Menu** > **Enroll** > **Departments**> **Add**. The **Department Creation** screen is displayed.



2. Enter a department name.
3. Tap **OK**.

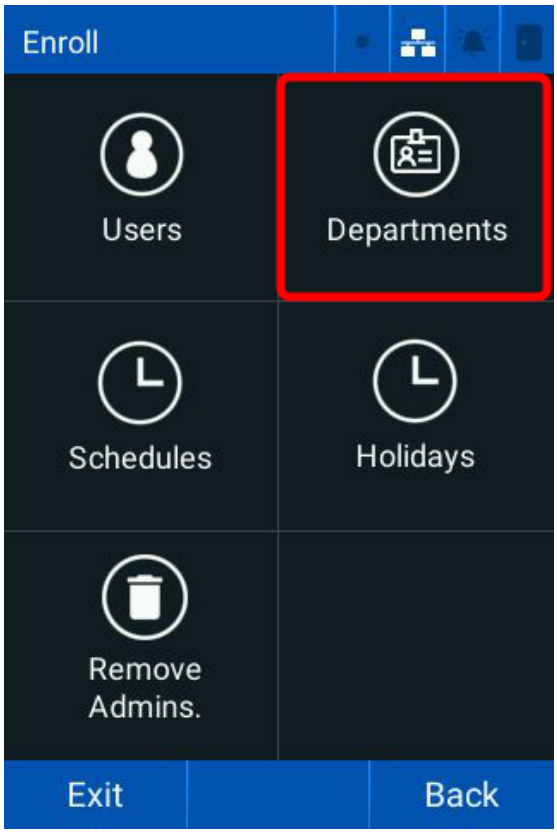
   Note: You can assign a schedule to the department.

4. Tap **OK** to save the department.

2.5.2 Associate a schedule with a department

You can associate multiple schedules with a single department. Department-linked schedules are applied to users belonging to that department.

1. Tap **Menu** > **Enroll** > **Departments**.

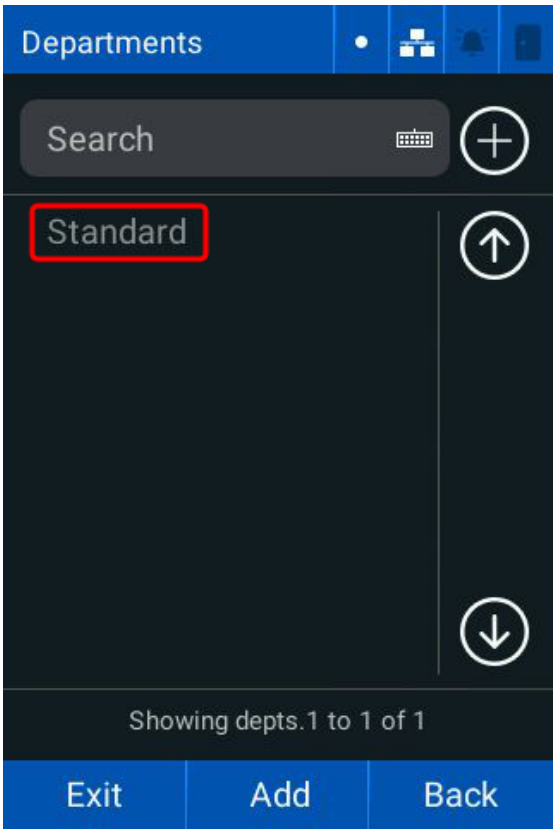


2. Enter the name of the **Department** in the search bar and tap the required schedules.
3. Tap **OK**.
4. Tap **OK** to save the department.

2.5.3 Associate a user to one or more departments

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap the required user.
3. Tap the **Departments** drop-down menu and tap the required departments.

   Note: You can enter the name of the department into the **Search** bar.



4. Tap **OK**.

2.5.4 Edit a department

1. Tap **Menu** > **Enroll** > **Departments**.
2. Tap the required department.
3. Tap the required data field and make the required changes.

> **Note:** The **Standard** department name cannot be changed.

2.5.5 Delete a department

1. Tap **Menu** > **Enroll** > **Departments**.
2. Tap the required department.
3. Tap **Delete**.

> **Note:** The **Standard** department cannot be deleted.

> **Caution:** When a department is deleted, all schedules linked to users in the department will no longer be associated with the users.

4. Tap **OK**.

2.6 Import and export data (VL70LF only)

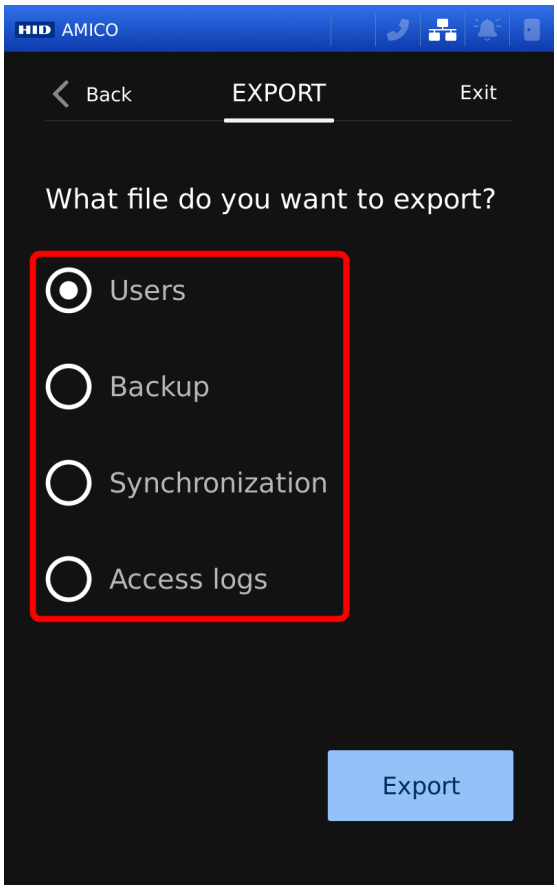
The VL70LF allows you to import and export the following data from the reader using a USB drive.

Data	Description
Users	All registered user data, including faces, cards, and passwords.
Backup	Data from the reader to perform a reader backup.
Synchronization	Transfer all data from one reader to another. Does not include access logs.
Access logs	All access logs.

Note: Internal alarms, relay, and all **Settings Menu** items cannot be imported or exported.

2.6.1 Export reader data

1. Tap **Menu** > **Enroll** > **Import/Export**.
2. Select the required file to export.



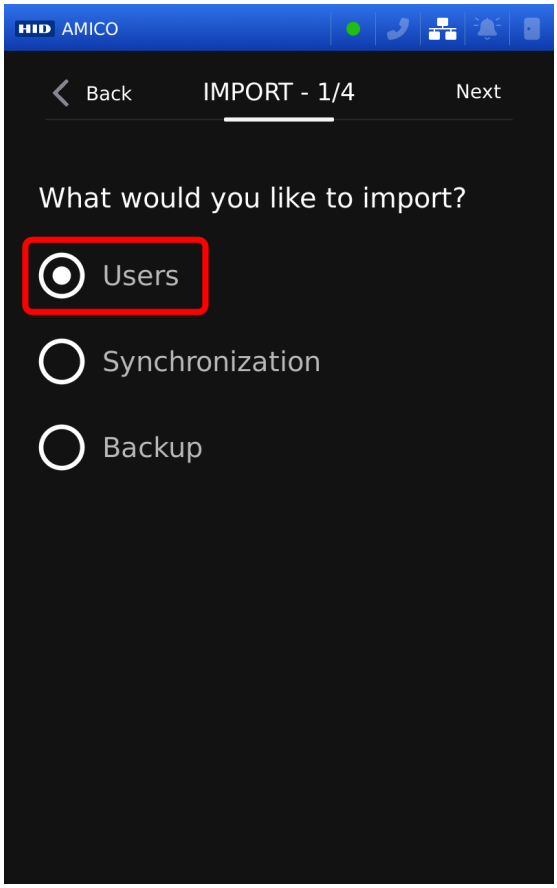
3. Insert a USB drive.
4. Tap **Export**.

   Note: A **.zip** file is created on the USB drive.

5. Tap **Exit**.

2.6.2 Import users (VL70LF only)

1. Tap **Menu** > **Enroll** > **Import/Export**.
2. Insert the USB drive containing the exported data.
3. Tap **Import**.
4. Tap **Users** > **Next**.



5. Tap how you would like to treat user types and tap **Next**:
   - **Keep current**: keeps the registered users on the reader
   - **Utilize from CSV**: updates the imported CSV file users
6. Tap how you would like to resolve conflicts and tap **Next**.

> **Note:** Conflicts happen when users with the same name are imported.

Update	Replaces the information of the registered user. No new registration is created. The user remains with the same ID.
Ignore	Keeps the registered user information and the imported user is not registered. No changes are made to the registered user.
Overwrite	Registers the imported user and removes the existing user. The imported user is assigned a new ID.

7. Tap what happens to the existing users not in the import file:

Keep them	Keeps the registered users.
Remove them	Permanently deletes the registered users

8. Tap **Save**.

2.6.3 Synchronization (VL70LF only)

1. Tap **Menu** > **Enroll** > **Import/Export** > **Import**.
2. Tap **Synchronization** > **Import**.
3. Insert the USB drive containing the required files.
4. Tap **OK** to import the data.

2.6.4 Backup (VL70LF only)

1. Tap **Menu** > **Enroll** > **Import/Export** > **Import**.
2. Tap **Backup** > **Import**.
3. Insert the USB drive containing the required files.
4. Tap **OK** to import the data.

2.7 Schedules

Allows you to determine the time intervals that the reader can authorize a specific user, or members of a department.

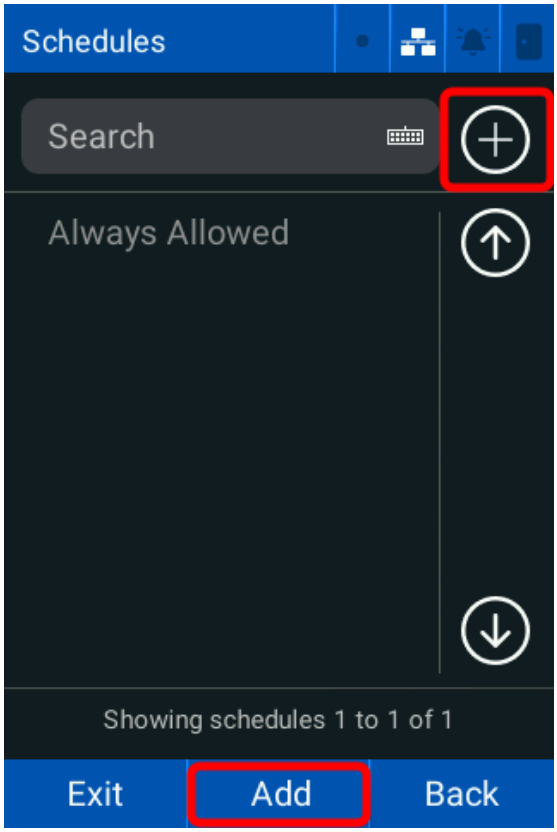
Schedules are defined by:

- **Name**: give schedules a unique name to avoid duplication. Naming the schedule is mandatory.
- **Intervals**: contains a time interval (for example, 08:00 to 18:00) and the days of the week that the interval is valid

> **Note:**
> - Each schedule can have more than one interval
> - The reader grants access in all intervals of the schedule linked to the user

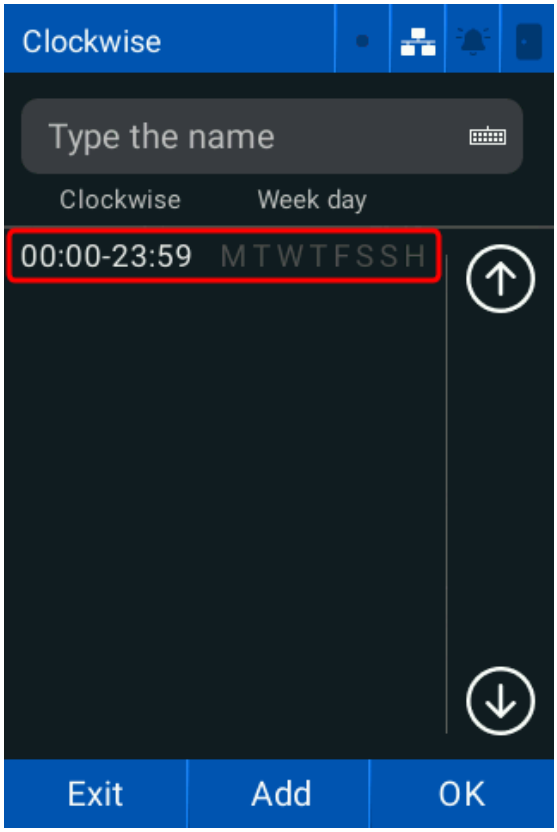
2.7.1 Create a schedule

1. Tap **Menu** > **Enroll** > **Schedules**.
2. Tap **Add**.



3. Enter the required **Name** of the schedule.

4. Tap the schedule and tap **Edit**.



5. Enter the required **Start** and **End** times of the interval and tap the **Days of the week** that the interval is valid.

> **Note:** Valid weekdays are displayed in white and invalid weekdays are displayed in gray.

6. Tap **OK**.

> **Note:**
> - Repeat the procedure to add more schedules as necessary.
> - Holiday types can be associated with valid weekday intervals. See **2.8 Holidays** for more information.

7. Tap **OK** then tap **OK** to save the schedule.

2.7.2 Assign Schedules to a new user

New users do not have a schedule assigned by default so access is always granted. Assign a schedule to the required user to restrict the users access to specific time periods.

1. Tap **Menu** > **Enroll** > **Users** > **Add**.
2. Enter the required information and tap **More**.
3. Tap the **Schedules** drop-down list.
4. Tap the required schedules.
5. Tap **OK**.
6. Tap **Back**.
7. Tap **OK**, then tap **OK** to save the user.

2.7.3 Assign Schedules to an existing user

Assign a schedule to the required user to restrict the users access to specific time periods.

1. Tap **Menu** > **Enroll** > **Users**.
2. Tap the required user.
3. Tap **More**.
4. Tap the **Schedules** drop-down list.
5. Tap the required schedules.
6. Tap **OK**.
7. Tap **Back**.
8. Tap **OK**, then tap **OK** to save the user.

2.7.4 Edit a schedule

> **Note:** The **Always Released** time cannot be edited.

1. Tap **Menu** > **Enroll** > **Schedules**.
2. Tap the required schedule.
3. Tap the required fields and tap **Edit**.
4. Make the required changes.
5. Tap **OK** then tap **OK** to save.

2.7.5 Delete a schedule

1. Tap **Menu** > **Enroll** > **Schedules**.
2. Tap the required schedule.
3. Tap **Remove**.
4. Tap **Remove**.
5. Tap **OK** to remove the schedule.

> **Important: All users linked to the schedule will lose access to the controlled area at the intervals specified by the schedule.**

2.8 Holidays

Allows you to reference special dates when creating breaks. All registered holidays are visible on the **Holidays** page. The holiday type allows you to define the type of holiday, for example, national holidays, local holidays, or personal holidays.

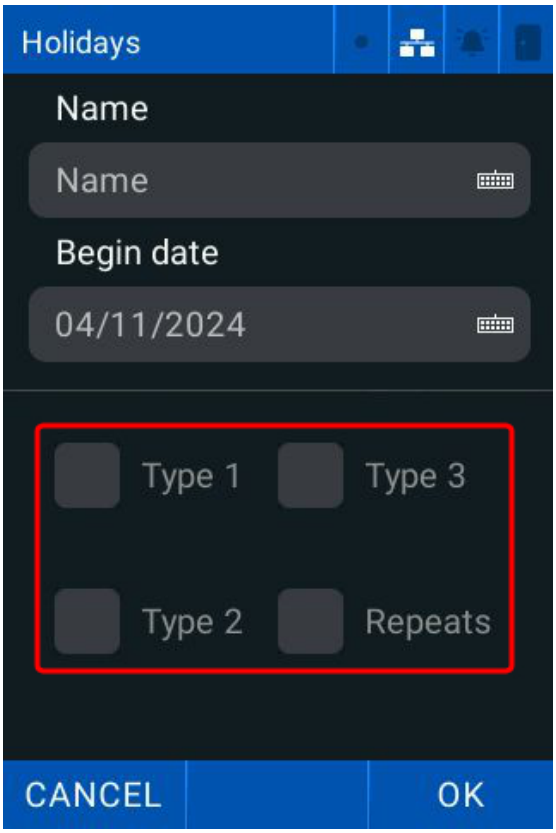
> **Note:** Holiday types are defined during integration and have no specific meaning by default.

Holidays are defined by:

- **Name**: give holidays a unique name to avoid duplication. Naming the holiday is mandatory.
- **Start date**: indicates the start date associated with the holiday
- **Type 1**: indicates that the holiday is type 1
- **Type 2**: indicates that the holiday is type 2
- **Type 3**: indicates that the holiday is type 3
- **Repeats**: indicates that the holiday is recurring, or recurring annually.

2.8.1 Create a holiday

1. Tap **Menu** > **Enroll** > **Holidays**.
2. Tap the **Add** icon.
3. Enter the holiday **Name** and enter a **Start Date**.
4. Tap the required **Holiday Type** and tap **Repeats** if required.



5. Tap **OK**.

2.8.2 Edit a holiday

1. Tap **Menu** > **Enroll** > **Holidays**.
2. Tap the required **Holiday**.
3. Tap the required fields and make the required changes.
4. Tap **OK** to save the changes.

2.8.3 Delete a holiday

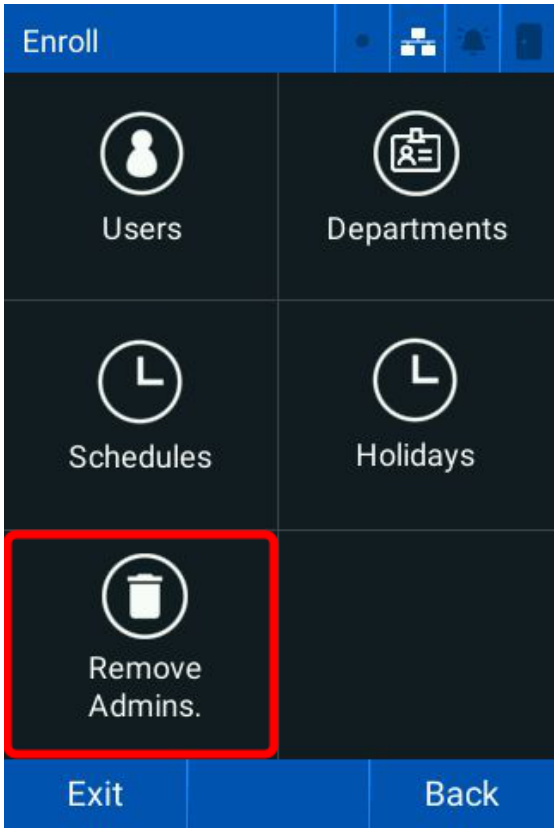
1. Tap **Menu** > **Enroll** > **Holidays**.
2. Tap the required **Holiday**.
3. Tap **Remove**.
4. Tap **OK**.

2.9 Delete administrators

> **Note:** Only registered reader administrators can access the main menu.

To delete an administrator from the reader:

1. Tap **Menu** > **Enroll** > **Remove Admins**.



> **Important: Deleting an administrator cannot be reversed. The main menu becomes accessible to all users until an administrator is registered to the reader.**

2. Tap **OK** to remove all administrators.

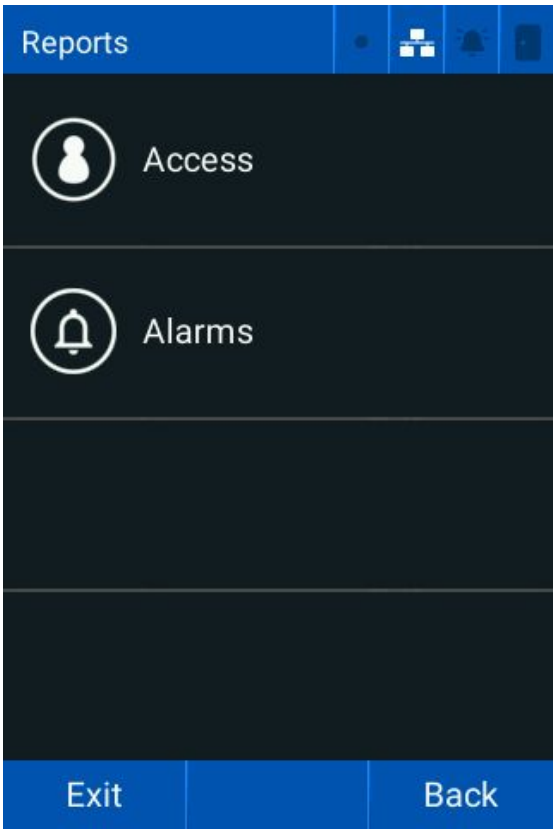
Section 03

Reports

3.1 Reports

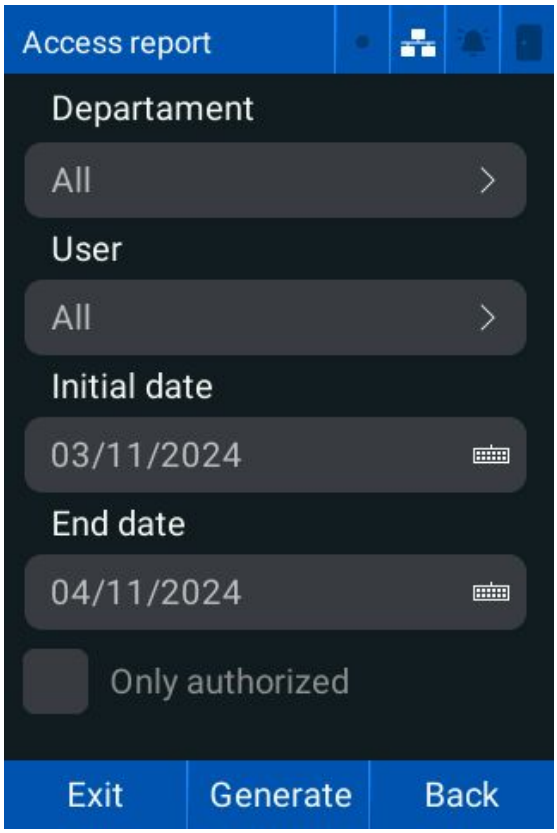
The **Reports** screen allows you to list the access and alarms chronologically, from specific time intervals.

Tap **Menu** > **Reports**. The **Reports** screen is displayed.



3.1.1 Access report

1. Tap **Menu** > **Reports** > **Access**. The **Access report** screen is displayed.



2. Tap **Department** and select the required departments to include in the report. Tap **OK**.
3. Tap **User** and select the required users to include in the report. Tap **OK**.
4. Tap the **Initial date** keyboard and enter the required start date.
5. Tap the **End date** keyboard and enter the required end date.
6. Tap **Only authorized** to only display authorized access events.

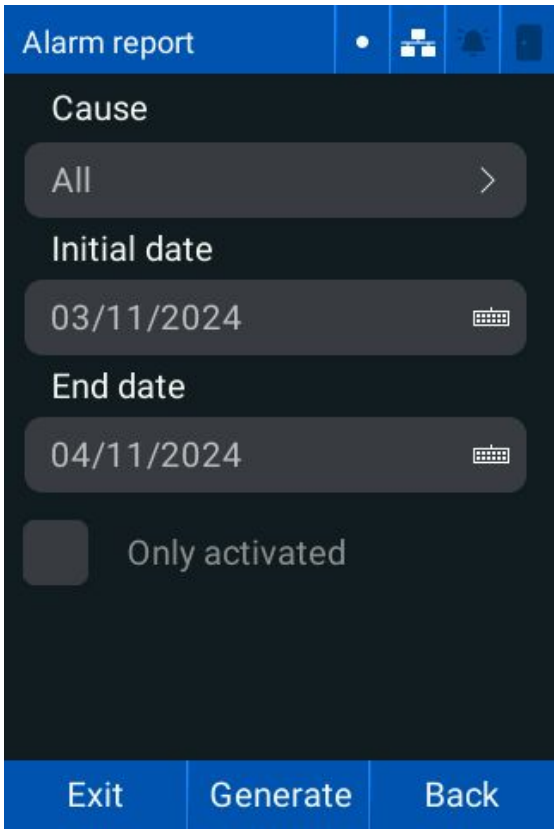
7. Tap **Generate** to view the report.

Note:
- The report is displayed in reverse chronological order.
- A green user name denotes access was granted, a red user name denotes that access was denied.

8. Tap **Exit**.

3.1.2 Alarm report

1. Tap **Menu** > **Reports** > **Alarms**. The **Alarm report** screen is displayed.



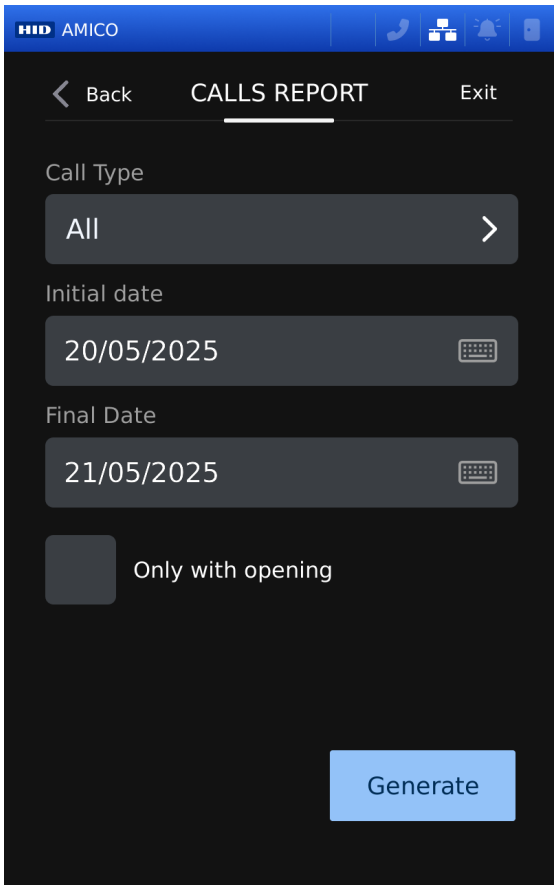
2. Tap **Cause** and tap the required alarm triggers to include in the report. Tap **OK**.
3. Tap the **Initial date** keyboard and enter the required start date.
4. Tap the **End date** keyboard and enter the required end date.
5. Tap **Only activated** to only display triggered alarms.
6. Tap **Generate** to view the report. The reports screen is displayed.

> **Note:**
> - The report is displayed in reverse chronological order.
> - A green alarm denotes access was granted, a red alarm denotes that access was denied.

7. Tap **Exit**.

3.1.3 Call report (VL70LF only)

1. Tap **Menu** > **Reports** > **Calls**. The **CALLS REPORT** screen is displayed.



2. Tap **Call type** and tap the required call type to include in the report.
3. Tap the **Initial date** keyboard and enter the required date.
4. Tap the **Final date** keyboard and enter the required date.
5. Tap **Only with opening** to only display answered calls.
6. Tap **Generate** to view the report. The **Reports** screen is displayed.

> **Note:**
> - The report is displayed in reverse chronological order.
> - Calls in red have not been answered. Calls in green have been answered.

7. Optionally, insert a USB drive and tap **Export** to export the report. Tap **Ok**.
8. Tap **Exit**.

Section 04

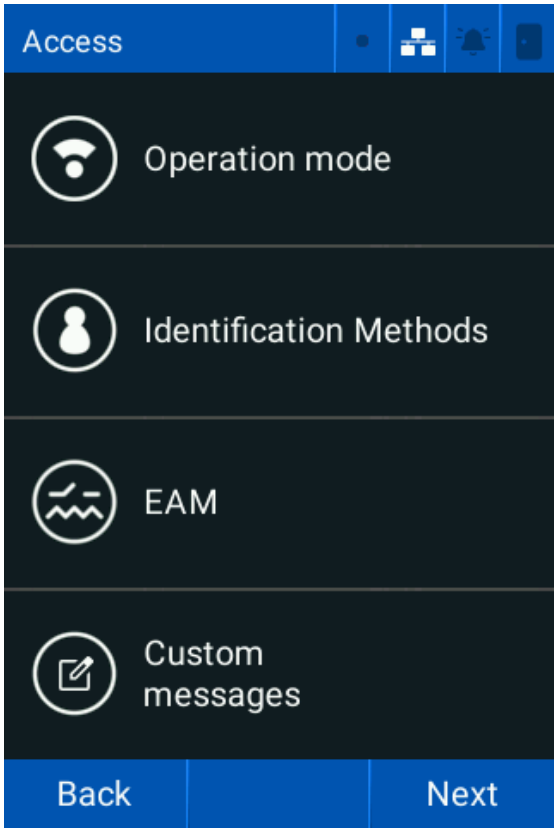
Configure Access settings

4.1 Access

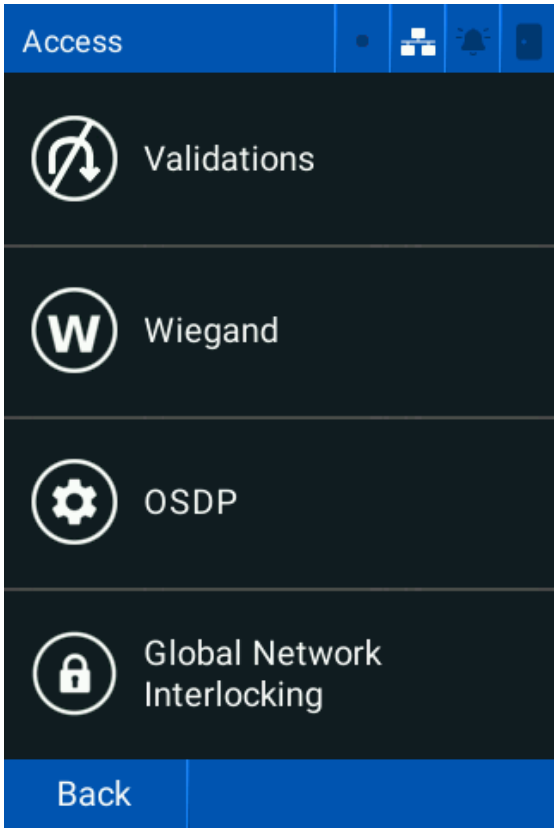
You can configure the following **Access** settings:

Setting	Description
Operating mode	Choose between Standalone and Online mode.
Identification Methods	Choose which methods of identification are enabled on the reader and configure the settings of each identification method.
External Access Module (EAM)	Allows you to configure the properties of an external access module.
Validations	Configure the Anti-passback settings, Access Log Level settings, and Clear Expired User settings.
Wiegand	Configure the input and output settings for Wiegand transmission.
OSDP	Configure the reader as a peripheral device for reading and transmitting information to a control panel.
Global Network Interlocking	Configure two readers to connect and control a zone by keeping one of the connected doors always closed. For example, a quarantine zone or mantrap system.
Relay and GPIOs (VL70LF only)	Configure the functionality of the built-in relay and inputs.
Audio messages (VL70LF only)	Configure the audible response for identification events.
Custom Messages (VL70LF only)	Configure custom messages for identification events.
Scheduled Release (VL70LF only)	Configure time periods that the door stays unlocked.

1. Tap **Menu** > **Access**. The **Access** screen is displayed.



2. Tap **Next** for more options.



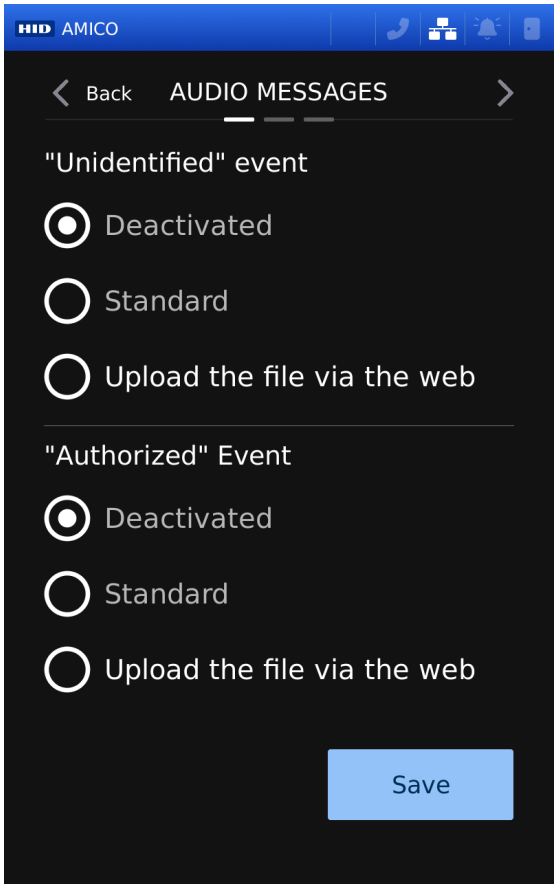
4.2 Audio messages

Sound events

Events with an audible response:

- Unidentified
- Authorized
- Unauthorized
- Wear mask

1. Tap **Menu** > **Access** > **Audio Messages**. The **Audio Messages** screen is displayed.

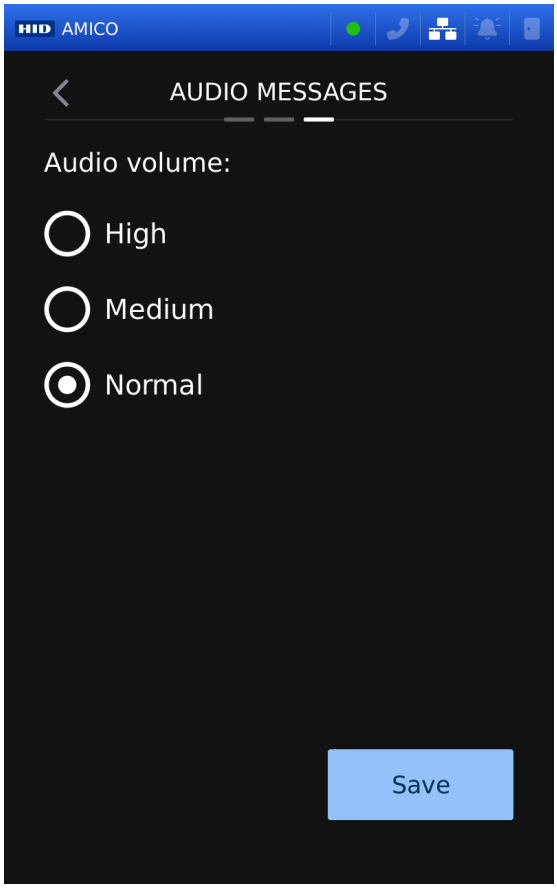


2. Tap the required **Unidentified** and **Authorized** event audio message settings:
   - **Deactivated** - no audio message
   - **Standard** - default audio message
   - **Upload the file via the web** - personalized audio message

   Note: Upload personalized audio files to the reader through the web interface, or by API request. See *HID Amico Biometric Reader API Guide* (PLT-07756) for more information.

3. Tap **Next** and tap the required **Unauthorized** and **Wear mask** event audio message settings.

4. Tap **Next**. The **Audio volume** screen is displayed.



5. Tap the required **Audio volume**:
   - **High**
   - **Medium**
   - **Normal** (default)
6. Tap **Save**.

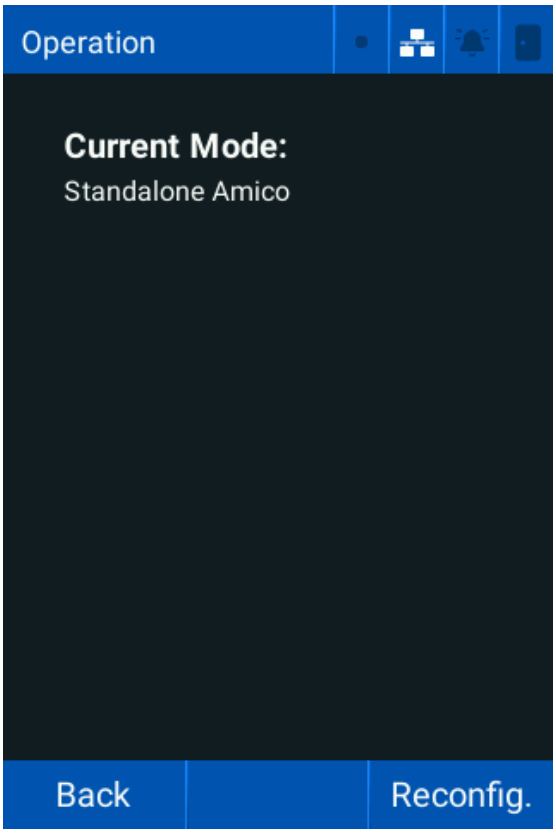
4.3 Operation mode

HID Amico has two operating modes:

- **Standalone (default)**: All information required to identify and authorize access is stored in the HID Amico readers local database. For example, user enrollment, biometrics templates, cards, departments, schedules, and access rules.
- **Online**: The reader identifies the user in its local database when identification is initiated. Access authorization is done through a connected server, which processes the access rules and grants or denies authorization.

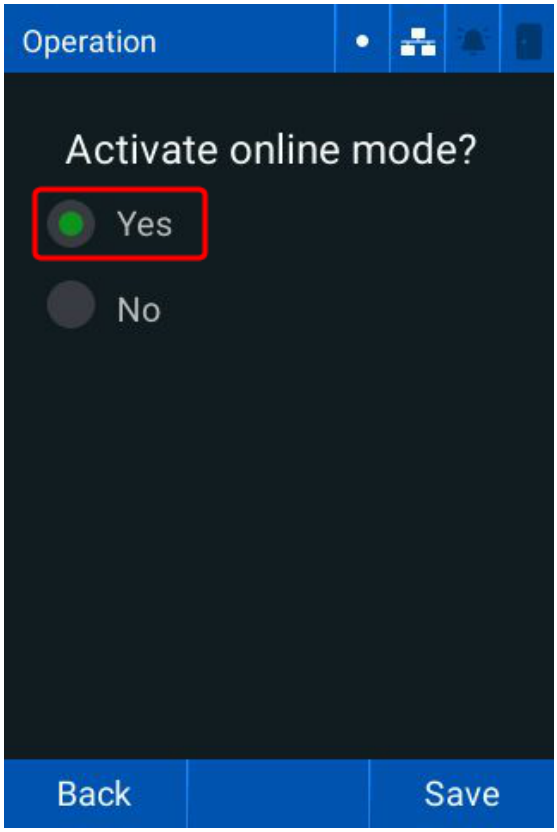
4.3.1 To change the operation mode

1. Tap **Menu** > **Access** > **Operation Mode**. The current operating mode is displayed.



2. Tap **Reconfig**.

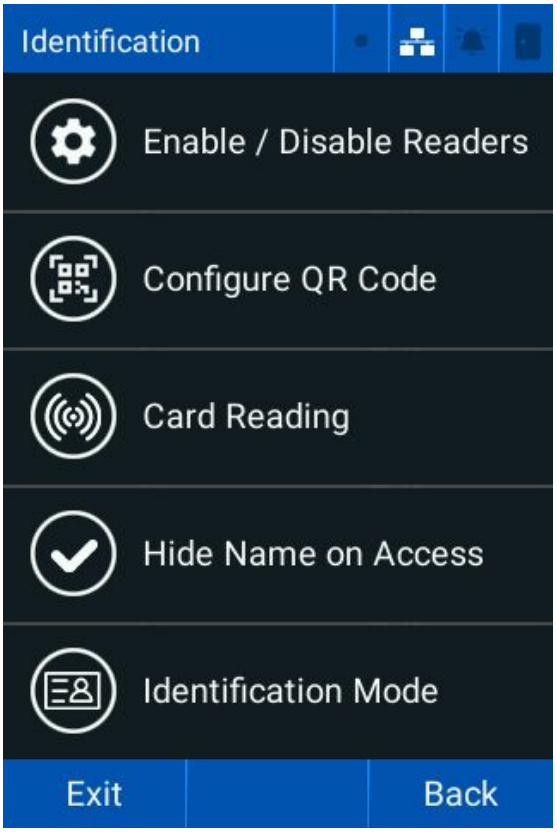
3. Tap **Yes** to select online mode.



4. Tap **Save**.
5. Tap **OK** to make the changes.

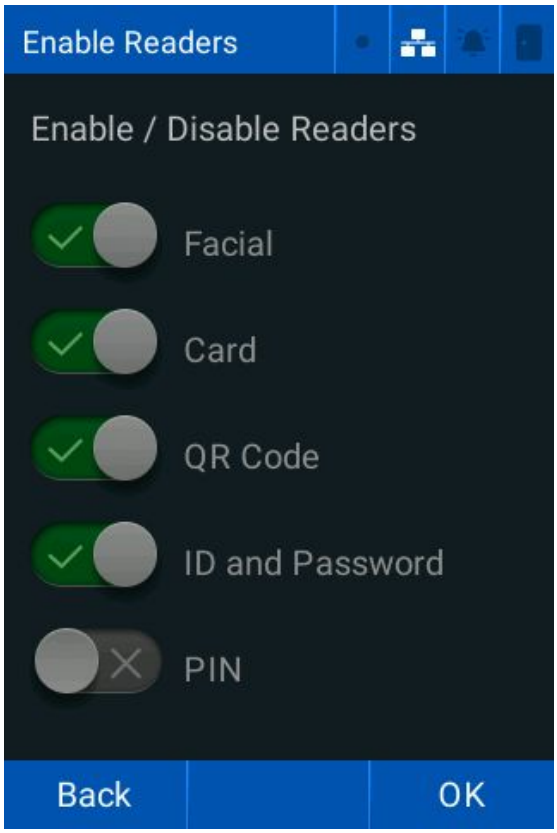
4.4 Identification methods

Tap **Menu** > **Access** > **Identification Methods**. The **Identification** screen is displayed.



4.4.1 Enable/disable reader identification methods

1. Tap **Menu** > **Access** > **Identification Methods** > **Enable / Disable readers**. The **Enable Readers** screen is displayed.

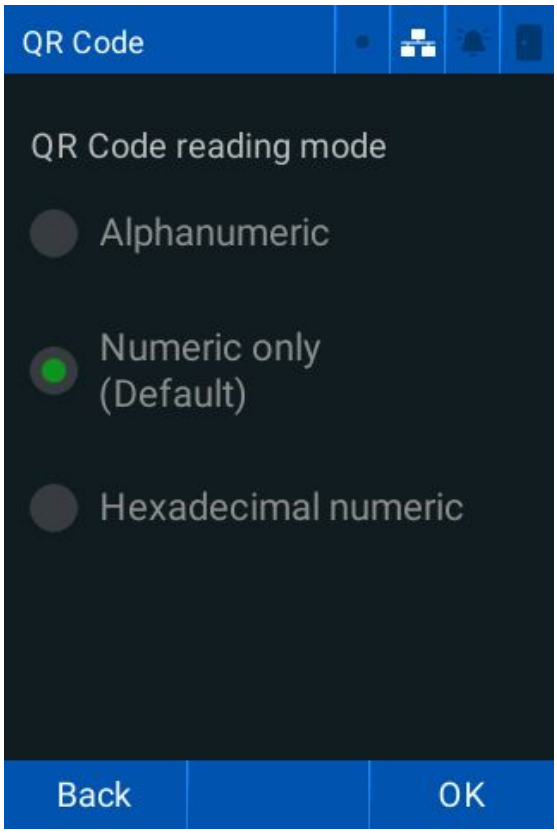


2. Tap the required identification method toggles to enable/disable them:
   - **Facial**: starts the face identification process when a person is detected by the camera.
   - **Card**: starts the card identification process when a card is presented to the reader.
   - **QR Code**: starts the QR code identification process when a QR code is detected by the camera.
   - **ID and Password**: identifies the user from the ID and password entered on the touchscreen.
   - **PIN**: identifies the user from the PIN entered on the touchscreen.

   > **Note:**
   > - **ID and Password**, and **PIN** cannot be enabled together.
   > - **Face**, **Card**, **QR Code**, and **ID and Password** are enabled by default.
   > - Tap the center of the idle screen to display the keypad to enter a **Password** or a **PIN**.

4.4.2 QR Codes

1. Tap **Menu** > **Access** > **Identification Methods** > **Configure QR Code**. The **QR Code** screen is displayed.

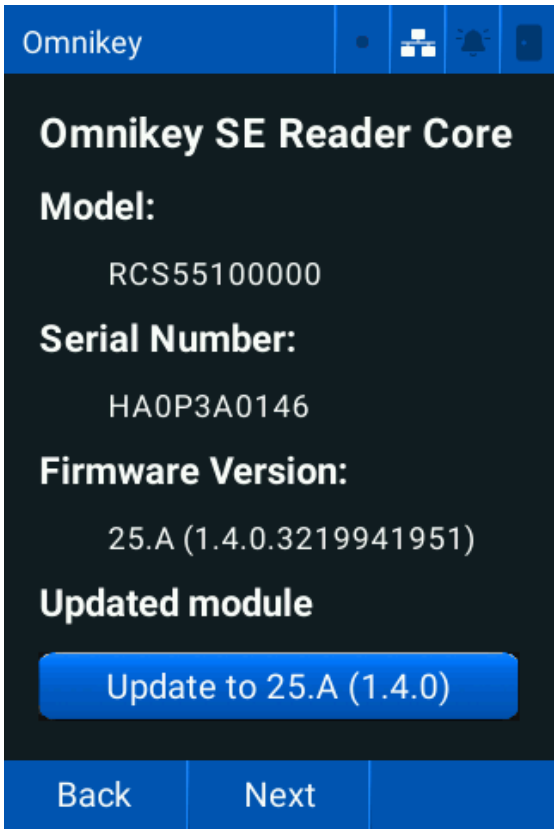


2. Tap the required **QR Code reading mode**:
   - **Alphanumeric** (default): accepts alphanumeric characters as the QR Code. The QR Code is saved as a **qrcodes** object.
   - **Numeric Only** (default): the QR Code must be 64-bit numeric. The QR Code is saved as a **cards** object.
   - **Hexadecimal numeric**: the QR Code must be 64-bit hexadecimal numeric. The QR Code is saved as a **cards** type object.
3. Tap **OK**.

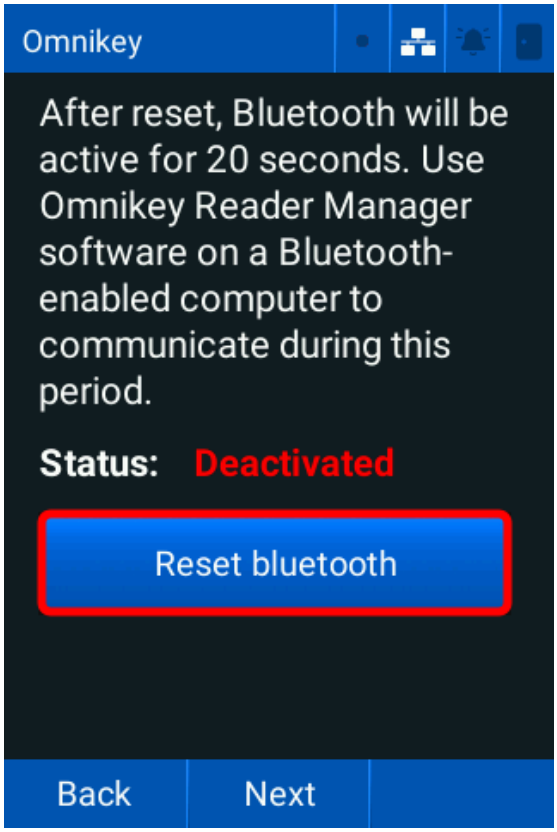
4.4.3 Card reading

The OMNIKEY® Reader Core module parameters can be configured independently via Bluetooth LE or USB connection with the OMNIKEY Reader Manager application. The communication channel is disabled by default. To temporarily open the communication channel:

1. Tap **Menu** > **Access** > **Identification Methods** > **Card Reading**. The **Omnikey SE Reader Core** screen is displayed. Tap **Next**.

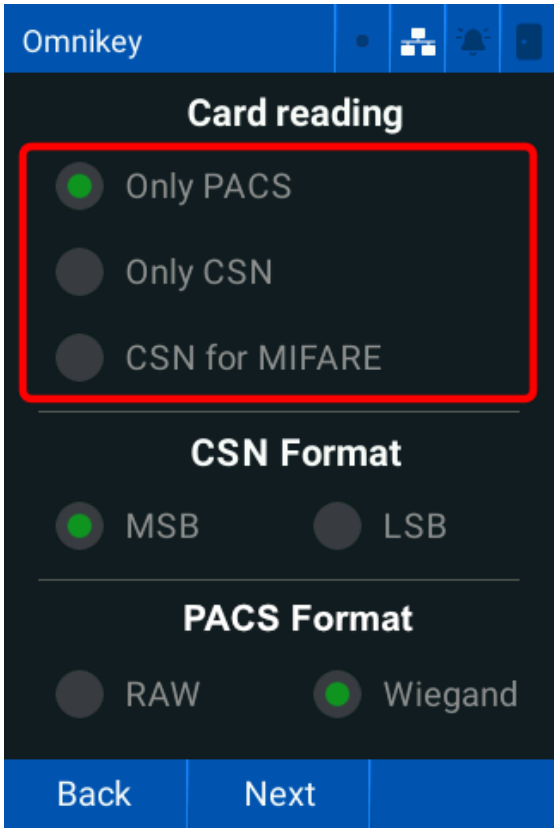


2. Tap **Reset bluetooth**. Tap **Next**.



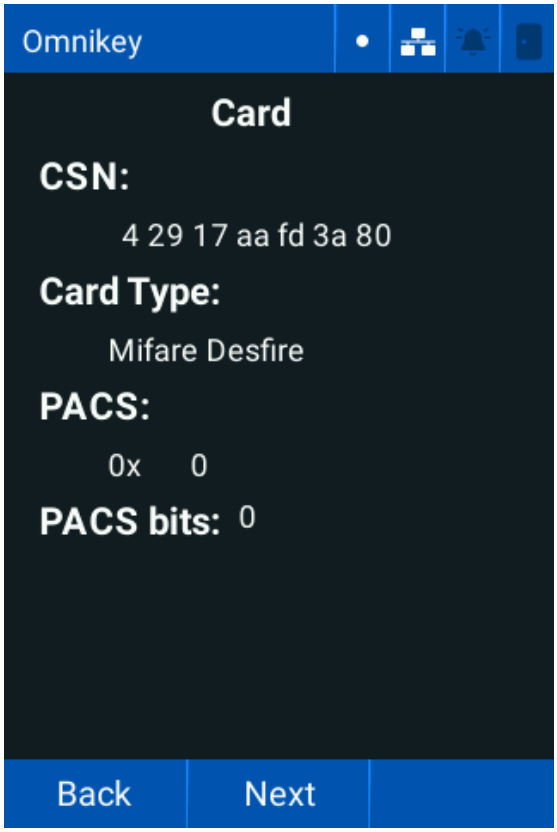
Note: See **4.5 Set Elite and MOB keys** for more information.

3. Tap the required **Card reading** setting:
   - **Only PACS**: The reader only reads PACS data from the card. CSN will be ignored.
   - **Only CSN**: The reader only reads CSN data from the card. PACS data will be ignored.
   - **CSN for MIFARE**: The reader will read PACS data from the card. If the card type is MIFARE, the reader will read CSN.



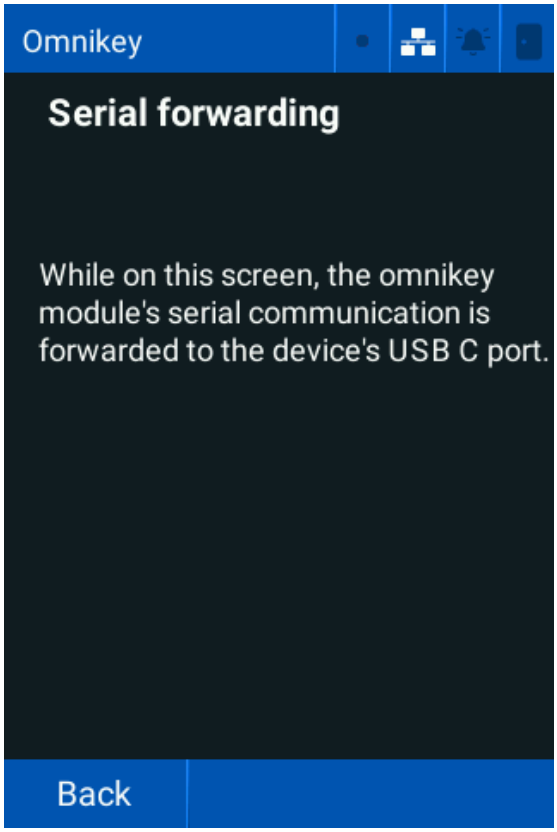
4. Tap the required CSN format:
   - **MSB**: Most significant bit first
   - **LSB**: Least significant bit first
5. Tap the required PACS format:
   RAW
   Wiegand

6. Tap **Next** to continue. The card screen is displayed.



7. Hold the card up to the reader to verify the card details. See **4.4.4 Antenna locations** for more information. Tap **Next** to continue.

8. The **Serial forwarding** screen is displayed.



Note: Serial forwarding is enabled while this screen is displayed. Tap back to disable serial forwarding.

4.4.4 Antenna locations

HID Amico readers can read various types of contactless cards, key fobs, or mobile credentials that operate across multiple frequencies. The antenna for individual frequencies are in different locations depending on the reader. Present the credential to the corresponding antenna for optimal user experience.

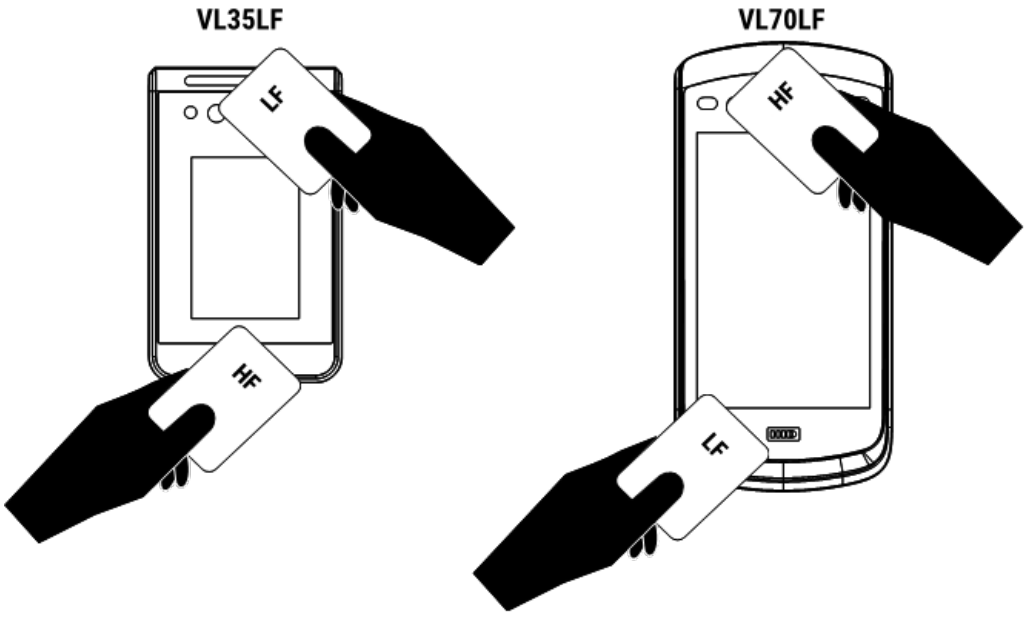
VL35LF

Frequency	Antenna Location	Credential
125 kHz Low Frequency (LF)	Top center	• HID Prox • Indala • EM
13.56 MHz High Frequency (HF)	Bottom center	• HID iCLASS • Seos • MIFARE DESFire • Mobile credentials using NFC technology

VL70LF

Frequency	Antenna Location	Credential
125 kHz Low Frequency (LF)	Bottom left	• HID Prox • Indala • EM
13.56 MHz High Frequency (HF)	Top center	• HID iCLASS • Seos • MIFARE DESFire • Mobile credentials using NFC technology

Note: Mobile credentials using Bluetooth Low Energy can be read from a greater distance and do not require specific positioning.



4.5 Set Elite and MOB keys

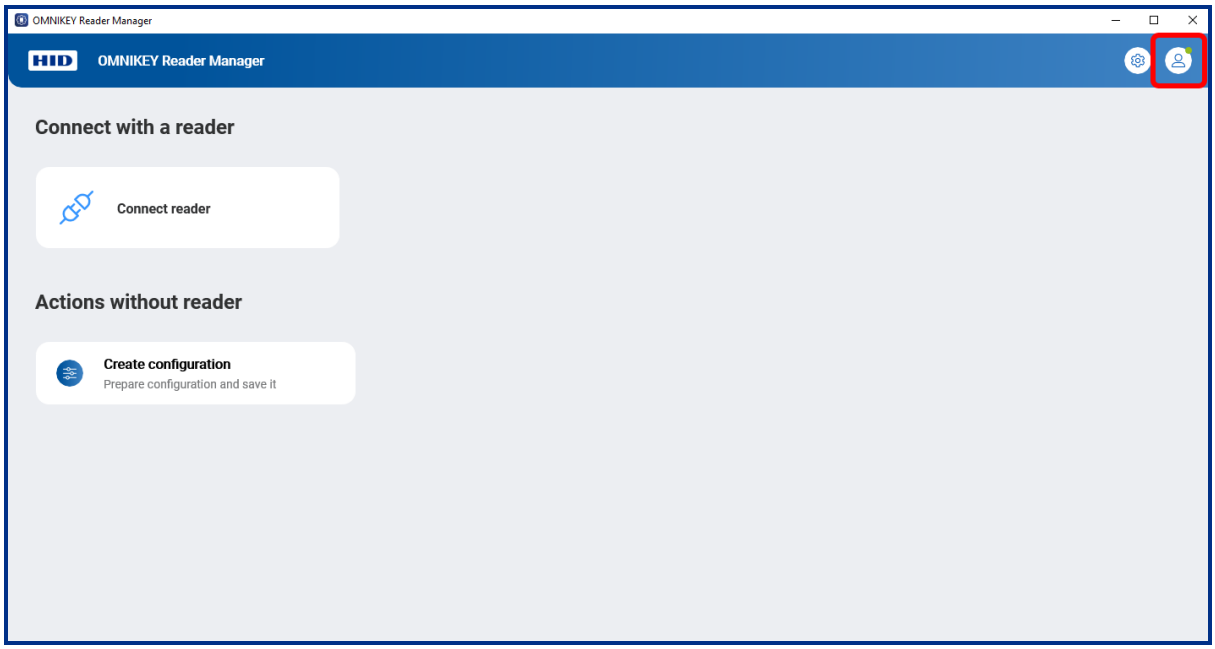
Download the OMNIKEY Reader Manager app (Microsoft Windows only) to load Elite (ICE) and MOB keys. Search the Microsoft Store for “OMNIKEY Reader Manager”.

Note:
- ICE and MOB keys can only be loaded using a Bluetooth LE connection.
- You must have an active HID Origo™ Reader Technician account with ICE and MOB keys assigned.

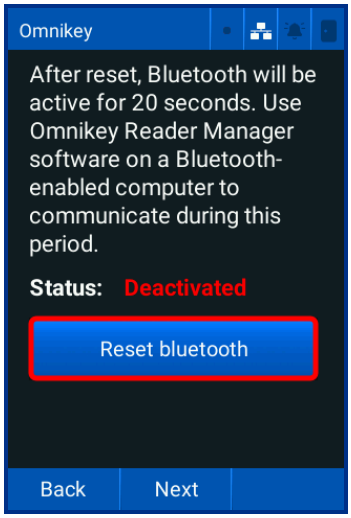
1. Open OMNIKEY Reader Manager.

   Note: Make sure Bluetooth is enabled on your computer via Windows System Settings.

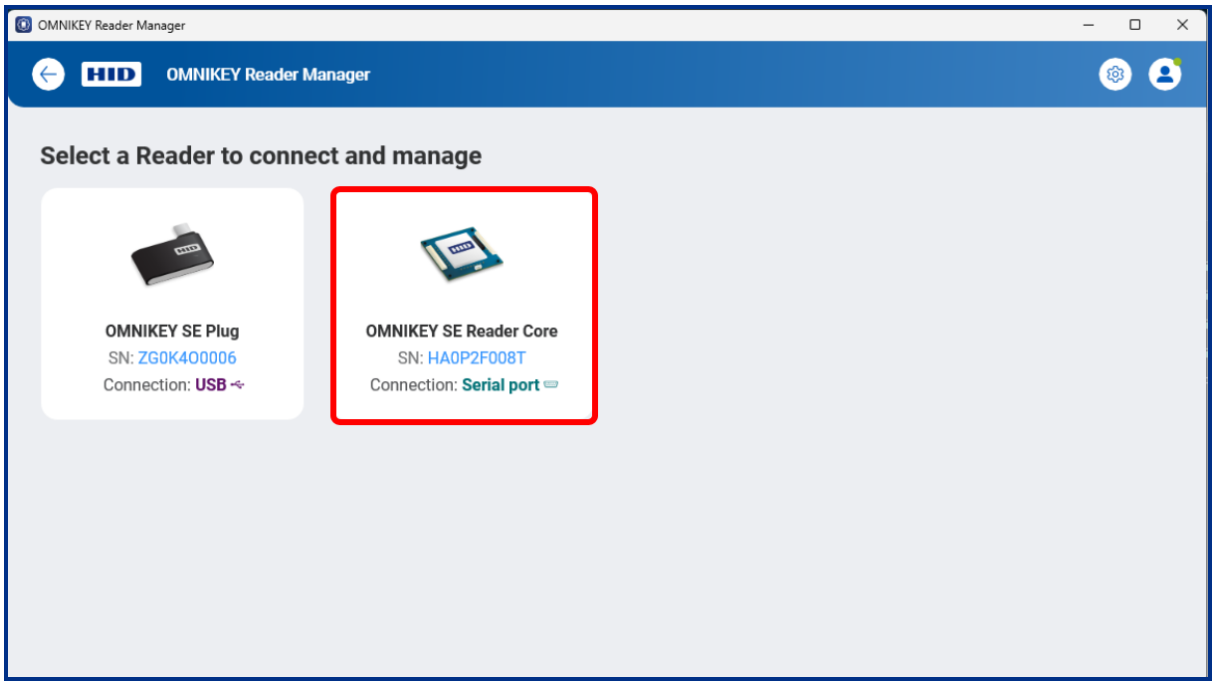
2. Click the **User** icon to log in to your HID Origo Reader Technician account.



3. On the HID Amico reader, tap **Menu** > **Access** > **Identification Methods** > **Card Reading** > **Next** > **Reset bluetooth**.

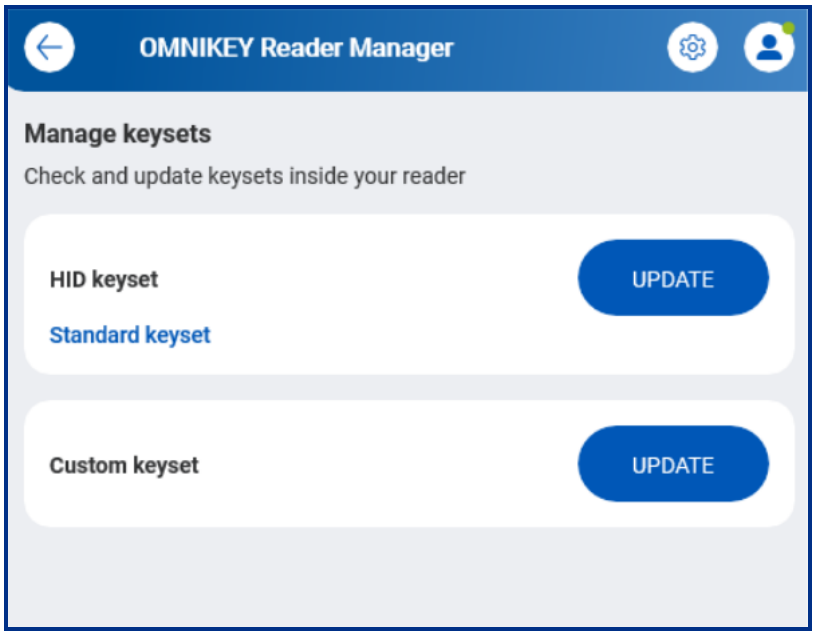


4. Once the reset is complete, communication between the HID Amico reader and OMNIKEY Reader Manager must be established within 20 seconds. If successful, the HID Amico reader will be visible on the OMNIKEY Reader Manager screen. Double click the required reader.

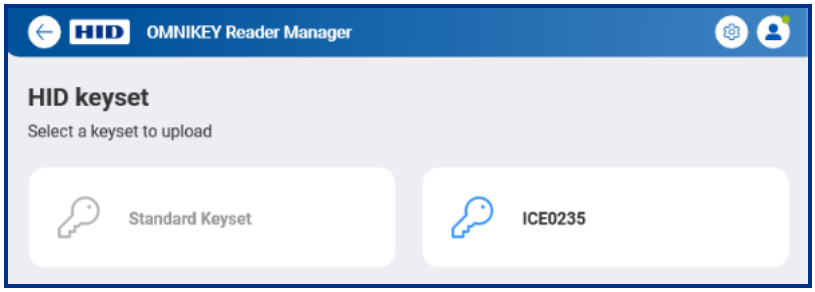


Note: Repeat steps 3 and 4 if the connection times out.

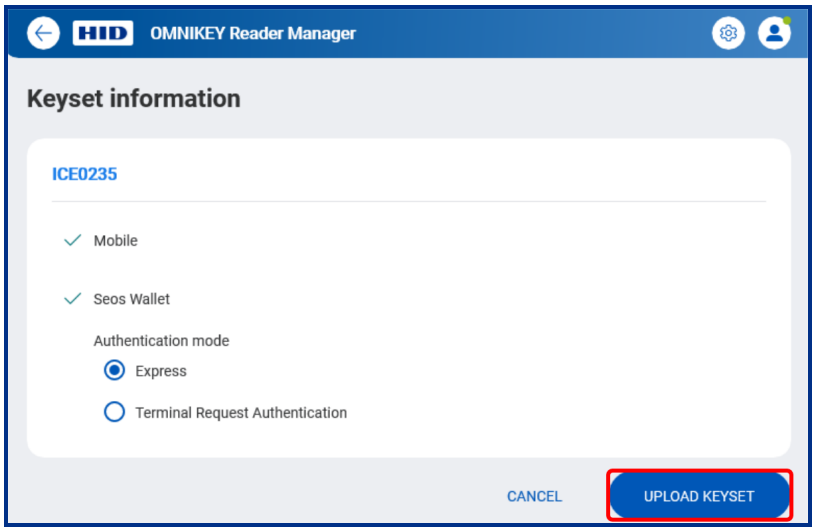
5. Click **Manage Keysets**.
6. Click **UPDATE** for the required keyset.



7. Click the required keyset.

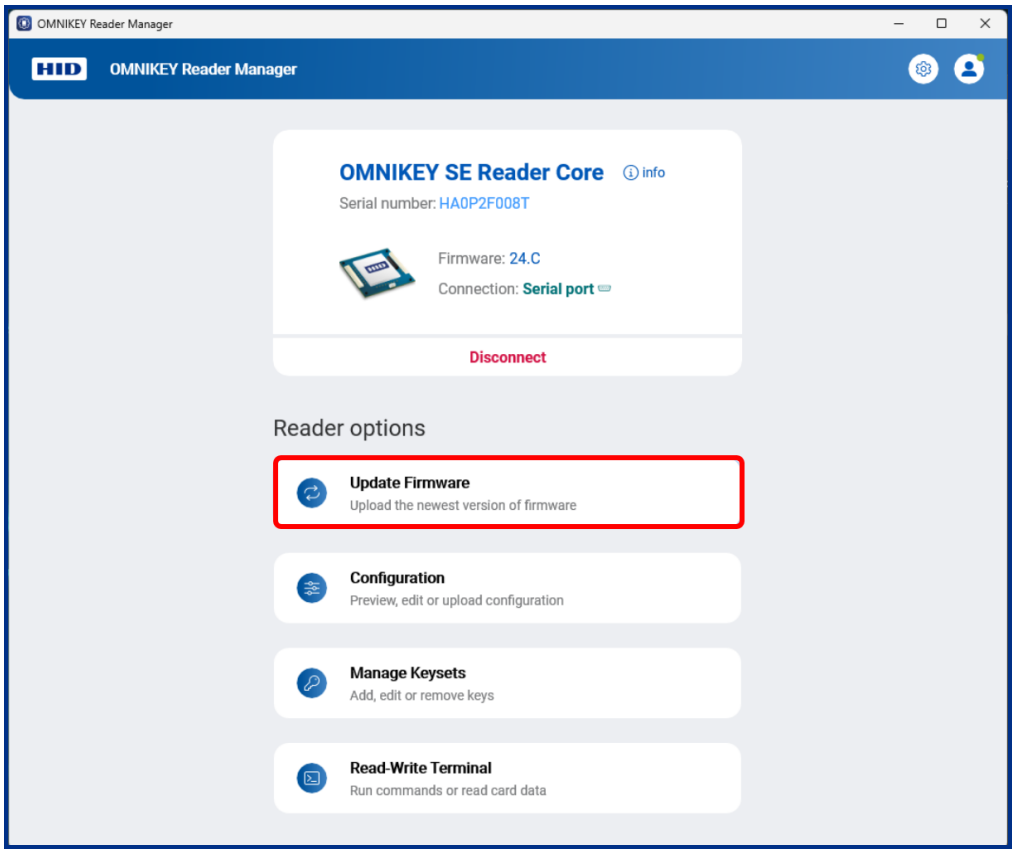


8. Select the required keyset and click **UPLOAD KEYSET**. Secure messages are generated in the cloud and uploaded to the reader. This process can take several seconds.



4.5.1 OMNIKEY Reader Core firmware update via OMNIKEY Reader Manager

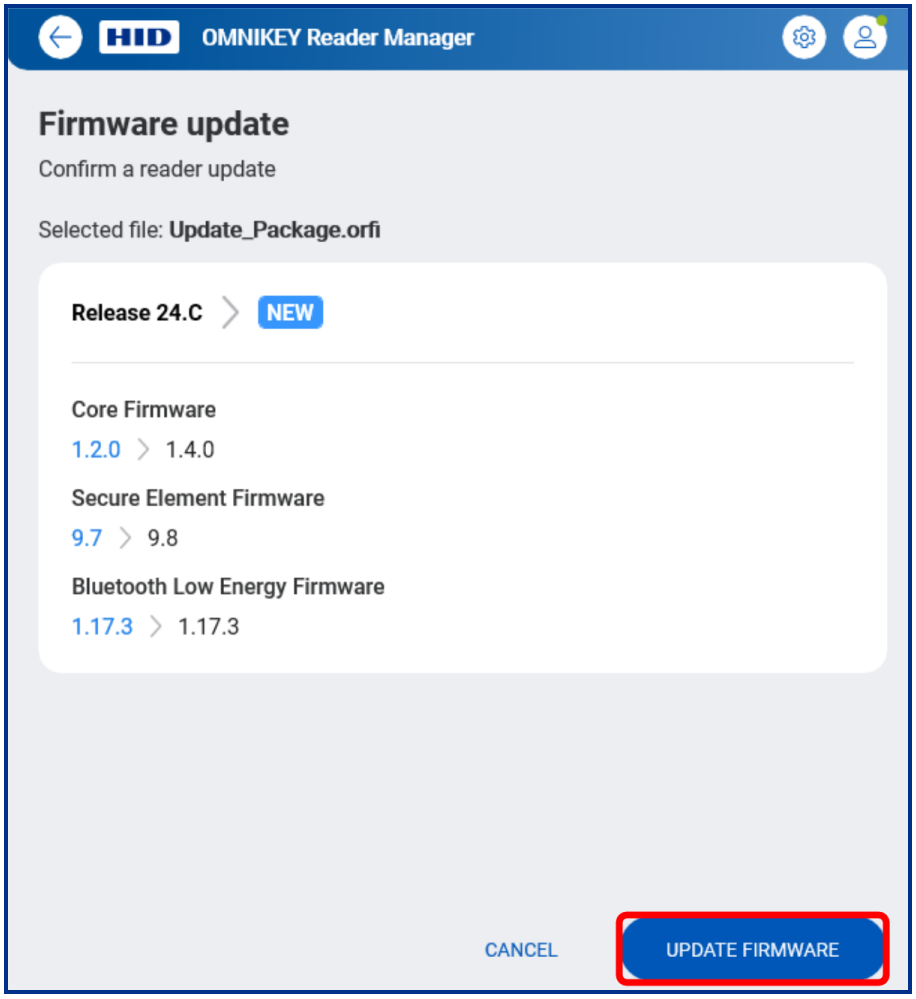
1. Connect to the required device. See **4.5 Set Elite and MOB keys**
2. Click **Update Firmware**.



3. Select the required firmware update file.

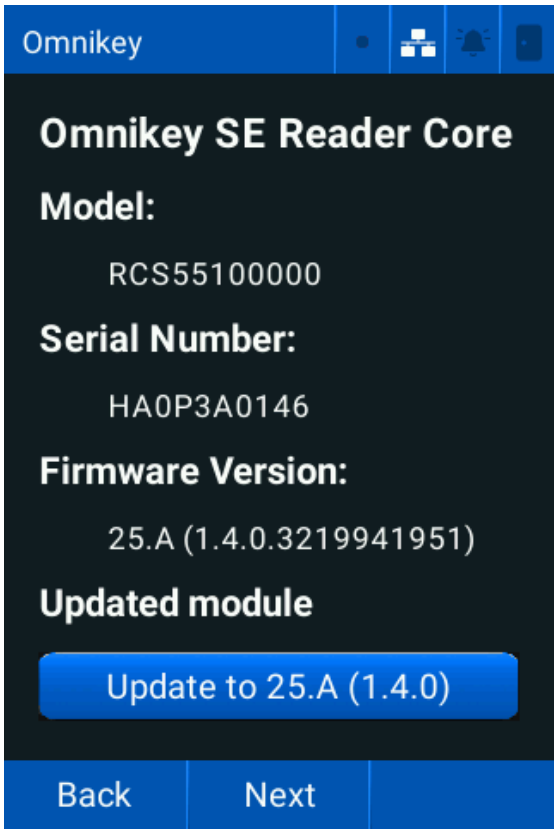
> **Note:** The update package (**.orfi**) can contain firmware updates for one or more readers.

4. The application displays the firmware and version information. Click **UPDATE FIRMWARE**. The update progress is displayed.



4.5.2 OMNIKEY Reader Core firmware update via Amico reader

1. Tap **Menu** > **Access** > **Identification Methods** > **Card Reading**. The **Omnikey SE Reader Core** screen is displayed.

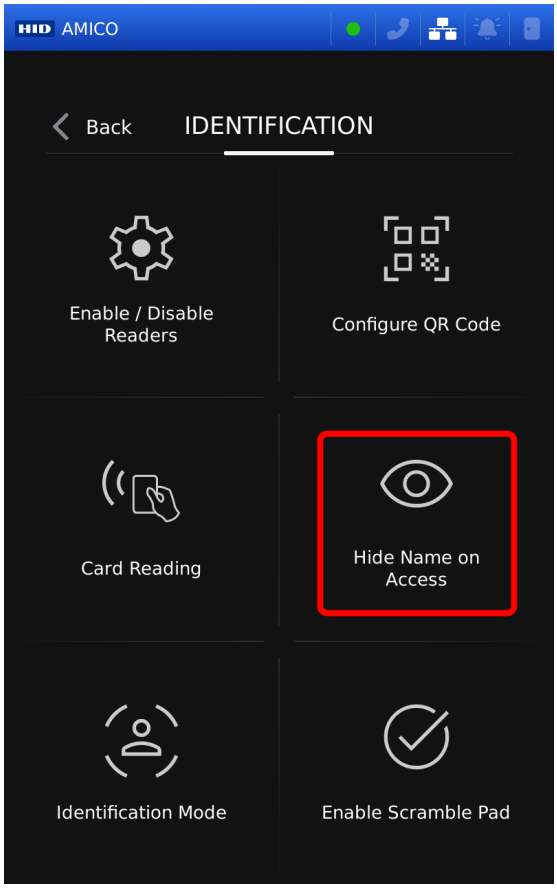


2. Tap **Update to 25.A (1.4.0)**. The update progress is displayed.

4.6 Hide name on access

This allows you to hide the name of the user during an identification event. This prevents a personal name being displayed on the reader screen to help avoid identity theft.

1. Tap **Menu** > **Access** > **Identification Forms** > **Hide Name on Access** to hide the user name on access.



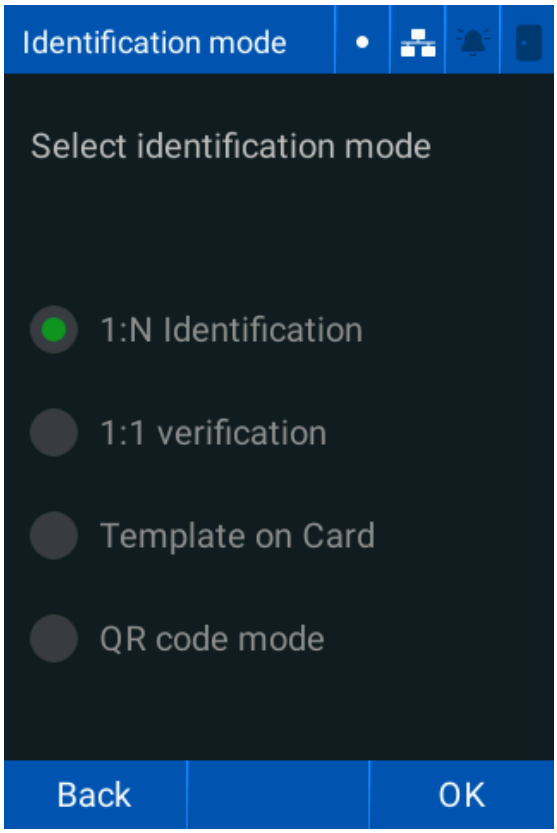
2. Tap **Menu** > **Access** > **Identification Forms** > **Display Name on Access** to display the user name on access.

4.7 Identification mode

This allows you to manage the required level of reader authentication.

Mode	Description
1:N	Single-factor authentication. The reader requires a single form of identification to grant access, for example, **Card**, **Face**, **Pin**, or **Password**.
1:1	Two-factor authentication. The reader requires two forms of identification to grant access, for example, a combination of a **Card** and **Face**.
Template on card	Extracts multiple information stored on a card, such as **User ID** and biometric template.
QR Code	The camera reads a QR code to grant access to the user. Facial recognition is not available in **QR Code** mode.

1. Tap **Menu** > **Access** > **Identification Methods** > **Identification Mode**.

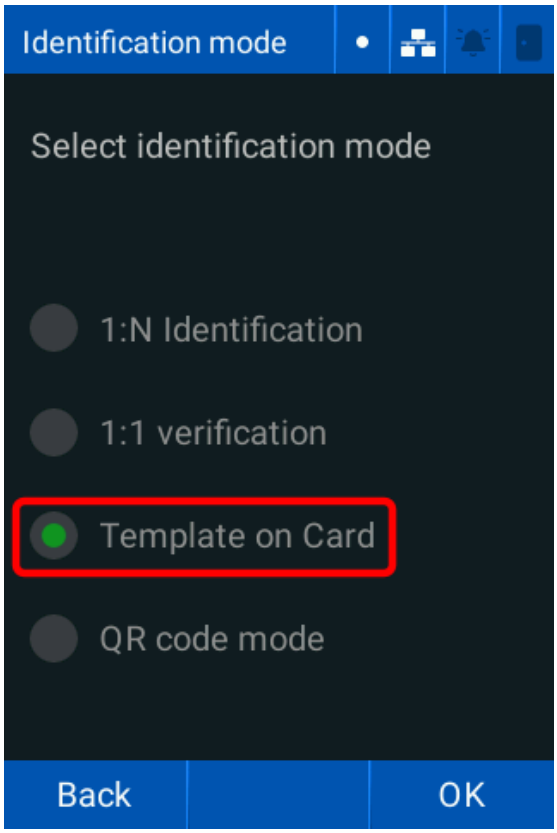


2. Tap the required **Identification mode**.

4.7.1 Enable Template on card

In **Template on card** mode, user records and biometric templates are stored on a card instead of the readers local database.

1. Tap **Menu** > **Access** > **Identification Methods** > **Identification Mode** > **Template on Card**.



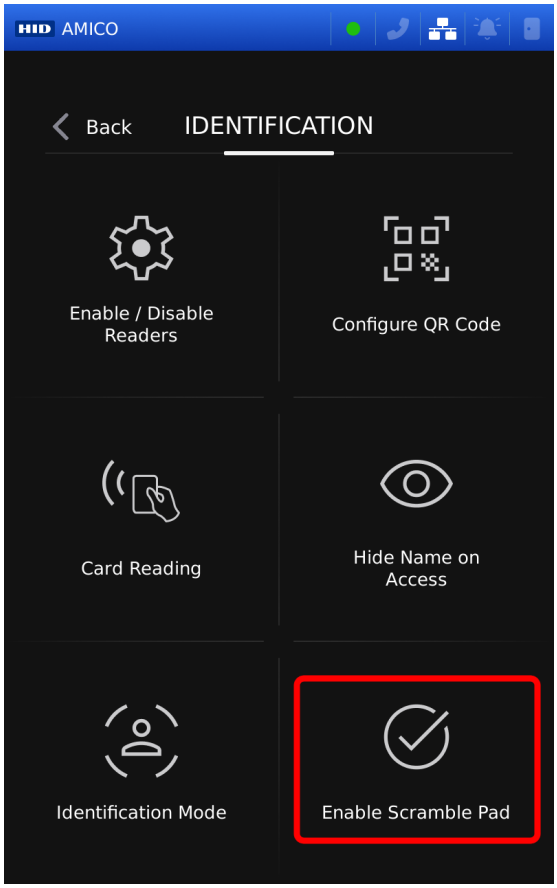
2. Tap **OK** to save.

In **Template on Card** mode, the user must hold their card up to the reader. The reader extracts the face template from the card and matches it to the user standing in front of the reader.

4.8 Enable/disable scramble pad (VL70LF only)

Enabling the scramble pad randomly positions the numeric keypad keys each time it is displayed. The scramble pad is a security feature that stops a user guessing a password if the previous user has left fingerprints on the screen.

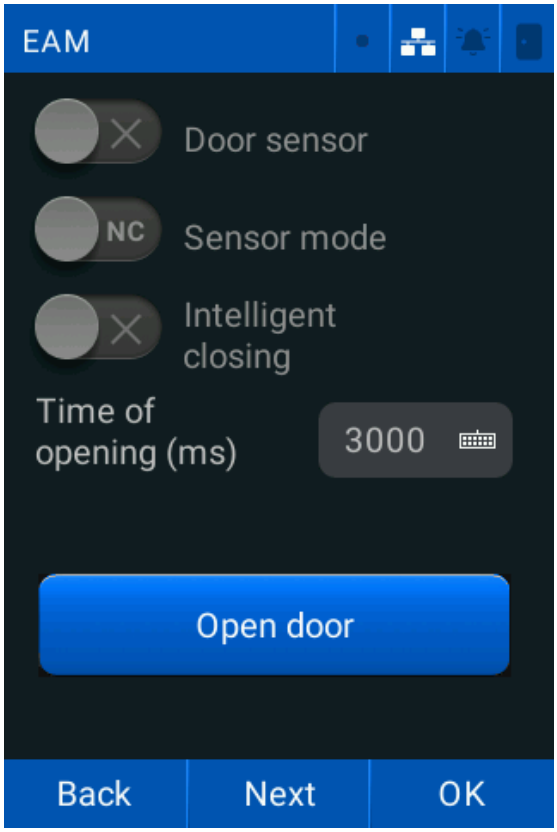
1. Tap **Menu** > **Access** > **Identification Forms** > **Enable Scramble Pad** to enable the scramble keypad.



2. Tap **Menu** > **Access** > **Identification Methods** > **Disable Scramble Pad** to disable the scramble keypad.

4.9 External Access Module

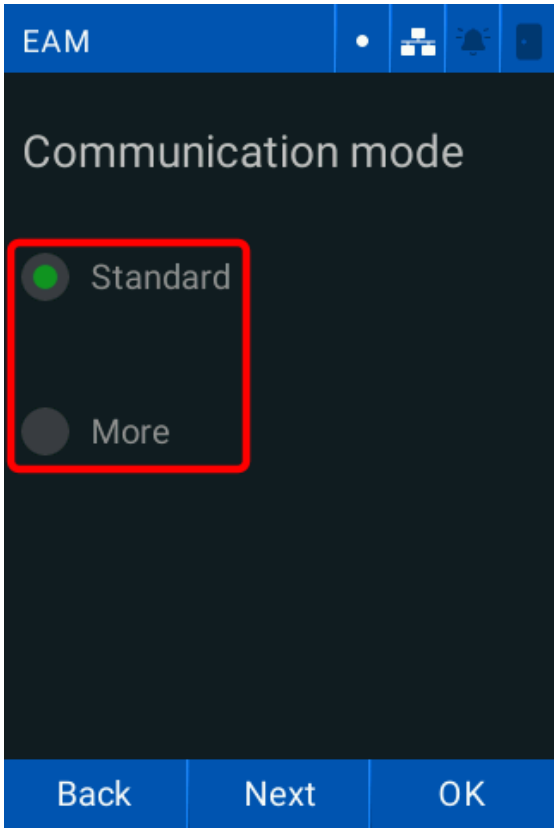
1. Tap **Menu** > **Access** > **EAM**. The **EAM** screen is displayed.



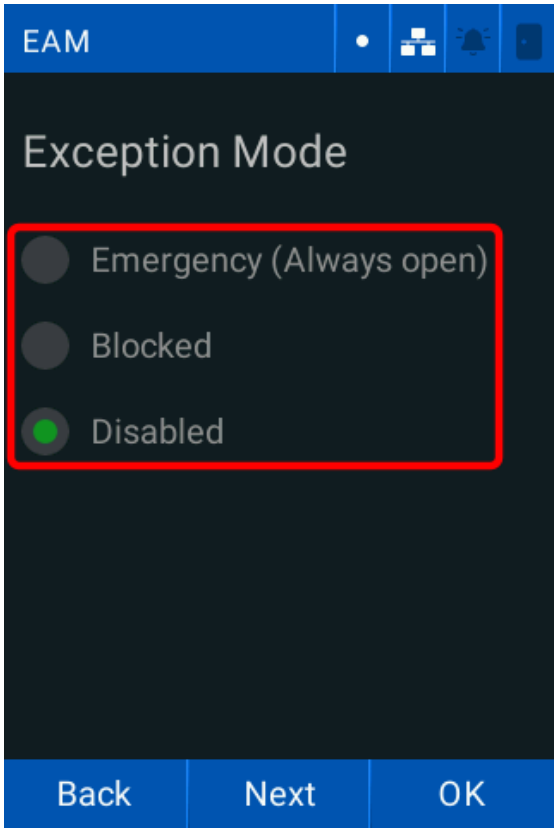
2. Tap the **Door sensor** toggle to activate/deactivate the door sensor.
3. Tap the **Sensor mode** toggle to set the sensor to Normally Open (**NO**) or Normally Closed (**NC**).
4. Tap the **Intelligent closing** toggle to set the relay to close when the door sensor opens.
5. Tap the **Time of opening (ms)** keyboard and enter the duration (milliseconds) that the EAM relay is open. Tap **Next**.

> **Note:** Tap **Open door** to manually open the door relay.

6. Tap the required **Communication mode**:
   - **Standard**: the EAM can communicate with any reader
   - **More**: the EAM only communicates with the reader that configured it

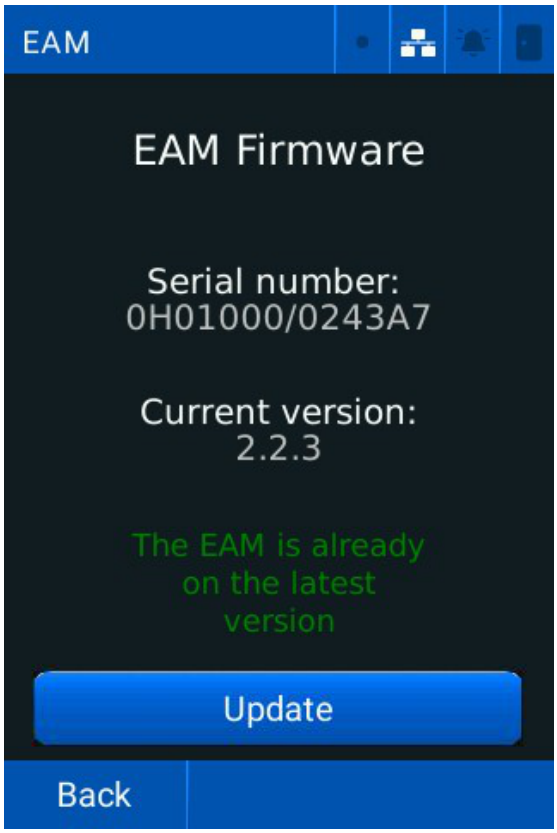


7. Tap **Next** and tap the required **Exception Mode**.
   - **Emergency**: in the case of an emergency, the doors are kept unlocked. This must be set manually.
   - **Blocked**: in the case of a lockdown, the doors are kept locked. This must be set manually.
   - **Disabled**: no exceptions are made. Access control continues as normal.



8. Tap **Next** and tap **Update** to update the EAM firmware version.

   Note: Tap **Back** to return to the previous screen if the EAM firmware is up to date.

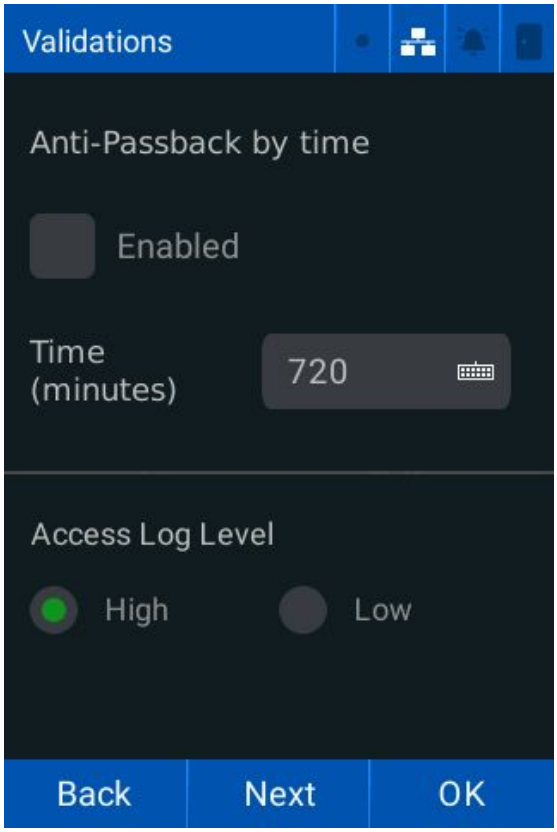


9. Tap **OK**.

4.10 Validations

The **Validations** screen allows you to configure the **Anti-Passback** settings, **Access Log Level** settings, and **Clear Expired User** settings. Anti-passback stops a user entering a location multiple times in a certain time period. To set the time a user must wait before they are granted access:

1. Tap **Menu** > **Access** > **Next** > **Validations**. The **Validations** screen is displayed.



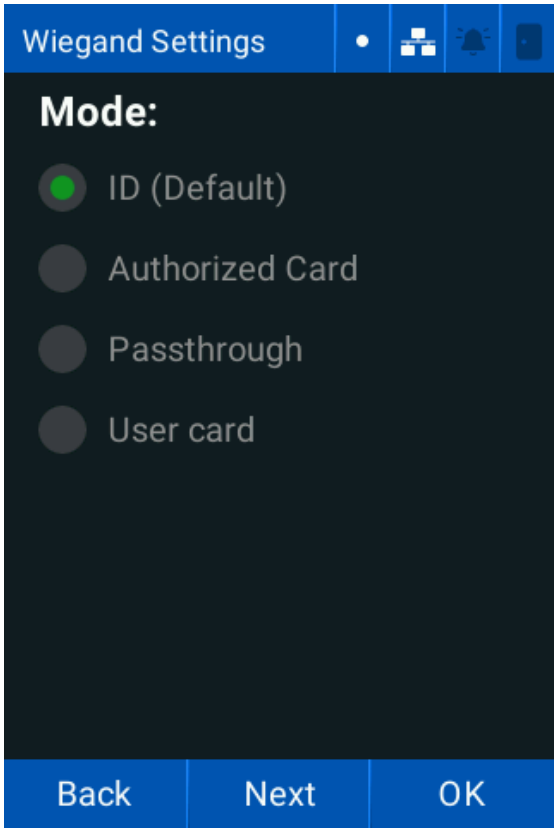
2. Tap the **Enabled** checkbox to enable **Anti-Passback by time**.
3. Tap the **Time (minutes)** keyboard to set the time in minutes.
4. Tap the required **Access Log Level**:
   - **High**: reader records all access attempts
   - **Low**: reader does not log failed access attempts

   Tap **Next** to continue.
5. Tap the required **Clear expired users** option:
   - **All**: deletes all users with an expired **End date**
   - **Visitors**: deletes only visitors with an expired **End date**
   - **Disable**: does not delete any expired users

   > **Note:** The **End date** must be set for expired users to be removed.
6. Tap **OK**.

4.11 Wiegand

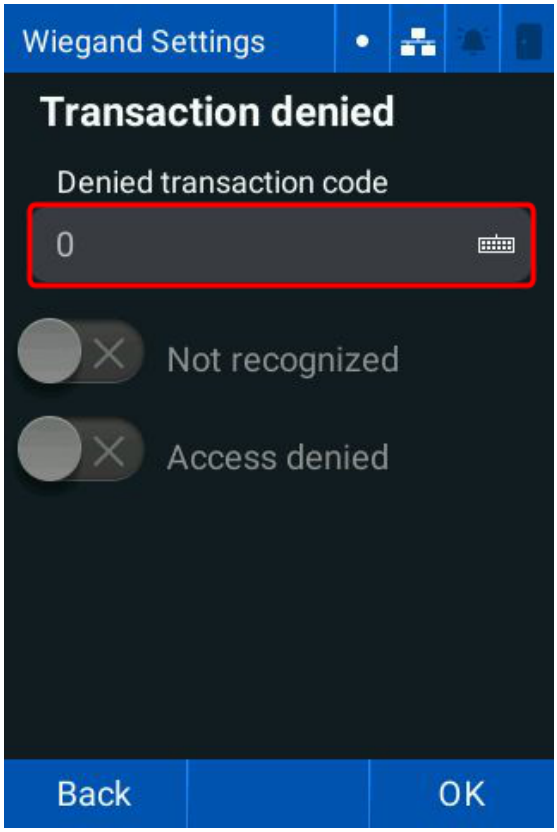
1. Tap **Menu** > **Access** > **Next** > **Wiegand**. The **Wiegand Settings** screen is displayed.



2. Tap the required **Identification Mode**:
   - **ID (default)**: transmits the user ID over Wiegand
   - **Authorized Card**: transmits the authorized card information over Wiegand
   - **Passthrough**: transmits the presented card data without any processing
   - **User card**: transmits only user card information over Wiegand, after a facial recognition
3. Tap **Next** and tap the required **Wiegand format**:
   - **Manual** - a custom Wiegand format defined in the web interface
   - **CSN mifare (32 bits)**
   - **C1K (35 bits)**
   - **W37 (10304)**
   - **W42**
   - **W56**
   - **W66**
   - **W26**
   - **W34**
   - **W37 (10302)**
   - **W40**
   - **C1K (48 bits)**
   - **W64**

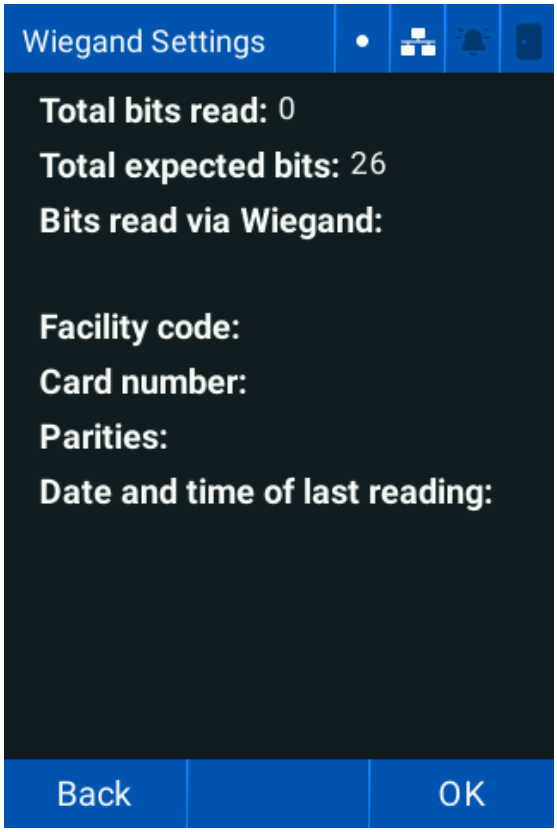
   Tap **Next** to continue.

4. Tap the **Denied transaction code** keyboard and enter the required code to create an unidentified event log.



5. Tap the **Not recognized** toggle to enable/disable not recognized event logs.
6. Tap the **Access denied** toggle to enable/disable access denied event logs.

7. Tap **Next**. The **Wiegand Debug** screen is displayed.

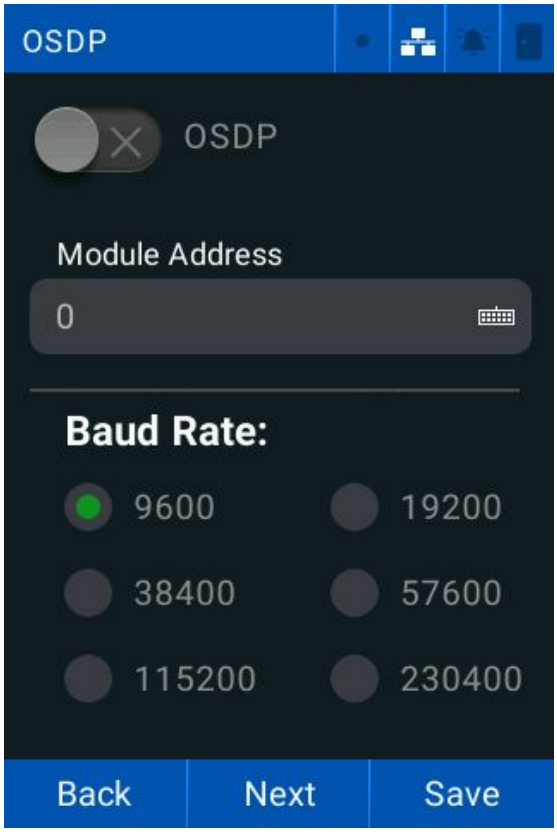


Note: This screen verifies the data received by the readers Wiegand input interface.

8. Tap **OK**.

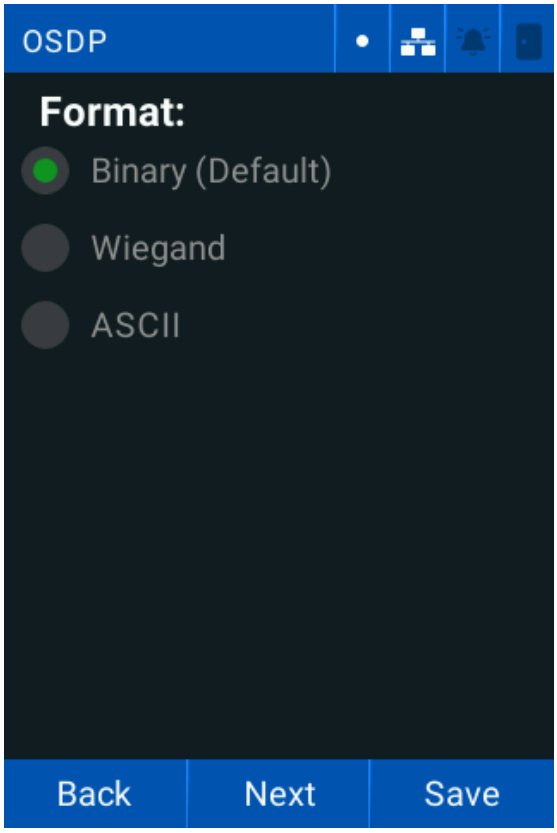
4.12 OSDP

1. Tap **Menu** > **Access** > **Next** > **OSDP**. The **OSDP** screen is displayed.



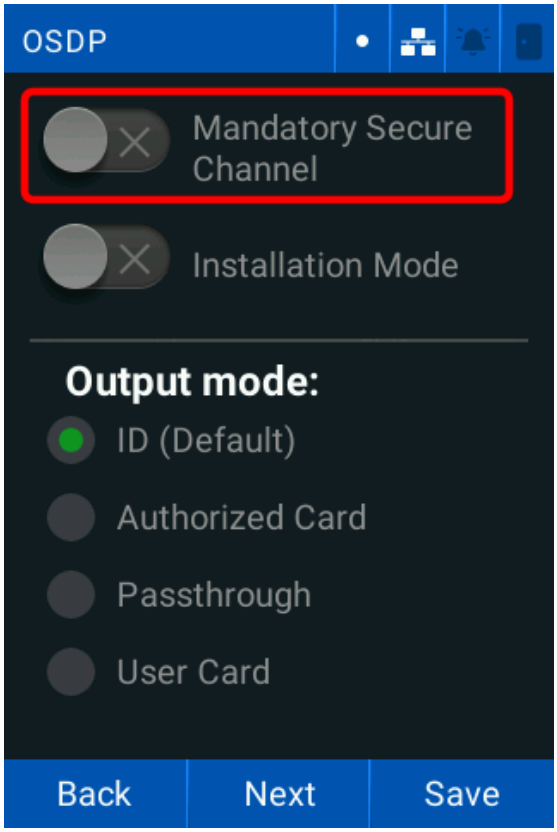
2. Tap the **OSDP** toggle to enable/disable the OSDP protocol.
3. Tap the **Module Address** keyboard and enter the required address.
4. Tap the required **Baud Rate** to set the communication speed of the RS-485 bus for the OSDP protocol. Tap **Next** to continue.

5. Tap the required **Format**.
   - **Binary**: reads directly from the card
   - **Wiegand**: reads Wiegand formats
   - **ASCII**: reads text representation of data



6. Tap the required **Size** if Wiegand is selected. Tap **Next** to continue.

7. Tap the **Mandatory Secure Channel** toggle to enable/disable it. This configures the reader to only work when connected to a secure channel.



8. Tap the **Installation Mode** toggle to enable/disable the on-screen message displaying the installation mode.

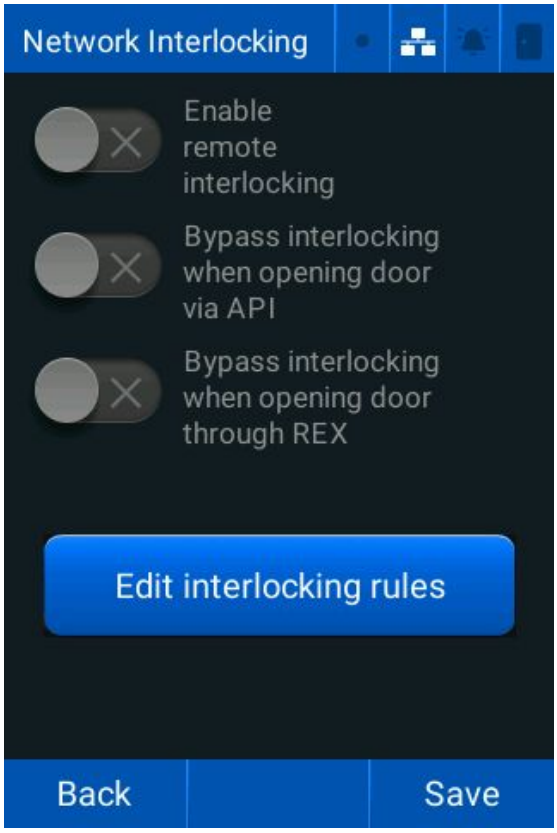
   > **Note:** You must wait for the mandatory OSDP activation to restart before **Installation Mode** is enabled.

9. Tap the required **Output mode**.
10. Tap **Save**.
11. Tap **OK** to restart the reader.

4.13 Global network interlocking

This allows you to configure two readers to connect and control a zone by keeping one of the connected doors always closed. For example, a quarantine zone or mantrap system.

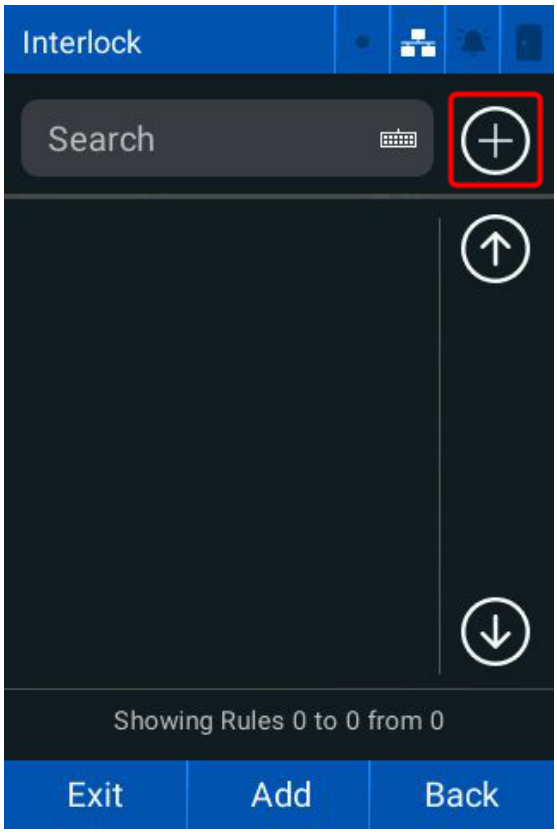
1. Tap **Menu** > **Access** > **Next** > **Global Network Interlocking**. The **Network Interlocking** screen is displayed.



2. Tap the **Enable remote interlocking** toggle to enable/disable remote interlocking.
3. Tap the **Bypass interlocking when opening door via API** toggle to enable/disable bypassing the interlock when opening a door via the API.
4. Tap the **Bypass interlocking when opening door through REX** toggle to enable/disable bypassing the interlock when opening a door via a request to exit button.
5. Tap **Save**.

4.13.1 To add an interlock

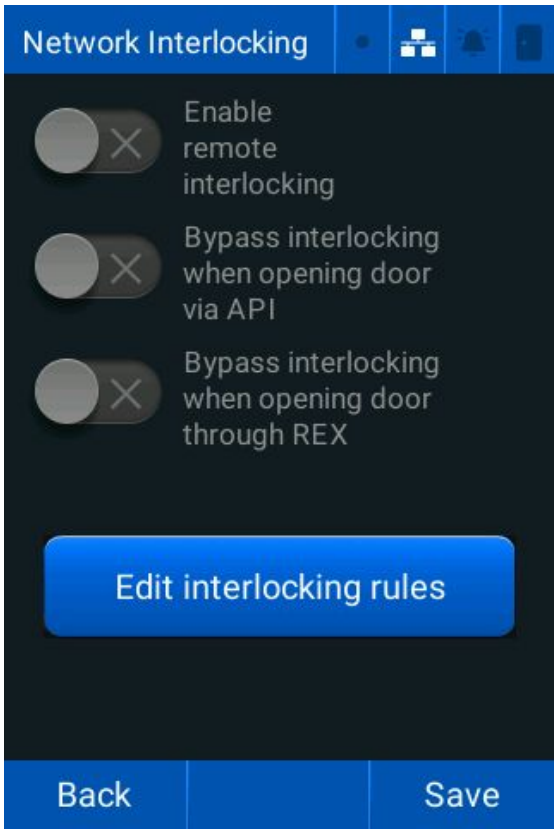
1. Tap **Menu** > **Access** > **Next** > **Global Network Interlocking**.
2. Tap the **Add** icon.



3. Tap the **Rule Name** keyboard and enter the required name.
4. Tap the **Remote Device IP** keyboard and enter the required name.
5. Tap the **Remote Device Login** keyboard and enter the required login.
6. Tap the **Remote Device Password** keyboard and enter the required password.
7. Tap the **Enable rule** toggle to enable the interlocking rule.
8. Tap **Test connection** to test the connection between the two readers.
9. Tap **OK**.

4.13.2 Edit interlocking rules

1. Tap **Menu** > **Access** > **Next** > **Global Network Interlocking**. The **Network Interlocking** screen is displayed.

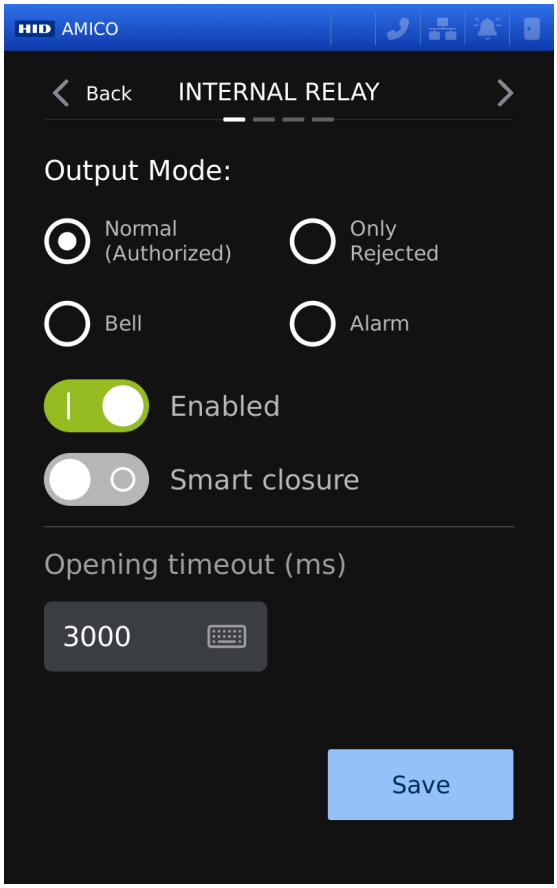


2. Tap **Edit interlocking rules**.
3. Tap the required data fields and make the required changes.
4. Tap **OK**.
5. Tap **Save**.

4.14 Relay and GPIOs (VL70LF only)

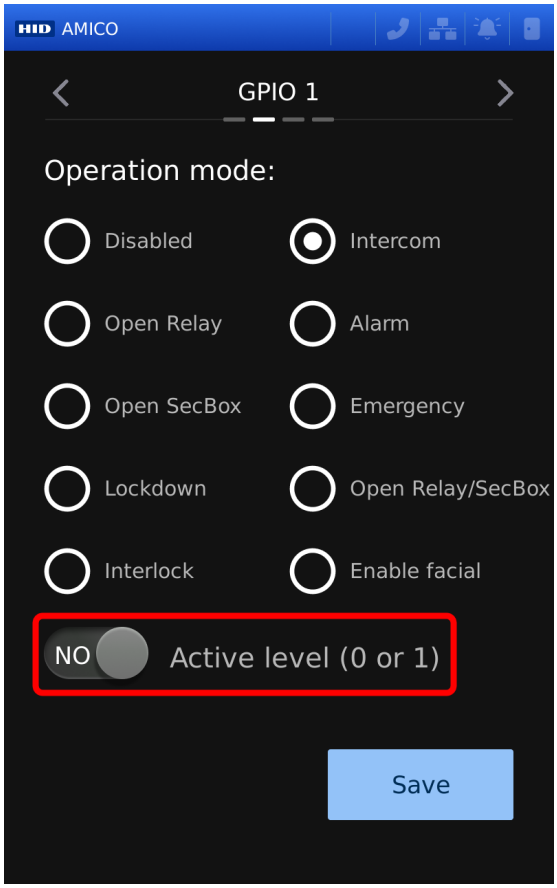
This allows you to set the functionality of the built-in relays and inputs.

1. Tap **Menu** > **Access** > **Next** > **Relay and GPIOs**. The **INTERNAL RELAY** page is displayed.



2. Tap the required **Output Mode**:
   - Normal (Authorized) - the relay is activated when an identification event is authorized
   - Only Rejected - the relay is activated when an identification attempt is rejected
   - Bell - the relay is activated when an operation is performed that activates the devices bell
   - Alarm - the relay is activated when the Panic PIN or Panic Password has been entered
3. Tap the **Enabled** toggle to enable/disable the internal relay.
4. Tap the **Smart closure** toggle to switch off the relay when the door is open.
5. Tap the **Opening timeout (ms)** keyboard and enter the required time in milliseconds. Tap **Next** to continue.

6. Tap the required **Operation mode** for **GPIO 1**:
   - **Disabled** - the input is disabled
   - **Open Relay** - the input activates the internal relay
   - **Open SecBox** - the input activates the EAM relay
   - **Lockdown** - locks the device. No identification is performed.
   - **Interlock** - prevents the door from opening. The door can receive commands to open normally while the GPIO is idle.
   - **Intercom** - the input initiates a call via the SIP intercom (doorbell)
   - **Alarm** - the input triggers an alarm event
   - **Emergency** - the input triggers an emergency event
   - **Open Relay/SecBox** - the input activates both the internal and EAM relays
   - **Enable facial** - the input enables the facial identification cameras
7. Tap the **Active level (0 or 1)** toggle to switch between Normally Open (**NO**) and Normally Closed (**NC**).

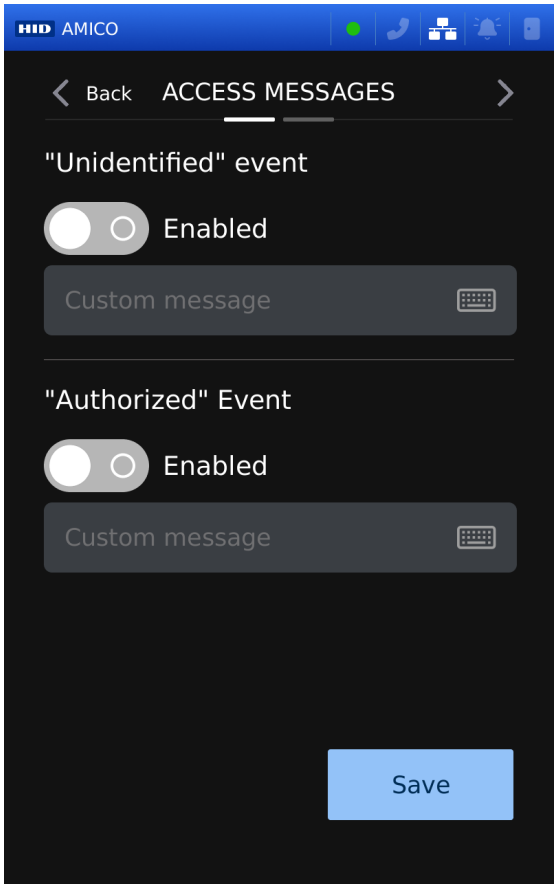


Note: Tap **Next** to repeat steps 6 and 7 for GPIO 2 and GPIO 3 if used.

8. Tap **Save**.

4.15 Custom messages

1. Tap **Menu** > **Access** > **Access Messages**. The **ACCESS MESSAGES** screen is displayed.



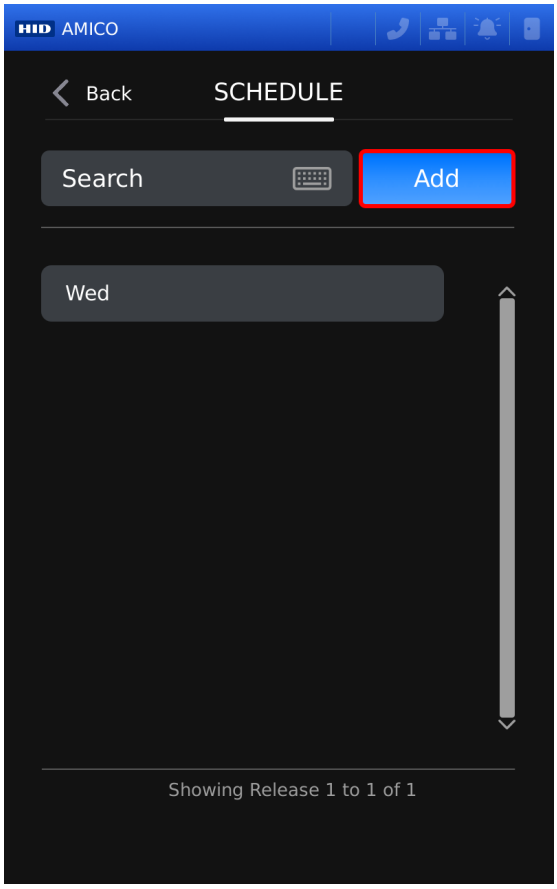
2. Tap the **"Unidentified" event** toggle to enable the audio message. Tap the **Custom message** keyboard and enter the required message.
3. Tap the **"Authorized" Event** toggle to enable the audio message. Tap the **Custom message** keyboard and enter the required message. Tap  **Next** for more events.
4. Tap the required **"Unauthorized" event** audio message. Tap the **Custom message** keyboard and enter the required message.
5. Tap the required **"Wear Mask" event** audio message. Tap the **Custom message** keyboard and enter the required message.
6. Tap **Save**.

4.16 Scheduled release (VL70LF only)

This allows you to configure a time period that the door stays unlocked.

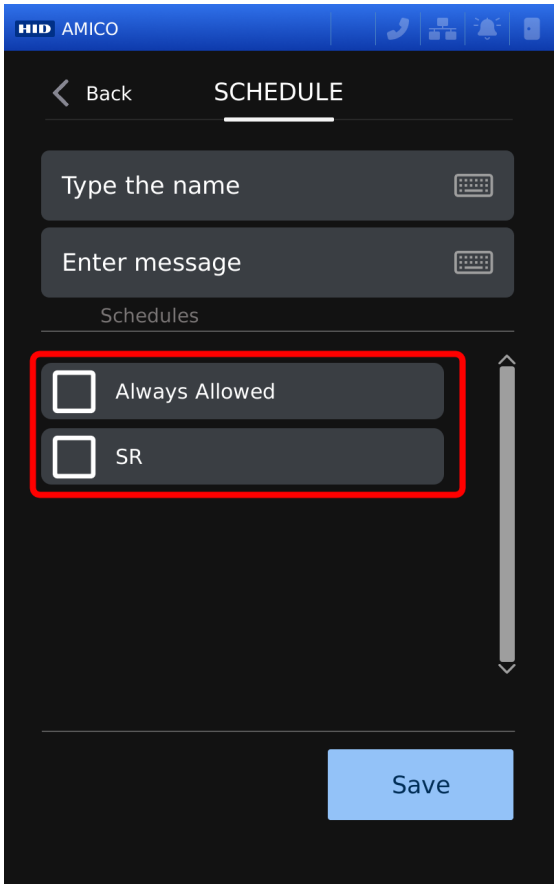
> **Note:** Schedules must be created before a scheduled release can be configured. See **2.7 Schedules** for more information on creating schedules.

1. Tap **Menu** > **Access** > **Next** > **Scheduled Release**. The **SCHEDULE** page is displayed.
2. Tap **Add** to add a release schedule.



3. Enter the required schedule name.
4. Enter a description or message to describe the release schedule.

5. Tap the checkbox of the required schedules for the release schedule.



6. Tap **Save**.

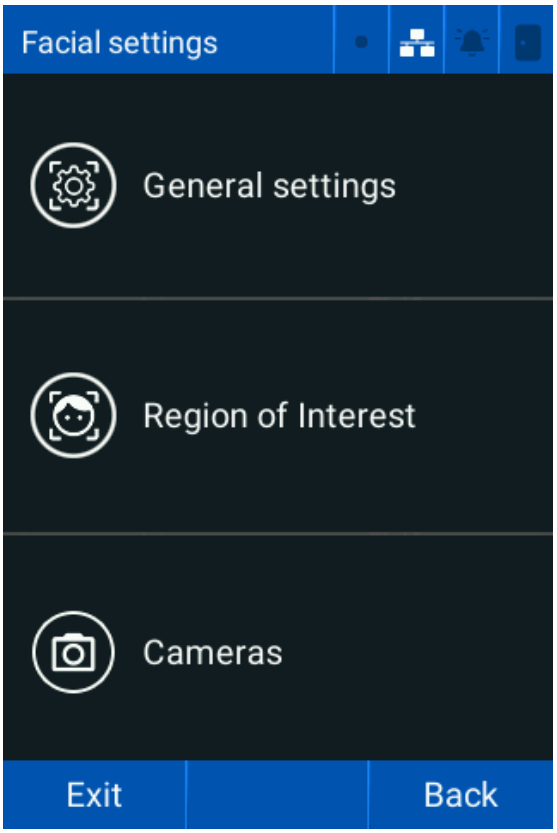
Section 05

Facial settings

5.1 Facial settings

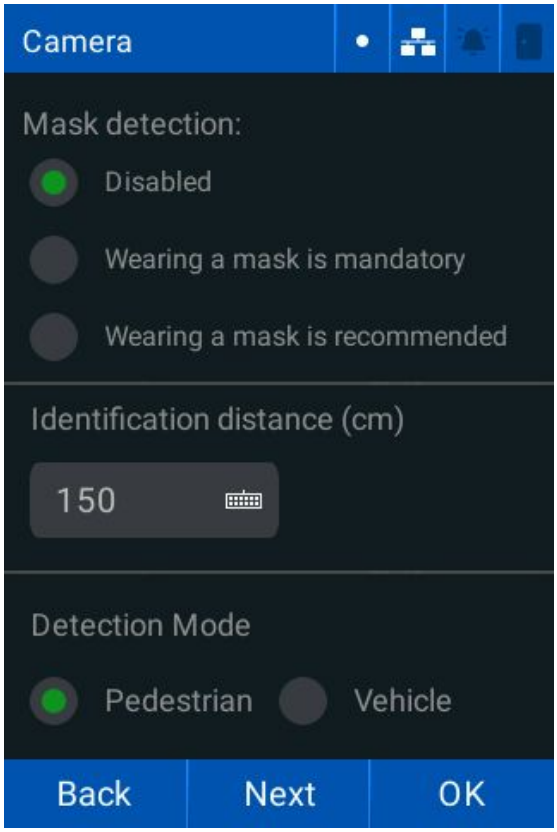
The **Facial Settings** screen allows you to adjust all camera, video, and facial identification settings.

Tap **Menu** > **Facial Settings**. The **Facial Settings** screen is displayed.



5.2 General settings

1. Tap **Menu** > **Facial settings** > **General settings**. The **Camera** screen is displayed.

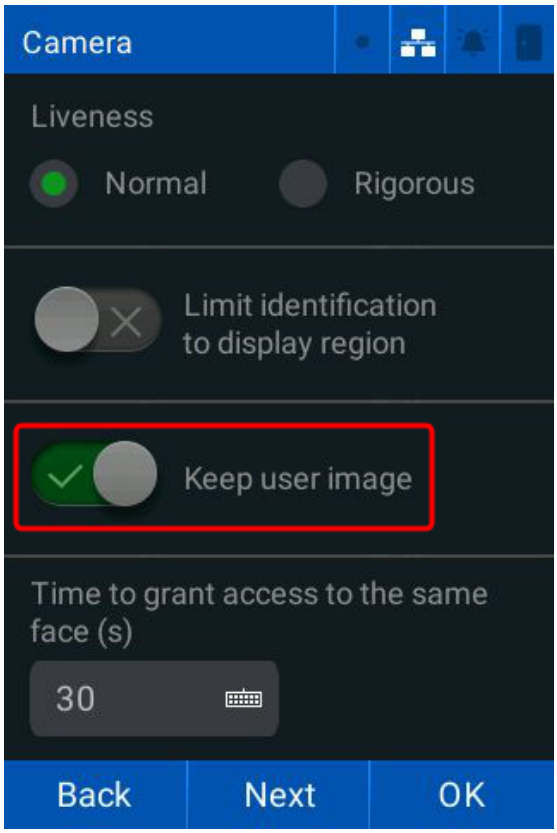


2. Tap the required **Mask detection** setting:
   - **Disabled**
   - **Wearing a mask is mandatory**
   - **Wearing a mask is recommended**
3. Tap the **Identification distance (cm)** keyboard and enter the required distance in centimeters.
4. Tap the required **Detection Mode**:
   - **Pedestrian**
   - **Vehicle**

   Tap **Next** to continue.
5. Tap the required **Liveness** mode:
   - **Normal** (default): normal environments
   - **Rigorous**: environments with poor lighting
6. Tap the **Limit identification to display region** toggle to only identify faces in the region of interest.

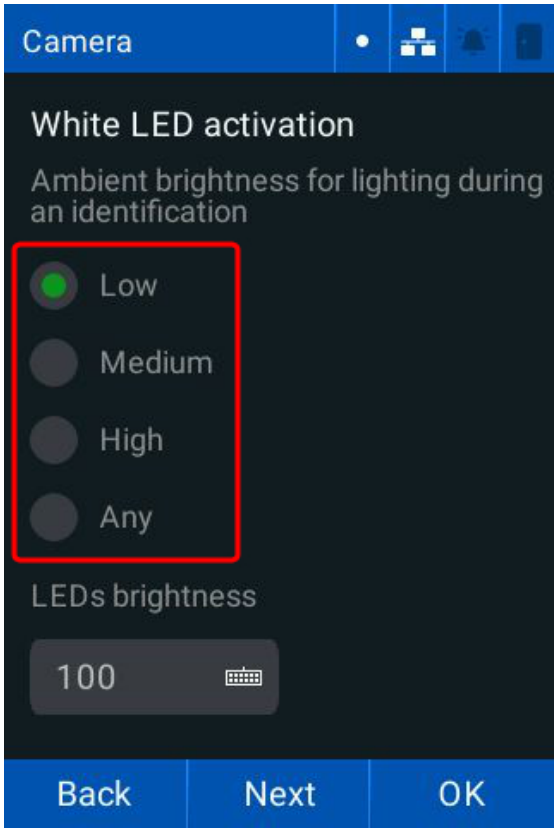
7. Tap the **Keep user image** toggle to keep/remove user photos after enrollment.

   Note: Depending on reader model, HID Amico readers with extended user capacity may not support user image storage.



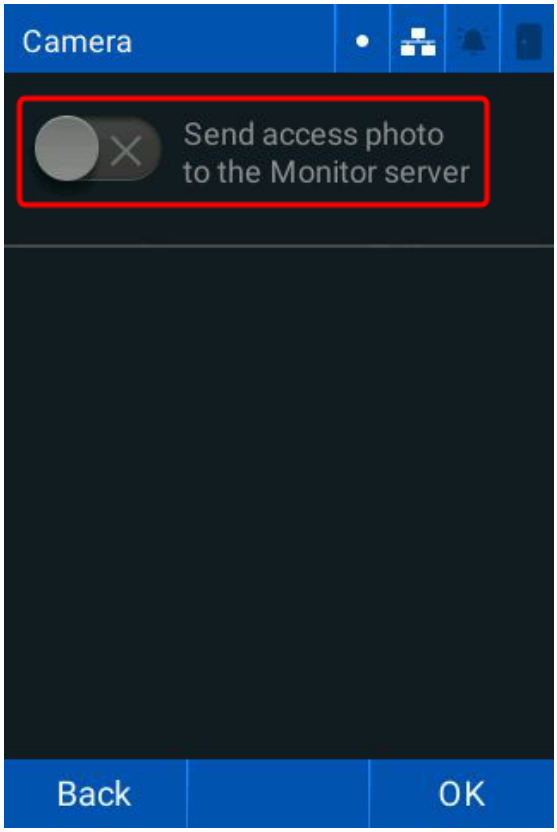
8. Tap the **Time to grant access to the same face (s)** keyboard and enter the duration a user must wait to be identified after their last facial identification. Tap **Next** to continue.

9. Tap the required **White LED activation** brightness.
   - **Low**
   - **Medium**
   - **High**
   - **Any**



10. Tap the **LEDs brightness** keyboard to enter the required LED brightness (**1**-**100**). Tap **Next** to continue.

11. Tap **Send access photo to the Monitor server** toggle to send the access photo of the identified user to the Monitor server.



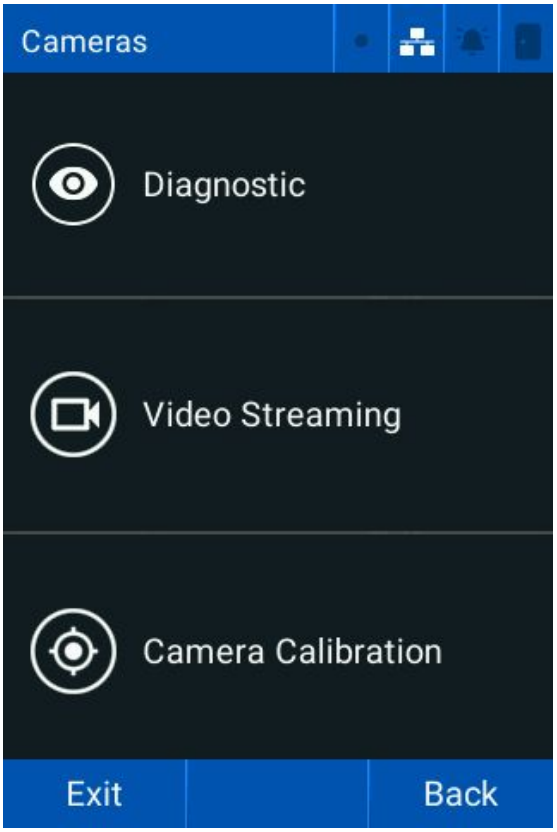
12. Tap **OK**.

5.3 Region of interest

1. Tap **Menu** > **Facial settings** > **Region of Interest**. The **Region of Interest** adjustment screen is displayed.
2. Make the required adjustments:
   - **Vertical Image Shift**: moves the region of interest up or down
   - **Zoom**: zooms in or out
3. Tap **Confirm**.

5.4 Cameras

Tap **Menu** > **Facial settings** > **Cameras**. The **Cameras** menu screen is displayed.



5.4.1 Diagnostics

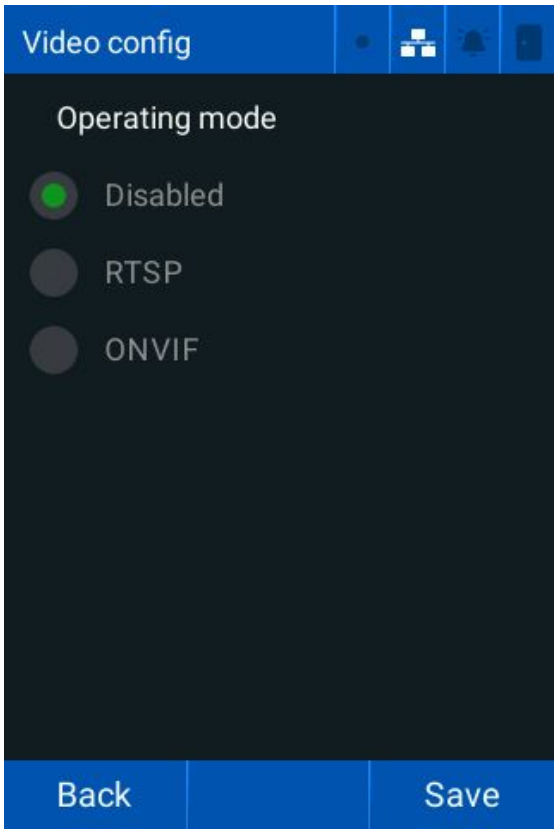
1. Tap **Menu** > **Facial settings** > **Cameras** > **Diagnostic**.
2. Tap **White LEDs** to test that the white LEDs are operating.
3. Tap **IR LEDs** to test that the infrared LEDs are operating.
4. Tap **Infrared/Colored** to alternate between the infrared camera and color camera.
5. Tap **Back** to return to the previous menu.

5.4.2 Video streaming (VL35LF)

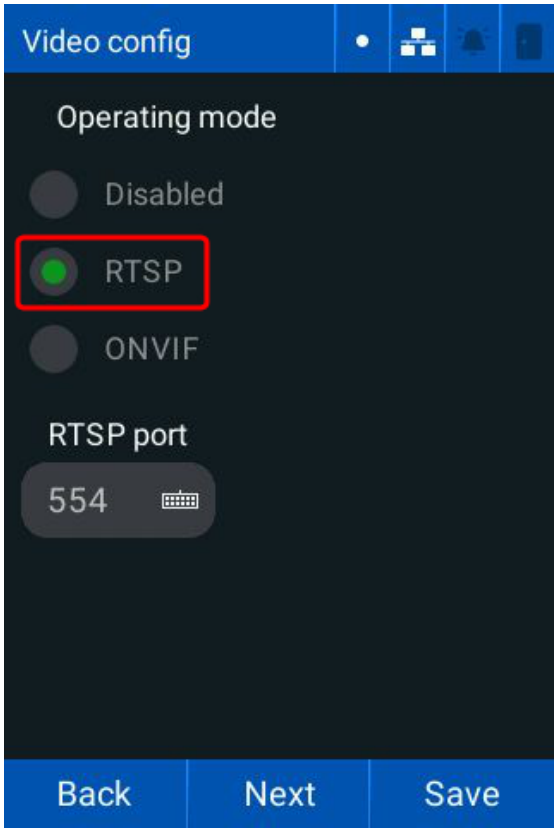
This allows you to configure the reader to stream video from the camera via RTSP, or ONVIF protocols.

RTSP

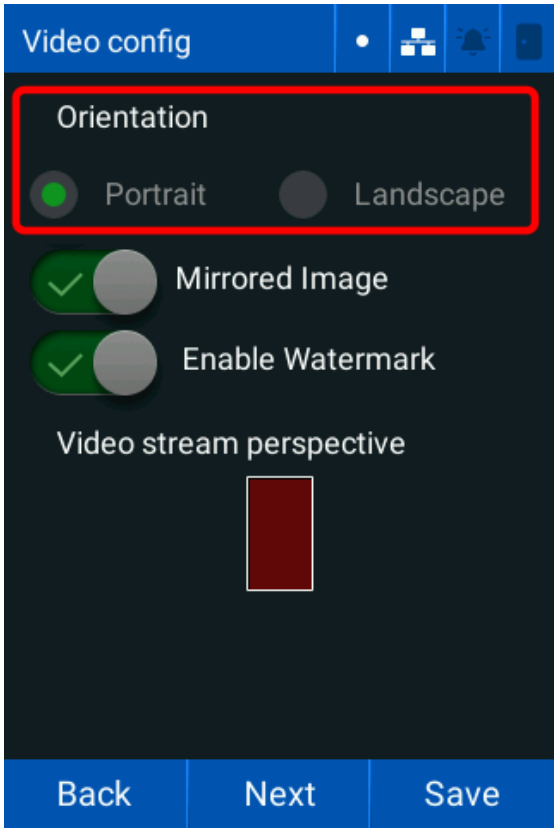
1. Tap **Menu** > **Facial settings** > **Cameras** > **Video Streaming**. The **Video config** screen is displayed.



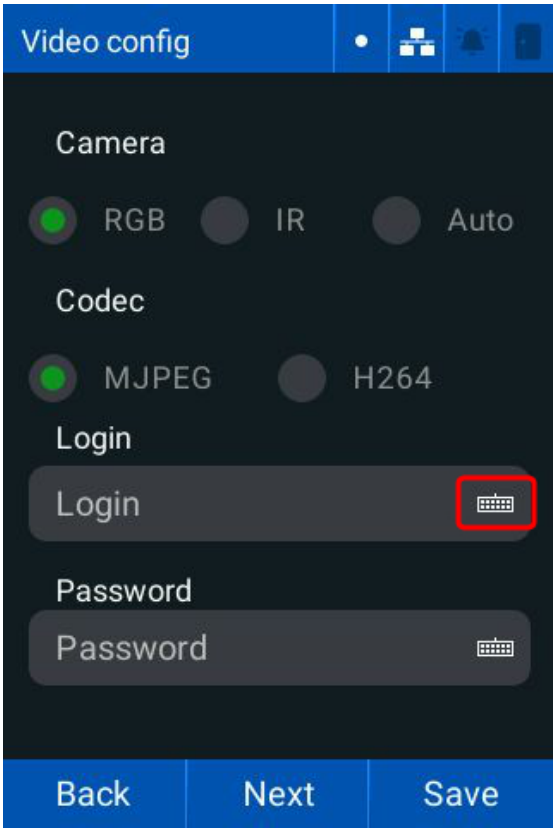
2. Tap **RTSP**.



3. Tap the **RTSP port** keyboard and enter the required port (554 by default). Tap **Next** to continue.
4. Tap the required video **Orientation**.

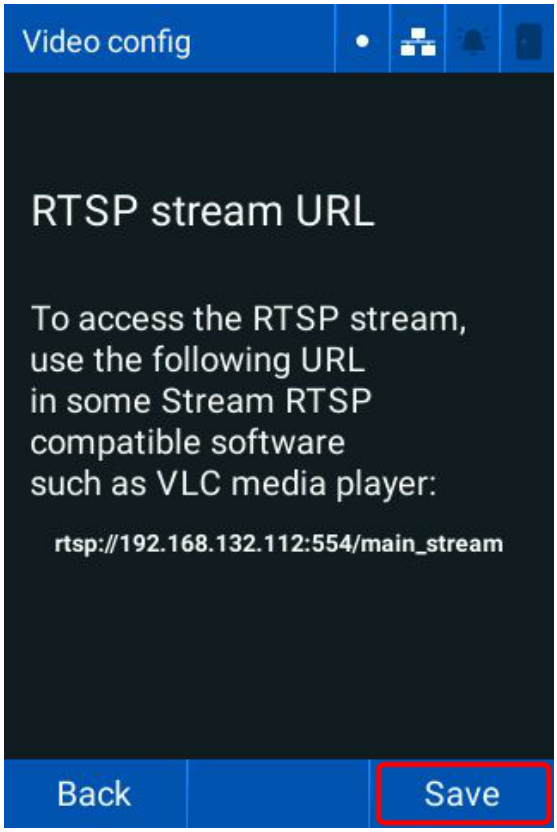


5. Tap the **Mirrored Image** toggle to flip the image horizontally.
6. Tap the **Enable Watermark** toggle to enable/disable the watermark that appears on the facial recognition screen. Tap **Next** to continue.
7. Tap the required **Camera Configuration**:
   - **RGB** (default)
   - **IR** (InfraRed)
   - **Auto**
8. Tap the required **Codec**:
   - **MJPEG** (default)
   - **H264**
9. Tap the **Login** keyboard and enter the required login.



10. Tap the **Password** keyboard and enter the required password. Tap **Next** to continue.

11. Tap **Save** to use the **RTSP stream URL** with compatible software (for example, VLC media player or Windows media player).

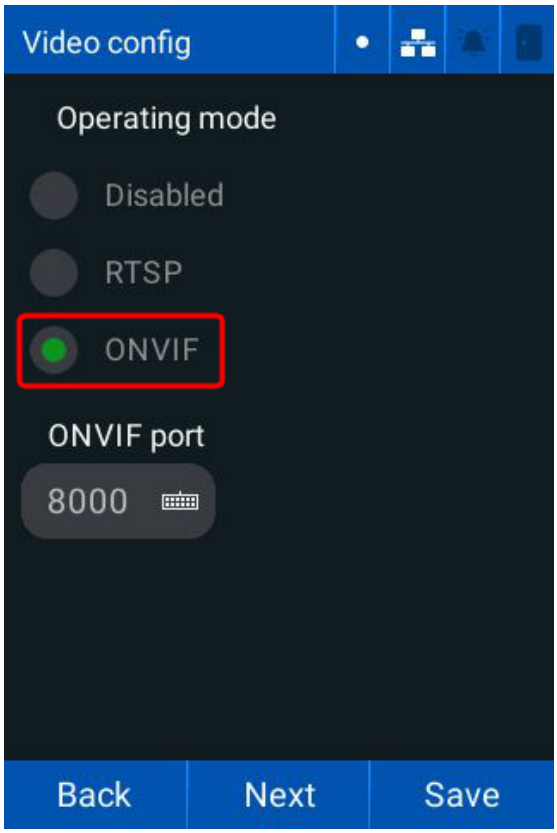


> **Note:** Write down the URL for future use.

12. Restart the reader for the configuration changes to take effect. See **7.15 Restart** for more information.

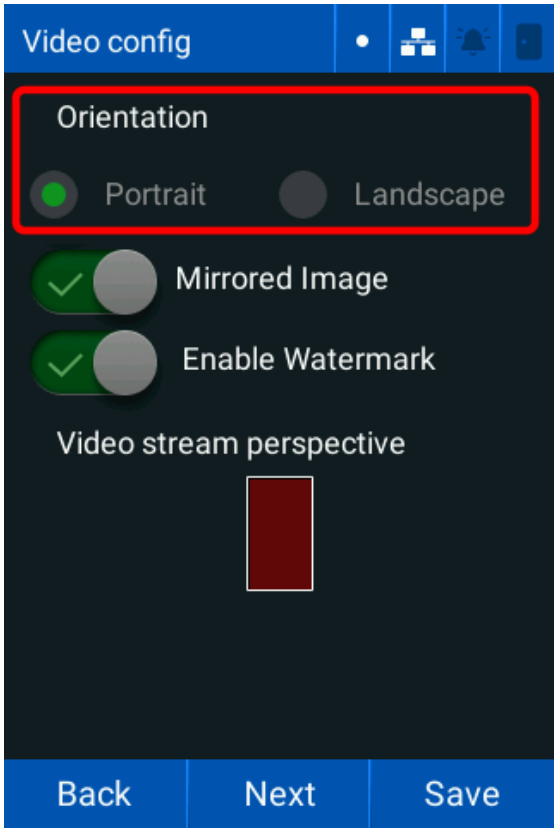
ONVIF streaming

1. Tap **Menu** > **Facial settings** > **Cameras** > **Video Streaming**. The **Video config** screen is displayed.
2. Tap **ONVIF**.



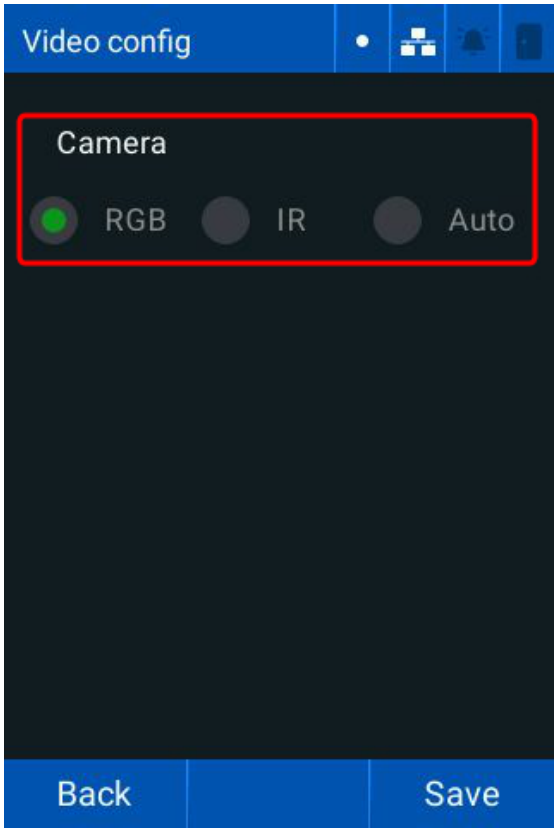
3. Tap the **ONVIF Port** keyboard and enter the required port (8000 by default). Tap **Next** to continue.

4. Tap the required **Orientation**.



5. Tap the **Mirrored Image** toggle to flip the image horizontally.
6. Tap the **Enable Watermark** toggle to enable/disable the watermark that appears on the facial recognition screen. Tap **Next** to continue.

7. Tap the required **Camera Configuration**:
   - **RGB** (default)
   - **IR** (InfraRed)
   - **Auto**



8. Tap **Save**.
9. Restart the reader for the configuration changes to take effect. See **7.15 Restart** for more information.

Note:
- ONVIF uses the default credentials:
  - Login - **admin**
  - Password - **admin**
- ONVIF streaming only works if RTSP is active and operating correctly.

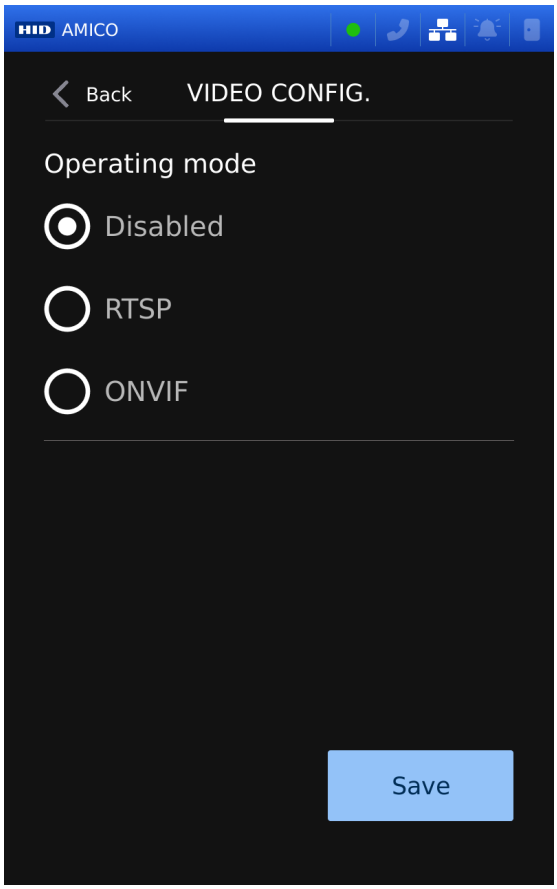
Optionally, validate the ONVIF Streaming using the **ONVIF Device Manager**.

5.4.3 Video streaming (VL70LF)

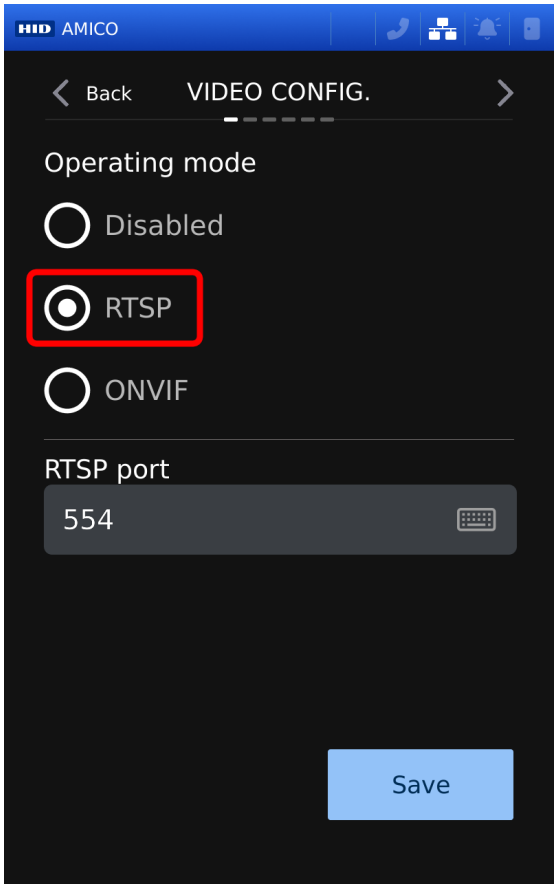
This allows you to configure the reader to stream video from the camera via RTSP, or ONVIF protocols.

RTSP

1. Tap **Menu** > **Facial settings** > **Video Streaming**. The **Video config** screen is displayed.

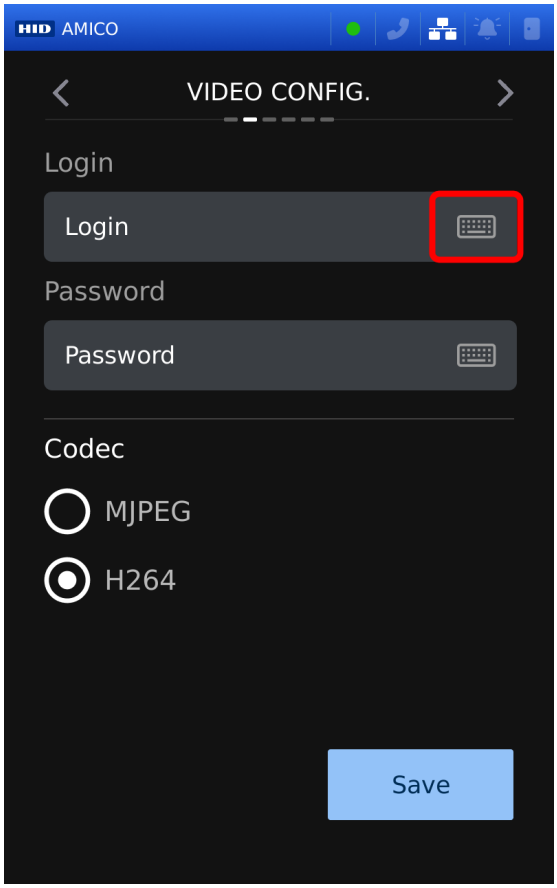


2. Tap **RTSP**.



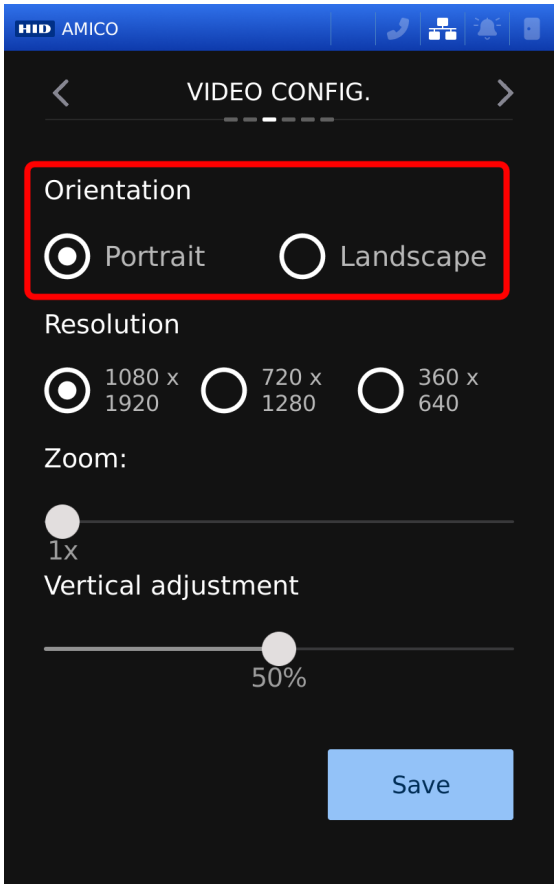
3. Tap the **RTSP port** keyboard and enter the required port (554 by default). Tap **Next** to continue.

4. Tap the **Login** keyboard and enter the required login.



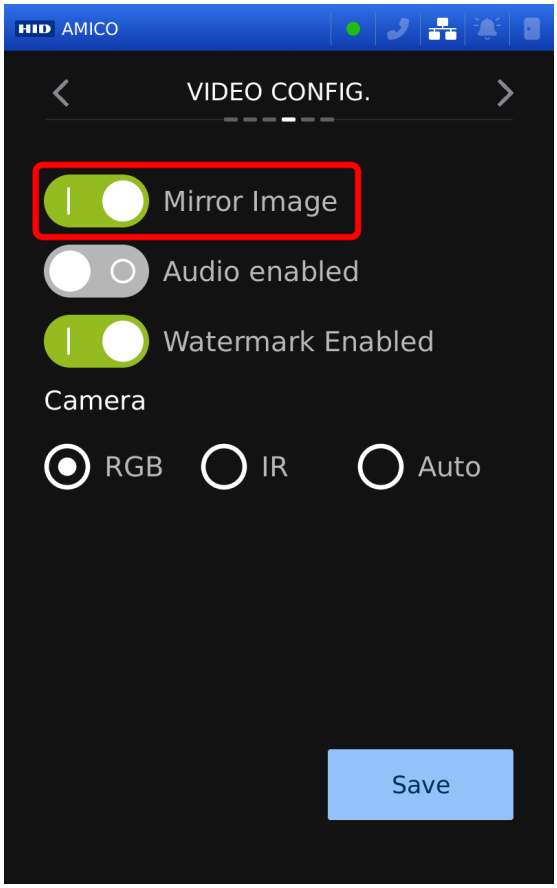
5. Tap the **Password** keyboard and enter the required password. Tap **Next** to continue.
6. Tap the required **Codec**:
   - **MJPEG** (default)
   - **H264**

7. Tap the required video **Orientation**.



8. Tap the required screen **Resolution**.
9. Slide the **Zoom** slider to the required value.
10. Slide the **Vertical adjustment** slider to the required value. Tap **Next** to continue.

11. Tap the **Mirror Image** toggle to flip the image horizontally.



12. Tap the **Audio enabled** toggle to enable audio for video.
13. Tap the **Enable Watermark** toggle to enable/disable the watermark that appears on the facial recognition screen. Tap **Next** to continue.
14. Tap the required **Camera** configuration:
    - **RGB** (default)
    - **IR** (InfraRed)
    - **Auto**

    Tap **Next** to continue.
15. Tap the required **Bitrate Mode**:
    - **Constant**
    - **Variable**
16. Tap the **Bitrate (Kb/s)** keyboard and enter the required bitrate. Tap **Next** to continue.

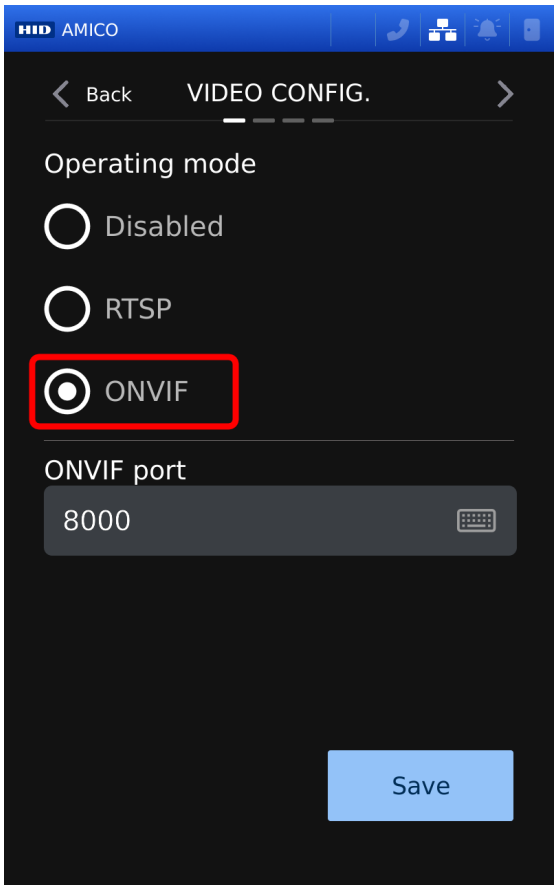
17. Tap **Save** to use the **RTSP stream URL** with compatible software (VLC media player or Windows media player).

Note: Write down the URL for future use.

18. Restart the reader for the configuration changes to take effect. See **1.1 Restart (VL70LF only)** for more information.

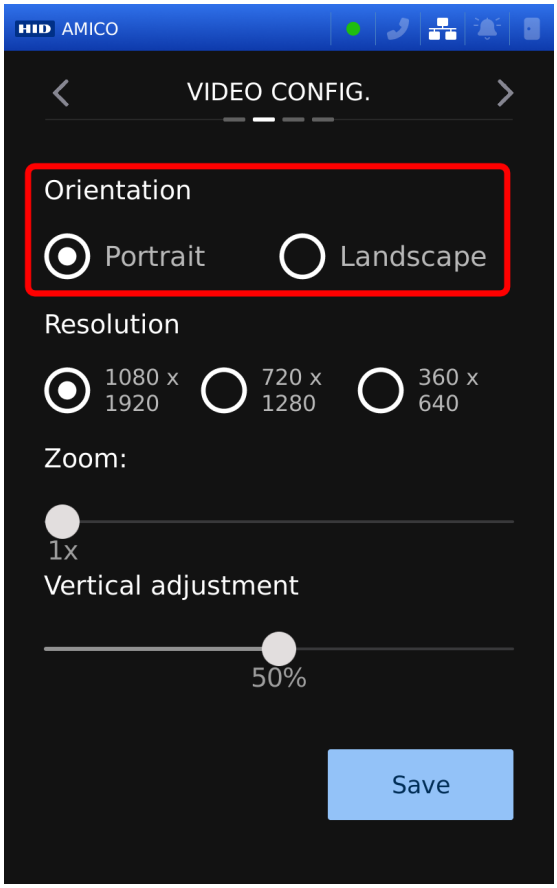
ONVIF streaming

1. Tap **Menu** > **Facial settings** > **Video Streaming**. The **Video config** screen is displayed.
2. Tap **ONVIF**.



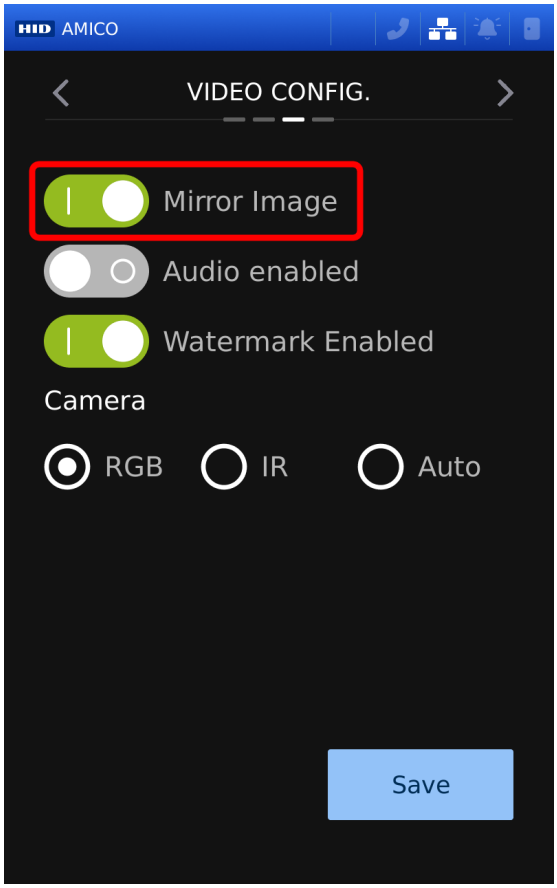
3. Tap the **ONVIF Port** keyboard and enter the required port (8000 by default). Tap **Next** to continue.

4. Tap the required video **Orientation**.



5. Tap the required screen **Resolution**.
6. Slide the **Zoom** slider to the required value.
7. Slide the **Vertical adjustment** slider to the required value. Tap **Next** to continue.

8. Tap the **Mirror Image** toggle to flip the image horizontally.



9. Tap the **Audio enabled** toggle to enable audio for video.
10. Tap the **Enable Watermark** toggle to enable/disable the watermark that appears on the facial recognition screen. Tap **Next** to continue.
11. Tap the required **Camera** configuration:
    - **RGB** (default)
    - **IR** (InfraRed)
    - **Auto**

    Tap **Next** to continue.
12. Tap the required **Bitrate Mode**:
    - **Constant**
    - **Variable**
13. Tap the **Bitrate (Kb/s)** keyboard and enter the required bitrate. Tap **Next** to continue.

14. Tap **Save** to use the **RTSP stream URL** with compatible software (VLC media player or Windows media player).

> **Note:** Copy and save the URL in a safe place.

15. Restart the reader for the configuration changes to take effect. See **1.1 Restart (VL70LF only)** for more information.

> **Note:**
> - ONVIF uses the default credentials:
>   - Login - **admin**
>   - Password - **admin**
> - ONVIF streaming only works if RTSP is active and operating correctly.

Optionally, validate the ONVIF Streaming using the **ONVIF Device Manager**.

5.4.4 Camera calibration

This allows you to calibrate the camera.

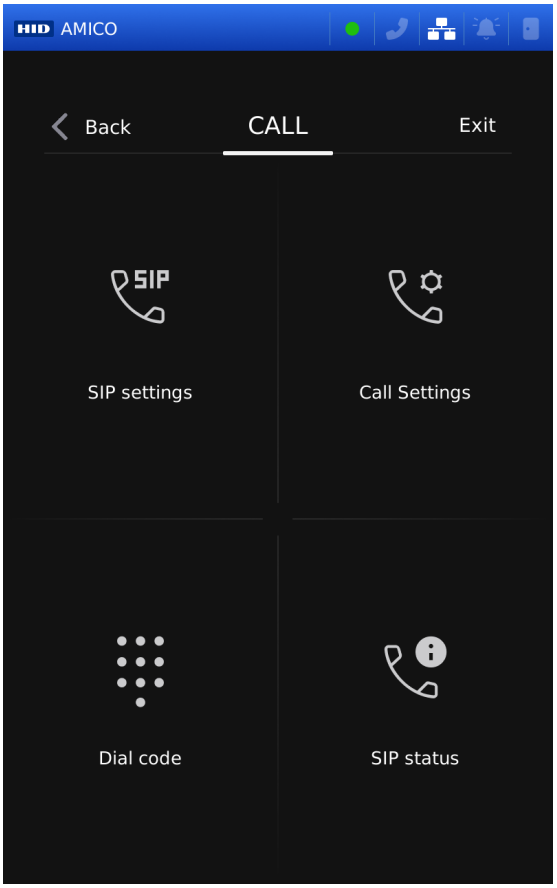
1. Tap **Menu** > **Facial Settings** > **Cameras** > **Camera Calibration**.
2. Tap **Start calibration** and follow the on-screen prompts.

Section 06

Intercom

6.1 Intercom (VL70LF only)

The intercom allows the reader to make audio calls via the Session Initiation Protocol (SIP). You can make calls using the button displayed on the touchscreen once it is configured.



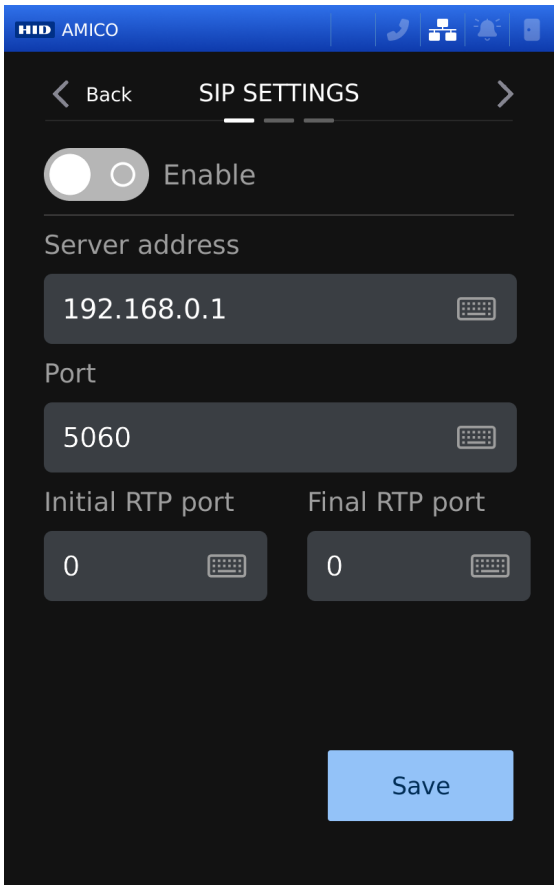
The three dialing modes you can set are:

Dialing mode	Description
Automatic	Tap the green **Dial** button to begin a call to the configured contact.
Contact list	Tap the green **Dial** button to display your contact list.
Numeric keypad	Tap the green **Dial** button to display the numeric keypad. Enter a number to dial.

See **6.2 Call settings** for more information on setting dialing modes.

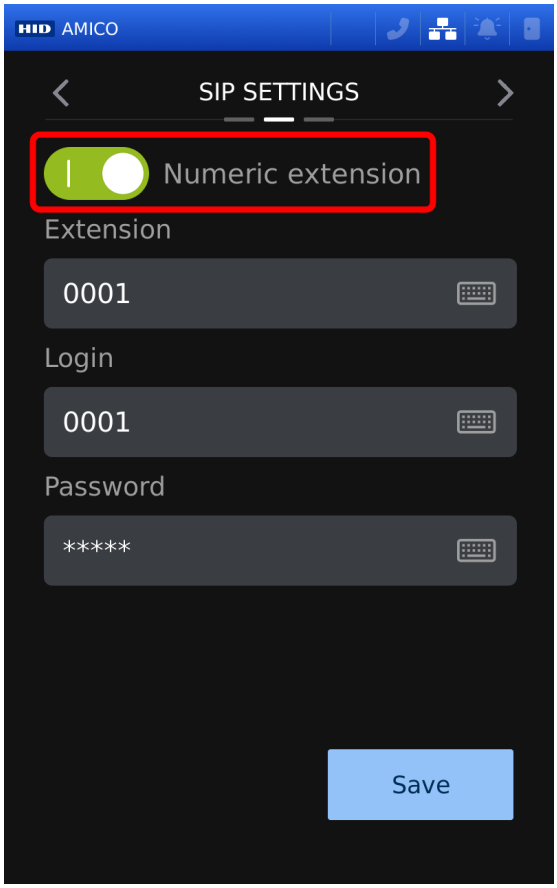
6.1.1 Intercom settings

1. Tap **Menu** > **Intercom** > **SIP Settings**. The **SIP SETTINGS** screen is displayed.



2. Tap the **Enable** toggle to enable SIP.
3. Tap the **Server Address** keyboard and enter the required server address.
4. Tap the **Port** keyboard and enter the required port.
5. Tap the **Initial RTP Port** keyboard and enter the required initial RTP port.
6. Tap the **Final RTP Port** keyboard and enter the required Final RTP port. Tap **Next** to continue.

7. Tap the **Numeric extension** toggle to read an extension as a numeric value.



8. Tap the **Extension**, **Login** and **Password** keyboards to enter the required information. Tap **Next** to continue.
9. Tap the required **Operating Mode**:
   - **SIP Client**
   - **Peer-to-Peer**
10. Tap the required **Protocol**:
    - **UDP**
    - **TCP**

    > **Note:** Tap the **Video** toggle to enable video. The intercom will work as a videophone. Only audio is transmitted when disabled.

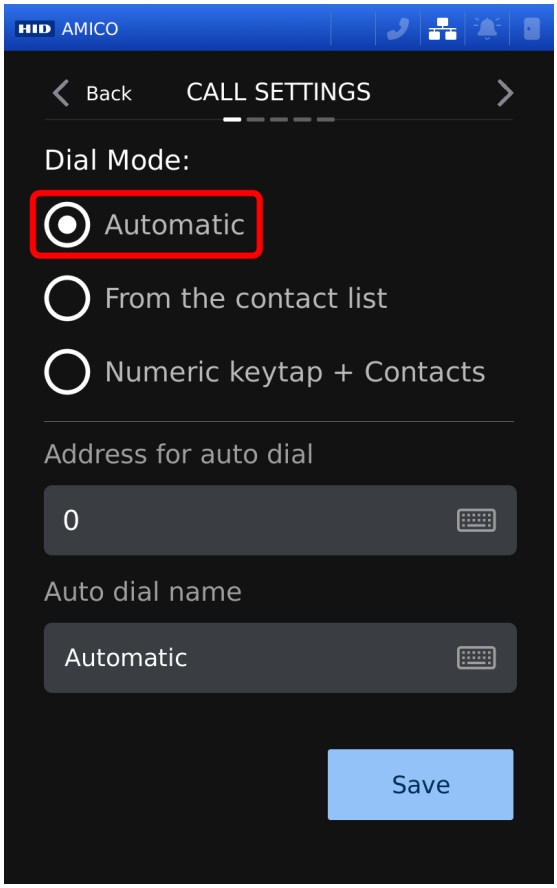
11. Tap **Save**.

6.2 Call settings

The **Call Settings** menu allows you to configure call settings.

6.2.1 Automatic dialing

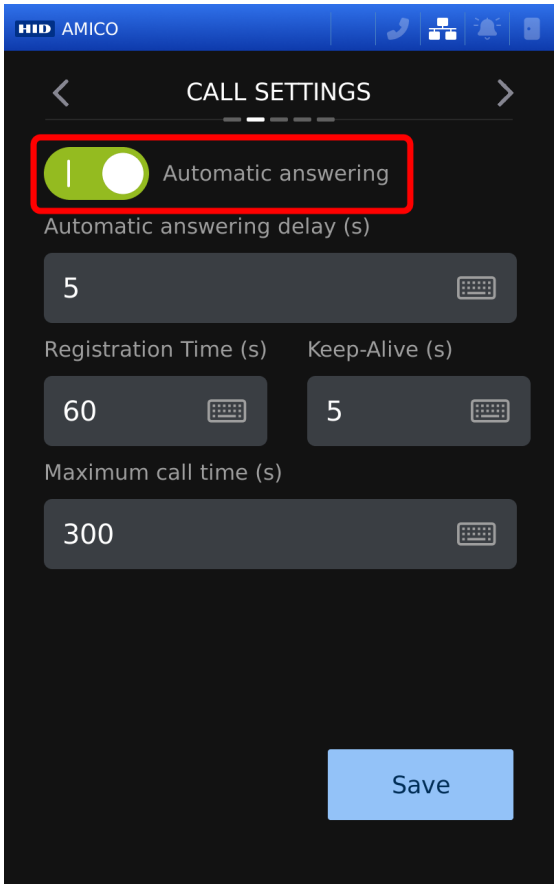
1. Tap **Menu** > **Intercom** > **Call Settings**. The **CALL SETTINGS** screen is displayed.
2. Tap **Automatic**.



3. Tap the **Address for auto dial** keyboard and enter the required address.
4. Tap the **Auto dial name** keyboard and enter the required name.
5. Tap **Save**.

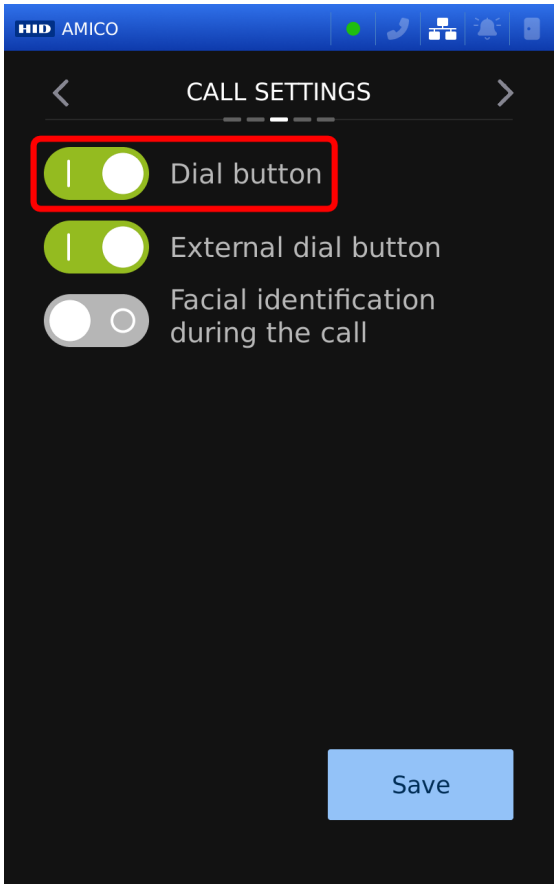
6.2.2 Contact list and Keypad and Contact List

1. Tap **Menu** > **Intercom** > **Call Settings**. The **CALL SETTINGS** screen is displayed.
2. Tap the required **Dial Mode**:
   - **From the Contact List**: select a contact from the contact list.
   - **Numeric keytap + Contacts**: enter a number or select a contact from the contact list.
3. Tap **Edit Contacts** to edit the contacts in the contact list. See **6.3 Intercom contacts** for more information.
   Tap **Next** to continue.
4. Tap the **Automatic answering** toggle to enable/disable automatic call answering after a set delay time.



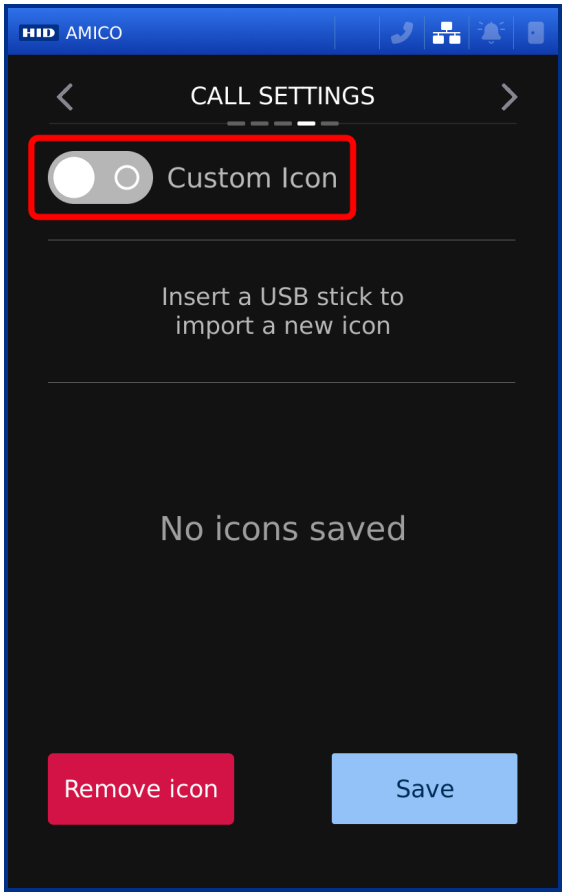
5. Tap the **Automatic answer delay (s)** keyboard and enter the required time in seconds.
6. Tap the **Registration Time (s)** keyboard and enter the required time in seconds.
7. Tap the **Keep-Alive (s)** keyboard and enter the required time in seconds.
8. Tap the **Maximum Call Time (s)** keyboard and enter the required time in seconds. Tap **Next** to continue.

9. Tap the **Dial button** toggle to enable/disable the main menu dial button.



10. Tap **External dial button** toggle to enable/disable push-button dialing.
11. Tap **Facial identification during the call** toggle to enable/disable facial identification during calls. Tap **Next** to continue.

12. Tap the **Custom Icon** toggle to enable a custom icon to signal an incoming call.

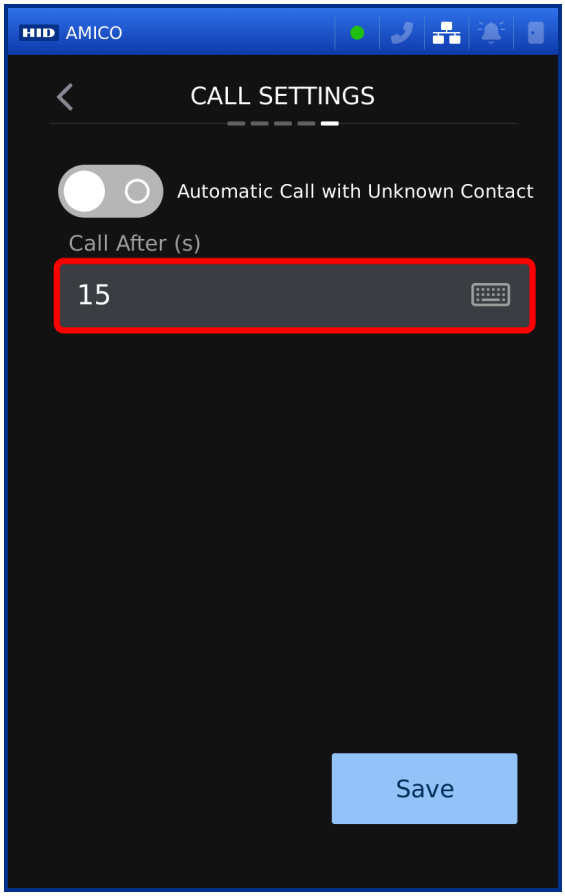


Note:
- Insert a USB drive to import a new icon.
- Tap **Remove icon** to remove the existing icon.

Tap **Next** to continue.

13. Tap the **Automatic Call with Unknown Contact** toggle to enable/disable automatic answering of callers not in the contact list.

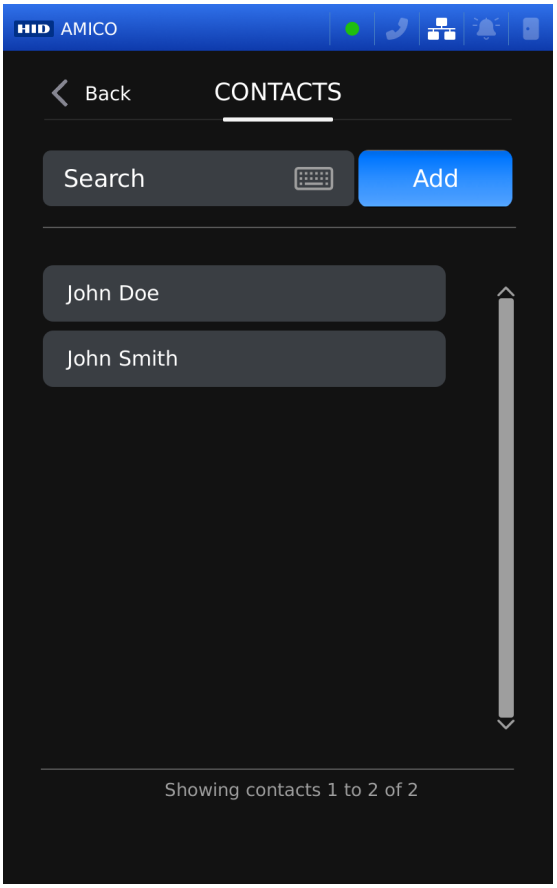
14. Tap the **Call After (s)** keyboard and enter the required time before the reader answers the unknown contact call.



15. Tap **Save**.

6.3 Intercom contacts

Tap **Menu** > **Intercom** > **Call Settings** > **Edit Contacts**. The **Contact Management** screen is displayed.

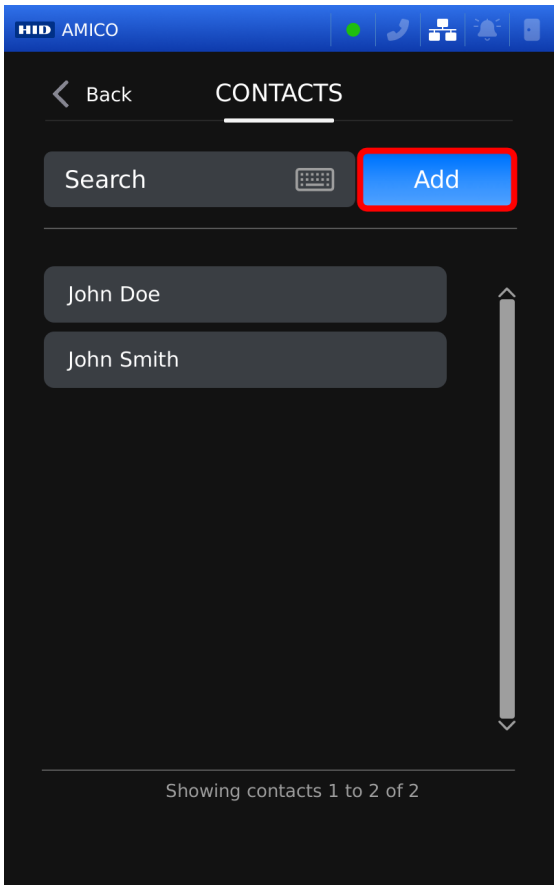


Each contact has the following features:

Feature	Description
Name	The name displayed on calls made with the contact.
Address	• Contact extension number for SIP Client mode. • Contact local IP address for Peer-To-Peer mode.

6.3.1 Create a contact

1. Tap **Menu** > **Intercom** > **Call Settings** > **Edit Contacts**.
2. Tap the **Add** icon.

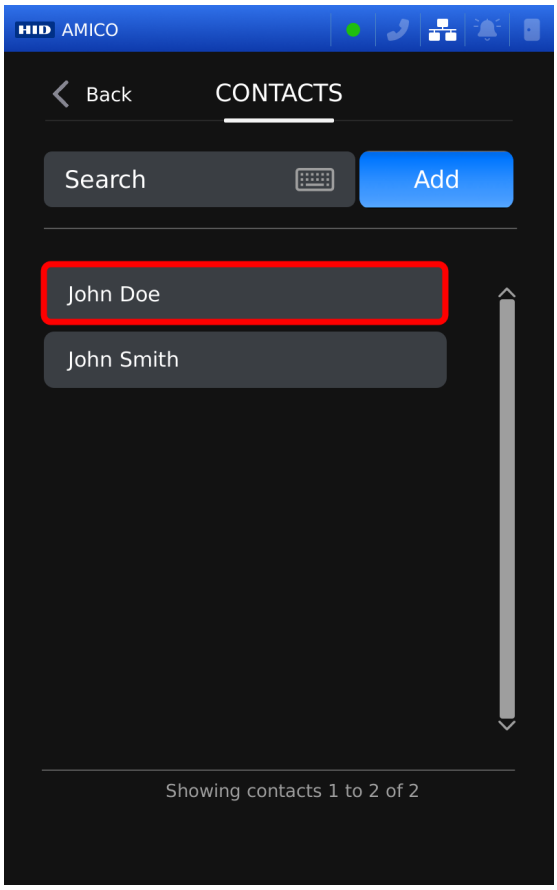


3. Tap the **Name** keyboard and enter the required information.
4. Tap the **Address** keyboard and enter the required information.
5. Tap **Save**.

> **Note:** Tap **Back** to stop creating a new contact.

6.3.2 To edit a contact

1. Tap **Menu** > **Intercom** > **Call Settings** > **Edit Contacts**.
2. Tap the required contact.



3. Tap the **Name** keyboard and edit the required information.
4. Tap the **Address** keyboard and edit the required information.
5. Tap **Save**.

6.3.3 To delete a contact

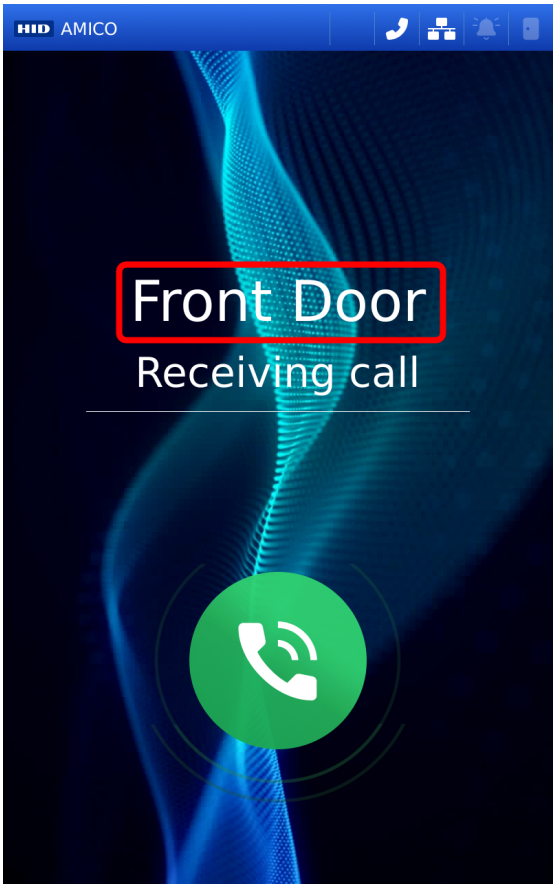
1. Tap **Menu** > **Intercom** > **Call Settings** > **Edit Contacts**.
2. Tap the required contact.
3. Tap **Delete**.

> **Note:** You cannot recover any contact data after they are deleted.

4. Tap **Save**.

6.4 SIP call ID

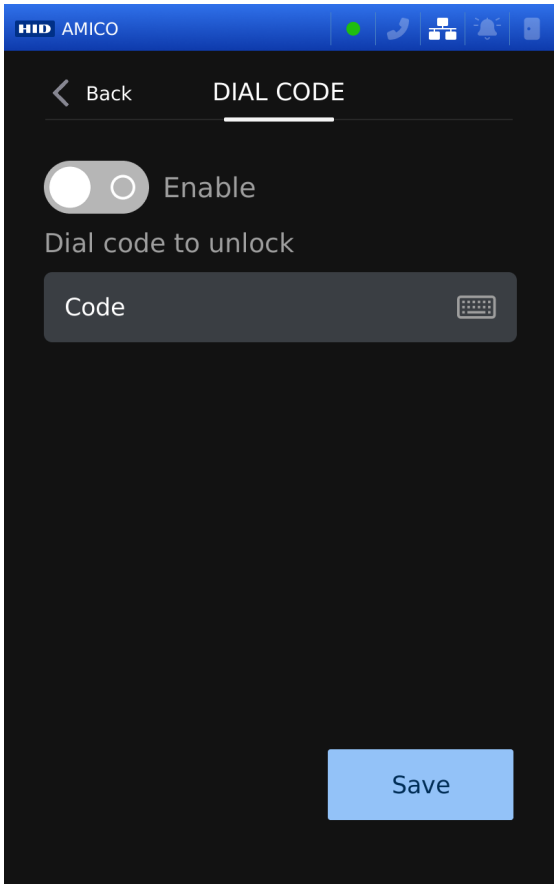
Allows you to view the incoming caller name on the reader touchscreen during a SIP audio or video call.



6.5 Access Release via Intercom

You can configure a code to release access to the reader when another active user on the call enters it.

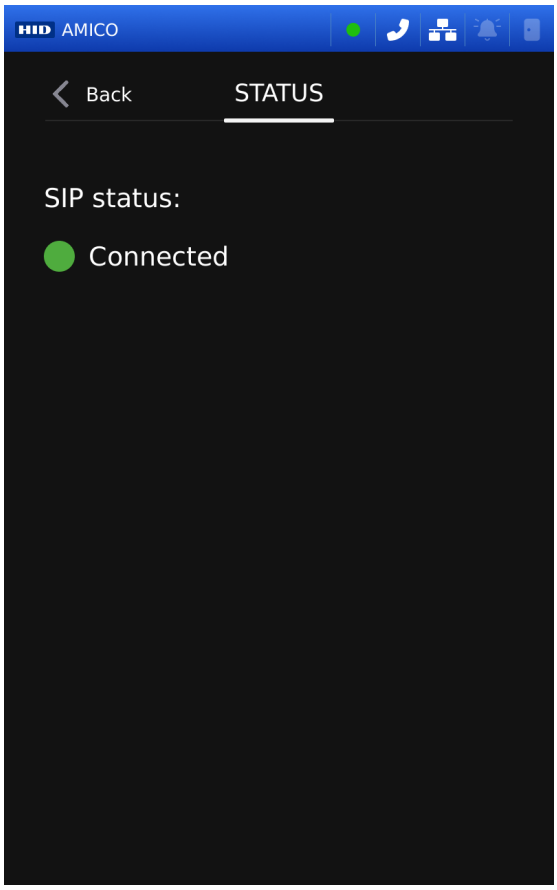
1. Tap **Menu** > **Intercom** > **Dial Code**. The **DIAL CODE** screen is displayed.



2. Tap the **Enable** toggle to enable the dialing code.
3. Tap the **Dial code to unlock** keyboard to enter the required code.
4. Tap **Save**.

6.5.1 SIP Status

1. Tap **Menu** > **Intercom** > **SIP Status**. The **SIP Status** screen is displayed.



Color	Status
Green	Reader connected to the server.
Gray	SIP disabled.
Red	• Connecting. • Authentication failed to connect to the server or network.

2. Tap **Back**.

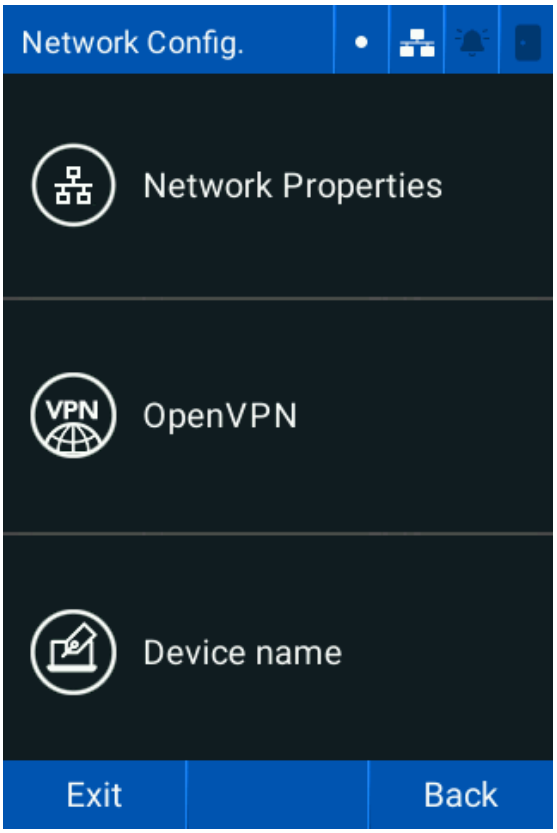
Section 07

Settings

7.1 Network settings

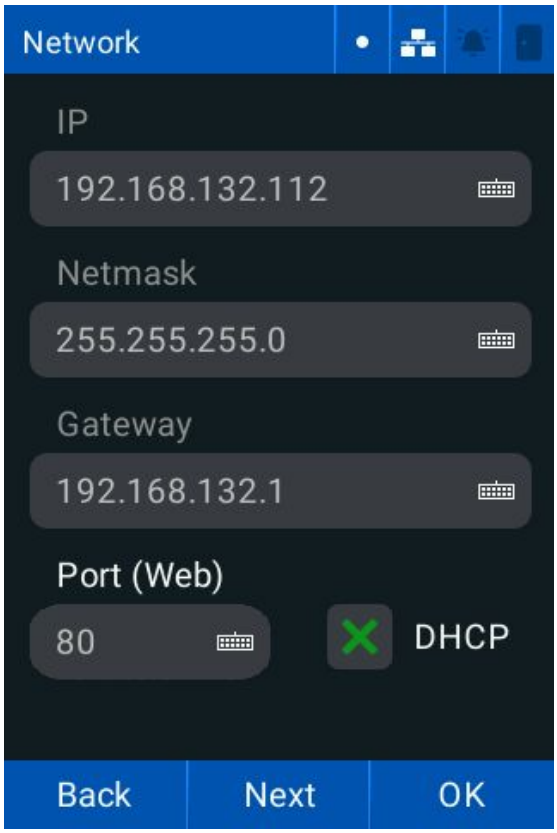
The HID Amico can connect to a network via an Ethernet cable (10/100Mbps), using the TCP/IP protocol. Configure the IP address, the subnet mask, and the gateway of the reader to access the web interface.

Tap **Menu** > **Settings** > **Network**. The **Network settings** menu is displayed.



7.1.1 Network properties

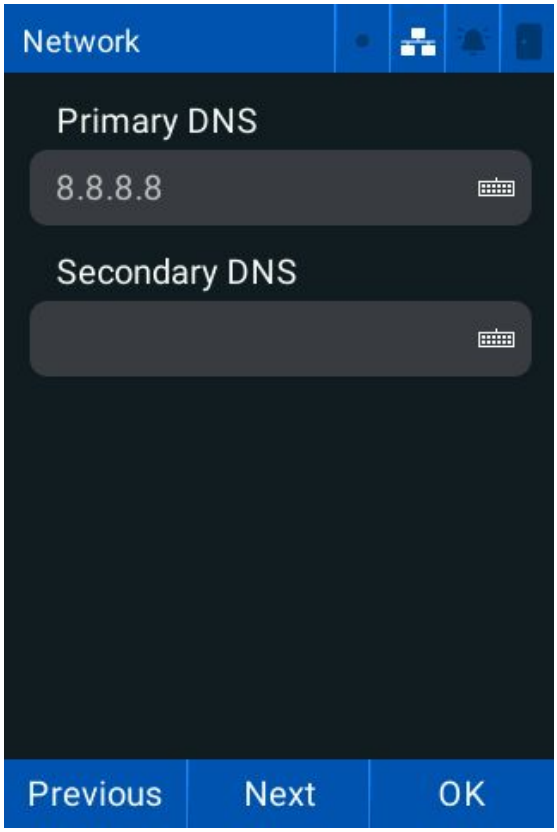
1. Tap **Menu** > **Settings** > **Network** > **Network Properties**. The **Network** screen is displayed.



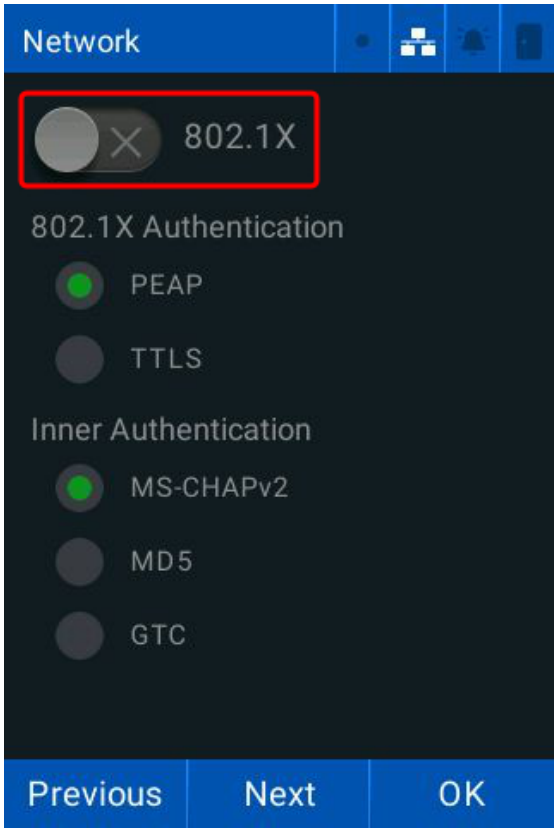
2. Tap the **IP** keyboard and enter the required static reader IP address.
3. Tap the **Netmask** keyboard and enter the required Netmask.
4. Tap the **Gateway** keyboard and enter the required network gateway IP address.
5. Tap the **Port (Web)** keyboard and enter the required network port.
6. Tap the **DHCP** checkbox to enable/disable the DHCP protocol for network configuration. Tap **Next** to continue.

> **Note:** The **IP**, **Netmask**, and **Gateway** settings are configured automatically and they cannot be changed when the **DHCP** protocol is enabled.

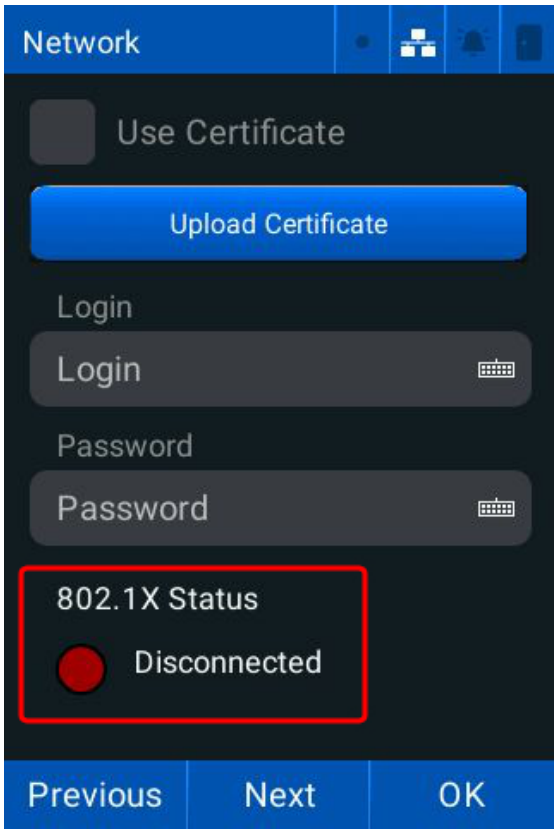
7. Tap the **Primary** and **Secondary** DNS keyboards and enter the required DNS server information. Tap **Next** to continue.



8. Tap the **802.1X** toggle to enable/disable the 802.1X protocol.

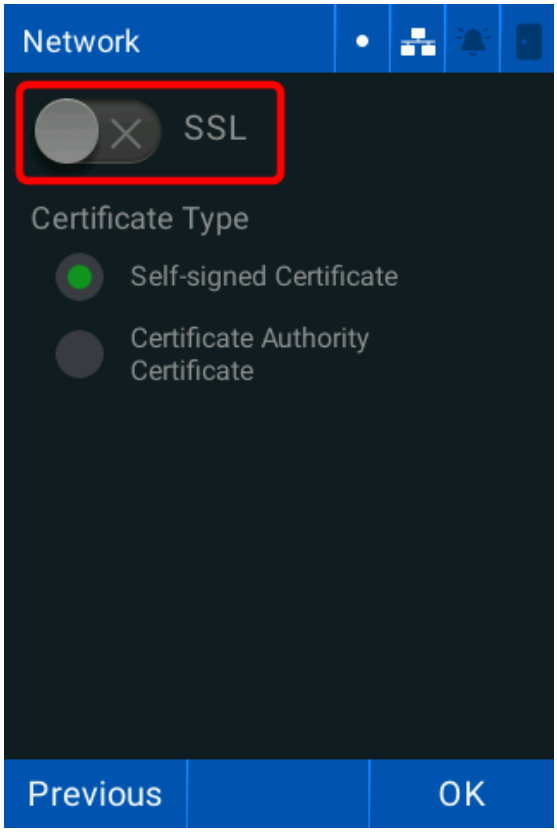


9. Tap the required **802.1X Authentication** option:
   - **PEAP**
   - **TTLS**
10. Tap the required **Inner Authentication** option:
   - **MS-CHAPv2**
   - **MD5**
   - **GTC**
11. Tap **Next** to continue.
12. Tap the **Login** keyboard and enter the required login.
13. Tap the **Password** keyboard and enter the required password.
14. The **802.1X status** is displayed at the bottom of the screen. See **A.1 802.1X status** for more information.



15. Tap **Next** to continue.

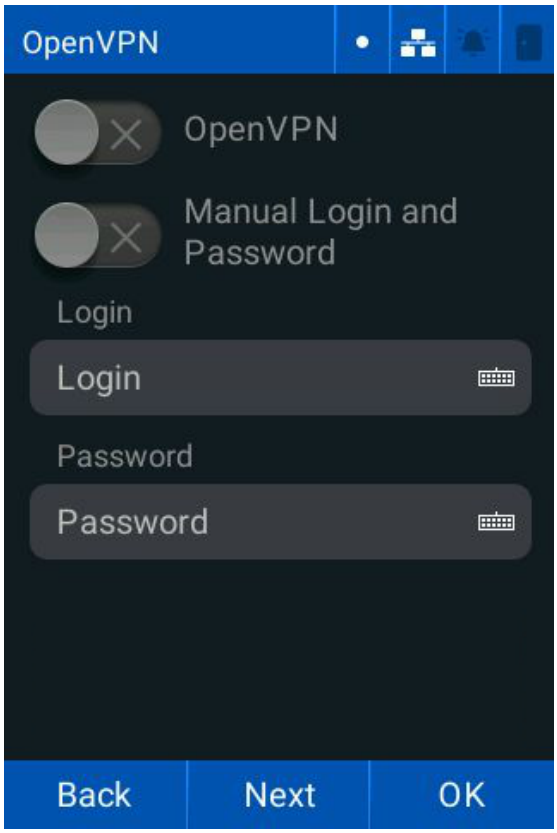
16. Tap the **SSL Protocol** toggle to enable/disable the SSL protocol.



17. Tap **OK** to save the network settings.

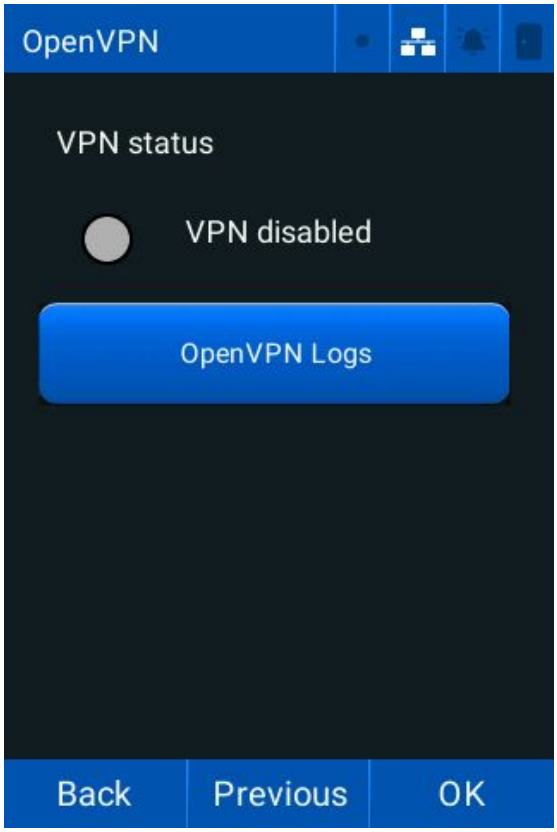
7.1.2 OpenVPN

1. Tap **Menu** > **Settings** > **Network** > **OpenVPN**. The **OpenVPN** screen is displayed.



2. Tap the **OpenVPN** toggle to enable/disable OpenVPN.
3. Tap the **Manual Login and Password** toggle to enable/disable the manual login.
4. Tap the **Login** keyboard and enter the required login.
5. Tap the **Password** keyboard and enter the required password.

6. Tap **Next** to continue. The **VPN Status** screen is displayed.

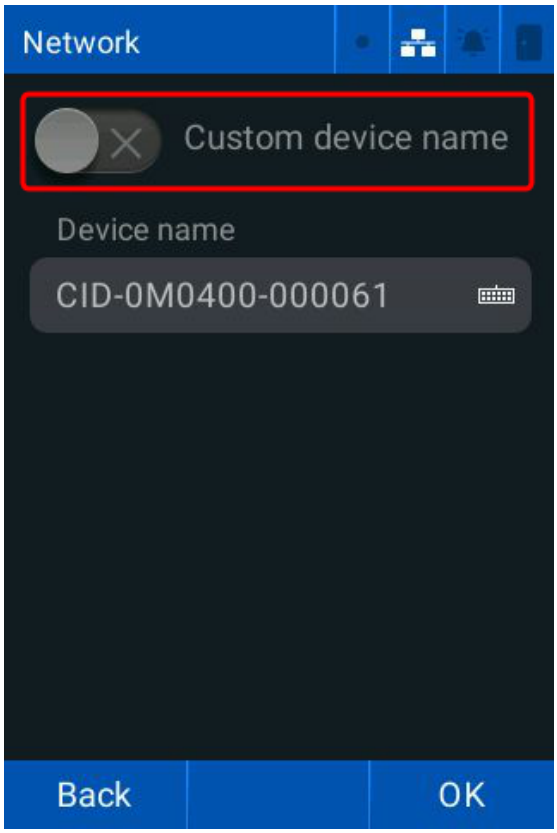


Status	Description
Green	Reader connected to OpenVPN
Grey	OpenVPN disabled or failed security protocol.
Red	Reader authentication failure.

7. Tap **OpenVPN Logs** to view the VPN logs.
8. Tap **OK**.

7.1.3 Reader name

1. Tap **Menu** > **Settings** > **Network** > **Device name**.
2. Tap the **Custom device name** toggle to enable/disable the option to change the reader name.



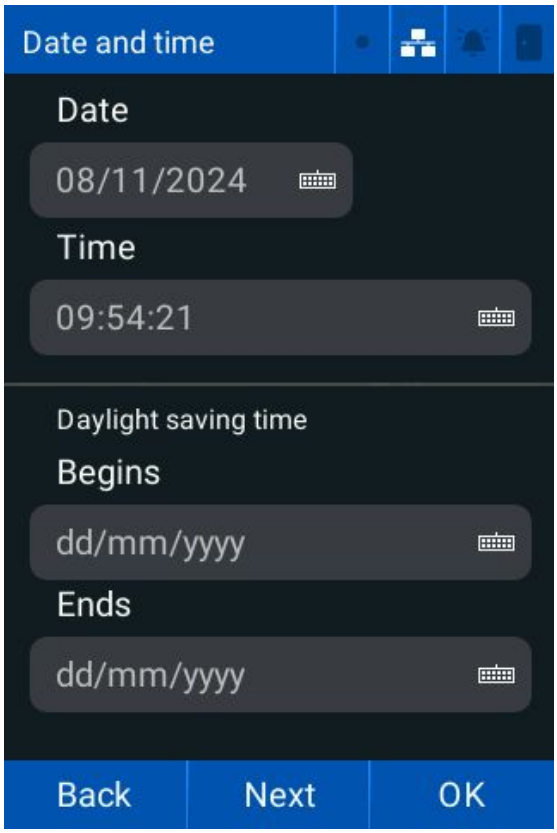
3. Tap the **Device name** keyboard and enter the required reader name.
4. Tap **OK**.

7.2 Date and time

The **Date and time** screen allows you to set the readers Real Time Clock (RTC) manually, or enable automatic synchronization with an NTP server.

> **Note:** Regular automatic synchronization with an NTP server keeps system time accurate and allows all events, transactions, and reader logs to be recorded consistently.

1. Tap **Menu** > **Settings** > **Date and time**. The **Date and time** screen is displayed.



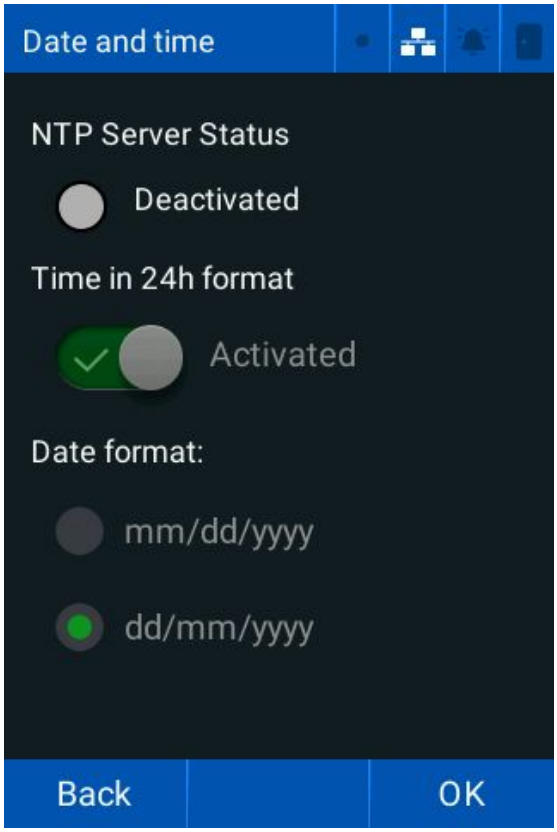
2. Tap the **Date** keyboard and enter the required date.
3. Tap the **Time** keyboard and enter the required time.
4. Tap the **Daylight saving time - Begins** keyboard and enter the required start date.
5. Tap the **Daylight saving time - Ends** keyboard and enter the required end date. Tap **Next** to continue.
6. Tap the **NTP** toggle to enable/disable the **Network Time Protocol**.

7. Tap the **Server** keyboards and enter the required server addresses.

Note:
- **Server 2** is optional.
- The reader must be connected to the internet and the server must be reachable to use NTP.

8. Select the required **Time zone** from the drop-down list.

9. Tap **Next** to continue. The **NTP Server Status** is displayed.



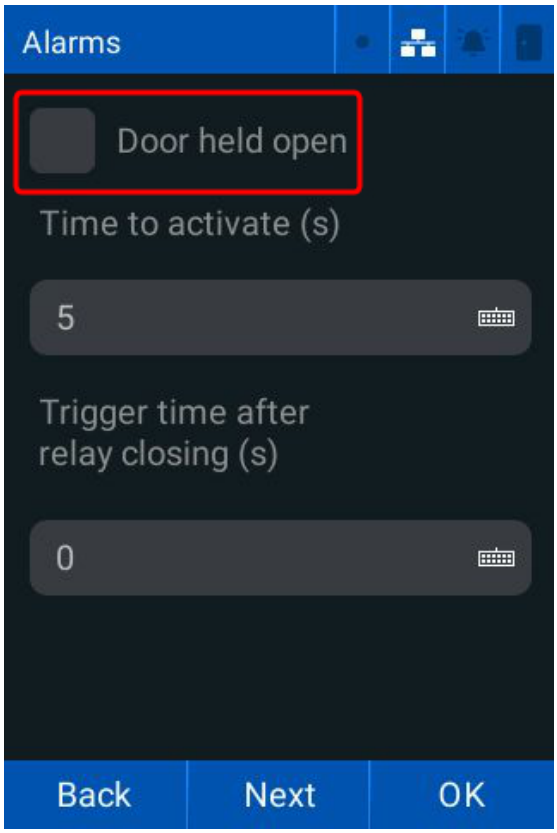
Color	Status
White	Deactivated
Green	Connected
Red	Disconnected

10. Tap the **Time in 24h format** toggle to alternate between 24 hour clock or 12 hour clock.
11. Tap the required **Date format**.
12. Tap **OK** to save the date and time settings.

7.3 Alarms

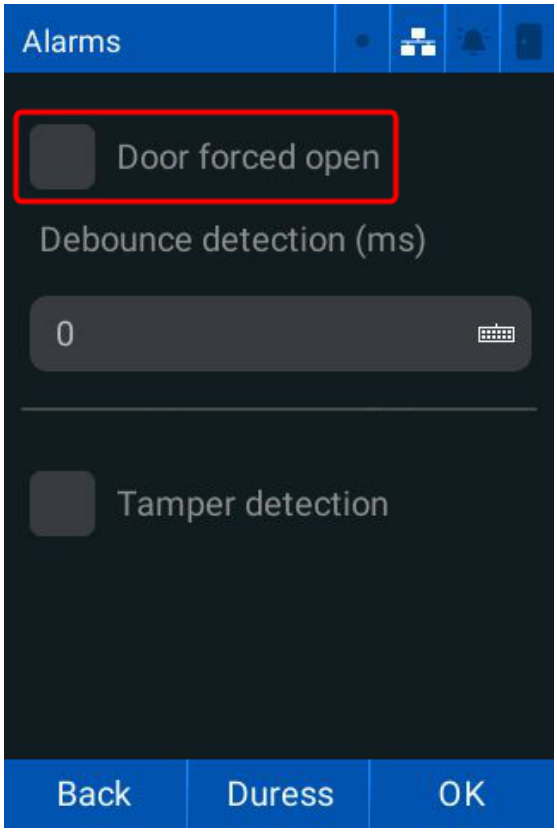
7.3.1 Internal alarms (VL35LF only)

1. Tap **Menu** > **Settings** > **Alarms** > **Internal alarms**.
2. Tap the **Door held open** checkbox to enable/disable the detection of an open door.



3. Tap the **Time to activate (s)** keyboard and enter the required time (seconds) for the alarm to trigger after sensor activation.
4. Tap the **Trigger time after relay closing (s)** keyboard and enter the required time in seconds that the alarm is triggered if the door is kept open. Tap **Next** to continue.

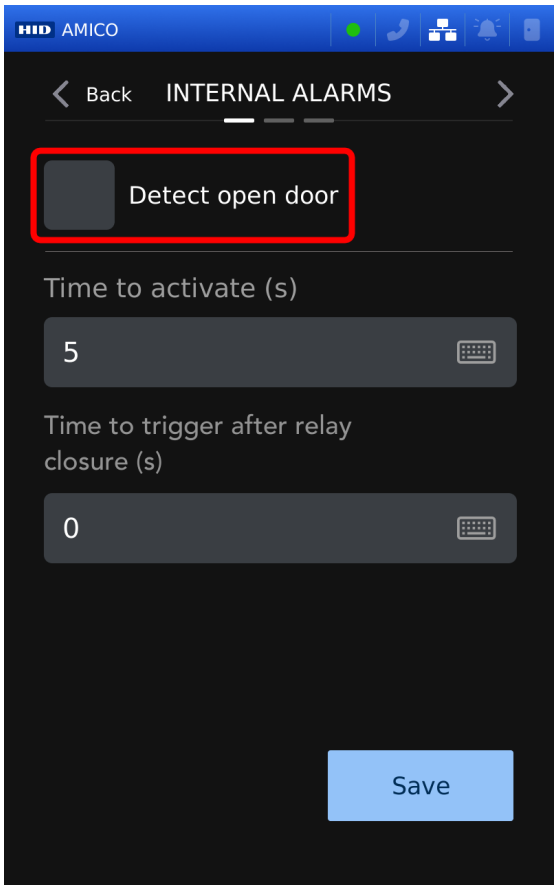
5. Tap the **Door forced open** checkbox to enable/disable the detection of a break-in.



6. Tap the **Debounce detection (ms)** keyboard and enter the required time (milliseconds) for a break-in detection alarm.
7. Tap the **Tamper detection** checkbox to enable/disable the reader tamper sensor.
8. Tap **OK** to save.

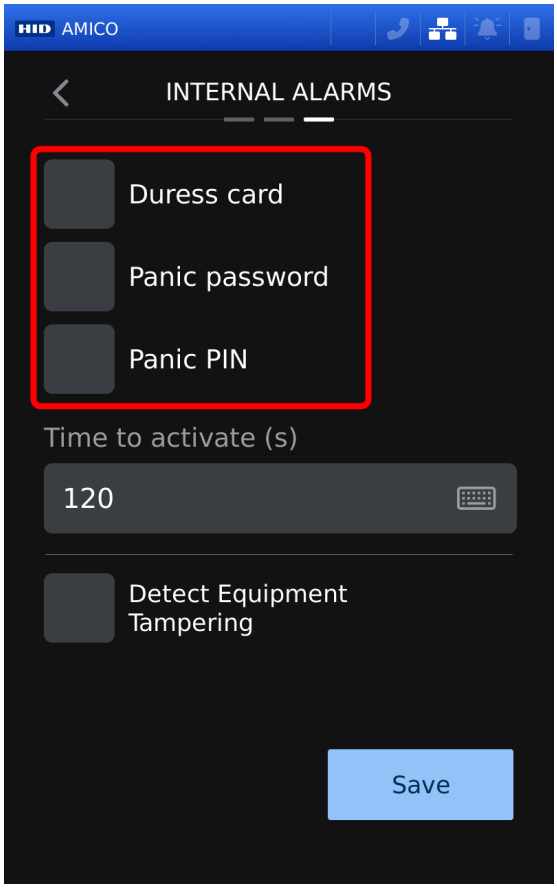
7.3.2 Internal alarms (VL70LF only)

1. Tap **Menu** > **Settings** > **Alarms** > **Internal alarms**. The **INTERNAL ALARMS** screen is displayed.
2. Tap the **Detect open door** checkbox to enable/disable the detection of an open door.



3. Tap the **Time to activate (s)** keyboard and enter the required time (seconds) for the alarm to trigger after sensor activation.
4. Tap the **Time to trigger after relay closure (s)** keyboard and enter the required time in seconds that the alarm is triggered if the door is kept open. Tap **Next** to continue.
5. Tap the **Burglary detection** checkbox to enable/disable the detection of a break-in.
6. Tap the **Debounce detection (ms)** keyboard and enter the required time (milliseconds) for a break-in detection alarm. Tap **Next** to continue.

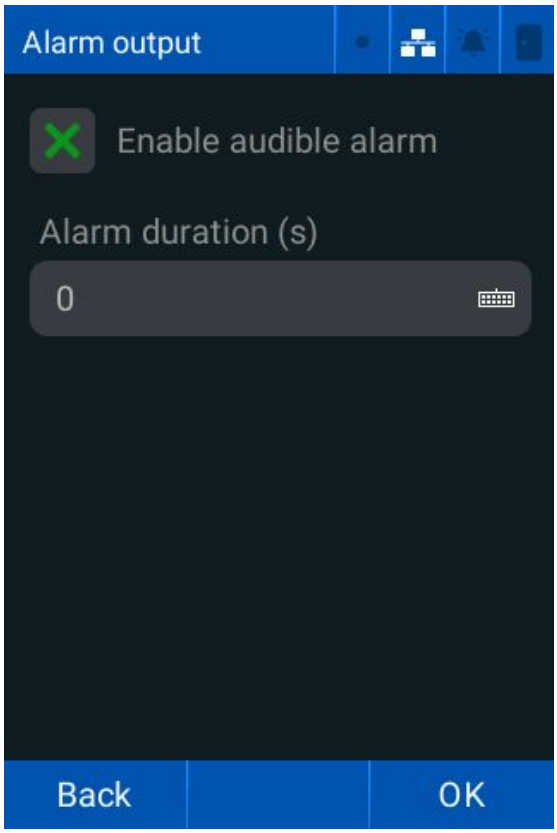
7. Tap the required **Panic Alarm** options.



8. Tap the **Time to activate (s)** keyboard and enter the required time (seconds) for the alarm to trigger after a panic event activation.
9. Tap the **Detect Equipment Tampering** check box to enable/disable the reader tamper sensor.
10. Tap **Save**.

7.3.3 Alarm output

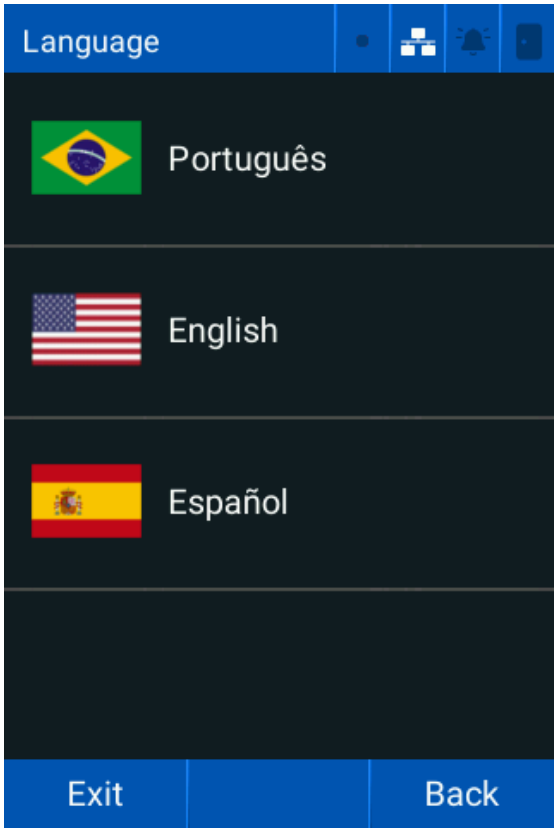
1. Tap **Menu** > **Settings** > **Alarm** > **Alarm Output**. The **Alarm Output** screen is displayed.



2. Tap the **Enable audible alarm** checkbox to enable/disable the audible alarm.
3. Tap the **Alarm duration (s)** keyboard and enter the required time (seconds) to trigger the audible alarm.
4. Tap **OK**.

7.4 Language settings

1. Tap **Menu** > **Settings** > **Languages**. The **Language** screen is displayed.



2. Tap the required **Language**.

7.5 Web interface

The web interface allows the administration and configuration of HID Amico, with the practicality of using a browser.

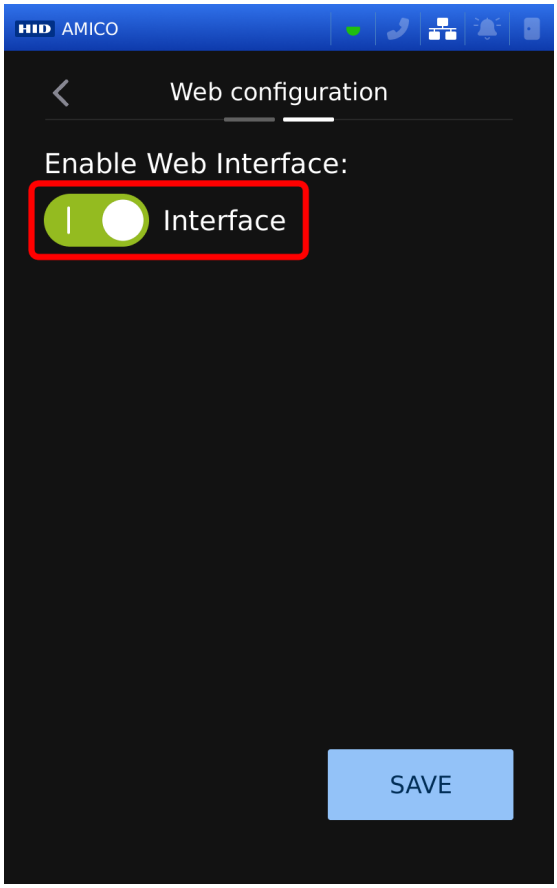
> **Note:** It is recommended to change the credentials from default as soon as possible to prevent unauthorized access to the equipment.

Open a browser to access the web interface, preferably **Google Chrome™**, and enter the default HID Amico biometric reader IP address (http://192.168.0.129/) in the search bar.

7.5.1 Enable the web interface

1. Tap **Menu** > **Settings** > **General settings** > **Web Interface**.
2. Tap **Next**.

3. Tap the **Interface** toggle to enable/disable the web interface.

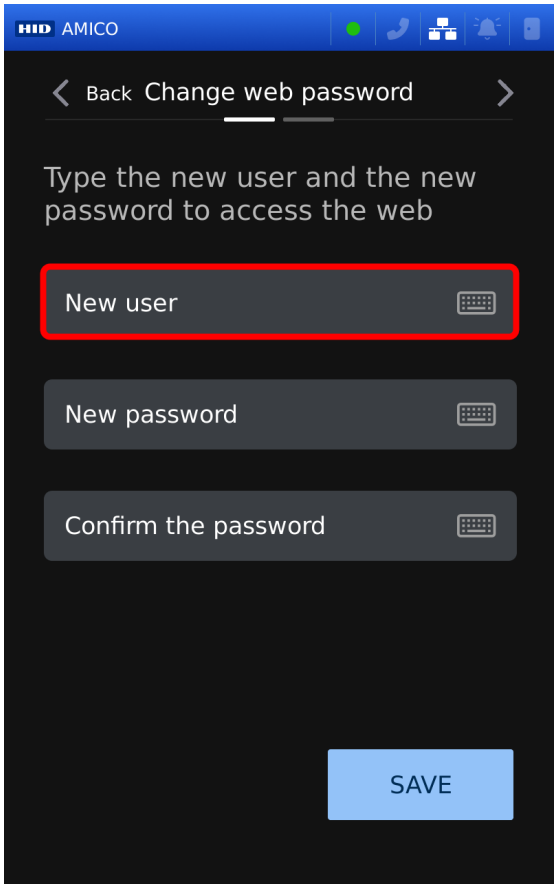


4. Tap **SAVE**.

7.5.2 Change web interface login credentials

Note: There is always a singular user defined for access to the web interface. Creating a new user will overwrite any previously configured users.

1. Tap **Menu** > **Settings** > **General settings** > **Web Interface**.
2. Tap the **New user** keyboard and enter the required user name.

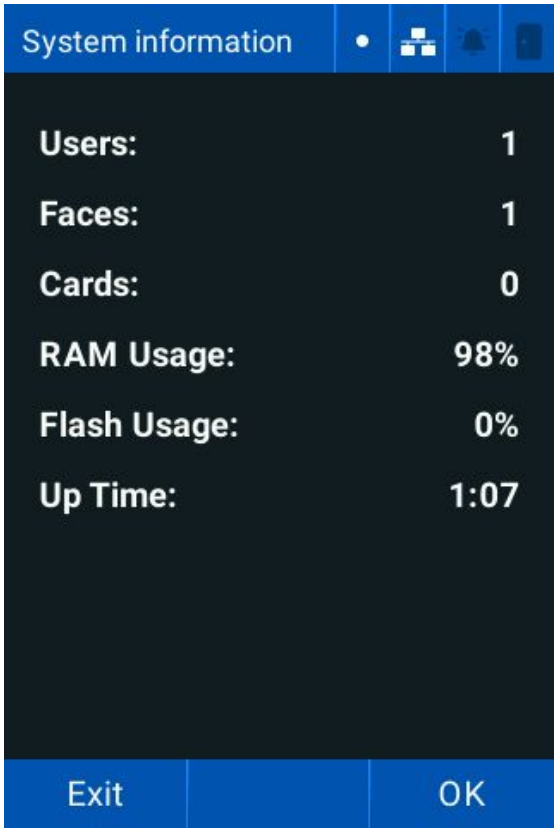


3. Tap the **New password** keyboard and enter the new password.
4. Tap the **Confirm the password** keyboard and re-enter the new password.
5. Tap **SAVE**.

7.6 System information

The **System information** screen allows you to see the reader and system information.

1. Tap **Menu** > **Settings** > **General settings** > **System** > **System information**. The **System information** screen is displayed.



2. Tap **OK**.

7.7 Upgrade to License mode

HID Amico readers are supplied with various user database capacities for facial recognition. Upgrading to License Mode allows you to increase the user database to **50,000**, or **100,000** faces. Contact your supplier (HID channel partner) to purchase a License Mode license.

> **Note:** You will need to provide the reader serial number when purchasing a License Mode license.

Limitations

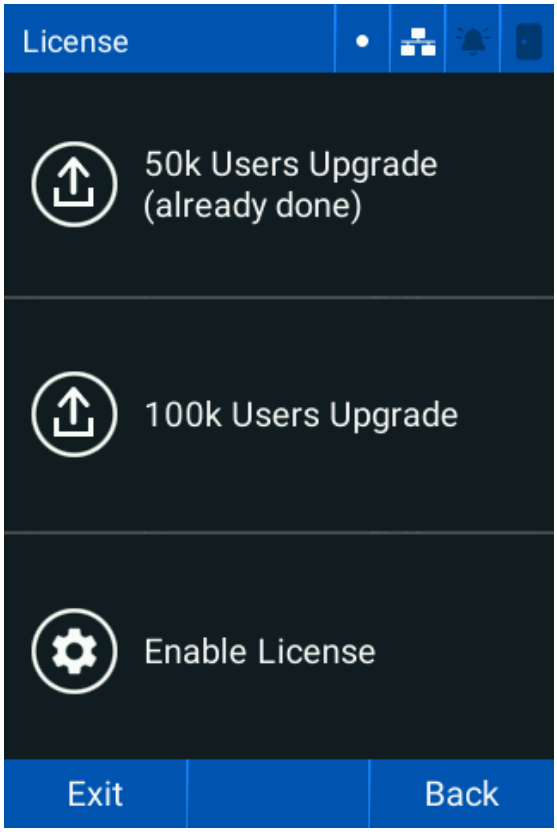
- At 50,000 and 100,000 users it is not possible to store users photos in the database. Any existing photos stored in the database will be deleted when License mode is enabled.

7.7.1 Upgrade License Mode 50k

The maximum limit of registered faces in **License 50k Mode** is 50,000.

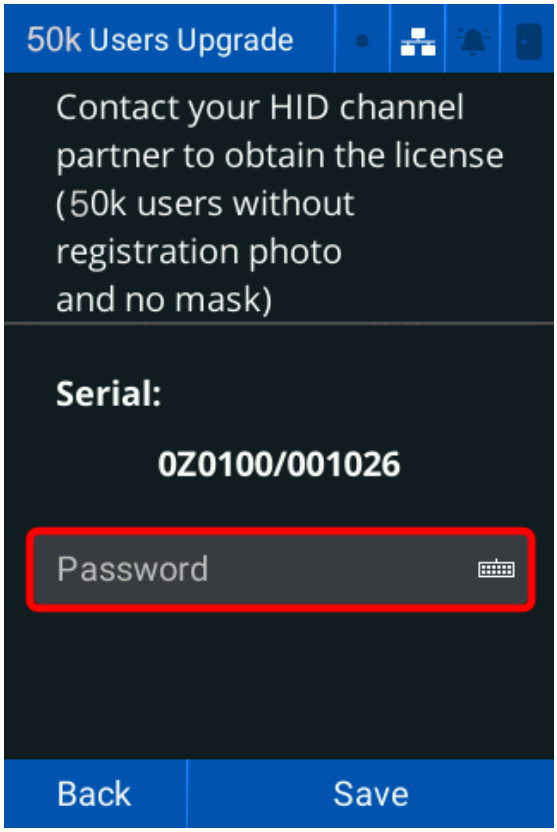
> **Important: You cannot store user registration photos.**

1. Tap **Menu** > **Settings** > **General Settings** > **License**. The **License Mode** screen is displayed.



2. Tap **50k Users Upgrade**.

3. Tap the **Password** keyboard and enter the upgrade password.



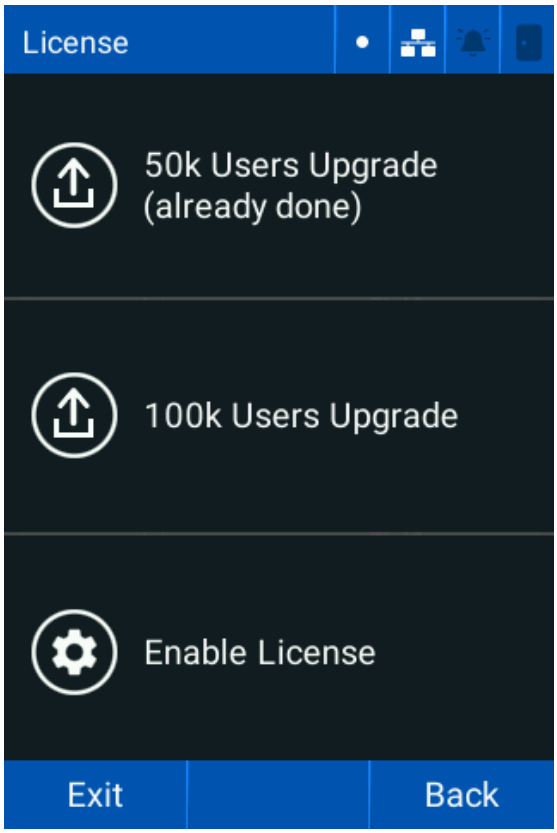
4. Tap **Save**.

7.7.2 Upgrade License 100k

The maximum limit of registered faces in **License 100k Mode** is 100,000.

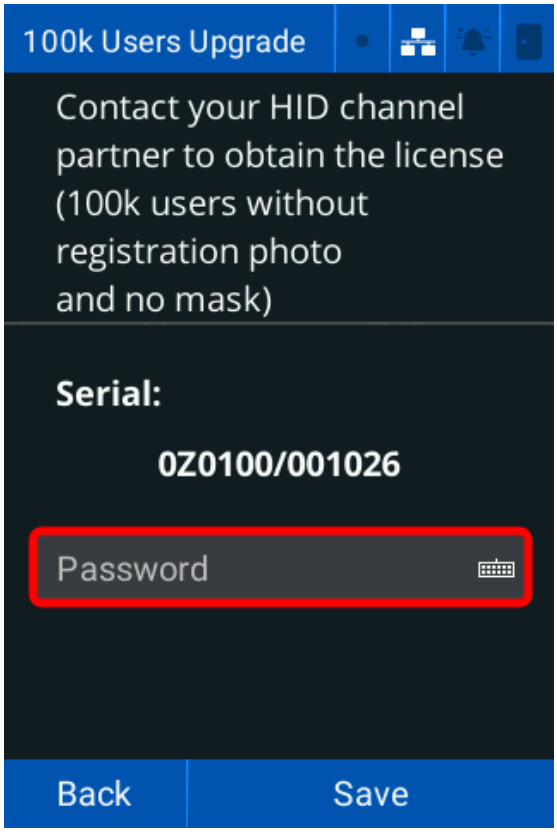
> **Important: You cannot store user registration photos, and registering templates with masks is unavailable in this mode.**

1. Tap **Menu** > **Settings** > **General Settings** > **Configure License Mode**. The **License Mode** screen is displayed.



2. Tap **100k Users Upgrade**.

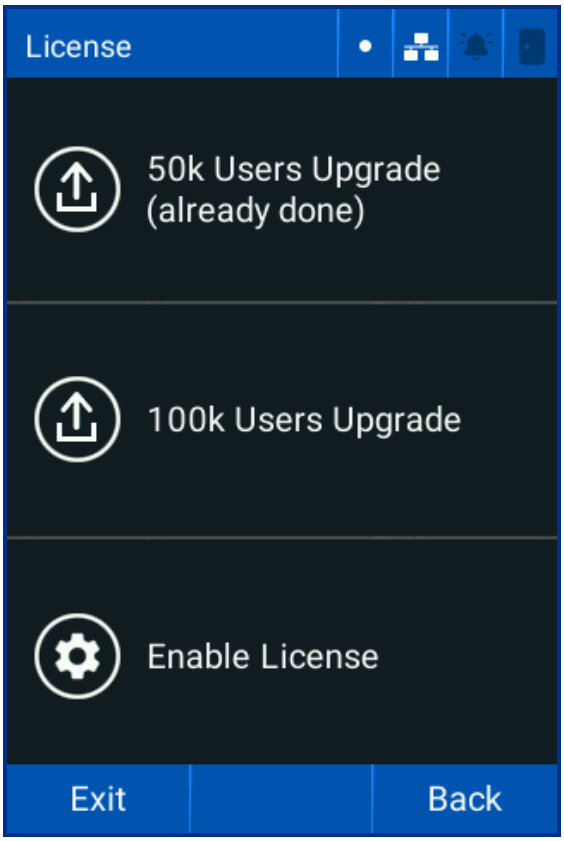
3. Tap the **Password** keyboard and enter the upgrade password.



4. Tap **Save**.

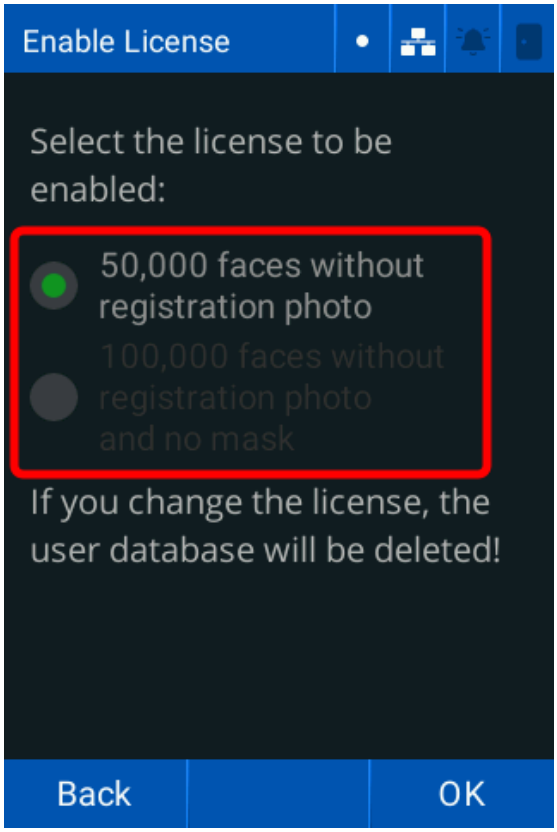
7.7.3 Enable License mode

1. Tap **Menu** > **Settings** > **General Settings** > **License**. The **License Mode** screen is displayed.



2. Tap **Enable License**.

3. Tap the required **License Mode**.



4. Tap **OK** to return to the menu.
5. Restart the reader for the changes to take place.

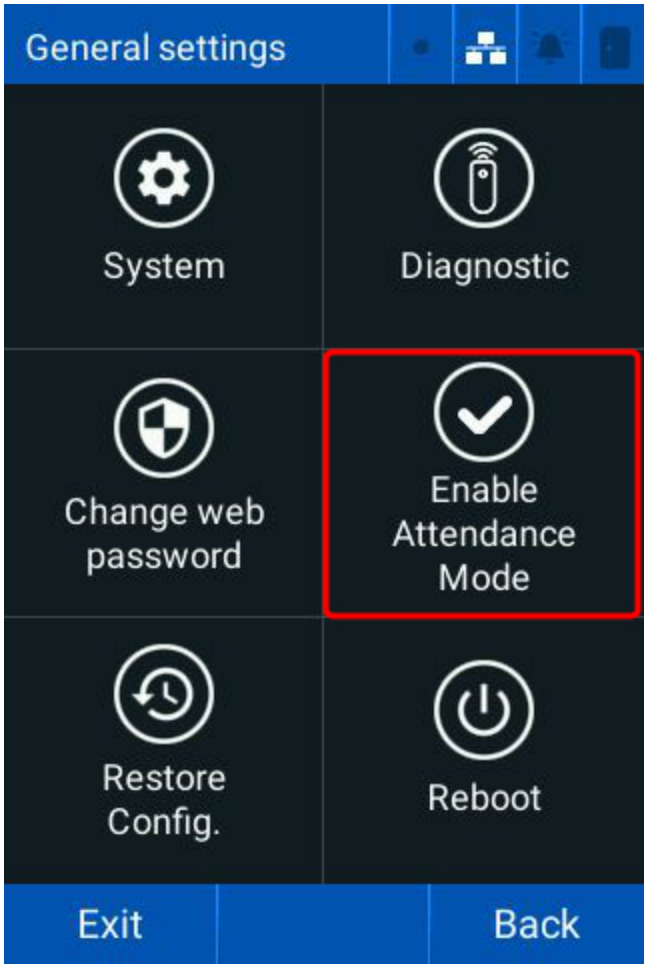
7.8 Attendance mode

Important: Some access control features are not available in this mode.

The HID Amico reader has two modes, Access Mode (default), and Attendance Mode. Attendance Mode allows the reader to record time and attendance status.

7.8.1 Enable Attendance Mode

1. Tap **Menu** > **Attendance** > **General Configuration**.
2. Tap **Enable Attendance Mode**.



Note: The main menu is changed from **Access** to **Attendance**.

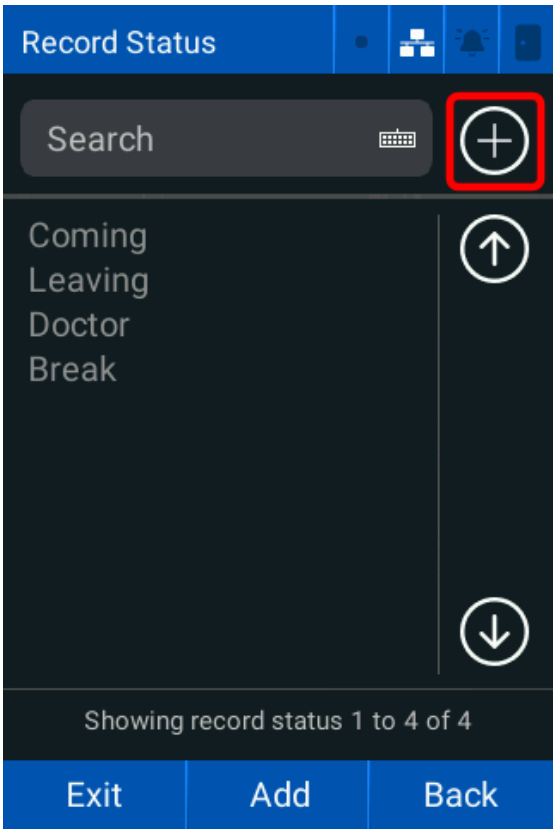
7.8.2 Attendance codes

Attendance code buttons can be added to the main menu to record attendance status (for example, arrival, leaving, and lunch break). You must tap the attendance code and identify yourself to the HID Amico reader.

> **Note:** A maximum of ten codes can be added.

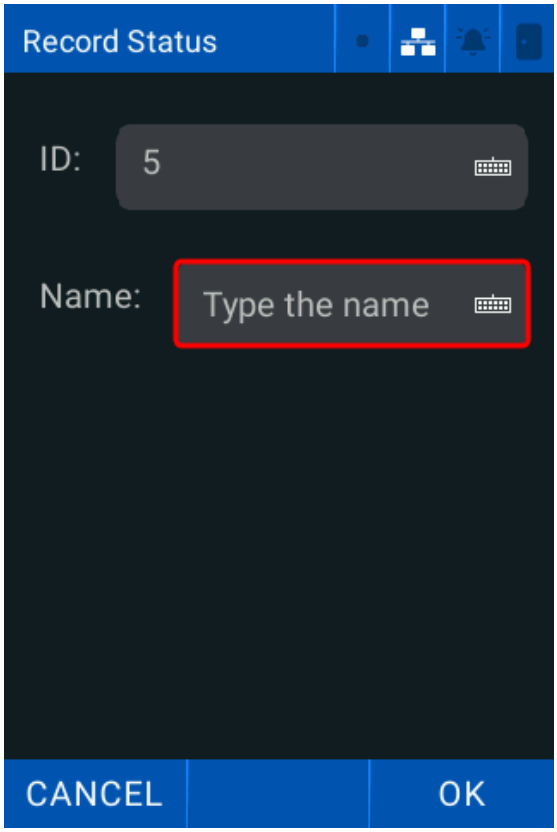
Set attendance codes

1. Tap **Menu** > **Attendance** > **Record Status**.
2. Tap **Add**.



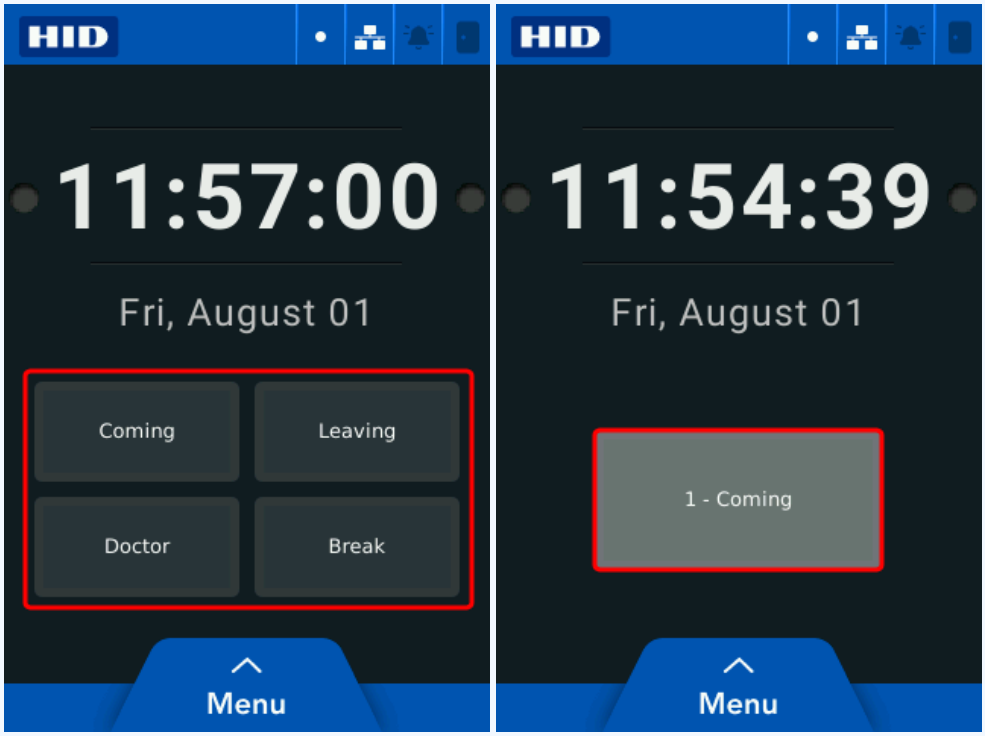
3. Tap the **ID** keyboard and enter the required ID.

4. Tap the **Name** keyboard and enter the required record name.



5. Tap **OK** to save.

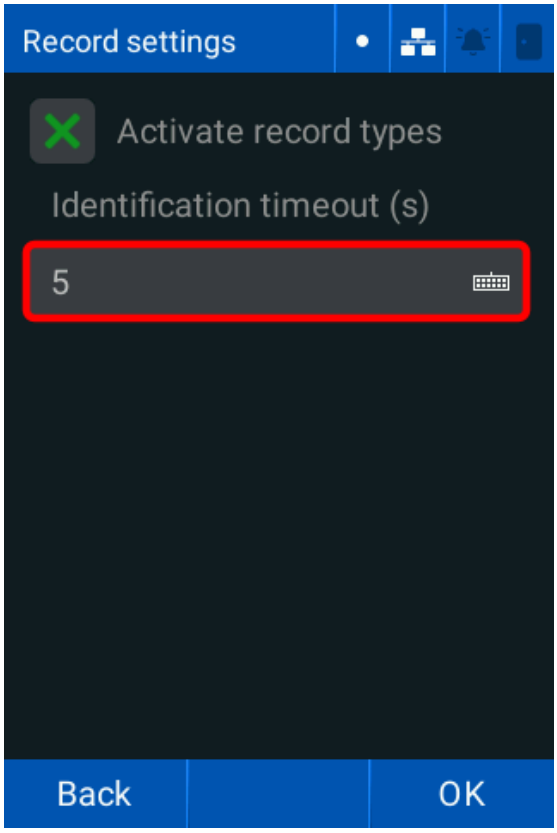
Note: If there are four or less status codes, they are displayed on the idle screen . If more than four codes are used, a larger button is displayed on the idle screen. Tap this button to reveal all status codes.



7.9 Enable status codes on idle screen

This allows you to display the status codes on the idle screen.

1. Tap > **Menu** > **Attendance** > **Record settings**.
2. Tap the **Activate record types** check box to enable/disable status code visibility on the idle screen.
3. Tap the **Identification timeout (s)** keyboard and enter the amount of time a user has to present a card or face to the reader for identification.

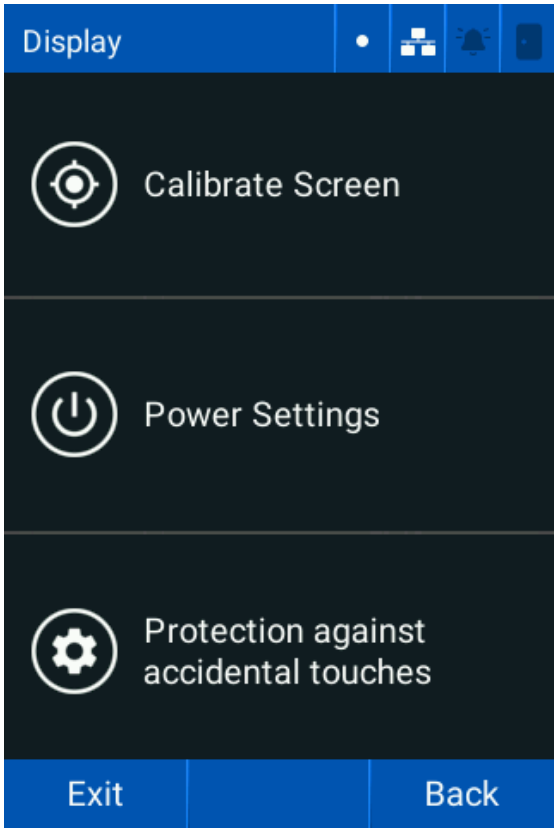


4. Tap **OK**.

7.10 Display

The **Display** screen allows you to configure the power settings and calibrate the screen.

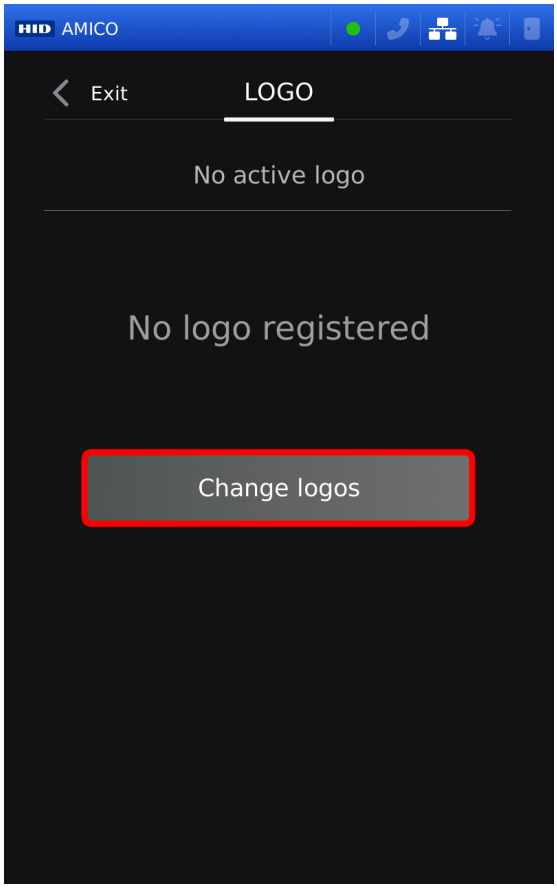
1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display**. The **Display** screen is displayed.



7.10.1 Idle screen logo

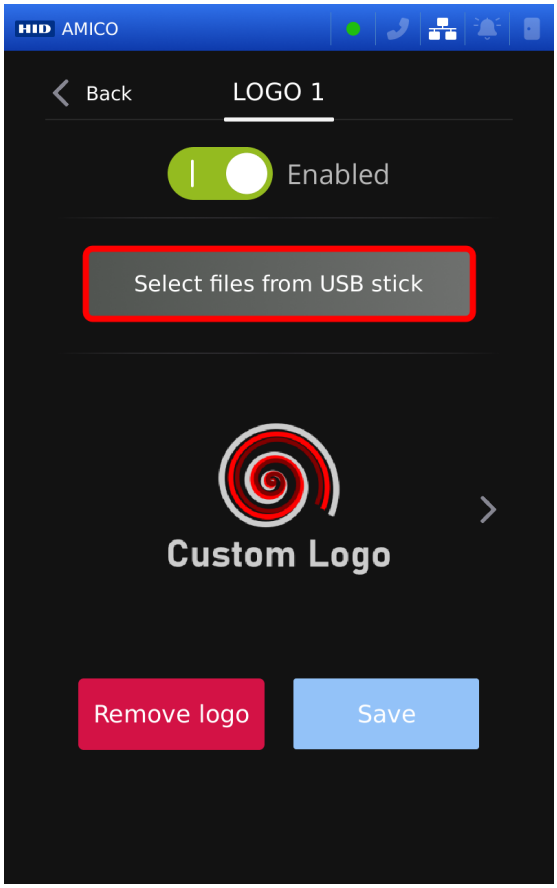
The **Logo** screen allows you to configure the reader idle screen logo.

1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display** > **Initial screen logo**. The **Logo** screen is displayed.
2. Tap **Change logos**.



3. Tap the **Enabled** toggle to enable/disable custom logo visibility.
4. Insert a USB drive with the required logo files.

5. Tap **Select files from USB stick**.

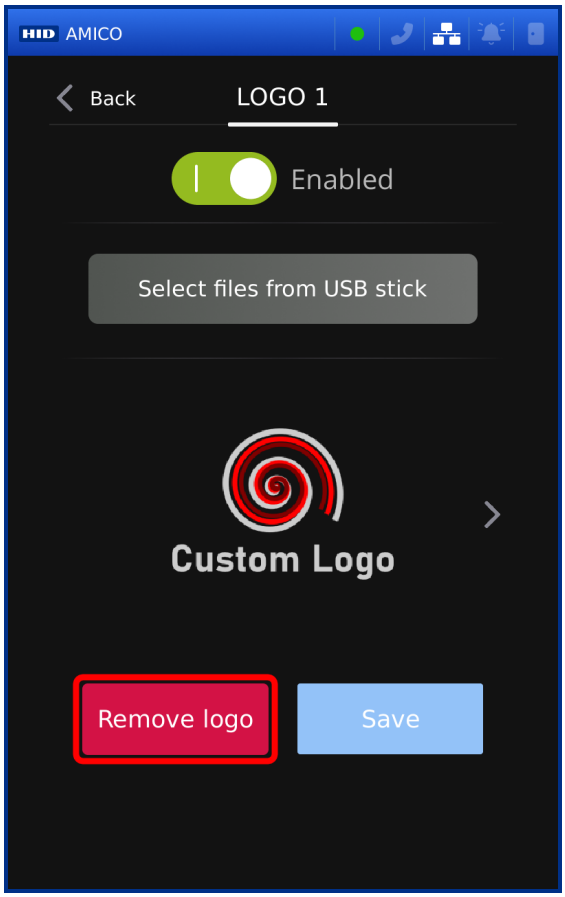


6. Select the required logo files and tap **Save**.

Note:
- Upload up to eight image files at a time to the VL70LF.
- Logo files can be uploaded to the VL70LF and VL35LF via the HID Amico web interface.
- Only one image file can be uploaded to the VL35LF.
- JPEG and PNG are the supported file types.
- Use images with a suitable resolution for optimal results. VL35LF screen width is 320px, VL70LF screen width is 800px.

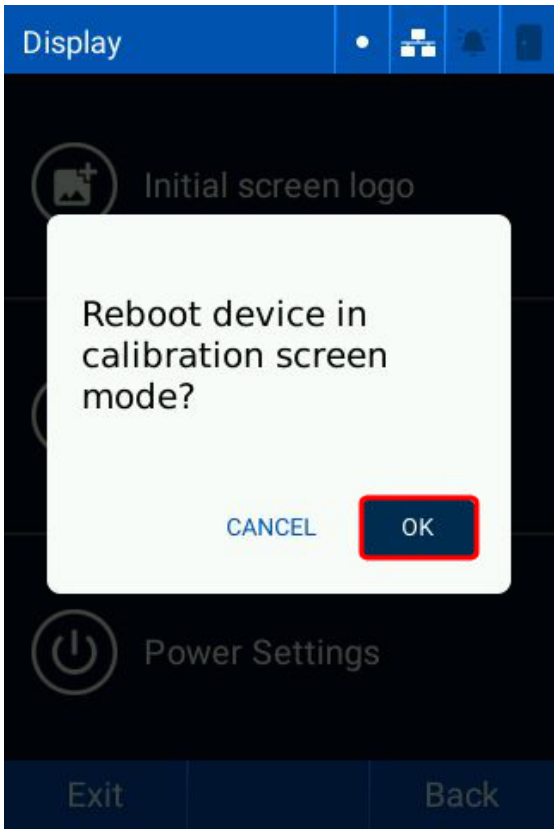
7.10.2 Remove logo files

1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display** > **Initial screen logo**. The **Logo** screen is displayed.
2. Use the left and right arrows to select the required logo.
3. Tap **Remove logo**.



7.10.3 Display calibration

1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display** > **Calibrate Screen**.
2. Read the message that is displayed and tap **OK**.

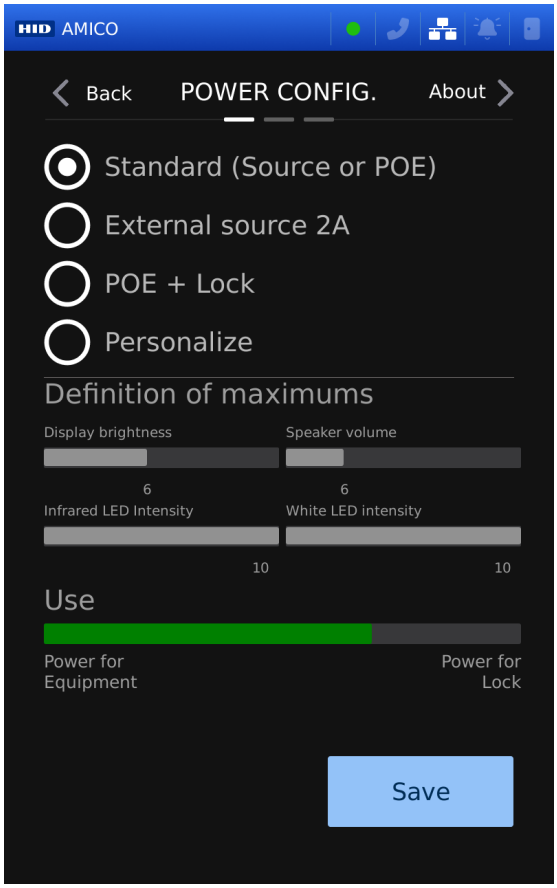


3. The reader will reboot in calibration mode. Tap the marks on the screen and wait for the reader to calibrate.

7.11 Power settings

The **POWER CONFIG** screen allows you to configure the readers power saving settings.

1. Tap **Menu** > **Settings** > **General settings** > **System** > **Power Settings**. The **POWER CONFIG** screen is displayed.



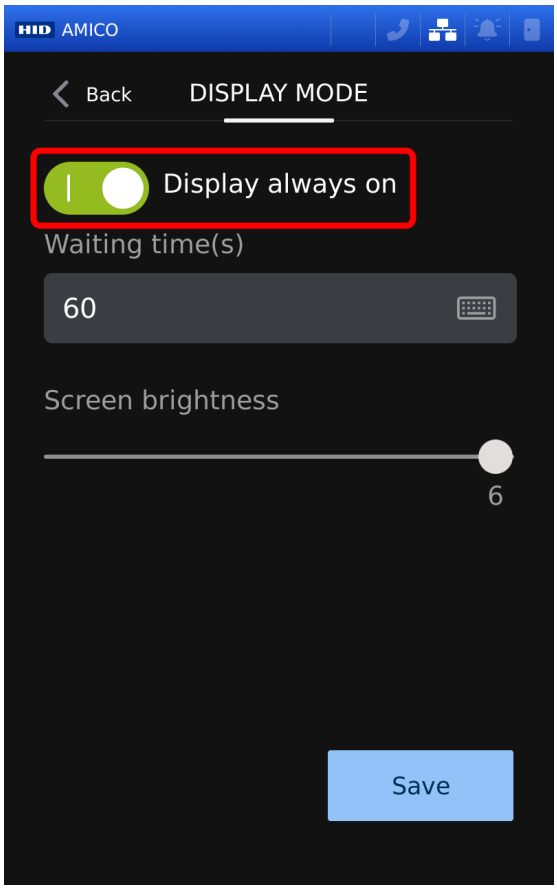
2. Tap the power source that the reader uses.

   Note: These are preconfigured settings optimized to the electrical current available from the power sources.

   Alternatively, tap personalize and configure each parameter manually.
3. Tap **About** for more information on the listed power source.

7.11.1 Display always on

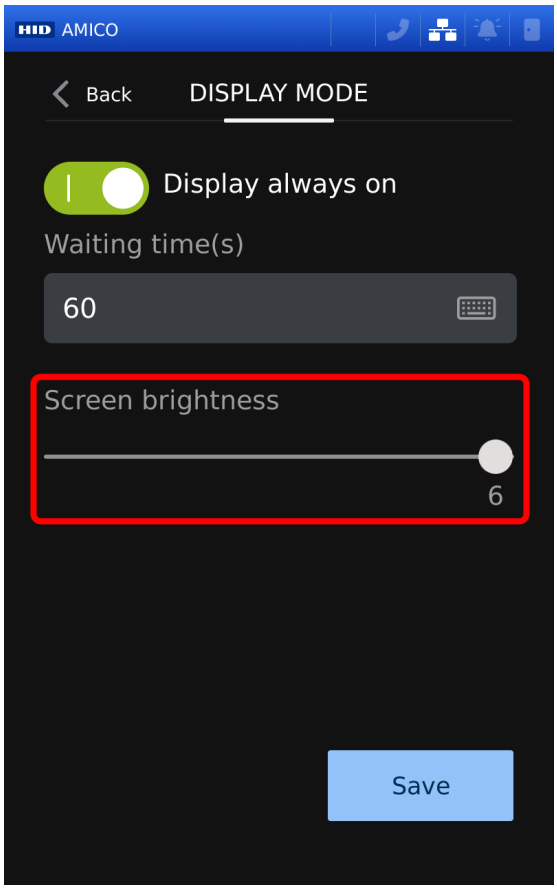
1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display** > **Power Settings**. The **DISPLAY** screen is displayed.
2. Tap the **Display always on** toggle to enable/disable to displaying the idle screen when the reader is idle.



3. If the **Display always on** mode is disabled, tap the **Waiting time (s)** keyboard and enter the required time before the screen turns off when idle.
4. Click **Save**.

7.11.2 Screen brightness

1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display** > **Power Settings**. The **DISPLAY** screen is displayed.
2. Slide the **Screen brightness** slider to adjust the screen brightness.



3. Click **Save**.

7.11.3 Protection against accidental touches

This allows you to configure the duration that a user must tap and hold the **Menu** button to access the menu.

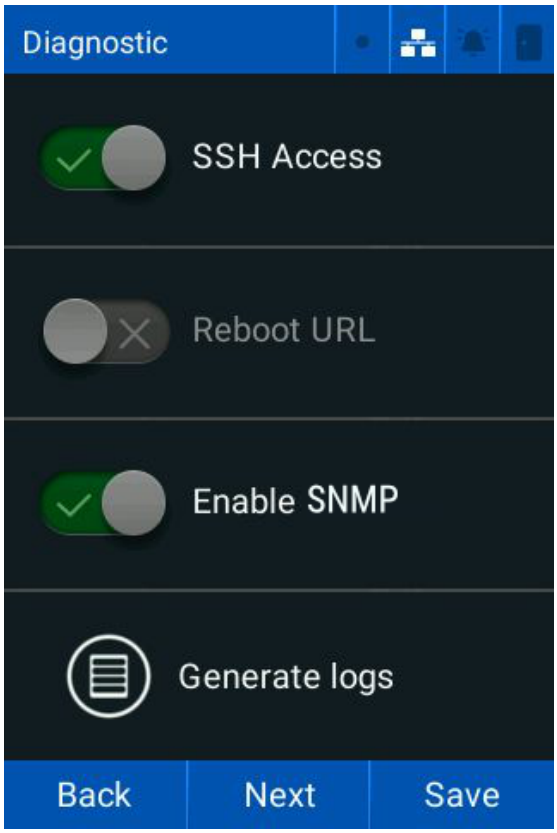
1. Tap **Menu** > **Settings** > **General settings** > **System** > **Display**.
2. Tap the **Protection activated** toggle to enable/disable protection against accidental touches.
3. Tap the **Touch duration (s)** keyboard and set the duration the user is required to tap and hold the active object (for example, Menu button, pin pad, Attendance button) on the idle screen.
4. Tap **OK** to save.

7.12 Diagnostics

The **Diagnostic** screen allows you to configure reader diagnosis and general report settings.

> **Caution:** The following features can cause the reader to reboot or be accessed remotely. Only use them for support if your reader has issues.

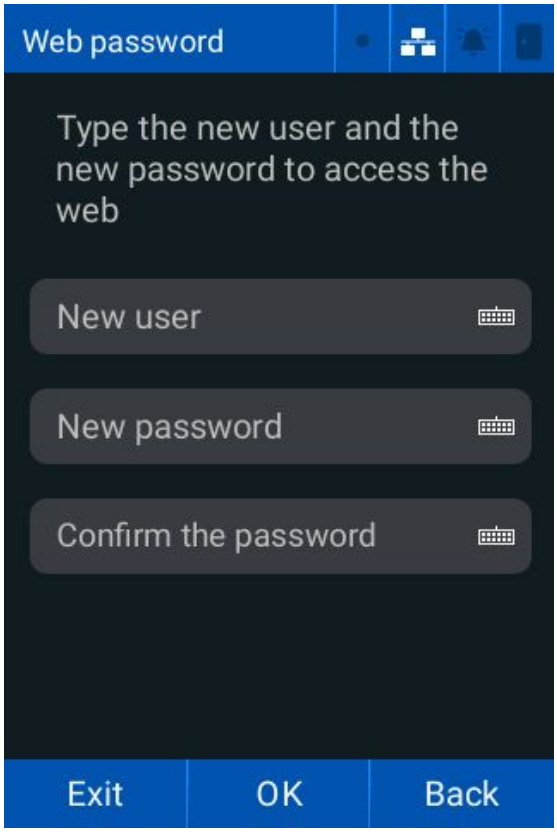
1. Tap **Menu** > **Settings** > **General settings** > **Diagnostic**. The **Diagnostic** screen is displayed.



2. Tap the **SSH Access** toggle to enable/disable access via SSH.
3. Tap the **Reboot URL** toggle to enable/disable restarting the reader without a valid session.
4. Tap the **Enable SNMP** toggle to enable/disable SNMP.
5. Tap **Save**.

7.13 Modify user name and web password

1. Tap **Menu** > **Settings** > **General settings** > **Change web password**. The **Web password** screen is displayed.

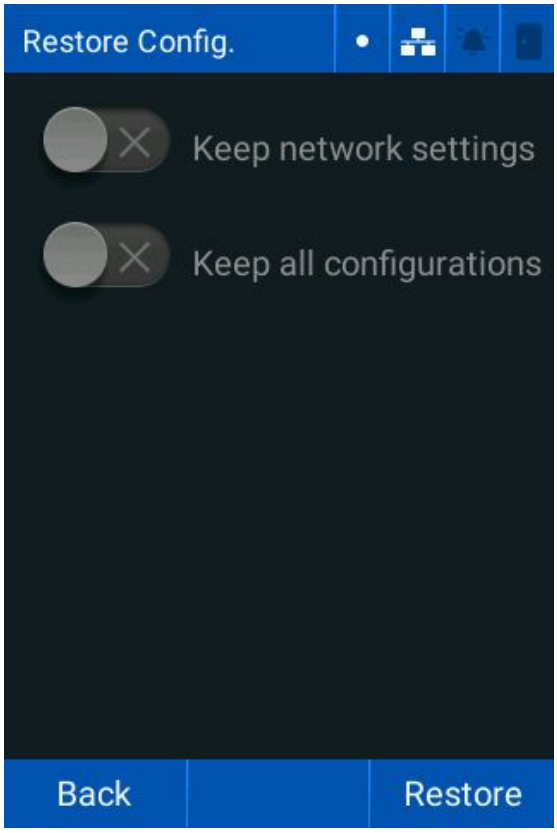


2. Tap the **New user** keyboard and enter the required user name.
3. Tap the **New password** keyboard and enter the required password.
4. Tap the **Confirm the password** keyboard and confirm the new password.
5. Tap **OK**.

7.14 Restore settings

The **Restore Configuration** screen allows you to restore the reader to default settings.

1. Tap **Menu** > **Settings** > **General settings** > **Restore Configuration**. The **Restore Configuration** screen is displayed.

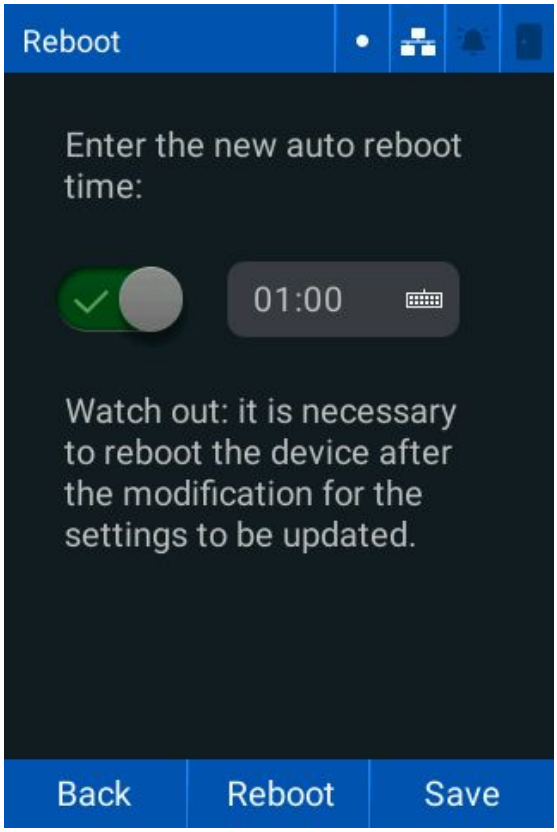


2. Tap the **Keep network settings** toggle to keep/remove the network settings.
3. Tap the **Keep all configurations** toggle to keep/remove all configurations.
4. Tap **Restore**.

7.15 Restart

The **Reboot** screen allows you to configure an automatic restart time for the reader or restart the system immediately.

1. Tap **Menu** > **Settings** > **General settings** > **Reboot**. The **Reboot** screen is displayed.



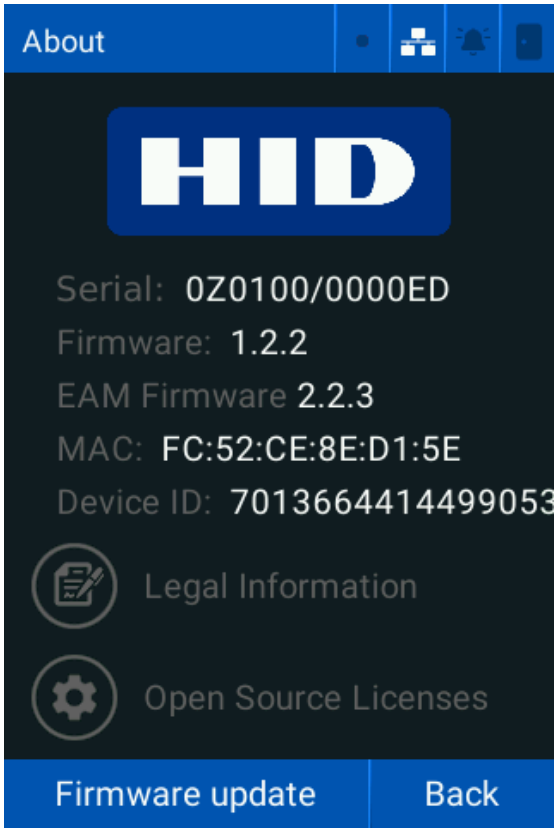
2. Tap the **Automatic reboot time** toggle to enable/disable the automatic restart time.
3. Tap the **Automatic reboot time** keyboard and enter the required restart time.

> **Note:** Tap **Reboot** to restart the reader immediately.

7.16 About

The **About** screen allows you to view the reader information, update the reader firmware, and view the terms and conditions of use.

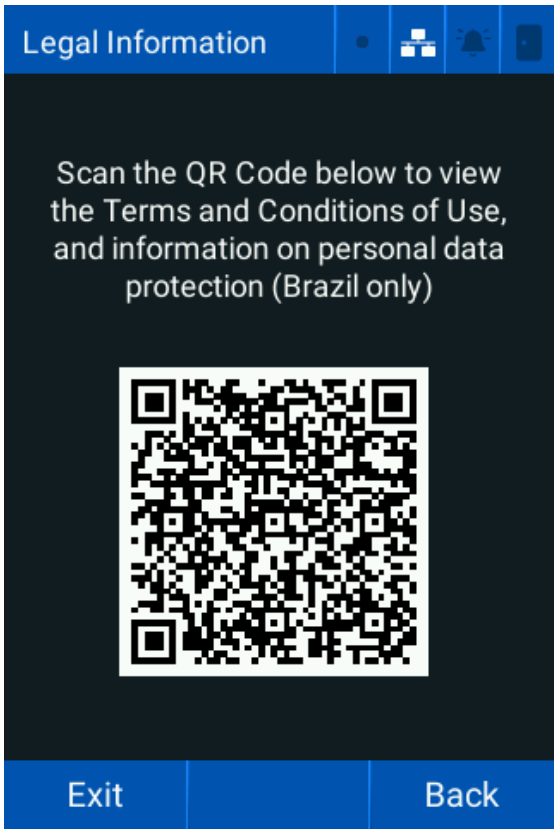
1. Tap **Menu** > **About**. The **About** screen is displayed.



2. Tap **Back** to return to the main menu.

7.16.1 Legal information

1. Tap **Menu** > **About** > **Legal Information**. The **Legal Information** screen is displayed.



2. Scan the **QR Code** for more information.

> **Note:** Enter the URL into a web browser if you cannot scan the code.

3. Tap **Exit** to return to the main menu.

7.16.2 Firmware update

This allows you to update the reader firmware version.

> **Important: It is recommended to keep the reader firmware up to date. Check regularly for new firmware versions.**

1. Tap **Menu** > **About**. The **About** screen is displayed.
2. Tap **Firmware update**.

3. The reader searches for new firmware versions and notifies you if a new version is available. Follow the on-screen instructions if a new firmware version is found.

Section 08

Technical specifications

8.1 Technical specifications

Features	VL35LF	VL70LF
LCD type	3.5" TFT color LCD display with capacitive touchscreen	7" TFT Color LCD Display (800x1280) with Capacitive Touchscreen
CPU	1.5 GHz quad-core processor	1.5 GHz quad-core processor
Audio feedback	Buzzer	Buzzer and Speaker, audio line-out
Intercom	N/A	Built-in SIP intercom
Visual feedback	On-screen feedback, multicolor LED indicator / illuminator	On-screen feedback
Operating temperature	-20°C to 50°C 0% ~ 80%, non-condensing	-20°C to 50°C 0% ~ 80%, non-condensing
Camera	Two 1080p full HD cameras (visible light and infrared light)	Two 1080p full HD cameras (visible light and infrared light)
RTSP and Onvif	Supported	Supported
Tamper	Supported	Supported
Dimensions mm (W × H × D)	86 × 142 × 26 (terminal) 52 × 52 × 22 (EAM)	119.4 x 247 x 34.6 (terminal) 52 × 52 × 22 (EAM)
Weight	343g (device) 35g ((EAM)	950g (device) 35g (EAM)
Power	12VDC 2A or PoE	12VDC 2A or PoE
Power consumption	400mA @ 12V idle, maximum 600mA @ 12V	600mA @ 12V idle, maximum 1A @ 12V
PoE	802.3af PoE (802.3at/PoE+)	802.3af PoE (802.3at/PoE+)
Authentication distance	Up to 3m	Up to 3m
Mounting height	1.40m	1.5m
Matching speed	Within 0.2 seconds	Within 0.2 seconds
Throughput	30 persons per min 1:N	30 persons per min 1:N
Live face detection (Anti-spoofing)	Presentation attack detection supported	Presentation attack detection supported
Minimum Light Level	0 lux (complete darkness)	0 lux (complete darkness)
HF (13.56 MHz)	Seos® iCLASS®, iCLASS SE™, ISO 14443A (MIFARE) CSN, ISO 14443B CSN, DESFIRE EV1/2/3 **	Seos® iCLASS®, iCLASS SE™, ISO 14443A (MIFARE) CSN, ISO 14443B CSN, DESFIRE EV1/2/3 **
LF (125 kHz)	HID Prox™	HID Prox™
Mobile (2.4GHz)	NFC, Bluetooth LE	NFC, Bluetooth LE
Wallet	Google, Apple***	Google, Apple***
Template on card	Seos Secure Identity Object™ (SIO)	Seos Secure Identity Object™ (SIO)
Mobile / Wallet	NFC, Bluetooth LE	NFC, Bluetooth LE

Features	VL35LF	VL70LF
Typical RF read range	Seos 0.4in (1cm), iCLASS 2.36in (6cm), Prox 1.57in (4cm)	Seos 0.4in (1cm), iCLASS 2.36in (6cm), Prox 1.57in (4cm)
Keypad (PIN)	Supported on TFT LCD	Supported on TFT LCD
QR	Static (ISO/IEC 18004:2015) and dynamic (6238 TOTP) QR Supported	Static (ISO/IEC 18004:2015) and dynamic (6238 TOTP) QR Supported
Max. user	200,000	200,000
Max credential	Face: 10,000 / PIN 200,000 / Card: 200,000 **Note:** Face credentials can be extended to 100,000 with a license upgrade.	Face: 50,000 / PIN 200,000 / Card: 200,000 **Note:** Face credentials can be extended to 100,000 with a license upgrade.
Event log capacity	200,000	200,000
Ethernet	1 native 10/100Mbps Ethernet port	1 native 10/100Mbps Ethernet port
RS-485	1 RS-485 port for communication with the external access control module or OSDP	1 RS-485 port for communication with the external access control module or OSDP
OSDP Protocol	OSDP v2 compliant	OSDP v2 compliant
USB	USB 2.0 available through a USB C connector in the back of the product (service only)	1 USB 2.0 Host
Relay	1x NO/NC, max. 30VAC / 5A (EAM)	1x NO/NC, max. 30VAC / 5A (Terminal) 1x NO/NC, max. 30VAC / 5A (EAM)
I/O	1x Door Sensor, 1x Pushbutton (EAM)	3x GPIO (Terminal) 1x Door Sensor, 1x Pushbutton (EAM)
Wiegand	1x Input, 1x Output (EAM)	1x Input, 1x Output (EAM)
IP Rating	IP65 (excluding EAM)	IP65 (excluding EAM)
Certifications	ANATEL | UKCA | CE | CB | IC | RoHS | and others	ANATEL | UKCA | CE | CB | IC | RoHS | and others
Warranty	12 months	12 months

* Read range listed is statistical mean rounded to nearest whole centimeter. HID Global testing occurs in open air. Some environmental conditions, including metallic mounting surfaces can significantly degrade read range and performance; plastic or ferrite spacers are recommended to improve performance on metallic mounting surfaces.

** EV3 in EV1 Compatibility Mode. Omnikey Reader Manager required to load (MOB and Elite Key) Origo account required.

*** Apple Wallet Certification pending.

Appendix A

802.1X Status

A.1 802.1X status

Status	Description
Initializing	Authentication process is initializing.
Disconnected	802.1X authentication is disabled or cannot connect to the authenticator or authenticator server.
Connecting	The reader is connecting to the authenticator and authentication server.
Authenticating	The authentication process is running.
Authenticated	The reader has been authenticated on the network.
Aborting	The authentication process is being aborted.
Detained	The reader authentication failed.
Forcibly authorizing	The 802.1X authentication process is disabled and the reader network port is authorized without performing the authentication process.
Forcibly deauthorizing	The reader network port is not authorized. Any authentication attempt is ignored.
Restarting	The reader is restarting.
Unknown 802.1X status	An internal error prevented the reader from booting correctly.

A.2 IP ports

The table below lists the IP ports used by HID Amico readers. Make sure they are not blocked by your firewall settings and the ports must be open for communication in your network environment.

Resource	Default Status	Default Port	Description
HTTP	Enabled	80	Used for the embedded web interface
HTTP/SSL	Disabled	443	Secure protocol for web interface with encryption
NTP	Disabled	123	Protocol for network time synchronization
RTSP	Disabled	554	Protocol for real-time audio and video streaming
ONVIF	Disabled	8000	Standard for video surveillance device interoperability
SIP	Disabled	5060	Protocol for VoIP signaling enabling SIP calls
DNS	Disabled	53	Domain name to IP address resolution
DHCP	Disabled	67/68	Protocol for automatic IP configuration
SNMP	Disabled	161/162	Protocol for network device monitoring and management
SSH	Disabled	22	Secure remote access to the device

Appendix **B**

Face capture best practices

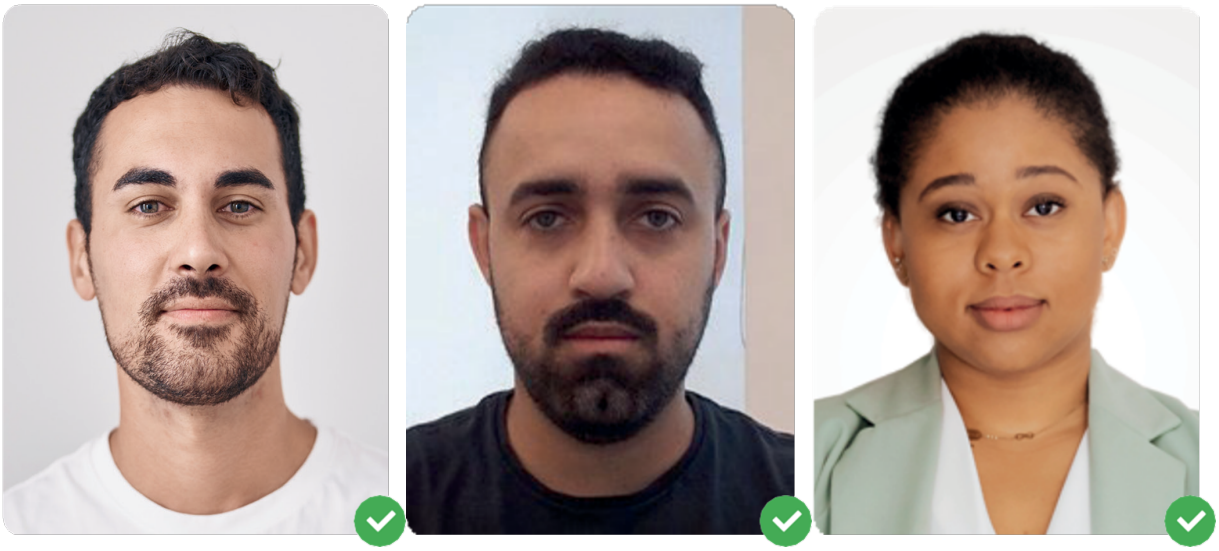
B.1 Face capture - best practices

Accurate user identification relies on correct face registration. Follow the best practices to ensure correct facial registration:

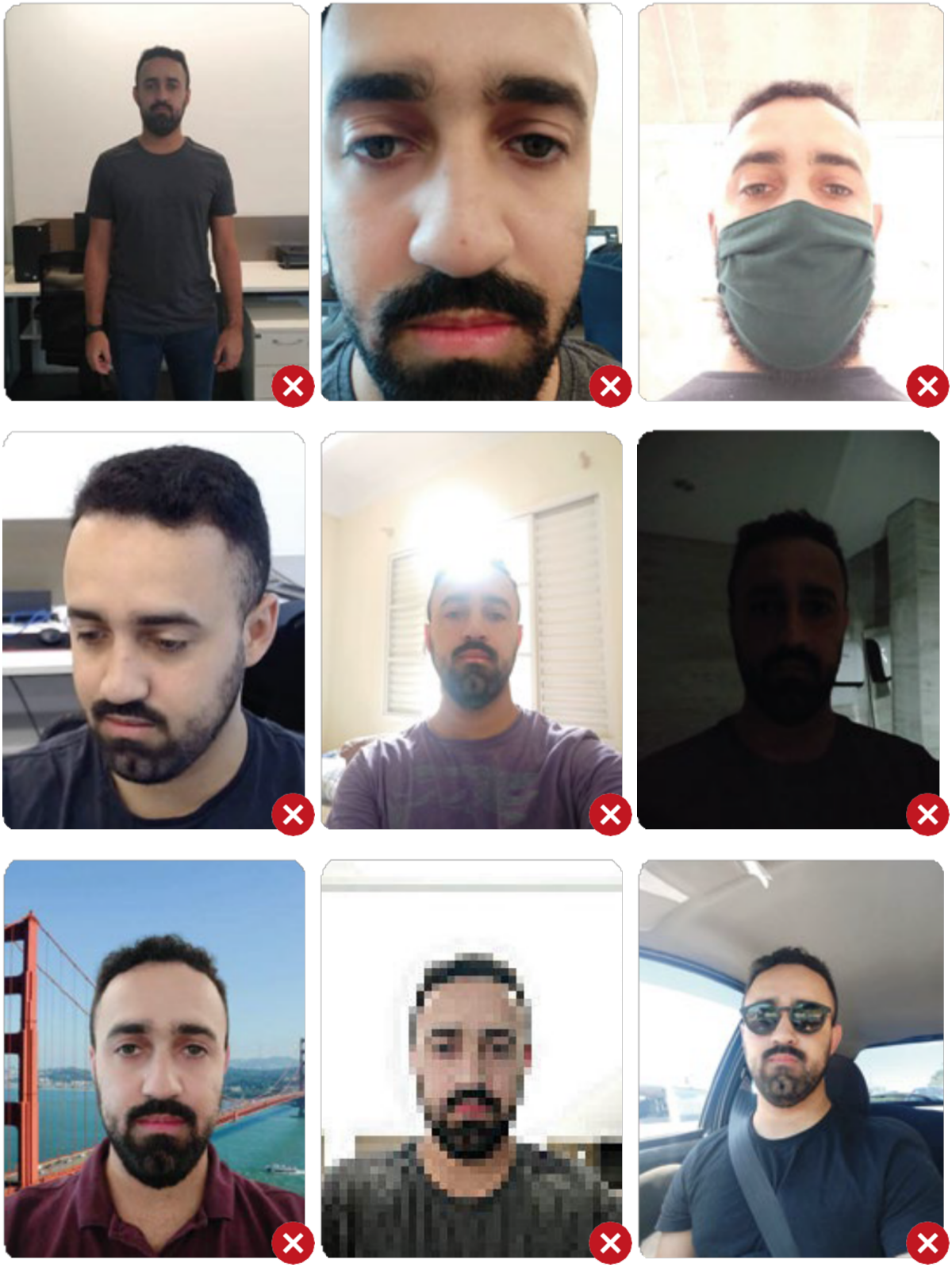
1. **Environment**
   - Lighting - ensure good, even lighting. Avoid very bright or low-light environments.
   - Background - use a white or neutral color background. Avoid complex or colorful backgrounds.
2. **Positioning**
   - Distance - between 60cm and 150cm from the reader
   - Centering - position the face in the center of the frame
   - Angle - the face should be straight and looking directly at the camera
3. **Taking the photo**
   - **Resolution** - the face should cover at least 160px from ear to ear. Do not resize the image or change its aspect ratio.
   - **Format** - PNG. (JPEG can be used with a quality factor of 95 or higher).
   - **Number of faces** - only one face must be present in the image
   - **Accessories** - no masks, hats, helmets, or sunglasses. Spectacles are acceptable if no reflections are visible in the lenses.
   - **Facial expressions** - the face must be in a neutral expression

B.2 Image examples

Correct image examples



Incorrect image examples



Revision history

Date	Description	Revision
November 2025	Minor updates.	A.2
November 2025	Updated to add VL70LF information.	A.1
April 2025	Initial release.	A.0

hidglobal.com

For technical support, please visit: https://support.hidglobal.com

PLT-07752, Rev. A.2

Part of ASSA ABLOY